Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Logfile Analysis: Identifying a Network Attack

A backup strategy is more complex then creating a redundant copy of disk storage and considering the strategy a success. A successful backup strategy must detail how the backup media are rotated, how the media are archived, how the system will be recovered, and what the backup software will do to create the backup. Although all parts of the backup strategy are equally important, this paper will focus on the backup script and will detail a flexible backup script that uses built-in Solaris software tools which create a r...

Copyright SANS Institute
Author Retains Full Rights

AD

Logfile Analysis: Identifying a Network Attack

Michael Fleming
February 12, 2003

Introduction:

This paper presents an in-depth look into what an automated network attack looks like in the logfiles to better understand the attacks "after-the-fact".

I will analyze two different attacks: one being easy to determine the type and the intended goal while the other attack is not so cut and dried – leaving some entertaining researching for readers. I will use two recent logfiles: June 23, 2001 and June 27, 2001 as each of these show an automated attack. I will detail what I see in the logs, attempt to determine the computer(s) involved, the operating system(s) they run, and the tool(s) that were used. I will suggest ways to prevent damage from such attacks and provide links to associated patches, if available.

Description:

The organization I work for has a class B Internet IP address space with an .EDU domain name. It is my theory that our network is scanned or attacked every day, mostly just filling portions of the daily log files with "access denied" messages, however, there is always the threat of something getting through. The security game today seems to be to prevent what you know about, keep an eye out for what you don't know yet, and when you DO know it, prevent that.

We provide email, ftp and web services to the public and to our internal corporate users while maintaining and hosting our own DNS servers. Our link to the Internet is via 100BASE-FX Ethernet to an University that has OC-3 Internet connectivity so we have a very high traffic capacity with low latency. The University blocks ICMP, the Sun RPC port 111 and the NetBIOS ports 137, 138 and 139 at their border routers. Blocking and filtering anything else is up to my organization and is handled by a border firewall device and router access lists. Contrary to my experience in "Corporate America", the general mood here is towards University-style "open access" regarding computers and the Internet. It's a challenging, politically-sensitive environment to secure.

Extensive logging is enabled for the firewall and all internal computers with operating systems that support central logging capabilities. Almost all routers, switches, computers and devices on the network synchronize their clocks – to within 0.10 seconds - using the sntp protocol to an internal ntp device. The internal ntp device tocks to a stratum 1 Internet ntp clock. Still, some devices do not use ntp and their clocks may differ resulting in some logfile data being more difficult to interpret.

Daily log data is divided into separate files, filtered, parsed, stripped – essentially made more human readable by various automated sed, awk and perl scripts, then archived. A

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

one year time frame of raw log files is maintained on-line. The "processed" log files are emailed to members of the System Admin group daily.

After reviewing the logfiles from a typical day, I've learned that every day leaves me with one or more of the following conclusions:

1. There was no attempted penetration of our network,
2. There was a successful penetration of our network and it affected one or more areas or machines,
3. There was a successful attack, however, we don't have any evidence to show it – so we don't know about it [yet].

For both attacks documented here I performed reconnaissance scans back to the indicated source IP using SuperScan[1]. Both of these reconnaissance scans showed poor security configurations on the attacking computers. The SuperScan scans were performed within 24 hours of each attack. In less than 24 hours after the attacks, each respective computer was off the air and one of them remained off the air up to the submission of this paper. Hmmm…

I suspect either the owners noticed something was amiss, assuming these attacking computers were compromised machines, or the ISPs received enough complaints to notify the owners or shutdown the service. This is a good thing (ISPs responding to complaints quickly), however, it doesn't stop the attacks – it just gives us a short break before the next round of incoming and allows some time to build up our defenses. The next attack will probably come from a different IP address as there appears to be no shortage of vulnerable Internet hosts from which to stage an attack.

Well, OK then. On to the fun part.

NOTE: Packets sent to IP addresses/ports blocked by the firewall do not have any packets returned to the source – the attacker does not get any reply.

Attack A:

The first logfile to examine is dated 06/24/2001 and was closed at 0300. The previous 24 hours are stored there and all of the examined attack traffic occurred on 06/23/2001. All times are MST.

This attack performed a quick, broad coverage of most of the class B address range starting at a.b.0.3 and ending at a.b.255.106 (see Appendix B), increasing the IP address in steps of between 540 and 560 (decimal).

[1] SuperScan from Foundstone: http://www.foundstone.com/rdlabs/tools.php?category=Scanner

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Referring to Table 1, a closer look shows the first scan occurred at 22:57:36 Hrs. and the last one was recorded at 23:30:12 Hrs. The following table shows connection attempts by protocol (sorted by time of access):

Port:	Tries	Denied by FW	Time Start	Time End	Time Total	Silence
tcp port 23	177	114	06/23 22:57:36	06/23 22:59:34	0:01:58	0:02:25
tcp Port 53	110	110	06/23 23:01:59	06/23 23:03:50	0:01:51	0:08:27
tcp port 21	278	116	06/23 23:12:17	06/23 23:30:17	0:18:00	---
Total	565	340	---	---	0:32:41	---

Table 1

Telnet (tcp port 23) was the first protocol scanned and lasted for just shy of 2 minutes while scanning 177 addresses with 114 attempts denied by the firewall. Approximately one and a half minutes later DNS (tcp port 53) was scanned, covering 110 addresses, all blocked, in just under 2 minutes. Lastly, 278 addresses were scanned for ftp services (tcp port 21) starting approximately 8 minutes after the DNS scan stopped where only 116 attempts were blocked at the firewall (only 42% of the attempts were blocked!!). The ftp scan lasted for 18 minutes. The denied tcp port 21 and 23 connection attempts are well documented by the firewall software whereas the connections allowed by the firewall are reported by the individual computer(s) where the connection(s) actually went, leaving it up to the various operating systems to report the connections via syslog.

I suspect the addresses used in the telnet and DNS scans were pre-programmed before the attack was started since 145 seconds isn't much time to interpret the data. However, it is possible that the results from the telnet and DNS scans were digested before the ftp scan started.

Where did the attack come from and why was it attacking (other than the obvious "The Internet" and "Because my servers were connected and running.")? **nslookup** identified the source IP as coming from a computer in Hong Kong:

```
ip-46-74-y-x.rev.<source>.com = x.y.74.46
Netname: APNIC-CIDR-BLK
Netblock: x.y.0.0 - x.y.255.255
Maintainer: AP
Kowloon, Hong Kong.
```

I was lucky enough to get a SuperScan report showing the following ports and header banners on 06/24/2001 at approximately 1615 Hrs MST as shown:

```
* + x.y.74.46
        |___    21  File Transfer Protocol [Control]
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
        |___     23  Telnet
        |___     79  Finger
        |___     80  World Wide Web HTTP
                   |___ HTTP/1.1 403 Forbidden..Date: Sun, 24
Jun 2001 18:17:45 GMT..Server: Apache/1.3.12 (Unix)  (Red
Hat/Linux) PHP/3.0.15 mod_perl/
        |___    113  Authentication Service
        |___    139  NETBIOS Session Service
        |___    513  remote login a la telnet;
        |___    514  cmd
        |___   1983
                   |___ SSH-1.5-1.2.27.
        |___  20002
        |___  20003
        |___  20004
        |___  20005
        |___  20006
        |___  20007
        |___  30002
        |___  30003
        |___  30004
        |___  30005
        |___  30006
        |___  30007
```

My impression is that this is a RedHat Linux box running ftp, telnet, and rlogin daemons, a web server, and perhaps a Samba server. I was curious about the high ports responding : 20002-20007 and 30002–30007. The limited data I found for common Trojan usage of those ports in a SANS document[2] shows port 20002 as possibly related to **AcidkoR** and 30003 as possibly related to **Lamers Death**. Other search data revealed the same port/Trojan assignments with nothing commonly listed for the other ports in the ranges of 20002-20007 and 30002–30007. Of course most of the tools I have in my personal arsenal, and others I've read about, allow manual port assignments, so port numbers aren't always a sure sign. Perhaps it's a new program or Trojan that's not been documented yet.

Internet search data[3] shows **AcidkoR** is a Win9x/NT Trojan which would agree with port 139 being listed above, however it is unlikely that a Windows box would be running finger and a RedHat version of Apache. **Lamers Death** is a remote access program for Windows that is rumored to have been written in Russia[4]. Neither of these programs normally uses the other listening ports in the 20002-20007 & 30002-30007 range. Perhaps the attacker was clever enough to run extraneous services and change the service headers.

---

[2] Intrusion Detection FAQ :http://www.sans.org/newlook/resources/IDFAQ/oddports.htm
[3] http://www.dark-e.com/archive/trojans/acidkor/index.shtml
[4] http://www.simovits.com/trojans/tr_data/y718.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Impression:

Inconclusive, more data is needed.

Let's now examine the packets that were rejected by the firewall. Then, we will examine packets allowed inside by the firewall and see how the individual computers responded to the connection attempts.

Appendix A shows the complete 06/23/2001 attack, sorted by time. Looking at the port, and IP addresses [sorted by time] we see a programmatic increase in IP address of the destination address for each packet between 540 and 560, decimal. The starting address for all three port scans was a.b.0.3.

A snippet of Appendix A as an example:

```
                                                    Address Delta
denied tcp x.y.74.46(23) -> a.b.32.79(23)                 Decimal
denied tcp x.y.74.46(23) -> a.b.34.119(23)  Increment:     556
denied tcp x.y.74.46(23) -> a.b.36.163(23)  Increment:     553
denied tcp x.y.74.46(23) -> a.b.38.204(23)  Increment:     550
denied tcp x.y.74.46(23) -> a.b.40.242(23)  Increment:     553
denied tcp x.y.74.46(23) -> a.b.43.27(23)   Increment:     553
denied tcp x.y.74.46(23) -> a.b.45.69(23)   Increment:     554
denied tcp x.y.74.46(23) -> a.b.47.112(23)  Increment:     555
denied tcp x.y.74.46(23) -> a.b.49.150(23)  Increment:     550
denied tcp x.y.74.46(23) -> a.b.51.187(23)  Increment:     549
denied tcp x.y.74.46(23) -> a.b.53.229(23)  Increment:     554
```

This logfile section shows a small selection of telnet connection attempts (to tcp port 23). Of interest to me is the IP address incremental steps: between 549 and 558 in the above example. The minimum/maximum step observed during the attack was between 540 and 560, decimal. Similar steps were shown in the dns and ftp sections. An automated tool performed this attack but I'm not aware of one that performs this type of address incrementing through a range of IP addresses. Perhaps a tool such as nmap[5] or strobe[6] was used with input from warscan[7] or a pre-defined input file of addresses to scan; however, it appears that the same input file was not used for the three different scans. My thinking is that another tool using random address selection within a specified range was utilized here. The fact that the source port always matches the destination port, for the dropped packets, indicates a custom packet crafting tool as this would not occur with normal traffic.

Appendix B shows time, port and IP address, sorted by IP address. Looking at Appendix B we see that scans for the three different ports started with IP a.b.0.3. There

[5] From Fyodor: http://www.insecure.org/nmap
[6] ftp://suburbia.net:/pub/strobe.tgz
[7] http://www.ussrback.com/UNIX/unixscanners.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

are 7 times where all three ports match the same IP address and 25 occurrences where two ports met at the same address (shown bold in Appendix B). The highest address for the tcp port 21 scan was a.b.255.106, tcp port 23 scan was a.b.255.64 and the tcp port 53 scan ended with a.b.239.161.

Appendices C & D show messages returned to syslog from each connection that was not blocked by the firewall and routers, sorted by time and node name, respectively.

There were some connections that appear to have been established and it is not clear from the limited data in the logfile whether these connections made any successful logins. Those connections that were refused, most likely, were due to TCP Wrappers configurations on the individual computers. Some telnet connection messages are shown below:

```
22:57:38 node44 in.telnetd[29410]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node54 inetd[6218]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
22:57:38 node51 inetd[96329]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
22:57:38 node64 in.telnetd[26214]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node9 in.telnetd[1603]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node49 in.telnetd[23703]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node43 in.telnetd[16378]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:35 node-a14 in.telnetd[13593]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node-a1 in.telnetd[6648]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
22:57:38 node27 in.telnetd[2166]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node-a13 in.telnetd[6724]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:40 node36 in.telnetd[25133]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:36 node3 in.telnetd[16261]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

There is a very similar result for ftp connections:

```
23:12:18 node4 in.ftpd[16070]: connect from
  ip-46-74-y-x.rev.xyz.com
23:05:40 node50 in.ftpd[2526]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:24 node26 in.ftpd[2567]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node33 in.ftpd[25377]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node7 in.ftpd[7641]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node64 in.ftpd[26318]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node9 in.ftpd[1623]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node6 in.ftpd[5972]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node6 ftpd[5972]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:18 node18 in.ftpd[9061]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node68 in.ftpd[16175]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node19 in.ftpd[4184]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node60 in.ftpd[1422]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node17 in.ftpd[23810]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

All of the above connections, ordered by time, appear to jump randomly from host to host. Appendix D shows connections sorted by node, where we see more than one attempted connection to almost every scanned IP address that wasn't blocked by the firewall. For instance, node14 had 4 ftp connections whereas node18 received 6 ftp and 2 telnet connections. Looking at the first four lines, we see two log messages with the same source port. Inetd catches the connection and launches tcpd (TCP Wrappers). Tcpd logs the first message (in.ftpd) then launches ftpd for the second entry (ftpd), if the connection is allowed by the TCP Wrappers configuration. It's curious that the same connection is made again about 17 minutes later. I did not notice these occurrences when viewing the scan data sorted by time of connection, so sorting by node was indeed revealing.

```
23:12:42 node14 in.ftpd[16757]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:43 node14 ftpd[16757]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:29:59 node14 in.ftpd[16758]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:59 node14 ftpd[16758]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:29:49 node15 in.ftpd[2321]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:49 node15 in.ftpd[2321]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:42 node16 in.ftpd[1379]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node17 in.ftpd[23810]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:25 node17 in.ftpd[23827]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8881]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9072]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9071]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8882]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node18 in.ftpd[9062]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node18 in.ftpd[9061]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node18 in.ftpd[9060]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node18 in.ftpd[9069]: connect from
  ip-46-74-y-x.rev.xyz.com
```

To better understand the log messages, I made telnet and ftp connections, intentionally failing the logins, to node14 and then observed the log messages. There are login failure messages for telnet, but not for ftp. This particular machine is running SunOS 4.1.4.

```
Jul 17 09:11:36 node14 in.telnetd[936]: connect from testhound
Jul 17 09:16:01 node14 login[937]: 4 LOGIN FAILURES FROM
  testhound, fleming
Jul 17 09:16:08 node14 in.ftpd[938]: connect from node14
Jul 17 09:16:08 node14 ftpd[938]: connection from testhound
  at Tue Jul 17   09:16:08 2001
```

Doing a proper login via telnet produces:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
Jul 17 09:49:04 node14 in.telnetd[966]: connect from testhound
Jul 17 09:49:09 node14 login[967]: login from testhound as
  fleming
```

Conclusion: Attack A:

The whole attack took only 33 minutes. This is not enough time to manually observe and respond. The address list used to scan for one service was not used as the address list for the other service scans. Until I determine what tools were used to generate the address lists, I will conclude the address lists were determined before the scanning started and different lists were used at least for the port 21 and 53 scans.

The various operating systems sent different descriptions of connections, logins, logouts, etc. which is initially confusing so a learning phase is required. There is no definite evidence in the logs that any of these connections resulted in a successful login or account compromise, however, there is no definite evidence otherwise. It appears that only the connections were made to the services and that logins weren't attempted as there are not any "LOGIN FAILED" messages associated with that source IP address in the logfile.

This type of attack speaks directly to "defense in depth", a major theme in the SANS curriculum:

- Stop the traffic you do not want inside your network at the border firewall and/or router(s),
- For traffic that is allowed, limit the allowed source addresses with TCP Wrappers at each computer,
- Use strong passwords to make password guessing difficult, and
- Keep the operating system patches up to date.

Oh yeah – and read the logfiles to see what is getting through, take appropriate action and keep records of all actions.

Follow-up on Attack A:

The attacking machine was removed from the Internet shortly after I discovered it and, I would conclude, it must have been scanning and/or attacking other sites as well. My guess would be that the ISP notified the owner(s) of the complaints and the owner(s) took action. Since then it appears to have been rebuilt with new or different services installed and looks more secured as shown by a follow-up SuperScan report on 07/15/2001, where it's running a different configuration of web server and now sendmail. Ports for FTP, telnet, finger, auth, rlogin, etc. are not responding. Another happy ending!

```
+ x.y.74.46
|___     25  Simple Mail Transfer
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
    |___ 220 javaserver.eyber.com ESMTP Sendmail
8.11.0/8.11.0; Sun, 15 Jul 2001 21:49:19 -0800..
  |___     80  World Wide Web HTTP
    |___ HTTP/1.1 403 Forbidden..Date: Mon, 16 Jul 2001
12:09:23 GMT..Server: Apache/1.3.12 (Unix)  (Red Hat/Linux)
mod_ssl/2.6.6 OpenSS
  |___ 20004
  |___ 20208
  |___ 30004
  |___ 30208
```

Attack B:

The second attack occurred on 06/27/2001 and appears to be a Sun Solaris box hunting for IIS web servers. There were slightly less than 3000 logfile entries, in just over 2 hours, coming from a computer in the USA scanning my network to tcp port 80. According to nslookup, the source IP address is registered to another University, which means it also has a high-bandwidth, low latency Internet connection!

This attack is commonly known as the sadmind/IIS worm[8]. AKA Backdoor.Sadmind (NAV) , Sadmin-iis (Panda), Solaris/Sadmind.worm, and Unix/Sadmind (Sophos) according to McAfee[9]; AKA sadmind/IIS, and Backdoor.Sadmind.dr according to Symantec[10].

A SuperScan reconnaissance scan (rapidly becoming my favorite recon tool!) back to the source IP address showed some evidence that it was a Solaris 7 box with many default services running:

```
 * + x.x.236.88
  |___     13  Daytime
    |___ Thu Jun 28 09:19:08 2001..
  |___     19  Character Generator
    |___  !"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg..
  |___     21  File Transfer Protocol [Control]
    |___ 220 node FTP server (SunOS 5.7) ready...
  |___     23  Telnet
    |___ ........#..'..$
  |___     25  Simple Mail Transfer
    |___ 220 node.domain.yyy ESMTP Sendmail
8.9.1b+Sun/8.9.1; Thu, 28 Jun 2001 09:19:09 -0500 (CDT)..
  |___     37  Time
```

[8] VIRUS ALERT - Solaris/sadmind.worm (sadmind/IIS) Internet Worm: http://www.unl.edu/security/virus_alerts/sadmind.htm
[9] http://vil.nai.com/vil/virusSummary.asp?virus_k=99085
[10] http://www.symantec.com/avcenter/venc/data/backdoor.sadmind.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  |___ ...^
|___     79  Finger
  |___ No one logged on..
|___    111  SUN Remote Procedure Call
|___    512  remote process execution;
|___    513  remote login a la telnet;
|___    514  cmd
|___    515  spooler
|___    540  uucpd
|___    600  Sun IPC server
  |___ #
|___   1338
|___   4045
|___   6000  6000-6063   X Window System
|___   6112  dtspcd
|___   7100  X Font Service
|___  32771
|___  32772
|___  32773
|___  32774
|___  32775
|___  32793
|___  32795
```

My research shows that port 600 is a useful identifier of the Solaris/sadmind.worm: "The Solaris/sadmind.worm places a rootshell listening on TCP port 600 using /dev/cuc/nc."[8] The compromised server appears to have randomly selected a Class B network (mine!) and then proceeded to scan that address range for Microsoft IIS servers – looking for the IIS Directory Traversal/Unicode vulnerability[11],[12] according to the sadmind/IIS.worm MO.

My organization operates some internal IIS4 & IIS5 servers running, however, to the best of my knowledge these servers are not accessible from the Internet. It's been a constant process to keep IIS servers patched as the vulnerability list increases almost daily[13]. (Note to self: Scan monthly for internal IIS servers and keep patch levels up to date.)

I wonder how much time it will take for someone to modify this worm to use the double-decode vulnerability in IIS servers[14],[15] and then see that mod in the wild? Most of the

[11] http://www.kb.cert.org/vuls/id/111677
[12] Microsoft Security Bulletin (MS00-078): http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp
[13] SANS Windows Security Digest Vol. 4 Num. 6.
[14] IIS decodes filenames superfluously after applying security checks: http://www.kb.cert.org/vuls/id/789543

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

files are easily located on the Internet, are quite easy to modify, and there seems to be no lack of vulnerable servers to host an attack.

Some logfile sections showing the incrementing of the addresses:

```
denied tcp r.s.236.88(33734) -> a.b.0.1(80), 1 packet
denied tcp r.s.236.88(33736) -> a.b.0.3(80), 1 packet
denied tcp r.s.236.88(34186) -> a.b.0.51(80), 1 packet
denied tcp r.s.236.88(34186) -> a.b.0.51(80), 1 packet
denied tcp r.s.236.88(34251) -> a.b.0.78(80), 1 packet
denied tcp r.s.236.88(34246) -> a.b.0.73(80), 1 packet
denied tcp r.s.236.88(34704) -> a.b.0.101(80), 1 packet
denied tcp r.s.236.88(34707) -> a.b.0.104(80), 1 packet
denied tcp r.s.236.88(35258) -> a.b.0.151(80), 1 packet
denied tcp r.s.236.88(35260) -> a.b.0.153(80), 1 packet
```

The above logfile snippets are but a very small section of the total scan. Most of the entire class B network range was scanned, increasing the IP address between 0 and 50, decimal. From the data I've read, this worm randomly selects the class B network to scan and then randomly increments the IP address to scan. The logfile entries are attached as Appendix E. (NOTE: Appendix E is slightly over 100 pages!!)

The scan started on Jun 27 04:35:02 and ended on Jun 27 06:37:58, which is slightly over 2 hours and, in total, there were 2838 connections denied by the firewall. Connection attempts were only made to tcp port 80, which agrees with searching for IIS servers. There were no scans to port 111 from that source IP address so it appears to have not selected my network to scan for vulnerable Solaris boxes.

Conclusion: Attack B:

This was a sadmind/IIS.worm attack originating from a poorly secured Solaris 7 machine at a location where abundant Internet bandwidth existed. All of the logfile and SuperScan data support this. This is a well known common attack and proves that at least some computers still aren't properly patched or secured to prevent it. This particular computer was removed from the Internet shortly after the attack, most likely indicating many complaints (including one from myself). As of the writing of this paper, that IP address still does not respond.

The current (as of this writing - as it's always a moving target) Microsoft IIS4, IIS5 and SunOS patches for this attack can be located at the following links (watch for URL links that wrap):

Microsoft Security Bulletin MS01-026:

15

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www.microsoft.com/technet/security/bulletin/MS01-026.asp
contains the following:
Microsoft IIS 4.0 Rollup Patch:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787
Microsoft IIS 5.0 Rollup Patch:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764

IIS4:
Security Configuration Checklist for IIS4:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/iischk.asp

IIS5:
Security Configuration Checklist for IIS5:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp

OWA:
Microsoft Exchange Server 5.5 running OWA:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30568

ISAPI Extension Patch:
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Solaris Patches can be located at the following links:
Sun Security Bulletin #00191:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?coll&doc=secbull/191&type=0&nav=sec.sba

Summary:

This paper looked at two different logfiles, attempted to determine if an attack occurred, to identify the type and methodology of attack, and note if the type of attack was well known in the wild.

It's very important to review the logfile data daily and act quickly. In both of these attacks, the attacking computers were available – in their attacking configuration – for less than 24 hours after the attack was executed. If we're going to investigate, collect data and analyze attacks, then we need to move quickly.

There is a tremendous amount of work involved in analyzing logfile data – it must be automated as it is overwhelming for a human to do manually. The data needs to be sorted by source IP, destination IP, service and time – at a minimum – and, most importantly, someone needs to read it.

An ideal tool would be an easily configurable Intrusion Detection System (IDS) that would detect the failed (denied) attempts, then proactively – in near-real-time – deny all related traffic. However, false positives would have serious political repercussions in an

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

educational/research environment such as this one. The next best thing would be an IDS that doesn't act – just logs, compiles, sorts, sifts, evaluates and recommends. And, naturally, a human with time to read the data output and act accordingly.

References:

(Beware of URLs that wrap.)
RPC attack was New unicode attack tool: URL:
http://www.incidents.org/archives/intrusions/msg00097.html
ELF_SADMIND.A: URL:
http://www.trend.com.tw/EncyclopediaV2/vinfo/virusencyclo/default5.asp?VName=ELF_SADMIND.A&VSect=T
Re: httpd and sunrpc probes from 'sunos 5.6' machines: URL:
http://archives.neohapsis.com/archives/incidents/2001-05/0100.html
Microsoft Security Bulletin MS01-026:
URL: http://www.microsoft.com/technet/security/bulletin/MS01-026.asp
Microsoft IIS 4.0 Rollup Patch:
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787
Microsoft IIS 5.0 Rollup Patch:
URL: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764
Security Configuration Checklist for IIS4:
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/iischk.asp
Security Configuration Checklist for IIS5: URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp
Microsoft Exchange Server 5.5 running OWA: URL:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30568

Footnotes:

[1] SuperScan from Foundstone: URL:
http://www.foundstone.com/rdlabs/tools.php?category=Scanner
[2] Intrusion Detection FAQ: URL:
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm
[3] URL: http://www.dark-e.com/archive/trojans/acidkor/index.shtml
[4] URL: http://www.simovits.com/trojans/tr_data/y718.html
[5] From Fyodor: URL: http://www.insecure.org/nmap
[6] URL: ftp://suburbia.net:/pub/strobe.tgz
[7] URL: http://www.ussrback.com/UNIX/unixscanners.htm
[8] VIRUS ALERT - Solaris/sadmind.worm (sadmind/IIS) Internet Worm: URL:
http://www.unl.edu/security/virus_alerts/sadmind.htm
[9] URL: http://vil.nai.com/vil/virusSummary.asp?virus_k=99085
[10] URL: http://www.symantec.com/avcenter/venc/data/backdoor.sadmind.html
[11] URL: http://www.kb.cert.org/vuls/id/111677

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[12] Microsoft Security Bulletin (MS00-078): URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp

[13] SANS Windows Security Digest Vol. 4 Num. 6.

[14] IIS decodes filenames superfluously after applying security checks: URL: http://www.kb.cert.org/vuls/id/789543

[15] URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp

© SANS Institute 2001, Author retains full rights

Logfile Analysis: Identifying a Network Attack

Michael Fleming
February 12, 2003

Appendix A: Attack A Complete, Sorted by Time (Denied)

```
22:57:36 1780329 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.0.3(23), 1 packet
22:57:36 1780330 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.2.40(23), 1 packet
22:57:38 1780331 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.4.82(23), 1 packet
22:57:39 1780332 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.6.109(23), 1 packet
22:57:40 1780333 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.8.149(23), 1 packet
22:57:41 1780334 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.10.192(23), 1 packet
22:57:42 1780335 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.12.229(23), 1 packet
22:57:43 1780336 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.15.17(23), 1 packet
22:57:44 1780337 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.17.54(23), 1 packet
22:57:45 1780338 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.19.100(23), 1 packet
22:57:45 1780339 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.21.139(23), 1 packet
22:57:47 1780340 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.23.177(23), 1 packet
22:57:48 1780341 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.25.215(23), 1 packet
22:57:49 1780342 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.28.3(23), 1 packet
22:57:50 1780343 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.30.39(23), 1 packet
22:57:51 1780344 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.32.79(23), 1 packet
22:57:52 1780345 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.34.119(23), 1 packet
22:57:52 1780346 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.36.163(23), 1 packet
22:57:54 1780347 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.38.204(23), 1 packet
22:57:54 1780348 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.40.242(23), 1 packet
22:57:56 1780349 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.43.27(23), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:57:57 1780350 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.45.69(23), 1 packet
22:57:58 1780351 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.47.112(23), 1 packet
22:57:58 1780352 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.49.150(23), 1 packet
22:58:00 1780353 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.51.187(23), 1 packet
22:58:00 1780354 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.53.229(23), 1 packet
22:58:02 1780355 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.56.1(23), 1 packet
22:58:02 1780356 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.58.57(23), 1 packet
22:58:04 1780357 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.60.1(23), 1 packet
22:58:04 1780358 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.62.172(23), 1 packet
22:58:05 1780359 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.64.205(23), 1 packet
22:58:07 1780361 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.66.243(23), 1 packet
22:58:08 1780362 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.69.27(23), 1 packet
22:58:09 1780363 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.71.67(23), 1 packet
22:58:10 1780364 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.73.113(23), 1 packet
22:58:11 1780365 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.75.147(23), 1 packet
22:58:12 1780366 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.77.190(23), 1 packet
22:58:12 1780367 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.79.227(23), 1 packet
22:58:13 1780369 %IDS-4-TCP_SYN_ATTACK_SIG Half-Open Syn Flood
   from x.y.74.46 to a.b.81.11
22:58:14 1780370 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.83.1(23), 1 packet
22:58:17 1780371 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.88.2(23), 1 packet
22:58:18 1780372 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.90.38(23), 1 packet
22:58:19 1780373 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.92.82(23), 1 packet
22:58:20 1780374 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.94.120(23), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:58:21 1780375 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.96.163(23), 1 packet
22:58:21 1780376 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.98.198(23), 1 packet
22:58:23 1780377 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.100.237(23), 1 packet
22:58:23 1780378 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.103.20(23), 1 packet
22:58:26 1780380 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.108.1(23), 1 packet
22:58:27 1780381 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.110.35(23), 1 packet
22:58:28 1780382 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.112.73(23), 1 packet
22:58:28 1780383 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.114.118(23), 1 packet
22:58:30 1780385 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.116.153(23), 1 packet
22:58:31 1780386 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.118.199(23), 1 packet
22:58:31 1780387 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.120.243(23), 1 packet
22:58:33 1780388 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.123.23(23), 1 packet
22:58:34 1780389 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.125.59(23), 1 packet
22:58:35 1780390 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.127.101(23), 1 packet
22:58:36 1780391 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.129.138(23), 1 packet
22:58:37 1780392 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.131.178(23), 1 packet
22:58:38 1780393 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.133.222(23), 1 packet
22:58:39 1780394 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.136.6(23), 1 packet
22:58:39 1780395 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.138.44(23), 1 packet
22:58:41 1780396 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.140.88(23), 1 packet
22:58:42 1780397 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.142.126(23), 1 packet
22:58:43 1780398 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.144.166(23), 1 packet
22:58:44 1780399 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.146.204(23), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:58:45 1780400 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.148.246(23), 1 packet
22:58:46 1780401 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.151.28(23), 1 packet
22:58:47 1780402 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.153.72(23), 1 packet
22:58:48 1780403 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.155.110(23), 1 packet
22:58:48 1780404 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.157.148(23), 1 packet
22:58:50 1780405 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.159.190(23), 1 packet
22:58:50 1780406 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.161.231(23), 1 packet
22:58:52 1780407 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.164.19(23), 1 packet
22:58:52 1780408 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.166.63(23), 1 packet
22:58:54 1780409 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.168.99(23), 1 packet
22:58:55 1780410 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.170.133(23), 1 packet
22:58:56 1780412 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.172.174(23), 1 packet
22:58:57 1780413 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.174.214(23), 1 packet
22:58:58 1780414 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.177.1(23), 1 packet
22:58:59 1780415 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.179.39(23), 1 packet
22:58:59 1780416 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.181.79(23), 1 packet
22:59:01 1780417 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.183.125(23), 1 packet
22:59:01 1780418 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.185.158(23), 1 packet
22:59:03 1780419 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.187.198(23), 1 packet
22:59:03 1780420 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.189.238(23), 1 packet
22:59:06 1780422 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.194.118(23), 1 packet
22:59:07 1780423 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.196.159(23), 1 packet
22:59:08 1780424 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.198.199(23), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:59:09 1780425 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.200.239(23), 1 packet
22:59:09 1780426 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.203.28(23), 1 packet
22:59:11 1780427 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.205.66(23), 1 packet
22:59:11 1780428 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.207.104(23), 1 packet
22:59:13 1780429 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.209.146(23), 1 packet
22:59:13 1780430 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.211.183(23), 1 packet
22:59:15 1780431 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.213.226(23), 1 packet
22:59:15 1780432 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.216.13(23), 1 packet
22:59:17 1780433 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.218.51(23), 1 packet
22:59:18 1780435 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.220.89(23), 1 packet
22:59:19 1780436 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.222.130(23), 1 packet
22:59:20 1780437 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.224.170(23), 1 packet
22:59:21 1780438 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.226.210(23), 1 packet
22:59:22 1780439 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.228.250(23), 1 packet
22:59:22 1780440 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.231.34(23), 1 packet
22:59:24 1780441 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.233.1(23), 1 packet
22:59:24 1780442 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.235.209(23), 1 packet
22:59:27 1780444 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.240.39(23), 1 packet
22:59:27 1780445 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.242.85(23), 1 packet
22:59:29 1780446 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.244.119(23), 1 packet
22:59:30 1780447 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.246.158(23), 1 packet
22:59:31 1780449 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.248.200(23), 1 packet
22:59:32 1780450 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.250.238(23), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:59:32 1780451 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.253.26(23), 1 packet
22:59:34 1780452 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(23)
   -> a.b.255.64(23), 1 packet
23:01:59 1780489 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.0.3(53), 1 packet
23:02:00 1780490 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.2.42(53), 1 packet
23:02:01 1780491 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.4.82(53), 1 packet
23:02:02 1780492 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.6.120(53), 1 packet
23:02:02 1780493 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.8.163(53), 1 packet
23:02:04 1780494 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.10.210(53), 1 packet
23:02:05 1780495 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.12.244(53), 1 packet
23:02:05 1780496 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.15.28(53), 1 packet
23:02:07 1780498 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.17.69(53), 1 packet
23:02:08 1780499 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.19.107(53), 1 packet
23:02:09 1780500 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.21.135(53), 1 packet
23:02:10 1780501 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.23.188(53), 1 packet
23:02:11 1780502 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.25.226(53), 1 packet
23:02:12 1780503 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.28.11(53), 1 packet
23:02:13 1780504 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.30.51(53), 1 packet
23:02:14 1780505 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.32.91(53), 1 packet
23:02:15 1780506 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.34.130(53), 1 packet
23:02:16 1780507 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.36.170(53), 1 packet
23:02:17 1780508 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.38.210(53), 1 packet
23:02:17 1780509 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.40.251(53), 1 packet
23:02:19 1780510 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.43.39(53), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:02:20 1780511 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.45.80(53), 1 packet
23:02:21 1780512 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.47.116(53), 1 packet
23:02:21 1780513 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.49.156(53), 1 packet
23:02:23 1780515 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.51.196(53), 1 packet
23:02:24 1780516 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.53.240(53), 1 packet
23:02:24 1780517 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.56.23(53), 1 packet
23:02:26 1780518 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.58.62(53), 1 packet
23:02:26 1780519 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.60.108(53), 1 packet
23:02:28 1780520 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.62.143(53), 1 packet
23:02:29 1780521 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.64.185(53), 1 packet
23:02:29 1780522 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.66.222(53), 1 packet
23:02:31 1780523 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.69.14(53), 1 packet
23:02:32 1780524 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.71.58(53), 1 packet
23:02:33 1780525 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.73.97(53), 1 packet
23:02:34 1780526 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.75.136(53), 1 packet
23:02:35 1780527 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.77.178(53), 1 packet
23:02:36 1780528 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.79.216(53), 1 packet
23:02:36 1780530 %IDS-4-TCP_SYN_ATTACK_SIG: Half-Open Syn
   Flood from x.y.74.46 to a.b.81.254
23:02:37 1780531 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.83.1(53), 1 packet
23:02:40 1780532 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.88.2(53), 1 packet
23:02:40 1780533 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.90.35(53), 1 packet
23:02:41 1780534 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.92.82(53), 1 packet
23:02:43 1780536 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.94.120(53), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:02:43 1780537 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.96.163(53), 1 packet
23:02:45 1780538 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.98.205(53), 1 packet
23:02:45 1780539 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.100.243(53), 1 packet
23:02:47 1780540 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.103.27(53), 1 packet
23:02:49 1780542 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.108.1(53), 1 packet
23:02:49 1780543 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.110.39(53), 1 packet
23:02:51 1780544 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.112.77(53), 1 packet
23:02:51 1780545 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.114.122(53), 1 packet
23:02:53 1780546 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.116.154(53), 1 packet
23:02:54 1780547 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.118.195(53), 1 packet
23:02:55 1780548 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.120.239(53), 1 packet
23:02:55 1780549 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.123.21(53), 1 packet
23:02:57 1780550 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.125.68(53), 1 packet
23:02:58 1780551 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.127.107(53), 1 packet
23:02:58 1780552 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.129.148(53), 1 packet
23:03:00 1780553 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.131.184(53), 1 packet
23:03:01 1780554 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.133.223(53), 1 packet
23:03:02 1780555 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.136.4(53), 1 packet
23:03:02 1780556 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.138.46(53), 1 packet
23:03:04 1780557 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.140.85(53), 1 packet
23:03:04 1780558 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.142.129(53), 1 packet
23:03:06 1780559 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.144.166(53), 1 packet
23:03:06 1780560 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.146.211(53), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:03:08 1780561 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.148.249(53), 1 packet
23:03:09 1780562 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.151.30(53), 1 packet
23:03:09 1780563 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.153.72(53), 1 packet
23:03:11 1780564 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.155.109(53), 1 packet
23:03:12 1780565 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.157.149(53), 1 packet
23:03:13 1780566 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.159.194(53), 1 packet
23:03:14 1780567 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.161.230(53), 1 packet
23:03:14 1780568 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.164.23(53), 1 packet
23:03:16 1780569 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.166.62(53), 1 packet
23:03:17 1780570 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.168.100(53), 1 packet
23:03:17 1780571 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.170.133(53), 1 packet
23:03:19 1780572 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.172.174(53), 1 packet
23:03:20 1780574 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.174.214(53), 1 packet
23:03:20 1780575 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.177.1(53), 1 packet
23:03:22 1780576 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.179.43(53), 1 packet
23:03:23 1780577 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.181.79(53), 1 packet
23:03:23 1780578 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.183.127(53), 1 packet
23:03:25 1780579 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.185.160(53), 1 packet
23:03:26 1780580 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.187.209(53), 1 packet
23:03:27 1780581 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.190.3(53), 1 packet
23:03:27 1780582 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.192.37(53), 1 packet
23:03:29 1780583 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.194.75(53), 1 packet
23:03:30 1780584 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.196.117(53), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:03:30 1780585 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.198.163(53), 1 packet
23:03:32 1780586 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.200.206(53), 1 packet
23:03:33 1780587 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.202.248(53), 1 packet
23:03:34 1780588 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.205.32(53), 1 packet
23:03:34 1780589 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.207.70(53), 1 packet
23:03:36 1780590 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.209.119(53), 1 packet
23:03:37 1780591 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.211.150(53), 1 packet
23:03:38 1780592 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.213.192(53), 1 packet
23:03:38 1780593 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.215.230(53), 1 packet
23:03:40 1780594 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.218.16(53), 1 packet
23:03:40 1780595 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.220.58(53), 1 packet
23:03:42 1780597 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.222.104(53), 1 packet
23:03:42 1780598 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.224.135(53), 1 packet
23:03:44 1780599 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.226.181(53), 1 packet
23:03:44 1780600 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.228.219(53), 1 packet
23:03:46 1780601 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.231.3(53), 1 packet
23:03:46 1780602 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.233.41(53), 1 packet
23:03:47 1780603 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.235.87(53), 1 packet
23:03:49 1780605 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.237.121(53), 1 packet
23:03:50 1780606 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(53)
   -> a.b.239.161(53), 1 packet
23:12:17 1780795 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.0.3(21), 1 packet
23:12:18 1780796 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.2.42(21), 1 packet
23:12:19 1780797 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.4.82(21), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:20 1780798 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.6.120(21), 1 packet
23:12:21 1780799 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.8.163(21), 1 packet
23:12:22 1780800 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.10.203(21), 1 packet
23:12:23 1780801 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.12.252(21), 1 packet
23:12:24 1780802 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.15.19(21), 1 packet
23:12:25 1780803 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.17.63(21), 1 packet
23:12:25 1780804 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.19.102(21), 1 packet
23:12:27 1780805 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.21.140(21), 1 packet
23:12:28 1780806 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.23.188(21), 1 packet
23:12:29 1780807 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.25.234(21), 1 packet
23:12:30 1780808 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.28.20(21), 1 packet
23:12:31 1780809 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.30.51(21), 1 packet
23:12:31 1780810 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.32.92(21), 1 packet
23:12:33 1780811 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.34.130(21), 1 packet
23:12:34 1780812 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.36.170(21), 1 packet
23:12:35 1780813 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.38.212(21), 1 packet
23:12:36 1780814 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.40.252(21), 1 packet
23:12:37 1780815 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.43.36(21), 1 packet
23:12:38 1780816 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.45.76(21), 1 packet
23:12:38 1780817 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.47.123(21), 1 packet
23:12:40 1780818 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.49.161(21), 1 packet
23:12:41 1780819 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.51.203(21), 1 packet
23:12:41 1780820 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.53.237(21), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:43 1780821 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.56.20(21), 1 packet
23:12:43 1780822 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.58.66(21), 1 packet
23:12:44 1780823 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.60.102(21), 1 packet
23:12:46 1780825 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.62.146(21), 1 packet
23:12:47 1780826 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.64.181(21), 1 packet
23:12:48 1780827 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.66.222(21), 1 packet
23:12:49 1780828 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.68.162(21), 1 packet
23:12:49 1780829 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.70.203(21), 1 packet
23:12:51 1780830 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.73.32(21), 1 packet
23:12:52 1780831 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.75.214(21), 1 packet
23:12:53 1780832 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.78.2(21), 1 packet
23:12:53 1780833 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.80.39(21), 1 packet
23:12:54 1780835 %IDS-4-TCP_SYN_ATTACK_SIG: Half-Open Syn
   Flood from x.y.74.46 to a.b.81.97
23:12:55 1780836 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.83.1(21), 1 packet
23:12:57 1780838 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.88.5(21), 1 packet
23:12:59 1780839 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.90.63(21), 1 packet
23:13:00 1780840 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.92.103(21), 1 packet
23:13:00 1780841 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.94.146(21), 1 packet
23:13:02 1780842 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.96.182(21), 1 packet
23:13:02 1780843 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.98.222(21), 1 packet
23:13:04 1780844 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.101.12(21), 1 packet
23:13:05 1780845 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.103.56(21), 1 packet
23:13:06 1780846 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.108.1(21), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:13:08 1780848 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.110.36(21), 1 packet
23:13:08 1780849 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.112.74(21), 1 packet
23:13:10 1780850 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.114.122(21), 1 packet
23:13:10 1780851 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.116.158(21), 1 packet
23:13:12 1780852 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.118.199(21), 1 packet
23:13:12 1780853 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.120.234(21), 1 packet
23:13:14 1780854 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.123.18(21), 1 packet
23:13:15 1780855 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.125.60(21), 1 packet
23:13:15 1780856 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.127.98(21), 1 packet
23:13:17 1780857 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.129.140(21), 1 packet
23:13:17 1780858 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.131.178(21), 1 packet
23:13:19 1780859 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.133.218(21), 1 packet
23:13:20 1780860 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.136.6(21), 1 packet
23:13:21 1780861 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.138.44(21), 1 packet
23:13:21 1780862 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.140.86(21), 1 packet
23:13:23 1780863 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.142.124(21), 1 packet
23:13:24 1780864 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.144.166(21), 1 packet
23:13:25 1780865 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.146.206(21), 1 packet
23:13:25 1780866 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.148.244(21), 1 packet
23:13:27 1780867 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.151.30(21), 1 packet
23:13:27 1780868 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.153.71(21), 1 packet
23:13:29 1780869 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.155.109(21), 1 packet
23:13:29 1780870 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.157.156(21), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:13:31 1780871 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.159.198(21), 1 packet
23:13:32 1780872 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.161.234(21), 1 packet
23:13:32 1780873 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.164.20(21), 1 packet
23:13:34 1780874 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.166.58(21), 1 packet
23:13:34 1780875 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.168.99(21), 1 packet
23:13:36 1780876 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.170.138(21), 1 packet
23:13:36 1780877 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.172.176(21), 1 packet
23:13:38 1780878 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.174.214(21), 1 packet
23:13:39 1780879 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.177.1(21), 1 packet
23:13:39 1780880 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.179.40(21), 1 packet
23:13:41 1780881 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.181.78(21), 1 packet
23:13:41 1780882 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.183.125(21), 1 packet
23:13:43 1780883 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.185.161(21), 1 packet
23:13:44 1780884 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.187.199(21), 1 packet
23:13:44 1780885 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.189.248(21), 1 packet
23:13:46 1780886 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.192.26(21), 1 packet
23:13:47 1780887 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.194.75(21), 1 packet
23:13:48 1780888 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.196.117(21), 1 packet
23:13:49 1780889 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.198.157(21), 1 packet
23:13:50 1780890 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.200.195(21), 1 packet
23:13:50 1780891 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.202.237(21), 1 packet
23:13:52 1780892 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.204.153(21), 1 packet
23:13:53 1780893 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.206.252(21), 1 packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:13:54 1780894 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.209.147(21), 1 packet
23:13:56 1780896 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.214.120(21), 1 packet
23:13:57 1780898 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.216.153(21), 1 packet
23:13:58 1780899 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.218.191(21), 1 packet
23:13:59 1780900 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.220.233(21), 1 packet
23:13:59 1780901 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.223.21(21), 1 packet
23:14:01 1780902 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.225.57(21), 1 packet
23:14:02 1780903 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.227.99(21), 1 packet
23:14:03 1780905 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.229.138(21), 1 packet
23:14:04 1780906 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.231.184(21), 1 packet
23:14:04 1780907 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.233.218(21), 1 packet
23:14:06 1780908 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.236.4(21), 1 packet
23:14:07 1780909 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.238.46(21), 1 packet
23:14:08 1780910 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.240.91(21), 1 packet
23:14:08 1780911 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.242.130(21), 1 packet
23:14:10 1780913 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.244.163(21), 1 packet
23:14:11 1780914 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.246.203(21), 1 packet
23:14:12 1780915 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.248.243(21), 1 packet
23:14:13 1780916 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.251.27(21), 1 packet
23:14:14 1780917 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.253.67(21), 1 packet
23:14:15 1780918 %SEC-6-IPACCESSLOGP: denied tcp x.y.74.46(21)
   -> a.b.255.106(21), 1 packet
```

Appendix B: Attack A Sorted by IP, Port

a.b.0.3	**21**	**23:12:17**
a.b.0.3	**23**	**22:57:36**
a.b.0.3	**53**	**23:01:59**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a.b.10.192	23	22:57:41
a.b.10.203	21	23:12:22
a.b.10.210	53	23:02:04
a.b.100.237	23	22:58:23
a.b.100.243	53	23:02:45
a.b.101.12	21	23:13:04
a.b.103.20	23	22:58:23
a.b.103.27	53	23:02:47
a.b.103.56	21	23:13:05
a.b.108.1	**21**	**23:13:06**
a.b.108.1	**23**	**22:58:26**
a.b.108.1	**53**	**23:02:49**
a.b.110.35	23	22:58:27
a.b.110.36	21	23:13:08
a.b.110.39	53	23:02:49
a.b.112.73	23	22:58:28
a.b.112.74	21	23:13:08
a.b.112.77	53	23:02:51
a.b.114.118	23	22:58:28
a.b.114.122	**21**	**23:13:10**
a.b.114.122	**53**	**23:02:51**
a.b.116.153	23	22:58:30
a.b.116.154	53	23:02:53
a.b.116.158	21	23:13:10
a.b.118.195	53	23:02:54
a.b.118.199	**21**	**23:13:12**
a.b.118.199	**23**	**22:58:31**
a.b.12.229	23	22:57:42
a.b.12.244	53	23:02:05
a.b.12.252	21	23:12:23
a.b.120.234	21	23:13:12
a.b.120.239	53	23:02:55
a.b.120.243	23	22:58:31
a.b.123.18	21	23:13:14
a.b.123.21	53	23:02:55
a.b.123.23	23	22:58:33
a.b.125.59	23	22:58:34
a.b.125.60	21	23:13:15
a.b.125.68	53	23:02:57
a.b.127.101	23	22:58:35
a.b.127.107	53	23:02:58
a.b.127.98	21	23:13:15
a.b.129.138	23	22:58:36
a.b.129.140	21	23:13:17
a.b.129.148	53	23:02:58
a.b.131.178	**21**	**23:13:17**
a.b.131.178	**23**	**22:58:37**

© SANS Institute 2001, Author retains full rights

a.b.131.184	53	23:03:00
a.b.133.218	21	23:13:19
a.b.133.222	23	22:58:38
a.b.133.223	53	23:03:01
a.b.136.4	53	23:03:02
a.b.136.6	21	23:13:20
a.b.136.6	23	22:58:39
a.b.138.44	**21**	**23:13:21**
a.b.138.44	**23**	**22:58:39**
a.b.138.46	53	23:03:02
a.b.140.85	53	23:03:04
a.b.140.86	21	23:13:21
a.b.140.88	23	22:58:41
a.b.142.124	21	23:13:23
a.b.142.126	23	22:58:42
a.b.142.129	53	23:03:04
a.b.144.166	**21**	**23:13:24**
a.b.144.166	**23**	**22:58:43**
a.b.144.166	**53**	**23:03:06**
a.b.146.204	23	22:58:44
a.b.146.206	21	23:13:25
a.b.146.211	53	23:03:06
a.b.148.244	21	23:13:25
a.b.148.246	23	22:58:45
a.b.148.249	53	23:03:08
a.b.15.17	23	22:57:43
a.b.15.19	21	23:12:24
a.b.15.28	53	23:02:05
a.b.151.28	23	22:58:46
a.b.151.30	**21**	**23:13:27**
a.b.151.30	**53**	**23:03:09**
a.b.153.71	21	23:13:27
a.b.153.72	**23**	**22:58:47**
a.b.153.72	**53**	**23:03:09**
a.b.155.109	**21**	**23:13:29**
a.b.155.109	**53**	**23:03:11**
a.b.155.110	23	22:58:48
a.b.157.148	23	22:58:48
a.b.157.149	53	23:03:12
a.b.157.156	21	23:13:29
a.b.159.190	23	22:58:50
a.b.159.194	53	23:03:13
a.b.159.198	21	23:13:31
a.b.161.230	53	23:03:14
a.b.161.231	23	22:58:50
a.b.161.234	21	23:13:32
a.b.164.19	23	22:58:52

© SANS Institute 2001, Author retains full rights

a.b.164.20	21	23:13:32
a.b.164.23	53	23:03:14
a.b.166.58	21	23:13:34
a.b.166.62	53	23:03:16
a.b.166.63	23	22:58:52
a.b.168.100	53	23:03:17
a.b.168.99	**21**	**23:13:34**
a.b.168.99	**23**	**22:58:54**
a.b.17.54	23	22:57:44
a.b.17.63	21	23:12:25
a.b.17.69	53	23:02:07
a.b.170.133	**23**	**22:58:55**
a.b.170.133	**53**	**23:03:17**
a.b.170.138	21	23:13:36
a.b.172.174	**23**	**22:58:56**
a.b.172.174	**53**	**23:03:19**
a.b.172.176	21	23:13:36
a.b.174.214	**21**	**23:13:38**
a.b.174.214	**23**	**22:58:57**
a.b.174.214	**53**	**23:03:20**
a.b.177.1	**21**	**23:13:39**
a.b.177.1	**23**	**22:58:58**
a.b.177.1	**53**	**23:03:20**
a.b.179.39	23	22:58:59
a.b.179.40	21	23:13:39
a.b.179.43	53	23:03:22
a.b.181.78	21	23:13:41
a.b.181.79	**23**	**22:58:59**
a.b.181.79	**53**	**23:03:23**
a.b.183.125	**21**	**23:13:41**
a.b.183.125	**23**	**22:59:01**
a.b.183.127	53	23:03:23
a.b.185.158	23	22:59:01
a.b.185.160	53	23:03:25
a.b.185.161	21	23:13:43
a.b.187.198	23	22:59:03
a.b.187.199	21	23:13:44
a.b.187.209	53	23:03:26
a.b.189.238	23	22:59:03
a.b.189.248	21	23:13:44
a.b.19.100	23	22:57:45
a.b.19.102	21	23:12:25
a.b.19.107	53	23:02:08
a.b.190.3	53	23:03:27
a.b.192.26	21	23:13:46
a.b.192.37	53	23:03:27
a.b.194.118	23	22:59:06

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a.b.194.75	**21**	**23:13:47**
a.b.194.75	**53**	**23:03:29**
a.b.196.117	**21**	**23:13:48**
a.b.196.117	**53**	**23:03:30**
a.b.196.159	23	22:59:07
a.b.198.157	21	23:13:49
a.b.198.163	53	23:03:30
a.b.198.199	23	22:59:08
a.b.2.40	23	22:57:36
a.b.2.42	**21**	**23:12:18**
a.b.2.42	**53**	**23:02:00**
a.b.200.195	21	23:13:50
a.b.200.206	53	23:03:32
a.b.200.239	23	22:59:09
a.b.202.237	21	23:13:50
a.b.202.248	53	23:03:33
a.b.203.28	23	22:59:09
a.b.204.153	21	23:13:52
a.b.205.32	53	23:03:34
a.b.205.66	23	22:59:11
a.b.206.252	21	23:13:53
a.b.207.104	23	22:59:11
a.b.207.70	53	23:03:34
a.b.209.119	53	23:03:36
a.b.209.146	23	22:59:13
a.b.209.147	21	23:13:54
a.b.21.135	53	23:02:09
a.b.21.139	23	22:57:45
a.b.21.140	21	23:12:27
a.b.211.150	53	23:03:37
a.b.211.183	23	22:59:13
a.b.213.192	53	23:03:38
a.b.213.226	23	22:59:15
a.b.214.120	21	23:13:56
a.b.215.230	53	23:03:38
a.b.216.13	23	22:59:15
a.b.216.153	21	23:13:57
a.b.218.16	53	23:03:40
a.b.218.191	21	23:13:58
a.b.218.51	23	22:59:17
a.b.220.233	21	23:13:59
a.b.220.58	53	23:03:40
a.b.220.89	23	22:59:18
a.b.222.104	53	23:03:42
a.b.222.130	23	22:59:19
a.b.223.21	21	23:13:59
a.b.224.135	53	23:03:42

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a.b.224.170	23	22:59:20
a.b.225.57	21	23:14:01
a.b.226.181	53	23:03:44
a.b.226.210	23	22:59:21
a.b.227.99	21	23:14:02
a.b.228.219	53	23:03:44
a.b.228.250	23	22:59:22
a.b.229.138	21	23:14:03
a.b.23.177	23	22:57:47
a.b.23.188	**21**	**23:12:28**
a.b.23.188	**53**	**23:02:10**
a.b.231.184	21	23:14:04
a.b.231.3	53	23:03:46
a.b.231.34	23	22:59:22
a.b.233.1	23	22:59:24
a.b.233.218	21	23:14:04
a.b.233.41	53	23:03:46
a.b.235.209	23	22:59:24
a.b.235.87	53	23:03:47
a.b.236.4	21	23:14:06
a.b.237.121	53	23:03:49
a.b.238.46	21	23:14:07
a.b.239.161	53	23:03:50
a.b.240.39	23	22:59:27
a.b.240.91	21	23:14:08
a.b.242.130	21	23:14:08
a.b.242.85	23	22:59:27
a.b.244.119	23	22:59:29
a.b.244.163	21	23:14:10
a.b.246.158	23	22:59:30
a.b.246.203	21	23:14:11
a.b.248.200	23	22:59:31
a.b.248.243	21	23:14:12
a.b.25.215	23	22:57:48
a.b.25.226	53	23:02:11
a.b.25.234	21	23:12:29
a.b.250.238	23	22:59:32
a.b.251.27	21	23:14:13
a.b.253.26	23	22:59:32
a.b.253.67	21	23:14:14
a.b.255.106	21	23:14:15
a.b.255.64	23	22:59:34
a.b.28.11	53	23:02:12
a.b.28.20	21	23:12:30
a.b.28.3	23	22:57:49
a.b.30.39	23	22:57:50
a.b.30.51	**21**	**23:12:31**

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a.b.30.51	**53**	**23:02:13**
a.b.32.79	23	22:57:51
a.b.32.91	53	23:02:14
a.b.32.92	21	23:12:31
a.b.34.119	23	22:57:52
a.b.34.130	**21**	**23:12:33**
a.b.34.130	**53**	**23:02:15**
a.b.36.163	23	22:57:52
a.b.36.170	**21**	**23:12:34**
a.b.36.170	**53**	**23:02:16**
a.b.38.204	23	22:57:54
a.b.38.210	53	23:02:17
a.b.38.212	21	23:12:35
a.b.4.82	**21**	**23:12:19**
a.b.4.82	**23**	**22:57:38**
a.b.4.82	**53**	**23:02:01**
a.b.40.242	23	22:57:54
a.b.40.251	53	23:02:17
a.b.40.252	21	23:12:36
a.b.43.27	23	22:57:56
a.b.43.36	21	23:12:37
a.b.43.39	53	23:02:19
a.b.45.69	23	22:57:57
a.b.45.76	21	23:12:38
a.b.45.80	53	23:02:20
a.b.47.112	23	22:57:58
a.b.47.116	53	23:02:21
a.b.47.123	21	23:12:38
a.b.49.150	23	22:57:58
a.b.49.156	53	23:02:21
a.b.49.161	21	23:12:40
a.b.51.187	23	22:58:00
a.b.51.196	53	23:02:23
a.b.51.203	21	23:12:41
a.b.53.229	23	22:58:00
a.b.53.237	21	23:12:41
a.b.53.240	53	23:02:24
a.b.56.1	23	22:58:02
a.b.56.20	21	23:12:43
a.b.56.23	53	23:02:24
a.b.58.57	23	22:58:02
a.b.58.62	53	23:02:26
a.b.58.66	21	23:12:43
a.b.6.109	23	22:57:39
a.b.6.120	**21**	**23:12:20**
a.b.6.120	**53**	**23:02:02**
a.b.60.1	23	22:58:04

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
a.b.60.102  21    23:12:44
a.b.60.108  53    23:02:26
a.b.62.143  53    23:02:28
a.b.62.146  21    23:12:46
a.b.62.172  23    22:58:04
a.b.64.181  21    23:12:47
a.b.64.185  53    23:02:29
a.b.64.205  23    22:58:05
a.b.66.222  21    23:12:48
a.b.66.222  53    23:02:29
a.b.66.243  23    22:58:07
a.b.68.162  21    23:12:49
a.b.69.14   53    23:02:31
a.b.69.27   23    22:58:08
a.b.70.203  21    23:12:49
a.b.71.58   53    23:02:32
a.b.71.67   23    22:58:09
a.b.73.113  23    22:58:10
a.b.73.32   21    23:12:51
a.b.73.97   53    23:02:33
a.b.75.136  53    23:02:34
a.b.75.147  23    22:58:11
a.b.75.214  21    23:12:52
a.b.77.178  53    23:02:35
a.b.77.190  23    22:58:12
a.b.78.2    21    23:12:53
a.b.79.216  53    23:02:36
a.b.79.227  23    22:58:12
a.b.8.149   23    22:57:40
a.b.8.163   21    23:12:21
a.b.8.163   53    23:02:02
a.b.80.39   21    23:12:53
a.b.81.11   22:58:13    # Syn-Flood
a.b.81.254  23:02:36    # Syn-Flood
a.b.81.97   23:12:54    # Syn-Flood
a.b.83.1    21    23:12:55
a.b.83.1    23    22:58:14
a.b.83.1    53    23:02:37
a.b.88.2    23    22:58:17
a.b.88.2    53    23:02:40
a.b.88.5    21    23:12:57
a.b.90.35   53    23:02:40
a.b.90.38   23    22:58:18
a.b.90.63   21    23:12:59
a.b.92.103  21    23:13:00
a.b.92.82   23    22:58:19
a.b.92.82   53    23:02:41
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a.b.94.120	**23**	**22:58:20**
a.b.94.120	**53**	**23:02:43**
a.b.94.146	21	23:13:00
a.b.96.163	23	22:58:21
a.b.96.163	53	23:02:43
a.b.96.182	21	23:13:02
a.b.98.198	23	22:58:21
a.b.98.205	53	23:02:45
a.b.98.222	21	23:13:02

Appendix C: Attack A Connections Sorted by Time

```
22:57:38 node44 in.telnetd[29410]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node54 inetd[6218]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
22:57:38 node51 inetd[96329]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
22:57:38 node64 in.telnetd[26214]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node9 in.telnetd[1603]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node49 in.telnetd[23703]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node43 in.telnetd[16378]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:35 node-a14 in.telnetd[13593]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node-a1 in.telnetd[6648]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
22:57:38 node27 in.telnetd[2166]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node-a13 in.telnetd[6724]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:40 node36 in.telnetd[25133]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:36 node3 in.telnetd[16261]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node66 in.telnetd[8969]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node-a3 in.telnetd[26524]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node-a6 in.telnetd[1772]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:41 node38 inetd[22506]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
22:57:41 node2 inetd[38559]: refused connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:57:42 node9 in.telnetd[1604]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node34 in.telnetd[5858]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node6 in.telnetd[5953]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node6 in.telnetd[5954]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8881]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node63 in.telnetd[20997]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8882]: refused connect from
  ip-46-74-y- x.rev.xyz.com
22:57:43 node39 in.telnetd[12954]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:43 node35 in.telnetd[4868]: refused connect from
  ip-46-74-y- x.rev.xyz.com
22:57:44 node23 in.telnetd[24366]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:52:46 node10 in.telnetd[18918]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:43 node37 in.telnetd[6982]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:45 node32 in.telnetd[8546]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node-a8 in.telnetd[9393]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:44 node55 in.telnetd[4192]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:45 node64 in.telnetd[26215]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:46 node31 in.telnetd[28781]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:46 node39 in.telnetd[12963]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:46 node62 in.telnetd[762]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node-a2 in.telnetd[4531]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:54:35 node5 in.telnetd[12457]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:52 node1 in.telnetd[23382]: refused connect from
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  root@ip-46-74-y-x.rev.xyz.com
22:57:53 node-a9 in.telnetd[3078]: [ID 927837 daemon.info]
  connect from ip-46-74-y-x.rev.xyz.com
22:57:54 node-a4 in.telnetd[23029]: [ID 947420
  daemon.warning]refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node8 in.telnetd[14745]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node48 in.telnetd[5980]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node52 in.telnetd[11421]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node61 in.telnetd[25938]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node21 in.telnetd[7786]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node11 in.telnetd[1788]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:00 node-a12 in.telnetd[20627]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node-a7 in.telnetd[13404]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node28 in.telnetd[4987]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:02 node45 in.telnetd[17631]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:02 node-a10 in.telnetd[12393]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:02 node-a11 in.telnetd[1639]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:04 node-a5 in.telnetd[8329]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:04 node47 in.telnetd[3874]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:04 node53 in.telnetd[5851]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:05 node25 in.telnetd[27814]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:07 node65 in.telnetd[551]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:10 node42 in.telnetd[349]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node9 in.ftpd[1622]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node34 in.ftpd[5869]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node38 inetd[22520]: connection from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node2 inetd[38573]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node40 inetd[23548]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node44 in.ftpd[29530]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node54 inetd[6236]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node51 inetd[96382]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node6 in.ftpd[5971]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node6 ftpd[5971]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:17 node18 in.ftpd[9060]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node39 in.ftpd[12984]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node64 in.ftpd[26317]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node63 in.ftpd[21201]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:15 node3 in.ftpd[16268]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node27 in.ftpd[2168]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node43 in.ftpd[16388]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node49 in.ftpd[23711]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node66 in.ftpd[8976]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node36 in.ftpd[25139]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:16 node12 in.ftpd[1788]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node35 in.ftpd[4870]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node23 in.ftpd[24368]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:07:19 node10 in.ftpd[18920]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node55 in.ftpd[4194]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:16 node37 in.ftpd[6984]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:18 node32 in.ftpd[8548]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node30 in.ftpd[12602]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node4 in.ftpd[16070]: connect from
  ip-46-74-y-x.rev.xyz.com
23:05:40 node50 in.ftpd[2526]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node26 in.ftpd[2567]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node33 in.ftpd[25377]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node7 in.ftpd[7641]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node64 in.ftpd[26318]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node9 in.ftpd[1623]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node6 in.ftpd[5972]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node6 ftpd[5972]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:18 node18 in.ftpd[9061]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node68 in.ftpd[16175]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node19 in.ftpd[4184]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node60 in.ftpd[1422]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node17 in.ftpd[23810]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node31 in.ftpd[28799]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:03:03 node29 in.ftpd[2232]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node24 in.ftpd[28770]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:19 node46 in.ftpd[8767]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:20 node62 in.ftpd[777]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:20 node56 in.ftpd[20889]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node18 in.ftpd[9062]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:21 node58 in.ftpd[7241]: refused connect from
```

© SANS Institute 2001, Author retains full rights

```
  ip-46-74-y-x.rev.xyz.com
23:12:21 node41 in.ftpd[10948]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node57 in.ftpd[16254]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:05:08 node58 in.ftpd[9666]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
23:12:22 node67 inetd[49203]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:23 node64 in.ftpd[26319]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node9 in.ftpd[1624]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node6 in.ftpd[5973]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node6 ftpd[5973]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:22 node22 in.ftpd[5983]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:09:16 node5 in.ftpd[12470]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:29 node20 in.ftpd[10395]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:32 node1 in.ftpd[23410]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:40 node48 in.ftpd[6425]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:40 node25 in.ftpd[27836]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node61 in.ftpd[25979]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node8 in.ftpd[14756]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node52 in.ftpd[11422]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node21 in.ftpd[7793]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node11 in.ftpd[1789]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node28 in.ftpd[5158]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:42 node13 in.ftpd[13421]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:42 node45 in.ftpd[17650]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:42 node45 ftpd[17650]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:12:42 node16 in.ftpd[1379]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:42 node14 in.ftpd[16757]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:43 node14 ftpd[16757]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:12:45 node47 in.ftpd[3875]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node53 in.ftpd[5962]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node65 in.ftpd[555]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node42 in.ftpd[353]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node40 inetd[24487]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node51 inetd[96420]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node2 inetd[38583]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node54 inetd[6246]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node6 in.ftpd[5991]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node6 ftpd[5991]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:28:16 node9 in.ftpd[1625]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node34 in.ftpd[5872]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node44 in.ftpd[29604]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node39 in.ftpd[12986]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node18 in.ftpd[9069]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:36 node38 inetd[22530]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:23:37 node10 in.ftpd[18923]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:35 node35 in.ftpd[4872]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:36 node63 in.ftpd[21366]: connect from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  ip-46-74-y-x.rev.xyz.com
23:28:46 node4 in.ftpd[16073]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node6 in.ftpd[5992]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node6 ftpd[5992]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:28:46 node9 in.ftpd[1626]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:52 node26 in.ftpd[2569]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node33 in.ftpd[25412]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node41 in.ftpd[10960]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:55 node68 in.ftpd[16177]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9071]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9072]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:05 node27 in.ftpd[2170]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node49 in.ftpd[23714]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:03 node3 in.ftpd[16276]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node43 in.ftpd[16392]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node64 in.ftpd[26324]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:07 node66 in.ftpd[8985]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:12 node67 inetd[49460]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:29:12 node36 in.ftpd[25147]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:11 node23 in.ftpd[24370]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:11 node55 in.ftpd[4196]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:10 node12 in.ftpd[1809]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:12 node37 in.ftpd[6986]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:16 node30 in.ftpd[12604]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:29:17 node32 in.ftpd[8551]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:22:39 node50 in.ftpd[2528]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:18 node7 in.ftpd[7677]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:19 node64 in.ftpd[26325]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:22 node9 in.ftpd[1627]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:23 node6 in.ftpd[5993]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:23 node6 ftpd[5993]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:29:21 node22 in.ftpd[5985]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:22 node60 in.ftpd[1457]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:23 node19 in.ftpd[4186]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:25 node17 in.ftpd[23827]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:20:12 node29 in.ftpd[2234]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:29 node31 in.ftpd[28809]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:32 node24 in.ftpd[28780]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:33 node46 in.ftpd[8777]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:34 node62 in.ftpd[787]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:33 node56 in.ftpd[20891]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:37 node58 in.ftpd[7244]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:37 node57 in.ftpd[16290]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:22:29 node59 in.ftpd[9681]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
23:29:45 node64 in.ftpd[26326]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:26:35 node5 in.ftpd[12486]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:49 node15 in.ftpd[2321]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:49 node15 in.ftpd[2321]: refused connect from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  root@ip-46-74-y-x.rev.xyz.com
23:29:50 node1 in.ftpd[23432]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:52 node21 in.ftpd[7800]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:56 node45 in.ftpd[17672]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:56 node45 ftpd[17672]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:29:59 node14 in.ftpd[16758]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:59 node14 ftpd[16758]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:30:01 node48 in.ftpd[6884]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:02 node25 in.ftpd[27854]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:05 node61 in.ftpd[26028]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:06 node8 in.ftpd[14759]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:06 node52 in.ftpd[11424]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:08 node11 in.ftpd[1790]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:08 node28 in.ftpd[5262]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:12 node13 in.ftpd[13440]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:12 node47 in.ftpd[3898]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:13 node53 in.ftpd[6094]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:14 node65 in.ftpd[564]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:17 node42 in.ftpd[361]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Appendix D: Attack A Connections Sorted by Node Name

```
23:12:32 node1 in.ftpd[23410]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:52 node1 in.telnetd[23382]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:50 node1 in.ftpd[23432]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:52:46 node10 in.telnetd[18918]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:23:37 node10 in.ftpd[18923]: connect from
  ip-46-74-y-x.rev.xyz.com
23:07:19 node10 in.ftpd[18920]: connect from
  ip-46-74-y-x.rev.xyz.com
23:30:08 node11 in.ftpd[1790]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node11 in.ftpd[1789]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node11 in.telnetd[1788]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:10 node12 in.ftpd[1809]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:16 node12 in.ftpd[1788]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:42 node13 in.ftpd[13421]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:12 node13 in.ftpd[13440]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:43 node14 ftpd[16757]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:12:42 node14 in.ftpd[16757]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:59 node14 ftpd[16758]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:29:59 node14 in.ftpd[16758]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:49 node15 in.ftpd[2321]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:48 node15 in.telnetd[2212]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:49 node15 in.ftpd[2321]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:28 node15 in.ftpd[2278]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:12:42 node16 in.ftpd[1379]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node17 in.ftpd[23810]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:25 node17 in.ftpd[23827]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8881]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9072]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:56 node18 in.ftpd[9071]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node18 in.telnetd[8882]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node18 in.ftpd[9062]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node18 in.ftpd[9061]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node18 in.ftpd[9060]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node18 in.ftpd[9069]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:23 node19 in.ftpd[4186]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node19 in.ftpd[4184]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node2 inetd[38583]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node2 inetd[38573]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
22:57:41 node2 inetd[38559]: refused connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
23:12:29 node20 in.ftpd[10395]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:52 node21 in.ftpd[7800]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node21 in.ftpd[7793]: connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node21 in.telnetd[7786]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:22 node22 in.ftpd[5983]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:21 node22 in.ftpd[5985]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:11 node23 in.ftpd[24370]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:44 node23 in.telnetd[24366]: refused connect from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  ip-46-74-y-x.rev.xyz.com
23:12:17 node23 in.ftpd[24368]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node24 in.ftpd[28770]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:32 node24 in.ftpd[28780]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:40 node25 in.ftpd[27836]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:02 node25 in.ftpd[27854]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:05 node25 in.telnetd[27814]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node26 in.ftpd[2567]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:52 node26 in.ftpd[2569]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node27 in.ftpd[2168]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:05 node27 in.ftpd[2170]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node27 in.telnetd[2166]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node28 in.telnetd[4987]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:08 node28 in.ftpd[5262]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node28 in.ftpd[5158]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:03:03 node29 in.ftpd[2232]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:20:12 node29 in.ftpd[2234]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:36 node3 in.telnetd[16261]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:03 node3 in.ftpd[16276]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:15 node3 in.ftpd[16268]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:16 node30 in.ftpd[12604]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node30 in.ftpd[12602]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node31 in.ftpd[28799]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:29 node31 in.ftpd[28809]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:57:46 node31 in.telnetd[28781]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:45 node32 in.telnetd[8546]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:17 node32 in.ftpd[8551]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node32 in.ftpd[8548]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node33 in.ftpd[25412]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node33 in.ftpd[25377]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node34 in.telnetd[5858]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node34 in.ftpd[5869]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node34 in.ftpd[5872]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:35 node35 in.ftpd[4872]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:43 node35 in.telnetd[4868]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node35 in.ftpd[4870]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:12 node36 in.ftpd[25147]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:40 node36 in.telnetd[25133]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node36 in.ftpd[25139]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:43 node37 in.telnetd[6982]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:12 node37 in.ftpd[6986]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:16 node37 in.ftpd[6984]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node38 inetd[22520]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
22:57:41 node38 inetd[22506]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
23:28:36 node38 inetd[22530]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:17 node39 in.ftpd[12984]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:46 node39 in.telnetd[12963]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:43 node39 in.telnetd[12954]: refused connect from
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  root@ip-46-74-y-x.rev.xyz.com
23:28:26 node39 in.ftpd[12986]: connect from I
  p-46-74-y-x.rev.xyz.com
23:12:18 node4 in.ftpd[16070]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node4 in.ftpd[16073]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node40 inetd[23548]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node40 inetd[24487]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:56 node41 in.ftpd[10960]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:21 node41 in.ftpd[10948]: connect from
  ip-46-74-y-x.rev.xyz.com
23:30:17 node42 in.ftpd[361]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:10 node42 in.telnetd[349]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node42 in.ftpd[353]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node43 in.ftpd[16388]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node43 in.ftpd[16392]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node43 in.telnetd[16378]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node44 in.telnetd[29410]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node44 in.ftpd[29530]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:26 node44 in.ftpd[29604]: connect from
  ip-46-74-y-x.rev.xyz.com
22:58:02 node45 in.telnetd[17631]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:56 node45 in.ftpd[17672]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:42 node45 in.ftpd[17650]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:56 node45 ftpd[17672]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:12:42 node45 ftpd[17650]: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun 23
23:29:33 node46 in.ftpd[8777]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:19 node46 in.ftpd[8767]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
23:30:12 node47 in.ftpd[3898]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node47 in.ftpd[3875]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:04 node47 in.telnetd[3874]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:01 node48 in.ftpd[6884]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node48 in.telnetd[5980]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:40 node48 in.ftpd[6425]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node49 in.telnetd[23703]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node49 in.ftpd[23711]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node49 in.ftpd[23714]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:09:16 node5 in.ftpd[12470]: connect from
  ip-46-74-y-x.rev.xyz.com
23:26:35 node5 in.ftpd[12486]: connect from
  ip-46-74-y-x.rev.xyz.com
22:54:35 node5 in.telnetd[12457]: connect from
  ip-46-74-y-x.rev.xyz.com
23:05:40 node50 in.ftpd[2526]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:22:39 node50 in.ftpd[2528]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node51 inetd[96329]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
23:12:17 node51 inetd[96382]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node51 inetd[96420]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:30:06 node52 in.ftpd[11424]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node52 in.telnetd[11421]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node52 in.ftpd[11422]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:13 node53 in.ftpd[6094]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:04 node53 in.telnetd[5851]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node53 in.ftpd[5962]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node54 inetd[6236]: connection from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:16 node54 inetd[6246]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
22:57:38 node54 inetd[6218]: connection from
  ip-46-74-y-x.rev.xyz.com, service telnetd (tcp)
23:29:11 node55 in.ftpd[4196]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node55 in.ftpd[4194]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:44 node55 in.telnetd[4192]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:20 node56 in.ftpd[20889]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:33 node56 in.ftpd[20891]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node57 in.ftpd[16254]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:37 node57 in.ftpd[16290]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:21 node58 in.ftpd[7241]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:37 node58 in.ftpd[7244]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:05:08 node58 in.ftpd[9666]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
23:22:29 node59 in.ftpd[9681]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
23:12:24 node6 ftpd[5973]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:24 node6 in.ftpd[5973]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node6 in.ftpd[5972]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node6 ftpd[5971]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:29:23 node6 ftpd[5993]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:29:23 node6 in.ftpd[5993]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node6 in.ftpd[5991]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node6 ftpd[5991]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:18 node6 ftpd[5972]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
22:57:42 node6 in.telnetd[5953]: refused connect from
  ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:57:42 node6 in.telnetd[5954]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node6 ftpd[5992]: FTPD: connection from
  ip-46-74-y-x.rev.xyz.com at Sat Jun
23:12:17 node6 in.ftpd[5971]: connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node6 in.ftpd[5992]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:22 node60 in.ftpd[1457]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node60 in.ftpd[1422]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node61 in.telnetd[25938]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node61 in.ftpd[25979]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:05 node61 in.ftpd[26028]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:46 node62 in.telnetd[762]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:12:20 node62 in.ftpd[777]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
23:29:34 node62 in.ftpd[787]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:42 node63 in.telnetd[20997]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:36 node63 in.ftpd[21366]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node63 in.ftpd[21201]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node64 in.ftpd[26317]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node64 in.ftpd[26318]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:06 node64 in.ftpd[26324]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:23 node64 in.ftpd[26319]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:45 node64 in.ftpd[26326]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:45 node64 in.telnetd[26215]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:19 node64 in.ftpd[26325]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node64 in.telnetd[26214]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:07 node65 in.telnetd[551]: refused connect from
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
  ip-46-74-y-x.rev.xyz.com
23:30:14 node65 in.ftpd[564]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:45 node65 in.ftpd[555]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node66 in.ftpd[8976]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:07 node66 in.ftpd[8985]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node66 in.telnetd[8969]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:29:12 node67 inetd[49460]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:12:22 node67 inetd[49203]: connection from
  ip-46-74-y-x.rev.xyz.com, service ftpd (tcp)
23:28:55 node68 in.ftpd[16177]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node68 in.ftpd[16175]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:18 node7 in.ftpd[7677]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:19 node7 in.ftpd[7641]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node8 in.telnetd[14745]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:30:06 node8 in.ftpd[14759]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:12:41 node8 in.ftpd[14756]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node9 in.telnetd[1604]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:46 node9 in.ftpd[1626]: connect from
  ip-46-74-y-x.rev.xyz.com
23:29:22 node9 in.ftpd[1627]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:17 node9 in.ftpd[1622]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:24 node9 in.ftpd[1624]: connect from
  ip-46-74-y-x.rev.xyz.com
23:12:18 node9 in.ftpd[1623]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node9 in.telnetd[1603]: refused connect from
  ip-46-74-y-x.rev.xyz.com
23:28:16 node9 in.ftpd[1625]: connect from
  ip-46-74-y-x.rev.xyz.com
22:57:39 node-a1 in.telnetd[6648]: [ID 947420 daemon.warning]
  refused connect from root@ip-46-74-y-x.rev.xyz.com
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
22:58:02 node-a10 in.telnetd[12393]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:02 node-a11 in.telnetd[1639]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:00 node-a12 in.telnetd[20627]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node-a13 in.telnetd[6724]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:35 node-a14 in.telnetd[13593]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:48 node-a2 in.telnetd[4531]: refused connect from
  root@ip-46-74-y-x.rev.xyz.com
22:57:39 node-a3 in.telnetd[26524]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:54 node-a4 in.telnetd[23029]: [ID 947420 daemon.warning]
  refused connect from ip-46-74-y-x.rev.xyz.com
22:58:04 node-a5 in.telnetd[8329]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:38 node-a6 in.telnetd[1772]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:58:01 node-a7 in.telnetd[13404]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:42 node-a8 in.telnetd[9393]: refused connect from
  ip-46-74-y-x.rev.xyz.com
22:57:53 node-a9 in.telnetd[3078]: [ID 927837 daemon.info]
  connect from ip-46-74-y-x.rev.xyz.com
```

Appendix E: Attack B Connections Sorted by Time

```
04:35:02 denied tcp r.s.236.88(33734) -> a.b.0.1(80), 1 packet
04:35:05 denied tcp r.s.236.88(33736) -> a.b.0.3(80), 1 packet
04:35:07 denied tcp r.s.236.88(34186) -> a.b.0.51(80), 1
packet
04:35:10 denied tcp r.s.236.88(34186) -> a.b.0.51(80), 1
packet
04:35:11 denied tcp r.s.236.88(34251) -> a.b.0.78(80), 1
packet
04:35:12 denied tcp r.s.236.88(34246) -> a.b.0.73(80), 1
packet
04:35:13 denied tcp r.s.236.88(34704) -> a.b.0.101(80), 1
packet
04:35:16 denied tcp r.s.236.88(34707) -> a.b.0.104(80), 1
packet
04:35:19 denied tcp r.s.236.88(35258) -> a.b.0.151(80), 1
packet
04:35:22 denied tcp r.s.236.88(35260) -> a.b.0.153(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:35:24 denied tcp r.s.236.88(35870) -> a.b.0.201(80), 1
packet
04:35:27 denied tcp r.s.236.88(35873) -> a.b.0.204(80), 1
packet
04:35:27 denied tcp r.s.236.88(35885) -> a.b.0.216(80), 1
packet
04:35:30 denied tcp r.s.236.88(36448) -> a.b.1.2(80), 1 packet
04:35:33 denied tcp r.s.236.88(36450) -> a.b.1.4(80), 1 packet
04:35:34 denied tcp r.s.236.88(36522) -> a.b.1.49(80), 1
packet
04:35:36 denied tcp r.s.236.88(37011) -> a.b.1.51(80), 1
packet
04:35:38 denied tcp r.s.236.88(37011) -> a.b.1.51(80), 1
packet
04:35:40 denied tcp r.s.236.88(37134) -> a.b.1.97(80), 1
packet
04:35:42 denied tcp r.s.236.88(37565) -> a.b.1.101(80), 1
packet
04:35:44 denied tcp r.s.236.88(37565) -> a.b.1.101(80), 1
packet
04:35:45 denied tcp r.s.236.88(37648) -> a.b.1.127(80), 1
packet
04:35:47 denied tcp r.s.236.88(38156) -> a.b.1.151(80), 1
packet
04:35:49 denied tcp r.s.236.88(38156) -> a.b.1.151(80), 1
packet
04:35:51 denied tcp r.s.236.88(38205) -> a.b.1.179(80), 1
packet
04:35:53 denied tcp r.s.236.88(38718) -> a.b.1.201(80), 1
packet
04:35:56 denied tcp r.s.236.88(38718) -> a.b.1.201(80), 1
packet
04:35:57 denied tcp r.s.236.88(38741) -> a.b.1.224(80), 1
packet
04:36:00 denied tcp r.s.236.88(39326) -> a.b.2.1(80), 1 packet
04:36:02 denied tcp r.s.236.88(39326) -> a.b.2.1(80), 1 packet
04:36:04 denied tcp r.s.236.88(39507) -> a.b.2.48(80), 1
packet
04:36:06 denied tcp r.s.236.88(39795) -> a.b.2.51(80), 1
packet
04:36:09 denied tcp r.s.236.88(39798) -> a.b.2.54(80), 1
packet
04:36:12 denied tcp r.s.236.88(40179) -> a.b.2.101(80), 1
packet
04:36:15 denied tcp r.s.236.88(40182) -> a.b.2.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:36:16 denied tcp r.s.236.88(40179) -> a.b.2.101(80), 1
packet
04:36:18 denied tcp r.s.236.88(40583) -> a.b.2.151(80), 1
packet
04:36:21 denied tcp r.s.236.88(40583) -> a.b.2.151(80), 1
packet
04:36:22 denied tcp r.s.236.88(40905) -> a.b.2.200(80), 1
packet
04:36:25 denied tcp r.s.236.88(41050) -> a.b.2.201(80), 1
packet
04:36:27 denied tcp r.s.236.88(41050) -> a.b.2.201(80), 1
packet
04:36:28 denied tcp r.s.236.88(41242) -> a.b.2.228(80), 1
packet
04:36:31 denied tcp r.s.236.88(41701) -> a.b.3.1(80), 1 packet
04:36:35 denied tcp r.s.236.88(41703) -> a.b.3.3(80), 1 packet
04:36:36 denied tcp r.s.236.88(41748) -> a.b.3.48(80), 1
packet
04:36:37 denied tcp r.s.236.88(41993) -> a.b.3.51(80), 1
packet
04:36:40 denied tcp r.s.236.88(41996) -> a.b.3.54(80), 1
packet
04:36:41 denied tcp r.s.236.88(41993) -> a.b.3.51(80), 1
packet
04:36:43 denied tcp r.s.236.88(42397) -> a.b.3.101(80), 1
packet
04:36:45 denied tcp r.s.236.88(42397) -> a.b.3.101(80), 1
packet
04:36:46 denied tcp r.s.236.88(42418) -> a.b.3.122(80), 1
packet
04:36:47 denied tcp r.s.236.88(42413) -> a.b.3.117(80), 1
packet
04:36:51 denied tcp r.s.236.88(42799) -> a.b.3.151(80), 1
packet
04:36:52 denied tcp r.s.236.88(42820) -> a.b.3.172(80), 1
packet
04:36:58 denied tcp r.s.236.88(43185) -> a.b.3.204(80), 1
packet
04:37:00 denied tcp r.s.236.88(43595) -> a.b.4.2(80), 1 packet
04:37:03 denied tcp r.s.236.88(43597) -> a.b.4.4(80), 1 packet
04:37:05 denied tcp r.s.236.88(43914) -> a.b.4.51(80), 1
packet
04:37:09 denied tcp r.s.236.88(43917) -> a.b.4.54(80), 1
packet
04:37:10 denied tcp r.s.236.88(44016) -> a.b.4.81(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:37:11 denied tcp r.s.236.88(44330) -> a.b.4.101(80), 1
packet
04:37:16 denied tcp r.s.236.88(44330) -> a.b.4.101(80), 1
packet
04:37:17 denied tcp r.s.236.88(44758) -> a.b.4.151(80), 1
packet
04:37:21 denied tcp r.s.236.88(44761) -> a.b.4.154(80), 1
packet
04:37:21 denied tcp r.s.236.88(44773) -> a.b.4.166(80), 1
packet
04:37:28 denied tcp r.s.236.88(45156) -> a.b.4.201(80), 1
packet
04:37:30 denied tcp r.s.236.88(45730) -> a.b.5.1(80), 1 packet
04:37:34 denied tcp r.s.236.88(45733) -> a.b.5.4(80), 1 packet
04:37:36 denied tcp r.s.236.88(46178) -> a.b.5.51(80), 1
packet
04:37:40 denied tcp r.s.236.88(46180) -> a.b.5.53(80), 1
packet
04:37:42 denied tcp r.s.236.88(46508) -> a.b.5.101(80), 1
packet
04:37:45 denied tcp r.s.236.88(46529) -> a.b.5.122(80), 1
packet
04:37:48 denied tcp r.s.236.88(46917) -> a.b.5.151(80), 1
packet
04:37:50 denied tcp r.s.236.88(46917) -> a.b.5.151(80), 1
packet
04:37:51 denied tcp r.s.236.88(46938) -> a.b.5.172(80), 1
packet
04:37:52 denied tcp r.s.236.88(46938) -> a.b.5.172(80), 1
packet
04:37:56 denied tcp r.s.236.88(47296) -> a.b.5.201(80), 1
packet
04:37:57 denied tcp r.s.236.88(47413) -> a.b.5.228(80), 1
packet
04:38:04 denied tcp r.s.236.88(47914) -> a.b.6.3(80), 1 packet
04:38:06 denied tcp r.s.236.88(48112) -> a.b.6.51(80), 1
packet
04:38:08 denied tcp r.s.236.88(48112) -> a.b.6.51(80), 1
packet
04:38:08 denied tcp r.s.236.88(48134) -> a.b.6.73(80), 1
packet
04:38:14 denied tcp r.s.236.88(48523) -> a.b.6.104(80), 1
packet
04:38:14 denied tcp r.s.236.88(48568) -> a.b.6.149(80), 1
packet
04:38:17 denied tcp r.s.236.88(48928) -> a.b.6.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:38:19 denied tcp r.s.236.88(48928) -> a.b.6.151(80), 1
packet
04:38:22 denied tcp r.s.236.88(49328) -> a.b.6.201(80), 1
packet
04:38:27 denied tcp r.s.236.88(49744) -> a.b.7.1(80), 1 packet
04:38:31 denied tcp r.s.236.88(49747) -> a.b.7.4(80), 1 packet
04:38:37 denied tcp r.s.236.88(50492) -> a.b.7.101(80), 1
packet
04:38:40 denied tcp r.s.236.88(50495) -> a.b.7.104(80), 1
packet
04:38:46 denied tcp r.s.236.88(50908) -> a.b.7.153(80), 1
packet
04:38:48 denied tcp r.s.236.88(51310) -> a.b.7.201(80), 1
packet
04:38:52 denied tcp r.s.236.88(51310) -> a.b.7.201(80), 1
packet
04:38:54 denied tcp r.s.236.88(51776) -> a.b.8.1(80), 1 packet
04:38:58 denied tcp r.s.236.88(51776) -> a.b.8.1(80), 1 packet
04:38:59 denied tcp r.s.236.88(52147) -> a.b.8.51(80), 1
packet
04:39:04 denied tcp r.s.236.88(52147) -> a.b.8.51(80), 1
packet
04:39:05 denied tcp r.s.236.88(52512) -> a.b.8.101(80), 1
packet
04:39:09 denied tcp r.s.236.88(52512) -> a.b.8.101(80), 1
packet
04:39:11 denied tcp r.s.236.88(52734) -> a.b.8.151(80), 1
packet
04:39:14 denied tcp r.s.236.88(52737) -> a.b.8.154(80), 1
packet
04:39:16 denied tcp r.s.236.88(53187) -> a.b.8.246(80), 1
packet
04:39:20 denied tcp r.s.236.88(53142) -> a.b.8.201(80), 1
packet
04:39:22 denied tcp r.s.236.88(53554) -> a.b.9.1(80), 1 packet
04:39:24 denied tcp r.s.236.88(53554) -> a.b.9.1(80), 1 packet
04:39:25 denied tcp r.s.236.88(53580) -> a.b.9.27(80), 1
packet
04:39:28 denied tcp r.s.236.88(53984) -> a.b.9.51(80), 1
packet
04:39:30 denied tcp r.s.236.88(53984) -> a.b.9.51(80), 1
packet
04:39:32 denied tcp r.s.236.88(54038) -> a.b.9.83(80), 1
packet
04:39:37 denied tcp r.s.236.88(54361) -> a.b.9.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:39:39 denied tcp r.s.236.88(54766) -> a.b.9.151(80), 1
packet
04:39:42 denied tcp r.s.236.88(54768) -> a.b.9.153(80), 1
packet
04:39:44 denied tcp r.s.236.88(55174) -> a.b.9.201(80), 1
packet
04:39:46 denied tcp r.s.236.88(55174) -> a.b.9.201(80), 1
packet
04:39:47 denied tcp r.s.236.88(55207) -> a.b.9.234(80), 1
packet
04:39:50 denied tcp r.s.236.88(55636) -> a.b.10.1(80), 1
packet
04:39:53 denied tcp r.s.236.88(55638) -> a.b.10.3(80), 1
packet
04:39:58 denied tcp r.s.236.88(56046) -> a.b.10.57(80), 1
packet
04:40:00 denied tcp r.s.236.88(56390) -> a.b.10.101(80), 1
packet
04:40:03 denied tcp r.s.236.88(56393) -> a.b.10.104(80), 1
packet
04:40:05 denied tcp r.s.236.88(56798) -> a.b.10.151(80), 1
packet
04:40:09 denied tcp r.s.236.88(56798) -> a.b.10.151(80), 1
packet
04:40:11 denied tcp r.s.236.88(57068) -> a.b.10.201(80), 1
packet
04:40:13 denied tcp r.s.236.88(57068) -> a.b.10.201(80), 1
packet
04:40:14 denied tcp r.s.236.88(57242) -> a.b.10.251(80), 1
packet
04:40:17 denied tcp r.s.236.88(57518) -> a.b.11.1(80), 1
packet
04:40:20 denied tcp r.s.236.88(57521) -> a.b.11.4(80), 1
packet
04:40:22 denied tcp r.s.236.88(57872) -> a.b.11.51(80), 1
packet
04:40:25 denied tcp r.s.236.88(57875) -> a.b.11.54(80), 1
packet
04:40:27 denied tcp r.s.236.88(58272) -> a.b.11.101(80), 1
packet
04:40:31 denied tcp r.s.236.88(58272) -> a.b.11.101(80), 1
packet
04:40:33 denied tcp r.s.236.88(58680) -> a.b.11.151(80), 1
packet
04:40:37 denied tcp r.s.236.88(58771) -> a.b.11.200(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:40:41 denied tcp r.s.236.88(59082) -> a.b.11.203(80), 1
packet
04:40:44 denied tcp r.s.236.88(59551) -> a.b.12.2(80), 1
packet
04:40:45 denied tcp r.s.236.88(59571) -> a.b.12.22(80), 1
packet
04:40:47 denied tcp r.s.236.88(59904) -> a.b.12.51(80), 1
packet
04:40:50 denied tcp r.s.236.88(59907) -> a.b.12.54(80), 1
packet
04:40:52 denied tcp r.s.236.88(60304) -> a.b.12.101(80), 1
packet
04:40:56 denied tcp r.s.236.88(60307) -> a.b.12.104(80), 1
packet
04:40:58 denied tcp r.s.236.88(60608) -> a.b.12.151(80), 1
packet
04:41:00 denied tcp r.s.236.88(60608) -> a.b.12.151(80), 1
packet
04:41:01 denied tcp r.s.236.88(60682) -> a.b.12.189(80), 1
packet
04:41:02 denied tcp r.s.236.88(60734) -> a.b.12.193(80), 1
packet
04:41:03 denied tcp r.s.236.88(61042) -> a.b.12.205(80), 1
packet
04:41:07 denied tcp r.s.236.88(61041) -> a.b.12.204(80), 1
packet
04:41:09 denied tcp r.s.236.88(61528) -> a.b.13.1(80), 1
packet
04:41:13 denied tcp r.s.236.88(61528) -> a.b.13.1(80), 1
packet
04:41:15 denied tcp r.s.236.88(61906) -> a.b.13.51(80), 1
packet
04:41:18 denied tcp r.s.236.88(61909) -> a.b.13.54(80), 1
packet
04:41:23 denied tcp r.s.236.88(62287) -> a.b.13.101(80), 1
packet
04:41:24 denied tcp r.s.236.88(62345) -> a.b.13.140(80), 1
packet
04:41:25 denied tcp r.s.236.88(62380) -> a.b.13.144(80), 1
packet
04:41:26 denied tcp r.s.236.88(62719) -> a.b.13.154(80), 1
packet
04:41:30 denied tcp r.s.236.88(62718) -> a.b.13.153(80), 1
packet
04:41:34 denied tcp r.s.236.88(63095) -> a.b.13.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:41:35 denied tcp r.s.236.88(63158) -> a.b.13.246(80), 1
packet
04:41:38 denied tcp r.s.236.88(63561) -> a.b.14.1(80), 1
packet
04:41:41 denied tcp r.s.236.88(63564) -> a.b.14.4(80), 1
packet
04:41:43 denied tcp r.s.236.88(63919) -> a.b.14.51(80), 1
packet
04:41:46 denied tcp r.s.236.88(63922) -> a.b.14.54(80), 1
packet
04:41:48 denied tcp r.s.236.88(64319) -> a.b.14.101(80), 1
packet
04:41:52 denied tcp r.s.236.88(64322) -> a.b.14.104(80), 1
packet
04:41:53 denied tcp r.s.236.88(64709) -> a.b.14.151(80), 1
packet
04:41:57 denied tcp r.s.236.88(64712) -> a.b.14.154(80), 1
packet
04:41:59 denied tcp r.s.236.88(65049) -> a.b.14.201(80), 1
packet
04:42:02 denied tcp r.s.236.88(65052) -> a.b.14.204(80), 1
packet
04:42:04 denied tcp r.s.236.88(65049) -> a.b.14.201(80), 1
packet
04:42:05 denied tcp r.s.236.88(65476) -> a.b.15.1(80), 1
packet
04:42:08 denied tcp r.s.236.88(65476) -> a.b.15.1(80), 1
packet
04:42:09 denied tcp r.s.236.88(32802) -> a.b.15.27(80), 1
packet
04:42:11 denied tcp r.s.236.88(33124) -> a.b.15.51(80), 1
packet
04:42:14 denied tcp r.s.236.88(33146) -> a.b.15.73(80), 1
packet
04:42:15 denied tcp r.s.236.88(33169) -> a.b.15.96(80), 1
packet
04:42:17 denied tcp r.s.236.88(33511) -> a.b.15.101(80), 1
packet
04:42:20 denied tcp r.s.236.88(33571) -> a.b.15.123(80), 1
packet
04:42:22 denied tcp r.s.236.88(33511) -> a.b.15.101(80), 1
packet
04:42:23 denied tcp r.s.236.88(33916) -> a.b.15.151(80), 1
packet
04:42:27 denied tcp r.s.236.88(33918) -> a.b.15.153(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:42:28 denied tcp r.s.236.88(33916) -> a.b.15.151(80), 1
packet
04:42:29 denied tcp r.s.236.88(34331) -> a.b.15.201(80), 1
packet
04:42:33 denied tcp r.s.236.88(34333) -> a.b.15.203(80), 1
packet
04:42:39 denied tcp r.s.236.88(34828) -> a.b.16.3(80), 1
packet
04:42:40 denied tcp r.s.236.88(34826) -> a.b.16.1(80), 1
packet
04:42:41 denied tcp r.s.236.88(35187) -> a.b.16.51(80), 1
packet
04:42:45 denied tcp r.s.236.88(35190) -> a.b.16.54(80), 1
packet
04:42:48 denied tcp r.s.236.88(35718) -> a.b.16.101(80), 1
packet
04:42:51 denied tcp r.s.236.88(35721) -> a.b.16.104(80), 1
packet
04:42:52 denied tcp r.s.236.88(35718) -> a.b.16.101(80), 1
packet
04:42:54 denied tcp r.s.236.88(36094) -> a.b.16.151(80), 1
packet
04:42:57 denied tcp r.s.236.88(36097) -> a.b.16.154(80), 1
packet
04:42:58 denied tcp r.s.236.88(36094) -> a.b.16.151(80), 1
packet
04:43:00 denied tcp r.s.236.88(36485) -> a.b.16.201(80), 1
packet
04:43:03 denied tcp r.s.236.88(36488) -> a.b.16.204(80), 1
packet
04:43:05 denied tcp r.s.236.88(36485) -> a.b.16.201(80), 1
packet
04:43:07 denied tcp r.s.236.88(37051) -> a.b.17.1(80), 1
packet
04:43:10 denied tcp r.s.236.88(37054) -> a.b.17.4(80), 1
packet
04:43:12 denied tcp r.s.236.88(37355) -> a.b.17.51(80), 1
packet
04:43:22 denied tcp r.s.236.88(37834) -> a.b.17.104(80), 1
packet
04:43:28 denied tcp r.s.236.88(38236) -> a.b.17.154(80), 1
packet
04:43:29 denied tcp r.s.236.88(38233) -> a.b.17.151(80), 1
packet
04:43:30 denied tcp r.s.236.88(38664) -> a.b.17.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:43:34 denied tcp r.s.236.88(38666) -> a.b.17.203(80), 1
packet
04:43:37 denied tcp r.s.236.88(39104) -> a.b.18.1(80), 1
packet
04:43:40 denied tcp r.s.236.88(39106) -> a.b.18.3(80), 1
packet
04:43:43 denied tcp r.s.236.88(39508) -> a.b.18.51(80), 1
packet
04:43:46 denied tcp r.s.236.88(39510) -> a.b.18.53(80), 1
packet
04:43:48 denied tcp r.s.236.88(39942) -> a.b.18.101(80), 1
packet
04:43:52 denied tcp r.s.236.88(39945) -> a.b.18.104(80), 1
packet
04:43:54 denied tcp r.s.236.88(40345) -> a.b.18.151(80), 1
packet
04:43:58 denied tcp r.s.236.88(40345) -> a.b.18.151(80), 1
packet
04:44:00 denied tcp r.s.236.88(40807) -> a.b.18.201(80), 1
packet
04:44:02 denied tcp r.s.236.88(40807) -> a.b.18.201(80), 1
packet
04:44:03 denied tcp r.s.236.88(40860) -> a.b.18.254(80), 1
packet
04:44:05 denied tcp r.s.236.88(40858) -> a.b.18.252(80), 1
packet
04:44:06 denied tcp r.s.236.88(41141) -> a.b.19.1(80), 1
packet
04:44:09 denied tcp r.s.236.88(41144) -> a.b.19.4(80), 1
packet
04:44:12 denied tcp r.s.236.88(41519) -> a.b.19.51(80), 1
packet
04:44:14 denied tcp r.s.236.88(41519) -> a.b.19.51(80), 1
packet
04:44:15 denied tcp r.s.236.88(41593) -> a.b.19.85(80), 1
packet
04:44:18 denied tcp r.s.236.88(42102) -> a.b.19.135(80), 1
packet
04:44:20 denied tcp r.s.236.88(41941) -> a.b.19.101(80), 1
packet
04:44:21 denied tcp r.s.236.88(42015) -> a.b.19.115(80), 1
packet
04:44:24 denied tcp r.s.236.88(42443) -> a.b.19.151(80), 1
packet
04:44:30 denied tcp r.s.236.88(42827) -> a.b.19.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:44:32 denied tcp r.s.236.88(42827) -> a.b.19.201(80), 1
packet
04:44:33 denied tcp r.s.236.88(42934) -> a.b.19.246(80), 1
packet
04:44:36 denied tcp r.s.236.88(43301) -> a.b.20.1(80), 1
packet
04:44:39 denied tcp r.s.236.88(43304) -> a.b.20.4(80), 1
packet
04:44:42 denied tcp r.s.236.88(43638) -> a.b.20.51(80), 1
packet
04:44:45 denied tcp r.s.236.88(43701) -> a.b.20.78(80), 1
packet
04:44:48 denied tcp r.s.236.88(44027) -> a.b.20.101(80), 1
packet
04:44:50 denied tcp r.s.236.88(44027) -> a.b.20.101(80), 1
packet
04:44:51 denied tcp r.s.236.88(44189) -> a.b.20.146(80), 1
packet
04:44:54 denied tcp r.s.236.88(44527) -> a.b.20.173(80), 1
packet
04:44:56 denied tcp r.s.236.88(44459) -> a.b.20.151(80), 1
packet
04:44:58 denied tcp r.s.236.88(44594) -> a.b.20.197(80), 1
packet
04:45:00 denied tcp r.s.236.88(44867) -> a.b.20.201(80), 1
packet
04:45:03 denied tcp r.s.236.88(44870) -> a.b.20.204(80), 1
packet
04:45:06 denied tcp r.s.236.88(45333) -> a.b.21.1(80), 1
packet
04:45:09 denied tcp r.s.236.88(45336) -> a.b.21.4(80), 1
packet
04:45:12 denied tcp r.s.236.88(45756) -> a.b.21.51(80), 1
packet
04:45:14 denied tcp r.s.236.88(45756) -> a.b.21.51(80), 1
packet
04:45:15 denied tcp r.s.236.88(45798) -> a.b.21.73(80), 1
packet
04:45:17 denied tcp r.s.236.88(46137) -> a.b.21.101(80), 1
packet
04:45:20 denied tcp r.s.236.88(46140) -> a.b.21.104(80), 1
packet
04:45:23 denied tcp r.s.236.88(46415) -> a.b.21.151(80), 1
packet
04:45:24 denied tcp r.s.236.88(46415) -> a.b.21.151(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:45:26 denied tcp r.s.236.88(46603) -> a.b.21.184(80), 1
packet
04:45:29 denied tcp r.s.236.88(47000) -> a.b.21.251(80), 1
packet
04:45:32 denied tcp r.s.236.88(47002) -> a.b.21.253(80), 1
packet
04:45:35 denied tcp r.s.236.88(47391) -> a.b.22.1(80), 1
packet
04:45:38 denied tcp r.s.236.88(47394) -> a.b.22.4(80), 1
packet
04:45:41 denied tcp r.s.236.88(47691) -> a.b.22.51(80), 1
packet
04:45:43 denied tcp r.s.236.88(47691) -> a.b.22.51(80), 1
packet
04:45:44 denied tcp r.s.236.88(47712) -> a.b.22.72(80), 1
packet
04:45:45 denied tcp r.s.236.88(47712) -> a.b.22.72(80), 1
packet
04:45:47 denied tcp r.s.236.88(48145) -> a.b.22.101(80), 1
packet
04:45:49 denied tcp r.s.236.88(48145) -> a.b.22.101(80), 1
packet
04:45:50 denied tcp r.s.236.88(48238) -> a.b.22.126(80), 1
packet
04:45:51 denied tcp r.s.236.88(48163) -> a.b.22.119(80), 1
packet
04:45:56 denied tcp r.s.236.88(48551) -> a.b.22.153(80), 1
packet
04:45:56 denied tcp r.s.236.88(48562) -> a.b.22.164(80), 1
packet
04:46:02 denied tcp r.s.236.88(48983) -> a.b.22.227(80), 1
packet
04:46:05 denied tcp r.s.236.88(49505) -> a.b.23.1(80), 1
packet
04:46:08 denied tcp r.s.236.88(49508) -> a.b.23.4(80), 1
packet
04:46:09 denied tcp r.s.236.88(49850) -> a.b.23.54(80), 1
packet
04:46:14 denied tcp r.s.236.88(49850) -> a.b.23.54(80), 1
packet
04:46:20 denied tcp r.s.236.88(50376) -> a.b.23.128(80), 1
packet
04:46:22 denied tcp r.s.236.88(50742) -> a.b.23.173(80), 1
packet
04:46:24 denied tcp r.s.236.88(50680) -> a.b.23.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:46:25 denied tcp r.s.236.88(50701) -> a.b.23.172(80), 1
packet
04:46:26 denied tcp r.s.236.88(50701) -> a.b.23.172(80), 1
packet
04:46:28 denied tcp r.s.236.88(51084) -> a.b.23.201(80), 1
packet
04:46:32 denied tcp r.s.236.88(51084) -> a.b.23.201(80), 1
packet
04:46:34 denied tcp r.s.236.88(51581) -> a.b.24.1(80), 1
packet
04:46:36 denied tcp r.s.236.88(51581) -> a.b.24.1(80), 1
packet
04:46:38 denied tcp r.s.236.88(51644) -> a.b.24.22(80), 1
packet
04:46:39 denied tcp r.s.236.88(51641) -> a.b.24.19(80), 1
packet
04:46:40 denied tcp r.s.236.88(52000) -> a.b.24.51(80), 1
packet
04:46:43 denied tcp r.s.236.88(52053) -> a.b.24.77(80), 1
packet
04:46:46 denied tcp r.s.236.88(52387) -> a.b.24.101(80), 1
packet
04:46:48 denied tcp r.s.236.88(52387) -> a.b.24.101(80), 1
packet
04:46:49 denied tcp r.s.236.88(52468) -> a.b.24.140(80), 1
packet
04:46:51 denied tcp r.s.236.88(52795) -> a.b.24.151(80), 1
packet
04:46:54 denied tcp r.s.236.88(52798) -> a.b.24.154(80), 1
packet
04:46:56 denied tcp r.s.236.88(53195) -> a.b.24.201(80), 1
packet
04:47:00 denied tcp r.s.236.88(53198) -> a.b.24.204(80), 1
packet
04:47:02 denied tcp r.s.236.88(53611) -> a.b.25.1(80), 1
packet
04:47:05 denied tcp r.s.236.88(53644) -> a.b.25.34(80), 1
packet
04:47:07 denied tcp r.s.236.88(53969) -> a.b.25.51(80), 1
packet
04:47:10 denied tcp r.s.236.88(53969) -> a.b.25.51(80), 1
packet
04:47:11 denied tcp r.s.236.88(54062) -> a.b.25.98(80), 1
packet
04:47:13 denied tcp r.s.236.88(54369) -> a.b.25.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:47:16 denied tcp r.s.236.88(54372) -> a.b.25.104(80), 1
packet
04:47:18 denied tcp r.s.236.88(54777) -> a.b.25.151(80), 1
packet
04:47:21 denied tcp r.s.236.88(54778) -> a.b.25.152(80), 1
packet
04:47:24 denied tcp r.s.236.88(55202) -> a.b.25.201(80), 1
packet
04:47:26 denied tcp r.s.236.88(55268) -> a.b.25.245(80), 1
packet
04:47:30 denied tcp r.s.236.88(55643) -> a.b.26.1(80), 1
packet
04:47:34 denied tcp r.s.236.88(55646) -> a.b.26.4(80), 1
packet
04:47:39 denied tcp r.s.236.88(56011) -> a.b.26.53(80), 1
packet
04:47:42 denied tcp r.s.236.88(56366) -> a.b.26.101(80), 1
packet
04:47:44 denied tcp r.s.236.88(56366) -> a.b.26.101(80), 1
packet
04:47:45 denied tcp r.s.236.88(56483) -> a.b.26.127(80), 1
packet
04:47:48 denied tcp r.s.236.88(56683) -> a.b.26.151(80), 1
packet
04:47:51 denied tcp r.s.236.88(56686) -> a.b.26.154(80), 1
packet
04:47:52 denied tcp r.s.236.88(56683) -> a.b.26.151(80), 1
packet
04:47:54 denied tcp r.s.236.88(57110) -> a.b.26.201(80), 1
packet
04:47:58 denied tcp r.s.236.88(57113) -> a.b.26.204(80), 1
packet
04:47:59 denied tcp r.s.236.88(57110) -> a.b.26.201(80), 1
packet
04:48:01 denied tcp r.s.236.88(57638) -> a.b.27.1(80), 1
packet
04:48:04 denied tcp r.s.236.88(57641) -> a.b.27.4(80), 1
packet
04:48:07 denied tcp r.s.236.88(57966) -> a.b.27.51(80), 1
packet
04:48:10 denied tcp r.s.236.88(57969) -> a.b.27.54(80), 1
packet
04:48:12 denied tcp r.s.236.88(58387) -> a.b.27.101(80), 1
packet
04:48:15 denied tcp r.s.236.88(58387) -> a.b.27.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:48:16 denied tcp r.s.236.88(58582) -> a.b.27.150(80), 1
packet
04:48:18 denied tcp r.s.236.88(58814) -> a.b.27.151(80), 1
packet
04:48:22 denied tcp r.s.236.88(58971) -> a.b.27.199(80), 1
packet
04:48:24 denied tcp r.s.236.88(59212) -> a.b.27.201(80), 1
packet
04:48:27 denied tcp r.s.236.88(59214) -> a.b.27.203(80), 1
packet
04:48:28 denied tcp r.s.236.88(59212) -> a.b.27.201(80), 1
packet
04:48:30 denied tcp r.s.236.88(59707) -> a.b.28.1(80), 1
packet
04:48:34 denied tcp r.s.236.88(59710) -> a.b.28.4(80), 1
packet
04:48:36 denied tcp r.s.236.88(60011) -> a.b.28.51(80), 1
packet
04:48:40 denied tcp r.s.236.88(60011) -> a.b.28.51(80), 1
packet
04:48:41 denied tcp r.s.236.88(60415) -> a.b.28.101(80), 1
packet
04:48:44 denied tcp r.s.236.88(60415) -> a.b.28.101(80), 1
packet
04:48:45 denied tcp r.s.236.88(60442) -> a.b.28.128(80), 1
packet
04:48:47 denied tcp r.s.236.88(60823) -> a.b.28.151(80), 1
packet
04:48:51 denied tcp r.s.236.88(60823) -> a.b.28.151(80), 1
packet
04:48:52 denied tcp r.s.236.88(61225) -> a.b.28.201(80), 1
packet
04:48:56 denied tcp r.s.236.88(61225) -> a.b.28.201(80), 1
packet
04:48:58 denied tcp r.s.236.88(61633) -> a.b.29.1(80), 1
packet
04:49:02 denied tcp r.s.236.88(61682) -> a.b.29.50(80), 1
packet
04:49:06 denied tcp r.s.236.88(62048) -> a.b.29.54(80), 1
packet
04:49:08 denied tcp r.s.236.88(62366) -> a.b.29.101(80), 1
packet
04:49:12 denied tcp r.s.236.88(62368) -> a.b.29.103(80), 1
packet
04:49:14 denied tcp r.s.236.88(62786) -> a.b.29.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:49:18 denied tcp r.s.236.88(62789) -> a.b.29.154(80), 1
packet
04:49:20 denied tcp r.s.236.88(63148) -> a.b.29.201(80), 1
packet
04:49:23 denied tcp r.s.236.88(63151) -> a.b.29.204(80), 1
packet
04:49:23 denied tcp r.s.236.88(63226) -> a.b.29.230(80), 1
packet
04:49:26 denied tcp r.s.236.88(63605) -> a.b.30.1(80), 1
packet
04:49:30 denied tcp r.s.236.88(63608) -> a.b.30.4(80), 1
packet
04:49:35 denied tcp r.s.236.88(63972) -> a.b.30.54(80), 1
packet
04:49:36 denied tcp r.s.236.88(63988) -> a.b.30.70(80), 1
packet
04:49:38 denied tcp r.s.236.88(64352) -> a.b.30.101(80), 1
packet
04:49:41 denied tcp r.s.236.88(64354) -> a.b.30.103(80), 1
packet
04:49:44 denied tcp r.s.236.88(64735) -> a.b.30.151(80), 1
packet
04:49:46 denied tcp r.s.236.88(64735) -> a.b.30.151(80), 1
packet
04:49:47 denied tcp r.s.236.88(64835) -> a.b.30.174(80), 1
packet
04:49:50 denied tcp r.s.236.88(65139) -> a.b.30.201(80), 1
packet
04:49:56 denied tcp r.s.236.88(32905) -> a.b.31.1(80), 1
packet
04:50:00 denied tcp r.s.236.88(32908) -> a.b.31.4(80), 1
packet
04:50:01 denied tcp r.s.236.88(32905) -> a.b.31.1(80), 1
packet
04:50:02 denied tcp r.s.236.88(33379) -> a.b.31.51(80), 1
packet
04:50:06 denied tcp r.s.236.88(33381) -> a.b.31.53(80), 1
packet
04:50:07 denied tcp r.s.236.88(33379) -> a.b.31.51(80), 1
packet
04:50:09 denied tcp r.s.236.88(33750) -> a.b.31.101(80), 1
packet
04:50:12 denied tcp r.s.236.88(33752) -> a.b.31.103(80), 1
packet
04:50:13 denied tcp r.s.236.88(33840) -> a.b.31.146(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:50:15 denied tcp r.s.236.88(34154) -> a.b.31.151(80), 1
packet
04:50:17 denied tcp r.s.236.88(34154) -> a.b.31.151(80), 1
packet
04:50:19 denied tcp r.s.236.88(34260) -> a.b.31.174(80), 1
packet
04:50:21 denied tcp r.s.236.88(34546) -> a.b.31.201(80), 1
packet
04:50:24 denied tcp r.s.236.88(34549) -> a.b.31.204(80), 1
packet
04:50:26 denied tcp r.s.236.88(34546) -> a.b.31.201(80), 1
packet
04:50:27 denied tcp r.s.236.88(35013) -> a.b.32.1(80), 1
packet
04:50:30 denied tcp r.s.236.88(35013) -> a.b.32.1(80), 1
packet
04:50:31 denied tcp r.s.236.88(35152) -> a.b.32.41(80), 1
packet
04:50:32 denied tcp r.s.236.88(35222) -> a.b.32.46(80), 1
packet
04:50:33 denied tcp r.s.236.88(35327) -> a.b.32.51(80), 1
packet
04:50:36 denied tcp r.s.236.88(35327) -> a.b.32.51(80), 1
packet
04:50:36 denied tcp r.s.236.88(35433) -> a.b.32.95(80), 1
packet
04:50:38 denied tcp r.s.236.88(35411) -> a.b.32.73(80), 1
packet
04:50:40 denied tcp r.s.236.88(35739) -> a.b.32.101(80), 1
packet
04:50:43 denied tcp r.s.236.88(35742) -> a.b.32.104(80), 1
packet
04:50:45 denied tcp r.s.236.88(36143) -> a.b.32.151(80), 1
packet
04:50:49 denied tcp r.s.236.88(36146) -> a.b.32.154(80), 1
packet
04:50:51 denied tcp r.s.236.88(36543) -> a.b.32.201(80), 1
packet
04:50:53 denied tcp r.s.236.88(36543) -> a.b.32.201(80), 1
packet
04:50:54 denied tcp r.s.236.88(36569) -> a.b.32.227(80), 1
packet
04:50:56 denied tcp r.s.236.88(36947) -> a.b.33.1(80), 1
packet
04:50:59 denied tcp r.s.236.88(36947) -> a.b.33.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:51:00 denied tcp r.s.236.88(37005) -> a.b.33.28(80), 1
packet
04:51:00 denied tcp r.s.236.88(37005) -> a.b.33.28(80), 1
packet
04:51:03 denied tcp r.s.236.88(37380) -> a.b.33.51(80), 1
packet
04:51:06 denied tcp r.s.236.88(37383) -> a.b.33.54(80), 1
packet
04:51:09 denied tcp r.s.236.88(37942) -> a.b.33.133(80), 1
packet
04:51:11 denied tcp r.s.236.88(37783) -> a.b.33.101(80), 1
packet
04:51:12 denied tcp r.s.236.88(37942) -> a.b.33.133(80), 1
packet
04:51:15 denied tcp r.s.236.88(38195) -> a.b.33.151(80), 1
packet
04:51:17 denied tcp r.s.236.88(38195) -> a.b.33.151(80), 1
packet
04:51:18 denied tcp r.s.236.88(38315) -> a.b.33.177(80), 1
packet
04:51:21 denied tcp r.s.236.88(38596) -> a.b.33.201(80), 1
packet
04:51:23 denied tcp r.s.236.88(38596) -> a.b.33.201(80), 1
packet
04:51:25 denied tcp r.s.236.88(38721) -> a.b.33.228(80), 1
packet
04:51:26 denied tcp r.s.236.88(38810) -> a.b.33.252(80), 1
packet
04:51:27 denied tcp r.s.236.88(39093) -> a.b.34.1(80), 1
packet
04:51:31 denied tcp r.s.236.88(39095) -> a.b.34.3(80), 1
packet
04:51:33 denied tcp r.s.236.88(39500) -> a.b.34.51(80), 1
packet
04:51:37 denied tcp r.s.236.88(39503) -> a.b.34.54(80), 1
packet
04:51:38 denied tcp r.s.236.88(39500) -> a.b.34.51(80), 1
packet
04:51:39 denied tcp r.s.236.88(39858) -> a.b.34.101(80), 1
packet
04:51:43 denied tcp r.s.236.88(39860) -> a.b.34.103(80), 1
packet
04:51:48 denied tcp r.s.236.88(40289) -> a.b.34.154(80), 1
packet
04:51:53 denied tcp r.s.236.88(40649) -> a.b.34.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:51:54 denied tcp r.s.236.88(40670) -> a.b.34.222(80), 1
packet
04:51:56 denied tcp r.s.236.88(41168) -> a.b.35.1(80), 1
packet
04:52:00 denied tcp r.s.236.88(41171) -> a.b.35.4(80), 1
packet
04:52:01 denied tcp r.s.236.88(41168) -> a.b.35.1(80), 1
packet
04:52:03 denied tcp r.s.236.88(41496) -> a.b.35.51(80), 1
packet
04:52:06 denied tcp r.s.236.88(41499) -> a.b.35.54(80), 1
packet
04:52:09 denied tcp r.s.236.88(41862) -> a.b.35.101(80), 1
packet
04:52:13 denied tcp r.s.236.88(41862) -> a.b.35.101(80), 1
packet
04:52:14 denied tcp r.s.236.88(42240) -> a.b.35.151(80), 1
packet
04:52:18 denied tcp r.s.236.88(42243) -> a.b.35.154(80), 1
packet
04:52:20 denied tcp r.s.236.88(42640) -> a.b.35.201(80), 1
packet
04:52:23 denied tcp r.s.236.88(42643) -> a.b.35.204(80), 1
packet
04:52:25 denied tcp r.s.236.88(43044) -> a.b.36.1(80), 1
packet
04:52:29 denied tcp r.s.236.88(43047) -> a.b.36.4(80), 1
packet
04:52:31 denied tcp r.s.236.88(43456) -> a.b.36.51(80), 1
packet
04:52:33 denied tcp r.s.236.88(43456) -> a.b.36.51(80), 1
packet
04:52:35 denied tcp r.s.236.88(43759) -> a.b.36.101(80), 1
packet
04:52:37 denied tcp r.s.236.88(43759) -> a.b.36.101(80), 1
packet
04:52:38 denied tcp r.s.236.88(43778) -> a.b.36.120(80), 1
packet
04:52:38 denied tcp r.s.236.88(43853) -> a.b.36.125(80), 1
packet
04:52:41 denied tcp r.s.236.88(44121) -> a.b.36.151(80), 1
packet
04:52:43 denied tcp r.s.236.88(44121) -> a.b.36.151(80), 1
packet
04:52:44 denied tcp r.s.236.88(44196) -> a.b.36.159(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:52:47 denied tcp r.s.236.88(44601) -> a.b.36.201(80), 1
packet
04:52:50 denied tcp r.s.236.88(44604) -> a.b.36.204(80), 1
packet
04:52:56 denied tcp r.s.236.88(45047) -> a.b.37.4(80), 1
packet
04:52:58 denied tcp r.s.236.88(45352) -> a.b.37.51(80), 1
packet
04:53:01 denied tcp r.s.236.88(45352) -> a.b.37.51(80), 1
packet
04:53:02 denied tcp r.s.236.88(45470) -> a.b.37.96(80), 1
packet
04:53:03 denied tcp r.s.236.88(45470) -> a.b.37.96(80), 1
packet
04:53:07 denied tcp r.s.236.88(45746) -> a.b.37.101(80), 1
packet
04:53:08 denied tcp r.s.236.88(45834) -> a.b.37.133(80), 1
packet
04:53:10 denied tcp r.s.236.88(46154) -> a.b.37.151(80), 1
packet
04:53:13 denied tcp r.s.236.88(46157) -> a.b.37.154(80), 1
packet
04:53:18 denied tcp r.s.236.88(46554) -> a.b.37.201(80), 1
packet
04:53:19 denied tcp r.s.236.88(46587) -> a.b.37.234(80), 1
packet
04:53:21 denied tcp r.s.236.88(46958) -> a.b.38.1(80), 1
packet
04:53:24 denied tcp r.s.236.88(46958) -> a.b.38.1(80), 1
packet
04:53:25 denied tcp r.s.236.88(47034) -> a.b.38.39(80), 1
packet
04:53:27 denied tcp r.s.236.88(47405) -> a.b.38.51(80), 1
packet
04:53:30 denied tcp r.s.236.88(47405) -> a.b.38.51(80), 1
packet
04:53:31 denied tcp r.s.236.88(47486) -> a.b.38.78(80), 1
packet
04:53:33 denied tcp r.s.236.88(47778) -> a.b.38.101(80), 1
packet
04:53:36 denied tcp r.s.236.88(47778) -> a.b.38.101(80), 1
packet
04:53:37 denied tcp r.s.236.88(47909) -> a.b.38.137(80), 1
packet
04:53:40 denied tcp r.s.236.88(48201) -> a.b.38.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:53:42 denied tcp r.s.236.88(48201) -> a.b.38.151(80), 1
packet
04:53:44 denied tcp r.s.236.88(48247) -> a.b.38.165(80), 1
packet
04:53:46 denied tcp r.s.236.88(48586) -> a.b.38.201(80), 1
packet
04:53:48 denied tcp r.s.236.88(48586) -> a.b.38.201(80), 1
packet
04:53:49 denied tcp r.s.236.88(48643) -> a.b.38.228(80), 1
packet
04:53:52 denied tcp r.s.236.88(49010) -> a.b.39.1(80), 1
packet
04:53:55 denied tcp r.s.236.88(49013) -> a.b.39.4(80), 1
packet
04:53:56 denied tcp r.s.236.88(49010) -> a.b.39.1(80), 1
packet
04:53:58 denied tcp r.s.236.88(49414) -> a.b.39.51(80), 1
packet
04:54:01 denied tcp r.s.236.88(49414) -> a.b.39.51(80), 1
packet
04:54:02 denied tcp r.s.236.88(49511) -> a.b.39.78(80), 1
packet
04:54:04 denied tcp r.s.236.88(49810) -> a.b.39.101(80), 1
packet
04:54:07 denied tcp r.s.236.88(49810) -> a.b.39.101(80), 1
packet
04:54:08 denied tcp r.s.236.88(49835) -> a.b.39.126(80), 1
packet
04:54:11 denied tcp r.s.236.88(50394) -> a.b.39.193(80), 1
packet
04:54:13 denied tcp r.s.236.88(50253) -> a.b.39.151(80), 1
packet
04:54:14 denied tcp r.s.236.88(50341) -> a.b.39.186(80), 1
packet
04:54:15 denied tcp r.s.236.88(50271) -> a.b.39.169(80), 1
packet
04:54:16 denied tcp r.s.236.88(50641) -> a.b.39.201(80), 1
packet
04:54:19 denied tcp r.s.236.88(50663) -> a.b.39.223(80), 1
packet
04:54:20 denied tcp r.s.236.88(50816) -> a.b.39.249(80), 1
packet
04:54:23 denied tcp r.s.236.88(51199) -> a.b.40.30(80), 1
packet
04:54:25 denied tcp r.s.236.88(51118) -> a.b.40.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:54:26 denied tcp r.s.236.88(51140) -> a.b.40.23(80), 1
packet
04:54:26 denied tcp r.s.236.88(51140) -> a.b.40.23(80), 1
packet
04:54:29 denied tcp r.s.236.88(51523) -> a.b.40.51(80), 1
packet
04:54:31 denied tcp r.s.236.88(51523) -> a.b.40.51(80), 1
packet
04:54:32 denied tcp r.s.236.88(51545) -> a.b.40.73(80), 1
packet
04:54:35 denied tcp r.s.236.88(51892) -> a.b.40.101(80), 1
packet
04:54:38 denied tcp r.s.236.88(51895) -> a.b.40.104(80), 1
packet
04:54:40 denied tcp r.s.236.88(52350) -> a.b.40.151(80), 1
packet
04:54:42 denied tcp r.s.236.88(52350) -> a.b.40.151(80), 1
packet
04:54:43 denied tcp r.s.236.88(52368) -> a.b.40.169(80), 1
packet
04:54:45 denied tcp r.s.236.88(52750) -> a.b.40.201(80), 1
packet
04:54:49 denied tcp r.s.236.88(52753) -> a.b.40.204(80), 1
packet
04:54:51 denied tcp r.s.236.88(53154) -> a.b.41.1(80), 1
packet
04:54:54 denied tcp r.s.236.88(53157) -> a.b.41.4(80), 1
packet
04:54:56 denied tcp r.s.236.88(53566) -> a.b.41.51(80), 1
packet
04:54:59 denied tcp r.s.236.88(53568) -> a.b.41.53(80), 1
packet
04:55:02 denied tcp r.s.236.88(53974) -> a.b.41.101(80), 1
packet
04:55:05 denied tcp r.s.236.88(54001) -> a.b.41.128(80), 1
packet
04:55:07 denied tcp r.s.236.88(54382) -> a.b.41.151(80), 1
packet
04:55:10 denied tcp r.s.236.88(54385) -> a.b.41.154(80), 1
packet
04:55:16 denied tcp r.s.236.88(54785) -> a.b.41.204(80), 1
packet
04:55:18 denied tcp r.s.236.88(55186) -> a.b.42.1(80), 1
packet
04:55:21 denied tcp r.s.236.88(55189) -> a.b.42.4(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:55:23 denied tcp r.s.236.88(55598) -> a.b.42.51(80), 1
packet
04:55:26 denied tcp r.s.236.88(55601) -> a.b.42.54(80), 1
packet
04:55:28 denied tcp r.s.236.88(56006) -> a.b.42.101(80), 1
packet
04:55:32 denied tcp r.s.236.88(56009) -> a.b.42.104(80), 1
packet
04:55:34 denied tcp r.s.236.88(56414) -> a.b.42.151(80), 1
packet
04:55:37 denied tcp r.s.236.88(56417) -> a.b.42.154(80), 1
packet
04:55:39 denied tcp r.s.236.88(56608) -> a.b.42.201(80), 1
packet
04:55:43 denied tcp r.s.236.88(56608) -> a.b.42.201(80), 1
packet
04:55:45 denied tcp r.s.236.88(57187) -> a.b.43.1(80), 1
packet
04:55:49 denied tcp r.s.236.88(57189) -> a.b.43.3(80), 1
packet
04:55:51 denied tcp r.s.236.88(57434) -> a.b.43.51(80), 1
packet
04:55:55 denied tcp r.s.236.88(57437) -> a.b.43.54(80), 1
packet
04:55:56 denied tcp r.s.236.88(57434) -> a.b.43.51(80), 1
packet
04:55:57 denied tcp r.s.236.88(57888) -> a.b.43.101(80), 1
packet
04:56:03 denied tcp r.s.236.88(58246) -> a.b.43.151(80), 1
packet
04:56:06 denied tcp r.s.236.88(58249) -> a.b.43.154(80), 1
packet
04:56:11 denied tcp r.s.236.88(58619) -> a.b.43.203(80), 1
packet
04:56:14 denied tcp r.s.236.88(59071) -> a.b.44.1(80), 1
packet
04:56:20 denied tcp r.s.236.88(59534) -> a.b.44.51(80), 1
packet
04:56:23 denied tcp r.s.236.88(59537) -> a.b.44.54(80), 1
packet
04:56:24 denied tcp r.s.236.88(59534) -> a.b.44.51(80), 1
packet
04:56:26 denied tcp r.s.236.88(59866) -> a.b.44.101(80), 1
packet
04:56:30 denied tcp r.s.236.88(59869) -> a.b.44.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:56:31 denied tcp r.s.236.88(60278) -> a.b.44.151(80), 1
packet
04:56:35 denied tcp r.s.236.88(60281) -> a.b.44.154(80), 1
packet
04:56:36 denied tcp r.s.236.88(60678) -> a.b.44.201(80), 1
packet
04:56:40 denied tcp r.s.236.88(60681) -> a.b.44.204(80), 1
packet
04:56:42 denied tcp r.s.236.88(61102) -> a.b.45.1(80), 1
packet
04:56:45 denied tcp r.s.236.88(61105) -> a.b.45.4(80), 1
packet
04:56:45 denied tcp r.s.236.88(61170) -> a.b.45.42(80), 1
packet
04:56:48 denied tcp r.s.236.88(61502) -> a.b.45.51(80), 1
packet
04:56:51 denied tcp r.s.236.88(61505) -> a.b.45.54(80), 1
packet
04:56:52 denied tcp r.s.236.88(61502) -> a.b.45.51(80), 1
packet
04:56:54 denied tcp r.s.236.88(61898) -> a.b.45.101(80), 1
packet
04:56:57 denied tcp r.s.236.88(61901) -> a.b.45.104(80), 1
packet
04:56:58 denied tcp r.s.236.88(61898) -> a.b.45.101(80), 1
packet
04:57:00 denied tcp r.s.236.88(62310) -> a.b.45.151(80), 1
packet
04:57:02 denied tcp r.s.236.88(62310) -> a.b.45.151(80), 1
packet
04:57:04 denied tcp r.s.236.88(62429) -> a.b.45.178(80), 1
packet
04:57:05 denied tcp r.s.236.88(62710) -> a.b.45.201(80), 1
packet
04:57:09 denied tcp r.s.236.88(62712) -> a.b.45.203(80), 1
packet
04:57:12 denied tcp r.s.236.88(63270) -> a.b.46.22(80), 1
packet
04:57:15 denied tcp r.s.236.88(63223) -> a.b.46.2(80), 1
packet
04:57:17 denied tcp r.s.236.88(63535) -> a.b.46.51(80), 1
packet
04:57:21 denied tcp r.s.236.88(63537) -> a.b.46.53(80), 1
packet
04:57:22 denied tcp r.s.236.88(63535) -> a.b.46.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:57:23 denied tcp r.s.236.88(63930) -> a.b.46.101(80), 1
packet
04:57:26 denied tcp r.s.236.88(63933) -> a.b.46.104(80), 1
packet
04:57:26 denied tcp r.s.236.88(64028) -> a.b.46.149(80), 1
packet
04:57:28 denied tcp r.s.236.88(64342) -> a.b.46.151(80), 1
packet
04:57:32 denied tcp r.s.236.88(64342) -> a.b.46.151(80), 1
packet
04:57:34 denied tcp r.s.236.88(64763) -> a.b.46.201(80), 1
packet
04:57:37 denied tcp r.s.236.88(64765) -> a.b.46.203(80), 1
packet
04:57:40 denied tcp r.s.236.88(65166) -> a.b.47.1(80), 1
packet
04:57:42 denied tcp r.s.236.88(65166) -> a.b.47.1(80), 1
packet
04:57:43 denied tcp r.s.236.88(65221) -> a.b.47.28(80), 1
packet
04:57:45 denied tcp r.s.236.88(32807) -> a.b.47.51(80), 1
packet
04:57:48 denied tcp r.s.236.88(32809) -> a.b.47.53(80), 1
packet
04:57:51 denied tcp r.s.236.88(33202) -> a.b.47.101(80), 1
packet
04:57:54 denied tcp r.s.236.88(33205) -> a.b.47.104(80), 1
packet
04:57:56 denied tcp r.s.236.88(33614) -> a.b.47.151(80), 1
packet
04:57:58 denied tcp r.s.236.88(33614) -> a.b.47.151(80), 1
packet
04:57:59 denied tcp r.s.236.88(33651) -> a.b.47.188(80), 1
packet
04:58:01 denied tcp r.s.236.88(34014) -> a.b.47.201(80), 1
packet
04:58:05 denied tcp r.s.236.88(34014) -> a.b.47.201(80), 1
packet
04:58:06 denied tcp r.s.236.88(34014) -> a.b.47.201(80), 1
packet
04:58:08 denied tcp r.s.236.88(34468) -> a.b.48.1(80), 1
packet
04:58:11 denied tcp r.s.236.88(34471) -> a.b.48.4(80), 1
packet
04:58:13 denied tcp r.s.236.88(34872) -> a.b.48.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:58:16 denied tcp r.s.236.88(34874) -> a.b.48.53(80), 1
packet
04:58:18 denied tcp r.s.236.88(35234) -> a.b.48.101(80), 1
packet
04:58:21 denied tcp r.s.236.88(35237) -> a.b.48.104(80), 1
packet
04:58:24 denied tcp r.s.236.88(35646) -> a.b.48.151(80), 1
packet
04:58:27 denied tcp r.s.236.88(35649) -> a.b.48.154(80), 1
packet
04:58:29 denied tcp r.s.236.88(36036) -> a.b.48.201(80), 1
packet
04:58:33 denied tcp r.s.236.88(36039) -> a.b.48.204(80), 1
packet
04:58:34 denied tcp r.s.236.88(36146) -> a.b.48.251(80), 1
packet
04:58:35 denied tcp r.s.236.88(36441) -> a.b.49.1(80), 1
packet
04:58:39 denied tcp r.s.236.88(36444) -> a.b.49.4(80), 1
packet
04:58:41 denied tcp r.s.236.88(36852) -> a.b.49.51(80), 1
packet
04:58:46 denied tcp r.s.236.88(36852) -> a.b.49.51(80), 1
packet
04:58:51 denied tcp r.s.236.88(37240) -> a.b.49.104(80), 1
packet
04:58:53 denied tcp r.s.236.88(37624) -> a.b.49.151(80), 1
packet
04:58:57 denied tcp r.s.236.88(37627) -> a.b.49.154(80), 1
packet
04:58:59 denied tcp r.s.236.88(38024) -> a.b.49.223(80), 1
packet
04:59:05 denied tcp r.s.236.88(38436) -> a.b.50.1(80), 1
packet
04:59:08 denied tcp r.s.236.88(38436) -> a.b.50.1(80), 1
packet
04:59:09 denied tcp r.s.236.88(38631) -> a.b.50.50(80), 1
packet
04:59:10 denied tcp r.s.236.88(38631) -> a.b.50.50(80), 1
packet
04:59:11 denied tcp r.s.236.88(38803) -> a.b.50.51(80), 1
packet
04:59:14 denied tcp r.s.236.88(38803) -> a.b.50.51(80), 1
packet
04:59:15 denied tcp r.s.236.88(38949) -> a.b.50.91(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
04:59:16 denied tcp r.s.236.88(39025) -> a.b.50.93(80), 1
packet
04:59:17 denied tcp r.s.236.88(39255) -> a.b.50.101(80), 1
packet
04:59:21 denied tcp r.s.236.88(39258) -> a.b.50.104(80), 1
packet
04:59:23 denied tcp r.s.236.88(39622) -> a.b.50.151(80), 1
packet
04:59:27 denied tcp r.s.236.88(39625) -> a.b.50.154(80), 1
packet
04:59:28 denied tcp r.s.236.88(39622) -> a.b.50.151(80), 1
packet
04:59:30 denied tcp r.s.236.88(40093) -> a.b.50.201(80), 1
packet
04:59:32 denied tcp r.s.236.88(40093) -> a.b.50.201(80), 1
packet
04:59:33 denied tcp r.s.236.88(40202) -> a.b.50.237(80), 1
packet
04:59:36 denied tcp r.s.236.88(40505) -> a.b.51.1(80), 1
packet
04:59:40 denied tcp r.s.236.88(40713) -> a.b.51.50(80), 1
packet
04:59:42 denied tcp r.s.236.88(40918) -> a.b.51.51(80), 1
packet
04:59:44 denied tcp r.s.236.88(40918) -> a.b.51.51(80), 1
packet
04:59:45 denied tcp r.s.236.88(40939) -> a.b.51.72(80), 1
packet
04:59:48 denied tcp r.s.236.88(41356) -> a.b.51.101(80), 1
packet
04:59:51 denied tcp r.s.236.88(41359) -> a.b.51.104(80), 1
packet
04:59:53 denied tcp r.s.236.88(41738) -> a.b.51.151(80), 1
packet
04:59:57 denied tcp r.s.236.88(41741) -> a.b.51.154(80), 1
packet
04:59:59 denied tcp r.s.236.88(42142) -> a.b.51.201(80), 1
packet
05:00:01 denied tcp r.s.236.88(42142) -> a.b.51.201(80), 1
packet
05:00:02 denied tcp r.s.236.88(42151) -> a.b.51.210(80), 1
packet
05:00:05 denied tcp r.s.236.88(42621) -> a.b.52.1(80), 1
packet
05:00:08 denied tcp r.s.236.88(42623) -> a.b.52.3(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:00:10 denied tcp r.s.236.88(42976) -> a.b.52.51(80), 1
packet
05:00:13 denied tcp r.s.236.88(42978) -> a.b.52.53(80), 1
packet
05:00:13 denied tcp r.s.236.88(43044) -> a.b.52.77(80), 1
packet
05:00:16 denied tcp r.s.236.88(43362) -> a.b.52.101(80), 1
packet
05:00:19 denied tcp r.s.236.88(43365) -> a.b.52.104(80), 1
packet
05:00:20 denied tcp r.s.236.88(43362) -> a.b.52.101(80), 1
packet
05:00:22 denied tcp r.s.236.88(43770) -> a.b.52.151(80), 1
packet
05:00:25 denied tcp r.s.236.88(43773) -> a.b.52.154(80), 1
packet
05:00:26 denied tcp r.s.236.88(43770) -> a.b.52.151(80), 1
packet
05:00:28 denied tcp r.s.236.88(44174) -> a.b.52.201(80), 1
packet
05:00:30 denied tcp r.s.236.88(44174) -> a.b.52.201(80), 1
packet
05:00:31 denied tcp r.s.236.88(44205) -> a.b.52.232(80), 1
packet
05:00:34 denied tcp r.s.236.88(44676) -> a.b.53.1(80), 1
packet
05:00:36 denied tcp r.s.236.88(44676) -> a.b.53.1(80), 1
packet
05:00:37 denied tcp r.s.236.88(44768) -> a.b.53.45(80), 1
packet
05:00:39 denied tcp r.s.236.88(45039) -> a.b.53.51(80), 1
packet
05:00:43 denied tcp r.s.236.88(45042) -> a.b.53.54(80), 1
packet
05:00:44 denied tcp r.s.236.88(45039) -> a.b.53.51(80), 1
packet
05:00:45 denied tcp r.s.236.88(45444) -> a.b.53.101(80), 1
packet
05:00:49 denied tcp r.s.236.88(45447) -> a.b.53.104(80), 1
packet
05:00:51 denied tcp r.s.236.88(45856) -> a.b.53.151(80), 1
packet
05:00:54 denied tcp r.s.236.88(45859) -> a.b.53.154(80), 1
packet
05:00:57 denied tcp r.s.236.88(46277) -> a.b.53.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:00:59 denied tcp r.s.236.88(46277) -> a.b.53.201(80), 1
packet
05:01:00 denied tcp r.s.236.88(46396) -> a.b.53.254(80), 1
packet
05:01:03 denied tcp r.s.236.88(46785) -> a.b.54.1(80), 1
packet
05:01:05 denied tcp r.s.236.88(46785) -> a.b.54.1(80), 1
packet
05:01:06 denied tcp r.s.236.88(46859) -> a.b.54.26(80), 1
packet
05:01:08 denied tcp r.s.236.88(47211) -> a.b.54.51(80), 1
packet
05:01:14 denied tcp r.s.236.88(47580) -> a.b.54.101(80), 1
packet
05:01:17 denied tcp r.s.236.88(47582) -> a.b.54.103(80), 1
packet
05:01:19 denied tcp r.s.236.88(47989) -> a.b.54.151(80), 1
packet
05:01:22 denied tcp r.s.236.88(47992) -> a.b.54.154(80), 1
packet
05:01:25 denied tcp r.s.236.88(48389) -> a.b.54.201(80), 1
packet
05:01:29 denied tcp r.s.236.88(48389) -> a.b.54.201(80), 1
packet
05:01:31 denied tcp r.s.236.88(48843) -> a.b.55.1(80), 1
packet
05:01:34 denied tcp r.s.236.88(48846) -> a.b.55.4(80), 1
packet
05:01:36 denied tcp r.s.236.88(49203) -> a.b.55.51(80), 1
packet
05:01:39 denied tcp r.s.236.88(49206) -> a.b.55.54(80), 1
packet
05:01:42 denied tcp r.s.236.88(49563) -> a.b.55.101(80), 1
packet
05:01:45 denied tcp r.s.236.88(49584) -> a.b.55.122(80), 1
packet
05:01:46 denied tcp r.s.236.88(49579) -> a.b.55.117(80), 1
packet
05:01:50 denied tcp r.s.236.88(50014) -> a.b.55.151(80), 1
packet
05:01:51 denied tcp r.s.236.88(50095) -> a.b.55.188(80), 1
packet
05:01:52 denied tcp r.s.236.88(50034) -> a.b.55.171(80), 1
packet
05:01:56 denied tcp r.s.236.88(50397) -> a.b.55.201(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:01:57 denied tcp r.s.236.88(50466) -> a.b.55.227(80), 1
packet
05:02:00 denied tcp r.s.236.88(50842) -> a.b.56.1(80), 1
packet
05:02:03 denied tcp r.s.236.88(50845) -> a.b.56.4(80), 1
packet
05:02:04 denied tcp r.s.236.88(50858) -> a.b.56.17(80), 1
packet
05:02:05 denied tcp r.s.236.88(51233) -> a.b.56.51(80), 1
packet
05:02:08 denied tcp r.s.236.88(51233) -> a.b.56.51(80), 1
packet
05:02:09 denied tcp r.s.236.88(51328) -> a.b.56.100(80), 1
packet
05:02:11 denied tcp r.s.236.88(51645) -> a.b.56.101(80), 1
packet
05:02:14 denied tcp r.s.236.88(51648) -> a.b.56.104(80), 1
packet
05:02:16 denied tcp r.s.236.88(52003) -> a.b.56.151(80), 1
packet
05:02:20 denied tcp r.s.236.88(52006) -> a.b.56.154(80), 1
packet
05:02:22 denied tcp r.s.236.88(52403) -> a.b.56.201(80), 1
packet
05:02:24 denied tcp r.s.236.88(52403) -> a.b.56.201(80), 1
packet
05:02:25 denied tcp r.s.236.88(52495) -> a.b.56.252(80), 1
packet
05:02:27 denied tcp r.s.236.88(52907) -> a.b.57.1(80), 1
packet
05:02:36 denied tcp r.s.236.88(53322) -> a.b.57.54(80), 1
packet
05:02:38 denied tcp r.s.236.88(53627) -> a.b.57.101(80), 1
packet
05:02:41 denied tcp r.s.236.88(53630) -> a.b.57.104(80), 1
packet
05:02:44 denied tcp r.s.236.88(54035) -> a.b.57.151(80), 1
packet
05:02:46 denied tcp r.s.236.88(54035) -> a.b.57.151(80), 1
packet
05:02:47 denied tcp r.s.236.88(54144) -> a.b.57.191(80), 1
packet
05:02:48 denied tcp r.s.236.88(54183) -> a.b.57.199(80), 1
packet
05:02:49 denied tcp r.s.236.88(54574) -> a.b.57.247(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:02:52 denied tcp r.s.236.88(54438) -> a.b.57.204(80), 1
packet
05:02:54 denied tcp r.s.236.88(54435) -> a.b.57.201(80), 1
packet
05:02:55 denied tcp r.s.236.88(54911) -> a.b.58.1(80), 1
packet
05:02:59 denied tcp r.s.236.88(54914) -> a.b.58.4(80), 1
packet
05:03:01 denied tcp r.s.236.88(55284) -> a.b.58.51(80), 1
packet
05:03:04 denied tcp r.s.236.88(55287) -> a.b.58.54(80), 1
packet
05:03:10 denied tcp r.s.236.88(55675) -> a.b.58.117(80), 1
packet
05:03:11 denied tcp r.s.236.88(55675) -> a.b.58.117(80), 1
packet
05:03:13 denied tcp r.s.236.88(56067) -> a.b.58.151(80), 1
packet
05:03:15 denied tcp r.s.236.88(56067) -> a.b.58.151(80), 1
packet
05:03:16 denied tcp r.s.236.88(56161) -> a.b.58.176(80), 1
packet
05:03:22 denied tcp r.s.236.88(56470) -> a.b.58.204(80), 1
packet
05:03:25 denied tcp r.s.236.88(57000) -> a.b.59.1(80), 1
packet
05:03:28 denied tcp r.s.236.88(57003) -> a.b.59.4(80), 1
packet
05:03:31 denied tcp r.s.236.88(57370) -> a.b.59.51(80), 1
packet
05:03:33 denied tcp r.s.236.88(57370) -> a.b.59.51(80), 1
packet
05:03:34 denied tcp r.s.236.88(57444) -> a.b.59.77(80), 1
packet
05:03:39 denied tcp r.s.236.88(57764) -> a.b.59.104(80), 1
packet
05:03:41 denied tcp r.s.236.88(57761) -> a.b.59.101(80), 1
packet
05:03:42 denied tcp r.s.236.88(58199) -> a.b.59.151(80), 1
packet
05:03:46 denied tcp r.s.236.88(58296) -> a.b.59.200(80), 1
packet
05:03:50 denied tcp r.s.236.88(58599) -> a.b.59.201(80), 1
packet
05:03:51 denied tcp r.s.236.88(58620) -> a.b.59.222(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:03:54 denied tcp r.s.236.88(59109) -> a.b.60.1(80), 1
packet
05:03:57 denied tcp r.s.236.88(59112) -> a.b.60.4(80), 1
packet
05:04:00 denied tcp r.s.236.88(59417) -> a.b.60.51(80), 1
packet
05:04:02 denied tcp r.s.236.88(59417) -> a.b.60.51(80), 1
packet
05:04:03 denied tcp r.s.236.88(59520) -> a.b.60.76(80), 1
packet
05:04:06 denied tcp r.s.236.88(59825) -> a.b.60.101(80), 1
packet
05:04:10 denied tcp r.s.236.88(59826) -> a.b.60.102(80), 1
packet
05:04:12 denied tcp r.s.236.88(60233) -> a.b.60.151(80), 1
packet
05:04:16 denied tcp r.s.236.88(60236) -> a.b.60.154(80), 1
packet
05:04:17 denied tcp r.s.236.88(60633) -> a.b.60.201(80), 1
packet
05:04:21 denied tcp r.s.236.88(60636) -> a.b.60.204(80), 1
packet
05:04:23 denied tcp r.s.236.88(61037) -> a.b.61.1(80), 1
packet
05:04:26 denied tcp r.s.236.88(61040) -> a.b.61.4(80), 1
packet
05:04:28 denied tcp r.s.236.88(61449) -> a.b.61.51(80), 1
packet
05:04:32 denied tcp r.s.236.88(61450) -> a.b.61.52(80), 1
packet
05:04:34 denied tcp r.s.236.88(61907) -> a.b.61.101(80), 1
packet
05:04:37 denied tcp r.s.236.88(61910) -> a.b.61.104(80), 1
packet
05:04:39 denied tcp r.s.236.88(62315) -> a.b.61.151(80), 1
packet
05:04:42 denied tcp r.s.236.88(62318) -> a.b.61.154(80), 1
packet
05:04:44 denied tcp r.s.236.88(62715) -> a.b.61.201(80), 1
packet
05:04:47 denied tcp r.s.236.88(62718) -> a.b.61.204(80), 1
packet
05:04:53 denied tcp r.s.236.88(63126) -> a.b.62.4(80), 1
packet
05:04:55 denied tcp r.s.236.88(63531) -> a.b.62.51(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:04:59 denied tcp r.s.236.88(63534) -> a.b.62.54(80), 1
packet
05:05:01 denied tcp r.s.236.88(63715) -> a.b.62.123(80), 1
packet
05:05:04 denied tcp r.s.236.88(63581) -> a.b.62.101(80), 1
packet
05:05:05 denied tcp r.s.236.88(63972) -> a.b.62.150(80), 1
packet
05:05:08 denied tcp r.s.236.88(64080) -> a.b.62.151(80), 1
packet
05:05:10 denied tcp r.s.236.88(64080) -> a.b.62.151(80), 1
packet
05:05:11 denied tcp r.s.236.88(64339) -> a.b.62.200(80), 1
packet
05:05:14 denied tcp r.s.236.88(64529) -> a.b.62.201(80), 1
packet
05:05:16 denied tcp r.s.236.88(64531) -> a.b.62.203(80), 1
packet
05:05:18 denied tcp r.s.236.88(64529) -> a.b.62.201(80), 1
packet
05:05:20 denied tcp r.s.236.88(65102) -> a.b.63.1(80), 1
packet
05:05:24 denied tcp r.s.236.88(65104) -> a.b.63.3(80), 1
packet
05:05:26 denied tcp r.s.236.88(65534) -> a.b.63.51(80), 1
packet
05:05:30 denied tcp r.s.236.88(32768) -> a.b.63.53(80), 1
packet
05:05:32 denied tcp r.s.236.88(33188) -> a.b.63.101(80), 1
packet
05:05:35 denied tcp r.s.236.88(33190) -> a.b.63.103(80), 1
packet
05:05:37 denied tcp r.s.236.88(33565) -> a.b.63.151(80), 1
packet
05:05:41 denied tcp r.s.236.88(33568) -> a.b.63.154(80), 1
packet
05:05:46 denied tcp r.s.236.88(33907) -> a.b.63.222(80), 1
packet
05:05:47 denied tcp r.s.236.88(33907) -> a.b.63.222(80), 1
packet
05:05:49 denied tcp r.s.236.88(34306) -> a.b.64.1(80), 1
packet
05:05:51 denied tcp r.s.236.88(34306) -> a.b.64.1(80), 1
packet
05:05:52 denied tcp r.s.236.88(34333) -> a.b.64.28(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:05:55 denied tcp r.s.236.88(34702) -> a.b.64.51(80), 1
packet
05:05:57 denied tcp r.s.236.88(34702) -> a.b.64.51(80), 1
packet
05:05:58 denied tcp r.s.236.88(34846) -> a.b.64.73(80), 1
packet
05:06:01 denied tcp r.s.236.88(35100) -> a.b.64.101(80), 1
packet
05:06:06 denied tcp r.s.236.88(35100) -> a.b.64.101(80), 1
packet
05:06:07 denied tcp r.s.236.88(35501) -> a.b.64.151(80), 1
packet
05:06:10 denied tcp r.s.236.88(35501) -> a.b.64.151(80), 1
packet
05:06:11 denied tcp r.s.236.88(35654) -> a.b.64.190(80), 1
packet
05:06:12 denied tcp r.s.236.88(35734) -> a.b.64.198(80), 1
packet
05:06:13 denied tcp r.s.236.88(35961) -> a.b.64.201(80), 1
packet
05:06:16 denied tcp r.s.236.88(35961) -> a.b.64.201(80), 1
packet
05:06:17 denied tcp r.s.236.88(36074) -> a.b.64.239(80), 1
packet
05:06:18 denied tcp r.s.236.88(36075) -> a.b.64.240(80), 1
packet
05:06:20 denied tcp r.s.236.88(36402) -> a.b.65.1(80), 1
packet
05:06:22 denied tcp r.s.236.88(36402) -> a.b.65.1(80), 1
packet
05:06:23 denied tcp r.s.236.88(36512) -> a.b.65.26(80), 1
packet
05:06:26 denied tcp r.s.236.88(36773) -> a.b.65.51(80), 1
packet
05:06:28 denied tcp r.s.236.88(36773) -> a.b.65.51(80), 1
packet
05:06:29 denied tcp r.s.236.88(36857) -> a.b.65.64(80), 1
packet
05:06:32 denied tcp r.s.236.88(37147) -> a.b.65.101(80), 1
packet
05:06:34 denied tcp r.s.236.88(37147) -> a.b.65.101(80), 1
packet
05:06:35 denied tcp r.s.236.88(37217) -> a.b.65.131(80), 1
packet
05:06:38 denied tcp r.s.236.88(37583) -> a.b.65.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:06:40 denied tcp r.s.236.88(37583) -> a.b.65.151(80), 1
packet
05:06:41 denied tcp r.s.236.88(37655) -> a.b.65.178(80), 1
packet
05:06:44 denied tcp r.s.236.88(38061) -> a.b.65.201(80), 1
packet
05:06:47 denied tcp r.s.236.88(38064) -> a.b.65.204(80), 1
packet
05:06:50 denied tcp r.s.236.88(38540) -> a.b.66.1(80), 1
packet
05:06:54 denied tcp r.s.236.88(38543) -> a.b.66.4(80), 1
packet
05:06:56 denied tcp r.s.236.88(38969) -> a.b.66.51(80), 1
packet
05:07:00 denied tcp r.s.236.88(39035) -> a.b.66.73(80), 1
packet
05:07:02 denied tcp r.s.236.88(39257) -> a.b.66.101(80), 1
packet
05:07:05 denied tcp r.s.236.88(39260) -> a.b.66.104(80), 1
packet
05:07:07 denied tcp r.s.236.88(39665) -> a.b.66.151(80), 1
packet
05:07:11 denied tcp r.s.236.88(39668) -> a.b.66.154(80), 1
packet
05:07:13 denied tcp r.s.236.88(40065) -> a.b.66.201(80), 1
packet
05:07:15 denied tcp r.s.236.88(40065) -> a.b.66.201(80), 1
packet
05:07:16 denied tcp r.s.236.88(40080) -> a.b.66.216(80), 1
packet
05:07:50 denied tcp r.s.236.88(42620) -> a.b.68.1(80), 1
packet
05:07:52 denied tcp r.s.236.88(42620) -> a.b.68.1(80), 1
packet
05:07:53 denied tcp r.s.236.88(42731) -> a.b.68.46(80), 1
packet
05:07:54 denied tcp r.s.236.88(42757) -> a.b.68.49(80), 1
packet
05:07:55 denied tcp r.s.236.88(43021) -> a.b.68.51(80), 1
packet
05:07:58 denied tcp r.s.236.88(43021) -> a.b.68.51(80), 1
packet
05:07:59 denied tcp r.s.236.88(43221) -> a.b.68.100(80), 1
packet
05:08:04 denied tcp r.s.236.88(43410) -> a.b.68.101(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:08:05 denied tcp r.s.236.88(43486) -> a.b.68.122(80), 1
packet
05:08:08 denied tcp r.s.236.88(43816) -> a.b.68.151(80), 1
packet
05:08:10 denied tcp r.s.236.88(43816) -> a.b.68.151(80), 1
packet
05:08:11 denied tcp r.s.236.88(43933) -> a.b.68.189(80), 1
packet
05:08:12 denied tcp r.s.236.88(43917) -> a.b.68.173(80), 1
packet
05:08:14 denied tcp r.s.236.88(44229) -> a.b.68.201(80), 1
packet
05:08:16 denied tcp r.s.236.88(44229) -> a.b.68.201(80), 1
packet
05:08:18 denied tcp r.s.236.88(44360) -> a.b.68.227(80), 1
packet
05:08:21 denied tcp r.s.236.88(44756) -> a.b.69.1(80), 1
packet
05:08:23 denied tcp r.s.236.88(44756) -> a.b.69.1(80), 1
packet
05:08:24 denied tcp r.s.236.88(44831) -> a.b.69.44(80), 1
packet
05:08:25 denied tcp r.s.236.88(44910) -> a.b.69.47(80), 1
packet
05:08:27 denied tcp r.s.236.88(45119) -> a.b.69.51(80), 1
packet
05:08:29 denied tcp r.s.236.88(45119) -> a.b.69.51(80), 1
packet
05:08:30 denied tcp r.s.236.88(45264) -> a.b.69.77(80), 1
packet
05:08:33 denied tcp r.s.236.88(45548) -> a.b.69.101(80), 1
packet
05:08:35 denied tcp r.s.236.88(45548) -> a.b.69.101(80), 1
packet
05:08:36 denied tcp r.s.236.88(45646) -> a.b.69.143(80), 1
packet
05:08:38 denied tcp r.s.236.88(45646) -> a.b.69.143(80), 1
packet
05:08:42 denied tcp r.s.236.88(45934) -> a.b.69.153(80), 1
packet
05:08:43 denied tcp r.s.236.88(45932) -> a.b.69.151(80), 1
packet
05:08:45 denied tcp r.s.236.88(46374) -> a.b.69.201(80), 1
packet
05:08:48 denied tcp r.s.236.88(46561) -> a.b.69.227(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:08:51 denied tcp r.s.236.88(46873) -> a.b.70.1(80), 1
packet
05:08:54 denied tcp r.s.236.88(46876) -> a.b.70.4(80), 1
packet
05:08:56 denied tcp r.s.236.88(47285) -> a.b.70.51(80), 1
packet
05:09:00 denied tcp r.s.236.88(47288) -> a.b.70.54(80), 1
packet
05:09:02 denied tcp r.s.236.88(47682) -> a.b.70.101(80), 1
packet
05:09:07 denied tcp r.s.236.88(47682) -> a.b.70.101(80), 1
packet
05:09:09 denied tcp r.s.236.88(48042) -> a.b.70.151(80), 1
packet
05:09:11 denied tcp r.s.236.88(48042) -> a.b.70.151(80), 1
packet
05:09:12 denied tcp r.s.236.88(48168) -> a.b.70.175(80), 1
packet
05:09:15 denied tcp r.s.236.88(48518) -> a.b.70.201(80), 1
packet
05:09:18 denied tcp r.s.236.88(48647) -> a.b.70.224(80), 1
packet
05:09:21 denied tcp r.s.236.88(49109) -> a.b.71.1(80), 1
packet
05:09:24 denied tcp r.s.236.88(49112) -> a.b.71.4(80), 1
packet
05:09:27 denied tcp r.s.236.88(49386) -> a.b.71.51(80), 1
packet
05:09:30 denied tcp r.s.236.88(49413) -> a.b.71.78(80), 1
packet
05:09:31 denied tcp r.s.236.88(49413) -> a.b.71.78(80), 1
packet
05:09:33 denied tcp r.s.236.88(49825) -> a.b.71.101(80), 1
packet
05:09:36 denied tcp r.s.236.88(49881) -> a.b.71.131(80), 1
packet
05:09:38 denied tcp r.s.236.88(50251) -> a.b.71.151(80), 1
packet
05:09:43 denied tcp r.s.236.88(50251) -> a.b.71.151(80), 1
packet
05:09:45 denied tcp r.s.236.88(50673) -> a.b.71.201(80), 1
packet
05:09:48 denied tcp r.s.236.88(50676) -> a.b.71.204(80), 1
packet
05:09:51 denied tcp r.s.236.88(51195) -> a.b.72.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:09:54 denied tcp r.s.236.88(51197) -> a.b.72.3(80), 1
packet
05:09:56 denied tcp r.s.236.88(51449) -> a.b.72.51(80), 1
packet
05:10:01 denied tcp r.s.236.88(51449) -> a.b.72.51(80), 1
packet
05:10:02 denied tcp r.s.236.88(51857) -> a.b.72.101(80), 1
packet
05:10:05 denied tcp r.s.236.88(51860) -> a.b.72.104(80), 1
packet
05:10:07 denied tcp r.s.236.88(52160) -> a.b.72.151(80), 1
packet
05:10:11 denied tcp r.s.236.88(52163) -> a.b.72.154(80), 1
packet
05:10:12 denied tcp r.s.236.88(52160) -> a.b.72.151(80), 1
packet
05:10:13 denied tcp r.s.236.88(52570) -> a.b.72.201(80), 1
packet
05:10:16 denied tcp r.s.236.88(52647) -> a.b.72.211(80), 1
packet
05:10:17 denied tcp r.s.236.88(52671) -> a.b.72.235(80), 1
packet
05:10:19 denied tcp r.s.236.88(53048) -> a.b.73.1(80), 1
packet
05:10:22 denied tcp r.s.236.88(53048) -> a.b.73.1(80), 1
packet
05:10:23 denied tcp r.s.236.88(53172) -> a.b.73.50(80), 1
packet
05:10:26 denied tcp r.s.236.88(53562) -> a.b.73.97(80), 1
packet
05:10:29 denied tcp r.s.236.88(53380) -> a.b.73.54(80), 1
packet
05:10:30 denied tcp r.s.236.88(53377) -> a.b.73.51(80), 1
packet
05:10:31 denied tcp r.s.236.88(53856) -> a.b.73.101(80), 1
packet
05:10:35 denied tcp r.s.236.88(53858) -> a.b.73.103(80), 1
packet
05:10:37 denied tcp r.s.236.88(54239) -> a.b.73.151(80), 1
packet
05:10:39 denied tcp r.s.236.88(54239) -> a.b.73.151(80), 1
packet
05:10:40 denied tcp r.s.236.88(54278) -> a.b.73.190(80), 1
packet
05:10:42 denied tcp r.s.236.88(54618) -> a.b.73.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:10:45 denied tcp r.s.236.88(54621) -> a.b.73.204(80), 1
packet
05:10:48 denied tcp r.s.236.88(55103) -> a.b.74.1(80), 1
packet
05:10:51 denied tcp r.s.236.88(55106) -> a.b.74.4(80), 1
packet
05:10:54 denied tcp r.s.236.88(55449) -> a.b.74.51(80), 1
packet
05:10:56 denied tcp r.s.236.88(55449) -> a.b.74.51(80), 1
packet
05:10:57 denied tcp r.s.236.88(55469) -> a.b.74.71(80), 1
packet
05:10:58 denied tcp r.s.236.88(55469) -> a.b.74.71(80), 1
packet
05:11:00 denied tcp r.s.236.88(55827) -> a.b.74.101(80), 1
packet
05:11:02 denied tcp r.s.236.88(55827) -> a.b.74.101(80), 1
packet
05:11:03 denied tcp r.s.236.88(55906) -> a.b.74.119(80), 1
packet
05:11:05 denied tcp r.s.236.88(56221) -> a.b.74.151(80), 1
packet
05:11:09 denied tcp r.s.236.88(56224) -> a.b.74.154(80), 1
packet
05:11:15 denied tcp r.s.236.88(56651) -> a.b.74.223(80), 1
packet
05:11:17 denied tcp r.s.236.88(57034) -> a.b.75.1(80), 1
packet
05:11:19 denied tcp r.s.236.88(57034) -> a.b.75.1(80), 1
packet
05:11:20 denied tcp r.s.236.88(57061) -> a.b.75.28(80), 1
packet
05:11:22 denied tcp r.s.236.88(57442) -> a.b.75.51(80), 1
packet
05:11:27 denied tcp r.s.236.88(57850) -> a.b.75.101(80), 1
packet
05:11:31 denied tcp r.s.236.88(57853) -> a.b.75.104(80), 1
packet
05:11:32 denied tcp r.s.236.88(58254) -> a.b.75.151(80), 1
packet
05:11:35 denied tcp r.s.236.88(58254) -> a.b.75.151(80), 1
packet
05:11:36 denied tcp r.s.236.88(58277) -> a.b.75.174(80), 1
packet
05:11:38 denied tcp r.s.236.88(58662) -> a.b.75.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:11:42 denied tcp r.s.236.88(58665) -> a.b.75.204(80), 1
packet
05:11:44 denied tcp r.s.236.88(59066) -> a.b.76.1(80), 1
packet
05:11:46 denied tcp r.s.236.88(59066) -> a.b.76.1(80), 1
packet
05:11:47 denied tcp r.s.236.88(59170) -> a.b.76.51(80), 1
packet
05:11:51 denied tcp r.s.236.88(59170) -> a.b.76.51(80), 1
packet
05:11:52 denied tcp r.s.236.88(59170) -> a.b.76.51(80), 1
packet
05:11:53 denied tcp r.s.236.88(59574) -> a.b.76.101(80), 1
packet
05:11:56 denied tcp r.s.236.88(59577) -> a.b.76.104(80), 1
packet
05:11:58 denied tcp r.s.236.88(59982) -> a.b.76.151(80), 1
packet
05:12:01 denied tcp r.s.236.88(59985) -> a.b.76.154(80), 1
packet
05:12:03 denied tcp r.s.236.88(60386) -> a.b.76.201(80), 1
packet
05:12:07 denied tcp r.s.236.88(60391) -> a.b.76.206(80), 1
packet
05:12:12 denied tcp r.s.236.88(60801) -> a.b.77.4(80), 1
packet
05:12:14 denied tcp r.s.236.88(61202) -> a.b.77.51(80), 1
packet
05:12:19 denied tcp r.s.236.88(61606) -> a.b.77.101(80), 1
packet
05:12:23 denied tcp r.s.236.88(61609) -> a.b.77.104(80), 1
packet
05:12:25 denied tcp r.s.236.88(61756) -> a.b.77.151(80), 1
packet
05:12:27 denied tcp r.s.236.88(61756) -> a.b.77.151(80), 1
packet
05:12:29 denied tcp r.s.236.88(61943) -> a.b.77.177(80), 1
packet
05:12:31 denied tcp r.s.236.88(62168) -> a.b.77.201(80), 1
packet
05:12:34 denied tcp r.s.236.88(62168) -> a.b.77.201(80), 1
packet
05:12:35 denied tcp r.s.236.88(62539) -> a.b.77.251(80), 1
packet
05:12:37 denied tcp r.s.236.88(62535) -> a.b.77.247(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:12:41 denied tcp r.s.236.88(62634) -> a.b.78.5(80), 1
packet
05:12:42 denied tcp r.s.236.88(62808) -> a.b.78.47(80), 1
packet
05:12:43 denied tcp r.s.236.88(62631) -> a.b.78.2(80), 1
packet
05:12:44 denied tcp r.s.236.88(63030) -> a.b.78.51(80), 1
packet
05:12:47 denied tcp r.s.236.88(63030) -> a.b.78.51(80), 1
packet
05:12:48 denied tcp r.s.236.88(63352) -> a.b.78.100(80), 1
packet
05:12:51 denied tcp r.s.236.88(63484) -> a.b.78.101(80), 1
packet
05:12:53 denied tcp r.s.236.88(63484) -> a.b.78.101(80), 1
packet
05:12:54 denied tcp r.s.236.88(63611) -> a.b.78.146(80), 1
packet
05:12:56 denied tcp r.s.236.88(63607) -> a.b.78.142(80), 1
packet
05:12:57 denied tcp r.s.236.88(63892) -> a.b.78.151(80), 1
packet
05:12:59 denied tcp r.s.236.88(63895) -> a.b.78.154(80), 1
packet
05:13:02 denied tcp r.s.236.88(64271) -> a.b.78.201(80), 1
packet
05:13:05 denied tcp r.s.236.88(64274) -> a.b.78.204(80), 1
packet
05:13:06 denied tcp r.s.236.88(64271) -> a.b.78.201(80), 1
packet
05:13:08 denied tcp r.s.236.88(64688) -> a.b.79.1(80), 1
packet
05:13:11 denied tcp r.s.236.88(64691) -> a.b.79.4(80), 1
packet
05:13:12 denied tcp r.s.236.88(64688) -> a.b.79.1(80), 1
packet
05:13:14 denied tcp r.s.236.88(65087) -> a.b.79.51(80), 1
packet
05:13:16 denied tcp r.s.236.88(65087) -> a.b.79.51(80), 1
packet
05:13:18 denied tcp r.s.236.88(65132) -> a.b.79.75(80), 1
packet
05:13:19 denied tcp r.s.236.88(65516) -> a.b.79.101(80), 1
packet
05:13:23 denied tcp r.s.236.88(32846) -> a.b.79.148(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:13:25 denied tcp r.s.236.88(32845) -> a.b.79.147(80), 1
packet
05:13:26 denied tcp r.s.236.88(33207) -> a.b.79.174(80), 1
packet
05:13:29 denied tcp r.s.236.88(33167) -> a.b.79.154(80), 1
packet
05:13:30 denied tcp r.s.236.88(33164) -> a.b.79.151(80), 1
packet
05:13:31 denied tcp r.s.236.88(33572) -> a.b.79.201(80), 1
packet
05:13:34 denied tcp r.s.236.88(33575) -> a.b.79.204(80), 1
packet
05:13:36 denied tcp r.s.236.88(33984) -> a.b.80.1(80), 1
packet
05:13:40 denied tcp r.s.236.88(33986) -> a.b.80.3(80), 1
packet
05:13:42 denied tcp r.s.236.88(34384) -> a.b.80.51(80), 1
packet
05:13:45 denied tcp r.s.236.88(34387) -> a.b.80.54(80), 1
packet
05:13:47 denied tcp r.s.236.88(34808) -> a.b.80.101(80), 1
packet
05:13:51 denied tcp r.s.236.88(34809) -> a.b.80.102(80), 1
packet
05:13:53 denied tcp r.s.236.88(35216) -> a.b.80.151(80), 1
packet
05:13:56 denied tcp r.s.236.88(35218) -> a.b.80.153(80), 1
packet
05:13:58 denied tcp r.s.236.88(35604) -> a.b.80.201(80), 1
packet
05:14:02 denied tcp r.s.236.88(35607) -> a.b.80.204(80), 1
packet
05:15:00 denied tcp r.s.236.88(40180) -> a.b.83.1(80), 1
packet
05:15:02 denied tcp r.s.236.88(40183) -> a.b.83.4(80), 1
packet
05:15:05 denied tcp r.s.236.88(40623) -> a.b.83.51(80), 1
packet
05:15:08 denied tcp r.s.236.88(40623) -> a.b.83.51(80), 1
packet
05:15:09 denied tcp r.s.236.88(40767) -> a.b.83.93(80), 1
packet
05:15:11 denied tcp r.s.236.88(40984) -> a.b.83.101(80), 1
packet
05:15:15 denied tcp r.s.236.88(40987) -> a.b.83.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:15:16 denied tcp r.s.236.88(40984) -> a.b.83.101(80), 1
packet
05:15:17 denied tcp r.s.236.88(41400) -> a.b.83.151(80), 1
packet
05:15:20 denied tcp r.s.236.88(41403) -> a.b.83.154(80), 1
packet
05:15:22 denied tcp r.s.236.88(41800) -> a.b.83.201(80), 1
packet
05:15:26 denied tcp r.s.236.88(41803) -> a.b.83.204(80), 1
packet
05:15:28 denied tcp r.s.236.88(42212) -> a.b.84.1(80), 1
packet
05:15:32 denied tcp r.s.236.88(42215) -> a.b.84.4(80), 1
packet
05:15:34 denied tcp r.s.236.88(42629) -> a.b.84.51(80), 1
packet
05:15:37 denied tcp r.s.236.88(42631) -> a.b.84.53(80), 1
packet
05:15:39 denied tcp r.s.236.88(43016) -> a.b.84.101(80), 1
packet
05:15:43 denied tcp r.s.236.88(43018) -> a.b.84.103(80), 1
packet
05:15:45 denied tcp r.s.236.88(43482) -> a.b.84.151(80), 1
packet
05:15:48 denied tcp r.s.236.88(43485) -> a.b.84.154(80), 1
packet
05:15:50 denied tcp r.s.236.88(43882) -> a.b.84.201(80), 1
packet
05:15:53 denied tcp r.s.236.88(43884) -> a.b.84.203(80), 1
packet
05:16:56 denied 9w0d: %IDS-4-TCP_SYN_ATTACK_SIG:
Sig:3050:Half-Open Syn Flood packet
05:17:21 denied tcp r.s.236.88(50390) -> a.b.88.1(80), 1
packet
05:17:25 denied tcp r.s.236.88(50390) -> a.b.88.1(80), 1
packet
05:17:27 denied tcp r.s.236.88(50744) -> a.b.88.51(80), 1
packet
05:17:30 denied tcp r.s.236.88(50747) -> a.b.88.54(80), 1
packet
05:17:32 denied tcp r.s.236.88(51026) -> a.b.88.101(80), 1
packet
05:17:36 denied tcp r.s.236.88(51026) -> a.b.88.101(80), 1
packet
05:17:39 denied tcp r.s.236.88(51418) -> a.b.88.161(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:17:40 denied tcp r.s.236.88(51272) -> a.b.88.151(80), 1
packet
05:17:42 denied tcp r.s.236.88(51440) -> a.b.88.183(80), 1
packet
05:17:42 denied tcp r.s.236.88(51435) -> a.b.88.178(80), 1
packet
05:17:45 denied tcp r.s.236.88(51697) -> a.b.88.201(80), 1
packet
05:17:48 denied tcp r.s.236.88(51697) -> a.b.88.201(80), 1
packet
05:17:49 denied tcp r.s.236.88(51847) -> a.b.88.226(80), 1
packet
05:17:50 denied tcp r.s.236.88(51843) -> a.b.88.222(80), 1
packet
05:17:52 denied tcp r.s.236.88(52345) -> a.b.89.1(80), 1
packet
05:17:55 denied tcp r.s.236.88(52347) -> a.b.89.3(80), 1
packet
05:17:57 denied tcp r.s.236.88(52607) -> a.b.89.51(80), 1
packet
05:18:01 denied tcp r.s.236.88(52609) -> a.b.89.53(80), 1
packet
05:18:02 denied tcp r.s.236.88(52607) -> a.b.89.51(80), 1
packet
05:18:04 denied tcp r.s.236.88(52926) -> a.b.89.101(80), 1
packet
05:18:07 denied tcp r.s.236.88(52926) -> a.b.89.101(80), 1
packet
05:18:08 denied tcp r.s.236.88(53099) -> a.b.89.128(80), 1
packet
05:18:10 denied tcp r.s.236.88(53500) -> a.b.89.151(80), 1
packet
05:18:14 denied tcp r.s.236.88(53502) -> a.b.89.153(80), 1
packet
05:18:15 denied tcp r.s.236.88(53500) -> a.b.89.151(80), 1
packet
05:18:16 denied tcp r.s.236.88(53859) -> a.b.89.201(80), 1
packet
05:18:19 denied tcp r.s.236.88(53859) -> a.b.89.201(80), 1
packet
05:18:20 denied tcp r.s.236.88(53979) -> a.b.89.243(80), 1
packet
05:18:21 denied tcp r.s.236.88(54081) -> a.b.89.254(80), 1
packet
05:18:23 denied tcp r.s.236.88(54425) -> a.b.90.1(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:18:26 denied tcp r.s.236.88(54427) -> a.b.90.3(80), 1
packet
05:18:29 denied tcp r.s.236.88(54654) -> a.b.90.51(80), 1
packet
05:18:31 denied tcp r.s.236.88(54654) -> a.b.90.51(80), 1
packet
05:18:32 denied tcp r.s.236.88(54787) -> a.b.90.77(80), 1
packet
05:18:38 denied tcp r.s.236.88(55081) -> a.b.90.103(80), 1
packet
05:18:40 denied tcp r.s.236.88(55079) -> a.b.90.101(80), 1
packet
05:18:41 denied tcp r.s.236.88(55533) -> a.b.90.151(80), 1
packet
05:18:44 denied tcp r.s.236.88(55533) -> a.b.90.151(80), 1
packet
05:18:44 denied tcp r.s.236.88(55640) -> a.b.90.195(80), 1
packet
05:18:46 denied tcp r.s.236.88(55751) -> a.b.90.200(80), 1
packet
05:18:48 denied tcp r.s.236.88(55922) -> a.b.90.201(80), 1
packet
05:18:50 denied tcp r.s.236.88(55922) -> a.b.90.201(80), 1
packet
05:18:51 denied tcp r.s.236.88(56030) -> a.b.90.214(80), 1
packet
05:18:54 denied tcp r.s.236.88(56516) -> a.b.91.36(80), 1
packet
05:18:57 denied tcp r.s.236.88(56441) -> a.b.91.3(80), 1
packet
05:19:00 denied tcp r.s.236.88(56742) -> a.b.91.51(80), 1
packet
05:19:03 denied tcp r.s.236.88(56745) -> a.b.91.54(80), 1
packet
05:19:04 denied tcp r.s.236.88(56742) -> a.b.91.51(80), 1
packet
05:19:06 denied tcp r.s.236.88(57192) -> a.b.91.101(80), 1
packet
05:19:09 denied tcp r.s.236.88(57192) -> a.b.91.101(80), 1
packet
05:19:09 denied tcp r.s.236.88(57451) -> a.b.91.127(80), 1
packet
05:19:13 denied tcp r.s.236.88(57616) -> a.b.91.151(80), 1
packet
05:19:15 denied tcp r.s.236.88(57616) -> a.b.91.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:19:16 denied tcp r.s.236.88(57702) -> a.b.91.172(80), 1
packet
05:19:17 denied tcp r.s.236.88(57697) -> a.b.91.167(80), 1
packet
05:19:19 denied tcp r.s.236.88(58008) -> a.b.91.201(80), 1
packet
05:19:22 denied tcp r.s.236.88(58011) -> a.b.91.204(80), 1
packet
05:19:24 denied tcp r.s.236.88(58420) -> a.b.92.1(80), 1
packet
05:19:27 denied tcp r.s.236.88(58423) -> a.b.92.4(80), 1
packet
05:19:29 denied tcp r.s.236.88(58824) -> a.b.92.51(80), 1
packet
05:19:34 denied tcp r.s.236.88(58824) -> a.b.92.51(80), 1
packet
05:19:35 denied tcp r.s.236.88(59224) -> a.b.92.101(80), 1
packet
05:19:38 denied tcp r.s.236.88(59226) -> a.b.92.103(80), 1
packet
05:19:40 denied tcp r.s.236.88(59632) -> a.b.92.151(80), 1
packet
05:19:44 denied tcp r.s.236.88(59634) -> a.b.92.153(80), 1
packet
05:19:48 denied tcp r.s.236.88(60040) -> a.b.92.201(80), 1
packet
05:19:49 denied tcp r.s.236.88(60061) -> a.b.92.222(80), 1
packet
05:19:51 denied tcp r.s.236.88(60452) -> a.b.93.1(80), 1
packet
05:19:54 denied tcp r.s.236.88(60452) -> a.b.93.1(80), 1
packet
05:19:55 denied tcp r.s.236.88(60490) -> a.b.93.39(80), 1
packet
05:19:57 denied tcp r.s.236.88(60856) -> a.b.93.51(80), 1
packet
05:20:00 denied tcp r.s.236.88(60858) -> a.b.93.53(80), 1
packet
05:20:02 denied tcp r.s.236.88(61256) -> a.b.93.101(80), 1
packet
05:20:06 denied tcp r.s.236.88(61259) -> a.b.93.104(80), 1
packet
05:20:07 denied tcp r.s.236.88(61664) -> a.b.93.151(80), 1
packet
05:20:11 denied tcp r.s.236.88(61667) -> a.b.93.154(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:20:13 denied tcp r.s.236.88(62072) -> a.b.93.201(80), 1
packet
05:20:16 denied tcp r.s.236.88(62075) -> a.b.93.204(80), 1
packet
05:20:18 denied tcp r.s.236.88(62484) -> a.b.94.1(80), 1
packet
05:20:22 denied tcp r.s.236.88(62487) -> a.b.94.4(80), 1
packet
05:20:24 denied tcp r.s.236.88(62713) -> a.b.94.51(80), 1
packet
05:20:27 denied tcp r.s.236.88(62716) -> a.b.94.54(80), 1
packet
05:20:29 denied tcp r.s.236.88(62713) -> a.b.94.51(80), 1
packet
05:20:30 denied tcp r.s.236.88(63088) -> a.b.94.101(80), 1
packet
05:20:33 denied tcp r.s.236.88(63090) -> a.b.94.103(80), 1
packet
05:20:35 denied tcp r.s.236.88(63088) -> a.b.94.101(80), 1
packet
05:20:36 denied tcp r.s.236.88(63563) -> a.b.94.151(80), 1
packet
05:20:40 denied tcp r.s.236.88(63565) -> a.b.94.153(80), 1
packet
05:20:42 denied tcp r.s.236.88(63954) -> a.b.94.201(80), 1
packet
05:20:45 denied tcp r.s.236.88(63954) -> a.b.94.201(80), 1
packet
05:20:46 denied tcp r.s.236.88(64112) -> a.b.94.248(80), 1
packet
05:20:51 denied tcp r.s.236.88(64460) -> a.b.95.1(80), 1
packet
05:20:52 denied tcp r.s.236.88(64481) -> a.b.95.22(80), 1
packet
05:20:53 denied tcp r.s.236.88(64481) -> a.b.95.22(80), 1
packet
05:20:55 denied tcp r.s.236.88(64862) -> a.b.95.51(80), 1
packet
05:20:57 denied tcp r.s.236.88(64862) -> a.b.95.51(80), 1
packet
05:20:58 denied tcp r.s.236.88(65003) -> a.b.95.95(80), 1
packet
05:21:00 denied tcp r.s.236.88(65241) -> a.b.95.101(80), 1
packet
05:21:03 denied tcp r.s.236.88(65241) -> a.b.95.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:21:04 denied tcp r.s.236.88(65524) -> a.b.95.151(80), 1
packet
05:21:07 denied tcp r.s.236.88(65527) -> a.b.95.154(80), 1
packet
05:21:09 denied tcp r.s.236.88(33176) -> a.b.95.201(80), 1
packet
05:21:12 denied tcp r.s.236.88(33178) -> a.b.95.203(80), 1
packet
05:21:15 denied tcp r.s.236.88(33634) -> a.b.96.1(80), 1
packet
05:21:18 denied tcp r.s.236.88(33637) -> a.b.96.4(80), 1
packet
05:21:21 denied tcp r.s.236.88(34007) -> a.b.96.51(80), 1
packet
05:21:24 denied tcp r.s.236.88(34009) -> a.b.96.53(80), 1
packet
05:21:26 denied tcp r.s.236.88(34412) -> a.b.96.101(80), 1
packet
05:21:29 denied tcp r.s.236.88(34415) -> a.b.96.104(80), 1
packet
05:21:31 denied tcp r.s.236.88(34797) -> a.b.96.151(80), 1
packet
05:21:34 denied tcp r.s.236.88(34797) -> a.b.96.151(80), 1
packet
05:21:35 denied tcp r.s.236.88(34887) -> a.b.96.195(80), 1
packet
05:21:37 denied tcp r.s.236.88(35209) -> a.b.96.201(80), 1
packet
05:21:40 denied tcp r.s.236.88(35209) -> a.b.96.201(80), 1
packet
05:21:41 denied tcp r.s.236.88(35351) -> a.b.96.243(80), 1
packet
05:21:43 denied tcp r.s.236.88(35696) -> a.b.97.1(80), 1
packet
05:21:46 denied tcp r.s.236.88(35696) -> a.b.97.1(80), 1
packet
05:21:47 denied tcp r.s.236.88(35806) -> a.b.97.48(80), 1
packet
05:21:49 denied tcp r.s.236.88(36095) -> a.b.97.51(80), 1
packet
05:21:55 denied tcp r.s.236.88(36425) -> a.b.97.101(80), 1
packet
05:21:58 denied tcp r.s.236.88(36428) -> a.b.97.104(80), 1
packet
05:22:00 denied tcp r.s.236.88(36829) -> a.b.97.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:22:03 denied tcp r.s.236.88(36832) -> a.b.97.154(80), 1
packet
05:22:05 denied tcp r.s.236.88(37241) -> a.b.97.201(80), 1
packet
05:22:11 denied tcp r.s.236.88(37645) -> a.b.98.1(80), 1
packet
05:22:15 denied tcp r.s.236.88(37694) -> a.b.98.50(80), 1
packet
05:22:16 denied tcp r.s.236.88(37694) -> a.b.98.50(80), 1
packet
05:22:20 denied tcp r.s.236.88(38056) -> a.b.98.54(80), 1
packet
05:22:22 denied tcp r.s.236.88(38457) -> a.b.98.101(80), 1
packet
05:22:25 denied tcp r.s.236.88(38460) -> a.b.98.104(80), 1
packet
05:22:27 denied tcp r.s.236.88(38861) -> a.b.98.151(80), 1
packet
05:22:31 denied tcp r.s.236.88(38864) -> a.b.98.154(80), 1
packet
05:22:33 denied tcp r.s.236.88(39273) -> a.b.98.201(80), 1
packet
05:22:37 denied tcp r.s.236.88(39273) -> a.b.98.201(80), 1
packet
05:22:41 denied tcp r.s.236.88(39680) -> a.b.99.4(80), 1
packet
05:22:47 denied tcp r.s.236.88(40066) -> a.b.99.53(80), 1
packet
05:22:49 denied tcp r.s.236.88(40384) -> a.b.99.101(80), 1
packet
05:22:53 denied tcp r.s.236.88(40387) -> a.b.99.104(80), 1
packet
05:22:53 denied tcp r.s.236.88(40404) -> a.b.99.121(80), 1
packet
05:22:55 denied tcp r.s.236.88(40689) -> a.b.99.151(80), 1
packet
05:23:00 denied tcp r.s.236.88(40689) -> a.b.99.151(80), 1
packet
05:23:02 denied tcp r.s.236.88(41101) -> a.b.99.201(80), 1
packet
05:23:04 denied tcp r.s.236.88(41101) -> a.b.99.201(80), 1
packet
05:23:05 denied tcp r.s.236.88(41234) -> a.b.99.229(80), 1
packet
05:23:12 denied tcp r.s.236.88(41646) -> a.b.100.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:23:14 denied tcp r.s.236.88(41934) -> a.b.100.51(80), 1
packet
05:23:17 denied tcp r.s.236.88(41936) -> a.b.100.53(80), 1
packet
05:23:18 denied tcp r.s.236.88(41934) -> a.b.100.51(80), 1
packet
05:23:20 denied tcp r.s.236.88(42337) -> a.b.100.101(80), 1
packet
05:23:24 denied tcp r.s.236.88(42550) -> a.b.100.146(80), 1
packet
05:23:26 denied tcp r.s.236.88(42858) -> a.b.100.187(80), 1
packet
05:23:30 denied tcp r.s.236.88(42774) -> a.b.100.154(80), 1
packet
05:23:32 denied tcp r.s.236.88(43187) -> a.b.100.201(80), 1
packet
05:23:35 denied tcp r.s.236.88(43190) -> a.b.100.204(80), 1
packet
05:23:42 denied tcp r.s.236.88(43694) -> a.b.101.4(80), 1
packet
05:23:44 denied tcp r.s.236.88(44149) -> a.b.101.97(80), 1
packet
05:23:46 denied tcp r.s.236.88(43999) -> a.b.101.51(80), 1
packet
05:23:47 denied tcp r.s.236.88(44059) -> a.b.101.78(80), 1
packet
05:23:52 denied tcp r.s.236.88(44399) -> a.b.101.101(80), 1
packet
05:23:53 denied tcp r.s.236.88(44456) -> a.b.101.125(80), 1
packet
05:23:59 denied tcp r.s.236.88(44858) -> a.b.101.154(80), 1
packet
05:24:05 denied tcp r.s.236.88(45216) -> a.b.101.202(80), 1
packet
05:24:11 denied tcp r.s.236.88(45726) -> a.b.102.4(80), 1
packet
05:24:14 denied tcp r.s.236.88(46167) -> a.b.102.73(80), 1
packet
05:24:17 denied tcp r.s.236.88(46104) -> a.b.102.53(80), 1
packet
05:24:19 denied tcp r.s.236.88(46507) -> a.b.102.101(80), 1
packet
05:24:23 denied tcp r.s.236.88(46510) -> a.b.102.104(80), 1
packet
05:24:25 denied tcp r.s.236.88(46889) -> a.b.102.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:24:28 denied tcp r.s.236.88(46892) -> a.b.102.154(80), 1
packet
05:24:30 denied tcp r.s.236.88(47197) -> a.b.102.201(80), 1
packet
05:24:33 denied tcp r.s.236.88(47197) -> a.b.102.201(80), 1
packet
05:24:34 denied tcp r.s.236.88(47405) -> a.b.102.254(80), 1
packet
05:24:35 denied tcp r.s.236.88(47404) -> a.b.102.253(80), 1
packet
05:24:36 denied tcp r.s.236.88(47755) -> a.b.103.1(80), 1
packet
05:24:40 denied tcp r.s.236.88(47758) -> a.b.103.4(80), 1
packet
05:24:45 denied tcp r.s.236.88(48115) -> a.b.103.54(80), 1
packet
05:24:46 denied tcp r.s.236.88(48112) -> a.b.103.51(80), 1
packet
05:24:52 denied tcp r.s.236.88(48470) -> a.b.103.104(80), 1
packet
05:24:57 denied tcp r.s.236.88(48876) -> a.b.103.160(80), 1
packet
05:24:59 denied tcp r.s.236.88(49324) -> a.b.103.246(80), 1
packet
05:25:01 denied tcp r.s.236.88(49216) -> a.b.103.201(80), 1
packet
05:25:02 denied tcp r.s.236.88(49285) -> a.b.103.227(80), 1
packet
05:25:04 denied tcp r.s.236.88(49637) -> a.b.104.1(80), 1
packet
05:25:08 denied tcp r.s.236.88(49637) -> a.b.104.1(80), 1
packet
05:26:59 denied tcp r.s.236.88(57575) -> a.b.108.1(80), 1
packet
05:27:01 denied tcp r.s.236.88(57575) -> a.b.108.1(80), 1
packet
05:27:02 denied tcp r.s.236.88(57636) -> a.b.108.15(80), 1
packet
05:27:05 denied tcp r.s.236.88(58011) -> a.b.108.51(80), 1
packet
05:27:08 denied tcp r.s.236.88(58014) -> a.b.108.54(80), 1
packet
05:27:11 denied tcp r.s.236.88(58423) -> a.b.108.101(80), 1
packet
05:27:17 denied tcp r.s.236.88(58875) -> a.b.108.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:27:19 denied tcp r.s.236.88(58875) -> a.b.108.151(80), 1
packet
05:27:20 denied tcp r.s.236.88(58896) -> a.b.108.172(80), 1
packet
05:27:22 denied tcp r.s.236.88(59281) -> a.b.108.201(80), 1
packet
05:27:26 denied tcp r.s.236.88(59434) -> a.b.108.247(80), 1
packet
05:27:27 denied tcp r.s.236.88(59440) -> a.b.108.253(80), 1
packet
05:27:28 denied tcp r.s.236.88(59747) -> a.b.109.1(80), 1
packet
05:27:31 denied tcp r.s.236.88(59747) -> a.b.109.1(80), 1
packet
05:27:32 denied tcp r.s.236.88(59843) -> a.b.109.47(80), 1
packet
05:27:34 denied tcp r.s.236.88(60147) -> a.b.109.51(80), 1
packet
05:27:37 denied tcp r.s.236.88(60150) -> a.b.109.54(80), 1
packet
05:27:40 denied tcp r.s.236.88(60559) -> a.b.109.101(80), 1
packet
05:27:42 denied tcp r.s.236.88(60559) -> a.b.109.101(80), 1
packet
05:27:43 denied tcp r.s.236.88(60595) -> a.b.109.128(80), 1
packet
05:27:44 denied tcp r.s.236.88(60580) -> a.b.109.122(80), 1
packet
05:27:46 denied tcp r.s.236.88(60959) -> a.b.109.151(80), 1
packet
05:27:49 denied tcp r.s.236.88(60961) -> a.b.109.153(80), 1
packet
05:27:51 denied tcp r.s.236.88(61367) -> a.b.109.201(80), 1
packet
05:27:55 denied tcp r.s.236.88(61370) -> a.b.109.204(80), 1
packet
05:27:56 denied tcp r.s.236.88(61442) -> a.b.109.240(80), 1
packet
05:27:58 denied tcp r.s.236.88(61902) -> a.b.110.1(80), 1
packet
05:28:01 denied tcp r.s.236.88(61905) -> a.b.110.4(80), 1
packet
05:28:02 denied tcp r.s.236.88(61902) -> a.b.110.1(80), 1
packet
05:28:04 denied tcp r.s.236.88(62283) -> a.b.110.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:28:06 denied tcp r.s.236.88(62283) -> a.b.110.51(80), 1
packet
05:28:07 denied tcp r.s.236.88(62400) -> a.b.110.79(80), 1
packet
05:28:09 denied tcp r.s.236.88(62712) -> a.b.110.101(80), 1
packet
05:28:12 denied tcp r.s.236.88(62712) -> a.b.110.101(80), 1
packet
05:28:13 denied tcp r.s.236.88(62733) -> a.b.110.122(80), 1
packet
05:28:14 denied tcp r.s.236.88(62733) -> a.b.110.122(80), 1
packet
05:28:15 denied tcp r.s.236.88(63117) -> a.b.110.151(80), 1
packet
05:28:18 denied tcp r.s.236.88(63117) -> a.b.110.151(80), 1
packet
05:28:19 denied tcp r.s.236.88(63291) -> a.b.110.198(80), 1
packet
05:28:21 denied tcp r.s.236.88(63503) -> a.b.110.201(80), 1
packet
05:28:24 denied tcp r.s.236.88(63503) -> a.b.110.201(80), 1
packet
05:28:25 denied tcp r.s.236.88(63688) -> a.b.110.253(80), 1
packet
05:28:28 denied tcp r.s.236.88(64020) -> a.b.111.1(80), 1
packet
05:28:31 denied tcp r.s.236.88(64083) -> a.b.111.40(80), 1
packet
05:28:33 denied tcp r.s.236.88(64157) -> a.b.111.45(80), 1
packet
05:28:34 denied tcp r.s.236.88(64410) -> a.b.111.51(80), 1
packet
05:28:37 denied tcp r.s.236.88(64413) -> a.b.111.54(80), 1
packet
05:28:38 denied tcp r.s.236.88(64410) -> a.b.111.51(80), 1
packet
05:28:40 denied tcp r.s.236.88(64723) -> a.b.111.101(80), 1
packet
05:28:43 denied tcp r.s.236.88(64745) -> a.b.111.123(80), 1
packet
05:28:44 denied tcp r.s.236.88(65045) -> a.b.111.150(80), 1
packet
05:28:46 denied tcp r.s.236.88(65240) -> a.b.111.151(80), 1
packet
05:28:49 denied tcp r.s.236.88(65240) -> a.b.111.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:28:50 denied tcp r.s.236.88(65400) -> a.b.111.183(80), 1
packet
05:28:52 denied tcp r.s.236.88(32825) -> a.b.111.201(80), 1
packet
05:28:56 denied tcp r.s.236.88(32828) -> a.b.111.204(80), 1
packet
05:28:59 denied tcp r.s.236.88(33373) -> a.b.112.1(80), 1
packet
05:29:02 denied tcp r.s.236.88(33376) -> a.b.112.4(80), 1
packet
05:29:03 denied tcp r.s.236.88(33373) -> a.b.112.1(80), 1
packet
05:29:05 denied tcp r.s.236.88(33766) -> a.b.112.51(80), 1
packet
05:29:08 denied tcp r.s.236.88(33768) -> a.b.112.53(80), 1
packet
05:29:09 denied tcp r.s.236.88(33766) -> a.b.112.51(80), 1
packet
05:29:10 denied tcp r.s.236.88(34244) -> a.b.112.101(80), 1
packet
05:29:14 denied tcp r.s.236.88(34245) -> a.b.112.102(80), 1
packet
05:29:14 denied tcp r.s.236.88(34314) -> a.b.112.112(80), 1
packet
05:29:17 denied tcp r.s.236.88(34671) -> a.b.112.151(80), 1
packet
05:29:20 denied tcp r.s.236.88(34671) -> a.b.112.151(80), 1
packet
05:29:21 denied tcp r.s.236.88(34806) -> a.b.112.200(80), 1
packet
05:29:23 denied tcp r.s.236.88(35032) -> a.b.112.201(80), 1
packet
05:29:27 denied tcp r.s.236.88(35034) -> a.b.112.203(80), 1
packet
05:29:29 denied tcp r.s.236.88(35554) -> a.b.113.1(80), 1
packet
05:29:34 denied tcp r.s.236.88(35554) -> a.b.113.1(80), 1
packet
05:29:35 denied tcp r.s.236.88(35827) -> a.b.113.51(80), 1
packet
05:29:39 denied tcp r.s.236.88(35830) -> a.b.113.54(80), 1
packet
05:29:40 denied tcp r.s.236.88(35827) -> a.b.113.51(80), 1
packet
05:29:41 denied tcp r.s.236.88(36288) -> a.b.113.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:29:44 denied tcp r.s.236.88(36288) -> a.b.113.101(80), 1
packet
05:29:45 denied tcp r.s.236.88(36552) -> a.b.113.151(80), 1
packet
05:29:48 denied tcp r.s.236.88(36554) -> a.b.113.153(80), 1
packet
05:29:50 denied tcp r.s.236.88(36939) -> a.b.113.201(80), 1
packet
05:29:53 denied tcp r.s.236.88(36939) -> a.b.113.201(80), 1
packet
05:29:54 denied tcp r.s.236.88(37003) -> a.b.113.245(80), 1
packet
05:29:56 denied tcp r.s.236.88(37446) -> a.b.114.1(80), 1
packet
05:30:00 denied tcp r.s.236.88(37447) -> a.b.114.2(80), 1
packet
05:30:02 denied tcp r.s.236.88(37809) -> a.b.114.51(80), 1
packet
05:30:05 denied tcp r.s.236.88(37809) -> a.b.114.51(80), 1
packet
05:30:07 denied tcp r.s.236.88(37809) -> a.b.114.51(80), 1
packet
05:30:08 denied tcp r.s.236.88(38230) -> a.b.114.101(80), 1
packet
05:30:12 denied tcp r.s.236.88(38232) -> a.b.114.103(80), 1
packet
05:30:12 denied tcp r.s.236.88(38331) -> a.b.114.139(80), 1
packet
05:30:14 denied tcp r.s.236.88(38634) -> a.b.114.151(80), 1
packet
05:30:17 denied tcp r.s.236.88(38634) -> a.b.114.151(80), 1
packet
05:30:18 denied tcp r.s.236.88(38738) -> a.b.114.175(80), 1
packet
05:30:20 denied tcp r.s.236.88(39088) -> a.b.114.201(80), 1
packet
05:30:23 denied tcp r.s.236.88(39088) -> a.b.114.201(80), 1
packet
05:30:24 denied tcp r.s.236.88(39261) -> a.b.114.249(80), 1
packet
05:30:25 denied tcp r.s.236.88(39266) -> a.b.114.254(80), 1
packet
05:30:27 denied tcp r.s.236.88(39587) -> a.b.115.1(80), 1
packet
05:30:29 denied tcp r.s.236.88(39587) -> a.b.115.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:30:30 denied tcp r.s.236.88(39608) -> a.b.115.22(80), 1
packet
05:30:32 denied tcp r.s.236.88(39882) -> a.b.115.51(80), 1
packet
05:30:36 denied tcp r.s.236.88(39885) -> a.b.115.54(80), 1
packet
05:30:38 denied tcp r.s.236.88(40241) -> a.b.115.101(80), 1
packet
05:30:41 denied tcp r.s.236.88(40244) -> a.b.115.104(80), 1
packet
05:30:43 denied tcp r.s.236.88(40645) -> a.b.115.151(80), 1
packet
05:30:45 denied tcp r.s.236.88(40645) -> a.b.115.151(80), 1
packet
05:30:47 denied tcp r.s.236.88(40668) -> a.b.115.174(80), 1
packet
05:30:49 denied tcp r.s.236.88(41053) -> a.b.115.201(80), 1
packet
05:30:52 denied tcp r.s.236.88(41054) -> a.b.115.202(80), 1
packet
05:30:54 denied tcp r.s.236.88(41461) -> a.b.116.1(80), 1
packet
05:30:57 denied tcp r.s.236.88(41463) -> a.b.116.3(80), 1
packet
05:30:59 denied tcp r.s.236.88(41873) -> a.b.116.51(80), 1
packet
05:31:03 denied tcp r.s.236.88(41875) -> a.b.116.53(80), 1
packet
05:31:04 denied tcp r.s.236.88(41873) -> a.b.116.51(80), 1
packet
05:31:05 denied tcp r.s.236.88(42273) -> a.b.116.101(80), 1
packet
05:31:08 denied tcp r.s.236.88(42276) -> a.b.116.104(80), 1
packet
05:31:10 denied tcp r.s.236.88(42677) -> a.b.116.151(80), 1
packet
05:31:14 denied tcp r.s.236.88(42680) -> a.b.116.154(80), 1
packet
05:31:15 denied tcp r.s.236.88(43086) -> a.b.116.201(80), 1
packet
05:31:19 denied tcp r.s.236.88(43089) -> a.b.116.204(80), 1
packet
05:31:21 denied tcp r.s.236.88(43494) -> a.b.117.1(80), 1
packet
05:31:25 denied tcp r.s.236.88(43497) -> a.b.117.4(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:31:26 denied tcp r.s.236.88(43806) -> a.b.117.51(80), 1
packet
05:31:29 denied tcp r.s.236.88(43806) -> a.b.117.51(80), 1
packet
05:31:30 denied tcp r.s.236.88(43943) -> a.b.117.100(80), 1
packet
05:31:35 denied tcp r.s.236.88(44159) -> a.b.117.104(80), 1
packet
05:31:37 denied tcp r.s.236.88(44560) -> a.b.117.151(80), 1
packet
05:31:41 denied tcp r.s.236.88(44563) -> a.b.117.154(80), 1
packet
05:31:43 denied tcp r.s.236.88(44960) -> a.b.117.201(80), 1
packet
05:31:46 denied tcp r.s.236.88(45013) -> a.b.117.254(80), 1
packet
05:31:48 denied tcp r.s.236.88(45376) -> a.b.118.1(80), 1
packet
05:31:52 denied tcp r.s.236.88(45379) -> a.b.118.4(80), 1
packet
05:31:54 denied tcp r.s.236.88(45784) -> a.b.118.51(80), 1
packet
05:31:58 denied tcp r.s.236.88(45784) -> a.b.118.51(80), 1
packet
05:31:59 denied tcp r.s.236.88(46188) -> a.b.118.101(80), 1
packet
05:32:02 denied tcp r.s.236.88(46190) -> a.b.118.103(80), 1
packet
05:32:04 denied tcp r.s.236.88(46592) -> a.b.118.151(80), 1
packet
05:32:08 denied tcp r.s.236.88(46595) -> a.b.118.154(80), 1
packet
05:32:10 denied tcp r.s.236.88(46992) -> a.b.118.201(80), 1
packet
05:32:13 denied tcp r.s.236.88(46994) -> a.b.118.203(80), 1
packet
05:32:15 denied tcp r.s.236.88(47408) -> a.b.119.1(80), 1
packet
05:32:19 denied tcp r.s.236.88(47411) -> a.b.119.4(80), 1
packet
05:32:21 denied tcp r.s.236.88(47716) -> a.b.119.51(80), 1
packet
05:32:24 denied tcp r.s.236.88(47719) -> a.b.119.54(80), 1
packet
05:32:24 denied tcp r.s.236.88(47727) -> a.b.119.62(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:32:27 denied tcp r.s.236.88(48020) -> a.b.119.101(80), 1
packet
05:32:30 denied tcp r.s.236.88(48020) -> a.b.119.101(80), 1
packet
05:32:31 denied tcp r.s.236.88(48131) -> a.b.119.126(80), 1
packet
05:32:31 denied tcp r.s.236.88(48127) -> a.b.119.122(80), 1
packet
05:32:33 denied tcp r.s.236.88(48424) -> a.b.119.151(80), 1
packet
05:32:36 denied tcp r.s.236.88(48427) -> a.b.119.154(80), 1
packet
05:32:38 denied tcp r.s.236.88(48424) -> a.b.119.151(80), 1
packet
05:32:40 denied tcp r.s.236.88(48933) -> a.b.119.201(80), 1
packet
05:32:42 denied tcp r.s.236.88(48933) -> a.b.119.201(80), 1
packet
05:32:43 denied tcp r.s.236.88(49074) -> a.b.119.234(80), 1
packet
05:32:46 denied tcp r.s.236.88(49356) -> a.b.120.1(80), 1
packet
05:32:49 denied tcp r.s.236.88(49358) -> a.b.120.3(80), 1
packet
05:32:50 denied tcp r.s.236.88(49356) -> a.b.120.1(80), 1
packet
05:32:52 denied tcp r.s.236.88(49697) -> a.b.120.51(80), 1
packet
05:32:54 denied tcp r.s.236.88(49697) -> a.b.120.51(80), 1
packet
05:32:56 denied tcp r.s.236.88(49867) -> a.b.120.77(80), 1
packet
05:32:58 denied tcp r.s.236.88(50052) -> a.b.120.101(80), 1
packet
05:33:01 denied tcp r.s.236.88(50055) -> a.b.120.104(80), 1
packet
05:33:04 denied tcp r.s.236.88(50456) -> a.b.120.151(80), 1
packet
05:33:06 denied tcp r.s.236.88(50456) -> a.b.120.151(80), 1
packet
05:33:07 denied tcp r.s.236.88(50524) -> a.b.120.178(80), 1
packet
05:33:12 denied tcp r.s.236.88(50877) -> a.b.120.201(80), 1
packet
05:33:14 denied tcp r.s.236.88(50946) -> a.b.120.227(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:33:16 denied tcp r.s.236.88(51309) -> a.b.121.1(80), 1
packet
05:33:21 denied tcp r.s.236.88(51309) -> a.b.121.1(80), 1
packet
05:33:22 denied tcp r.s.236.88(51698) -> a.b.121.51(80), 1
packet
05:33:26 denied tcp r.s.236.88(51701) -> a.b.121.54(80), 1
packet
05:33:27 denied tcp r.s.236.88(51698) -> a.b.121.51(80), 1
packet
05:33:28 denied tcp r.s.236.88(52084) -> a.b.121.101(80), 1
packet
05:33:32 denied tcp r.s.236.88(52162) -> a.b.121.128(80), 1
packet
05:33:34 denied tcp r.s.236.88(52488) -> a.b.121.151(80), 1
packet
05:33:38 denied tcp r.s.236.88(52491) -> a.b.121.154(80), 1
packet
05:33:38 denied tcp r.s.236.88(52497) -> a.b.121.160(80), 1
packet
05:33:41 denied tcp r.s.236.88(53087) -> a.b.121.223(80), 1
packet
05:33:43 denied tcp r.s.236.88(52909) -> a.b.121.201(80), 1
packet
05:33:44 denied tcp r.s.236.88(53091) -> a.b.121.227(80), 1
packet
05:33:45 denied tcp r.s.236.88(53101) -> a.b.121.237(80), 1
packet
05:33:51 denied tcp r.s.236.88(53522) -> a.b.122.3(80), 1
packet
05:33:52 denied tcp r.s.236.88(53520) -> a.b.122.1(80), 1
packet
05:33:54 denied tcp r.s.236.88(53878) -> a.b.122.51(80), 1
packet
05:33:56 denied tcp r.s.236.88(53878) -> a.b.122.51(80), 1
packet
05:33:57 denied tcp r.s.236.88(53978) -> a.b.122.76(80), 1
packet
05:34:00 denied tcp r.s.236.88(54288) -> a.b.122.101(80), 1
packet
05:34:03 denied tcp r.s.236.88(54291) -> a.b.122.104(80), 1
packet
05:34:05 denied tcp r.s.236.88(54622) -> a.b.122.151(80), 1
packet
05:34:09 denied tcp r.s.236.88(54625) -> a.b.122.154(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:34:14 denied tcp r.s.236.88(55025) -> a.b.122.204(80), 1
packet
05:34:16 denied tcp r.s.236.88(55434) -> a.b.123.1(80), 1
packet
05:34:19 denied tcp r.s.236.88(55437) -> a.b.123.4(80), 1
packet
05:34:25 denied tcp r.s.236.88(55948) -> a.b.123.65(80), 1
packet
05:34:30 denied tcp r.s.236.88(56223) -> a.b.123.104(80), 1
packet
05:34:32 denied tcp r.s.236.88(56604) -> a.b.123.151(80), 1
packet
05:34:35 denied tcp r.s.236.88(56631) -> a.b.123.178(80), 1
packet
05:34:38 denied tcp r.s.236.88(57004) -> a.b.123.201(80), 1
packet
05:34:40 denied tcp r.s.236.88(57004) -> a.b.123.201(80), 1
packet
05:34:41 denied tcp r.s.236.88(57026) -> a.b.123.223(80), 1
packet
05:34:41 denied tcp r.s.236.88(57041) -> a.b.123.238(80), 1
packet
05:34:44 denied tcp r.s.236.88(57416) -> a.b.124.1(80), 1
packet
05:34:46 denied tcp r.s.236.88(57416) -> a.b.124.1(80), 1
packet
05:34:47 denied tcp r.s.236.88(57454) -> a.b.124.39(80), 1
packet
05:34:48 denied tcp r.s.236.88(57458) -> a.b.124.43(80), 1
packet
05:34:52 denied tcp r.s.236.88(57822) -> a.b.124.53(80), 1
packet
05:34:58 denied tcp r.s.236.88(58235) -> a.b.124.104(80), 1
packet
05:35:02 denied tcp r.s.236.88(58636) -> a.b.124.151(80), 1
packet
05:35:03 denied tcp r.s.236.88(58674) -> a.b.124.189(80), 1
packet
05:35:08 denied tcp r.s.236.88(59039) -> a.b.124.204(80), 1
packet
05:35:11 denied tcp r.s.236.88(59448) -> a.b.125.1(80), 1
packet
05:35:14 denied tcp r.s.236.88(59450) -> a.b.125.3(80), 1
packet
05:35:16 denied tcp r.s.236.88(59852) -> a.b.125.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:35:19 denied tcp r.s.236.88(59855) -> a.b.125.54(80), 1
packet
05:35:21 denied tcp r.s.236.88(60134) -> a.b.125.101(80), 1
packet
05:35:25 denied tcp r.s.236.88(60137) -> a.b.125.104(80), 1
packet
05:35:26 denied tcp r.s.236.88(60134) -> a.b.125.101(80), 1
packet
05:35:32 denied tcp r.s.236.88(60518) -> a.b.125.151(80), 1
packet
05:35:33 denied tcp r.s.236.88(60918) -> a.b.125.201(80), 1
packet
05:35:37 denied tcp r.s.236.88(60921) -> a.b.125.204(80), 1
packet
05:35:38 denied tcp r.s.236.88(60918) -> a.b.125.201(80), 1
packet
05:35:43 denied tcp r.s.236.88(61438) -> a.b.126.4(80), 1
packet
05:35:43 denied tcp r.s.236.88(61535) -> a.b.126.33(80), 1
packet
05:35:45 denied tcp r.s.236.88(61777) -> a.b.126.51(80), 1
packet
05:35:49 denied tcp r.s.236.88(61892) -> a.b.126.83(80), 1
packet
05:35:51 denied tcp r.s.236.88(62146) -> a.b.126.101(80), 1
packet
05:35:54 denied tcp r.s.236.88(62148) -> a.b.126.103(80), 1
packet
05:36:00 denied tcp r.s.236.88(62553) -> a.b.126.154(80), 1
packet
05:36:00 denied tcp r.s.236.88(62577) -> a.b.126.178(80), 1
packet
05:36:02 denied tcp r.s.236.88(62950) -> a.b.126.201(80), 1
packet
05:36:05 denied tcp r.s.236.88(62965) -> a.b.126.216(80), 1
packet
05:36:11 denied tcp r.s.236.88(63357) -> a.b.127.4(80), 1
packet
05:36:16 denied tcp r.s.236.88(63765) -> a.b.127.54(80), 1
packet
05:36:18 denied tcp r.s.236.88(64178) -> a.b.127.101(80), 1
packet
05:36:22 denied tcp r.s.236.88(64178) -> a.b.127.101(80), 1
packet
05:36:23 denied tcp r.s.236.88(64582) -> a.b.127.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:36:27 denied tcp r.s.236.88(64585) -> a.b.127.154(80), 1
packet
05:36:29 denied tcp r.s.236.88(64982) -> a.b.127.201(80), 1
packet
05:36:33 denied tcp r.s.236.88(64982) -> a.b.127.201(80), 1
packet
05:36:34 denied tcp r.s.236.88(65386) -> a.b.128.1(80), 1
packet
05:36:38 denied tcp r.s.236.88(65389) -> a.b.128.4(80), 1
packet
05:36:40 denied tcp r.s.236.88(33034) -> a.b.128.51(80), 1
packet
05:36:43 denied tcp r.s.236.88(33037) -> a.b.128.54(80), 1
packet
05:36:45 denied tcp r.s.236.88(33385) -> a.b.128.101(80), 1
packet
05:36:49 denied tcp r.s.236.88(33385) -> a.b.128.101(80), 1
packet
05:36:51 denied tcp r.s.236.88(33683) -> a.b.128.151(80), 1
packet
05:36:55 denied tcp r.s.236.88(33686) -> a.b.128.154(80), 1
packet
05:36:57 denied tcp r.s.236.88(34300) -> a.b.128.247(80), 1
packet
05:37:01 denied tcp r.s.236.88(34248) -> a.b.128.228(80), 1
packet
05:37:03 denied tcp r.s.236.88(34604) -> a.b.129.1(80), 1
packet
05:37:07 denied tcp r.s.236.88(34607) -> a.b.129.4(80), 1
packet
05:37:09 denied tcp r.s.236.88(34985) -> a.b.129.51(80), 1
packet
05:37:12 denied tcp r.s.236.88(34987) -> a.b.129.53(80), 1
packet
05:37:15 denied tcp r.s.236.88(35342) -> a.b.129.101(80), 1
packet
05:37:19 denied tcp r.s.236.88(35342) -> a.b.129.101(80), 1
packet
05:37:21 denied tcp r.s.236.88(35736) -> a.b.129.151(80), 1
packet
05:37:24 denied tcp r.s.236.88(35739) -> a.b.129.154(80), 1
packet
05:37:26 denied tcp r.s.236.88(36136) -> a.b.129.201(80), 1
packet
05:37:29 denied tcp r.s.236.88(36139) -> a.b.129.204(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:37:31 denied tcp r.s.236.88(36540) -> a.b.130.1(80), 1
packet
05:37:35 denied tcp r.s.236.88(36542) -> a.b.130.3(80), 1
packet
05:37:37 denied tcp r.s.236.88(36948) -> a.b.130.51(80), 1
packet
05:37:40 denied tcp r.s.236.88(36951) -> a.b.130.54(80), 1
packet
05:37:45 denied tcp r.s.236.88(37355) -> a.b.130.104(80), 1
packet
05:37:47 denied tcp r.s.236.88(37768) -> a.b.130.151(80), 1
packet
05:37:51 denied tcp r.s.236.88(37770) -> a.b.130.153(80), 1
packet
05:37:53 denied tcp r.s.236.88(38168) -> a.b.130.201(80), 1
packet
05:37:57 denied tcp r.s.236.88(38168) -> a.b.130.201(80), 1
packet
05:37:58 denied tcp r.s.236.88(38572) -> a.b.131.1(80), 1
packet
05:38:01 denied tcp r.s.236.88(38575) -> a.b.131.4(80), 1
packet
05:38:06 denied tcp r.s.236.88(38835) -> a.b.131.51(80), 1
packet
05:38:07 denied tcp r.s.236.88(38974) -> a.b.131.100(80), 1
packet
05:38:08 denied tcp r.s.236.88(38974) -> a.b.131.100(80), 1
packet
05:38:09 denied tcp r.s.236.88(39219) -> a.b.131.101(80), 1
packet
05:38:12 denied tcp r.s.236.88(39219) -> a.b.131.101(80), 1
packet
05:38:13 denied tcp r.s.236.88(39319) -> a.b.131.115(80), 1
packet
05:38:16 denied tcp r.s.236.88(39538) -> a.b.131.151(80), 1
packet
05:38:18 denied tcp r.s.236.88(39538) -> a.b.131.151(80), 1
packet
05:38:19 denied tcp r.s.236.88(39663) -> a.b.131.173(80), 1
packet
05:38:22 denied tcp r.s.236.88(40049) -> a.b.131.250(80), 1
packet
05:38:25 denied tcp r.s.236.88(39973) -> a.b.131.203(80), 1
packet
05:38:26 denied tcp r.s.236.88(39971) -> a.b.131.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:38:29 denied tcp r.s.236.88(40560) -> a.b.132.1(80), 1
packet
05:38:32 denied tcp r.s.236.88(40563) -> a.b.132.4(80), 1
packet
05:38:35 denied tcp r.s.236.88(40931) -> a.b.132.51(80), 1
packet
05:38:38 denied tcp r.s.236.88(40934) -> a.b.132.54(80), 1
packet
05:38:39 denied tcp r.s.236.88(40931) -> a.b.132.51(80), 1
packet
05:38:41 denied tcp r.s.236.88(41368) -> a.b.132.101(80), 1
packet
05:38:47 denied tcp r.s.236.88(41782) -> a.b.132.151(80), 1
packet
05:38:51 denied tcp r.s.236.88(41785) -> a.b.132.154(80), 1
packet
05:38:52 denied tcp r.s.236.88(41782) -> a.b.132.151(80), 1
packet
05:38:53 denied tcp r.s.236.88(42182) -> a.b.132.201(80), 1
packet
05:38:56 denied tcp r.s.236.88(42185) -> a.b.132.204(80), 1
packet
05:38:57 denied tcp r.s.236.88(42182) -> a.b.132.201(80), 1
packet
05:39:04 denied tcp r.s.236.88(42646) -> a.b.133.1(80), 1
packet
05:39:05 denied tcp r.s.236.88(43037) -> a.b.133.51(80), 1
packet
05:39:10 denied tcp r.s.236.88(43037) -> a.b.133.51(80), 1
packet
05:39:11 denied tcp r.s.236.88(43398) -> a.b.133.101(80), 1
packet
05:39:14 denied tcp r.s.236.88(43398) -> a.b.133.101(80), 1
packet
05:39:15 denied tcp r.s.236.88(43814) -> a.b.133.151(80), 1
packet
05:39:19 denied tcp r.s.236.88(43817) -> a.b.133.154(80), 1
packet
05:39:24 denied tcp r.s.236.88(44216) -> a.b.133.203(80), 1
packet
05:39:26 denied tcp r.s.236.88(44668) -> a.b.134.1(80), 1
packet
05:39:29 denied tcp r.s.236.88(44671) -> a.b.134.4(80), 1
packet
05:39:32 denied tcp r.s.236.88(45076) -> a.b.134.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:39:34 denied tcp r.s.236.88(45076) -> a.b.134.51(80), 1
packet
05:39:35 denied tcp r.s.236.88(45085) -> a.b.134.60(80), 1
packet
05:39:37 denied tcp r.s.236.88(45430) -> a.b.134.101(80), 1
packet
05:39:40 denied tcp r.s.236.88(45433) -> a.b.134.104(80), 1
packet
05:39:42 denied tcp r.s.236.88(45846) -> a.b.134.151(80), 1
packet
05:39:46 denied tcp r.s.236.88(45849) -> a.b.134.154(80), 1
packet
05:39:51 denied tcp r.s.236.88(46249) -> a.b.134.204(80), 1
packet
05:39:54 denied tcp r.s.236.88(46700) -> a.b.135.1(80), 1
packet
05:39:58 denied tcp r.s.236.88(46700) -> a.b.135.1(80), 1
packet
05:40:00 denied tcp r.s.236.88(47108) -> a.b.135.51(80), 1
packet
05:40:03 denied tcp r.s.236.88(47109) -> a.b.135.52(80), 1
packet
05:40:08 denied tcp r.s.236.88(47485) -> a.b.135.103(80), 1
packet
05:40:10 denied tcp r.s.236.88(47878) -> a.b.135.151(80), 1
packet
05:40:14 denied tcp r.s.236.88(47881) -> a.b.135.154(80), 1
packet
05:40:16 denied tcp r.s.236.88(48165) -> a.b.135.201(80), 1
packet
05:40:18 denied tcp r.s.236.88(48165) -> a.b.135.201(80), 1
packet
05:40:19 denied tcp r.s.236.88(48281) -> a.b.135.228(80), 1
packet
05:40:22 denied tcp r.s.236.88(48659) -> a.b.136.1(80), 1
packet
05:40:25 denied tcp r.s.236.88(48662) -> a.b.136.4(80), 1
packet
05:40:28 denied tcp r.s.236.88(49218) -> a.b.136.96(80), 1
packet
05:40:31 denied tcp r.s.236.88(49013) -> a.b.136.53(80), 1
packet
05:40:32 denied tcp r.s.236.88(49011) -> a.b.136.51(80), 1
packet
05:40:34 denied tcp r.s.236.88(49394) -> a.b.136.101(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:40:37 denied tcp r.s.236.88(49517) -> a.b.136.134(80), 1
packet
05:40:40 denied tcp r.s.236.88(49798) -> a.b.136.151(80), 1
packet
05:40:43 denied tcp r.s.236.88(49801) -> a.b.136.154(80), 1
packet
05:40:44 denied tcp r.s.236.88(49798) -> a.b.136.151(80), 1
packet
05:40:46 denied tcp r.s.236.88(50231) -> a.b.136.201(80), 1
packet
05:40:49 denied tcp r.s.236.88(50233) -> a.b.136.203(80), 1
packet
05:40:52 denied tcp r.s.236.88(50664) -> a.b.137.1(80), 1
packet
05:40:56 denied tcp r.s.236.88(50664) -> a.b.137.1(80), 1
packet
05:40:57 denied tcp r.s.236.88(51042) -> a.b.137.51(80), 1
packet
05:41:00 denied tcp r.s.236.88(51045) -> a.b.137.54(80), 1
packet
05:41:03 denied tcp r.s.236.88(51426) -> a.b.137.101(80), 1
packet
05:41:06 denied tcp r.s.236.88(51448) -> a.b.137.123(80), 1
packet
05:41:07 denied tcp r.s.236.88(51448) -> a.b.137.123(80), 1
packet
05:41:09 denied tcp r.s.236.88(51830) -> a.b.137.151(80), 1
packet
05:41:11 denied tcp r.s.236.88(51830) -> a.b.137.151(80), 1
packet
05:41:12 denied tcp r.s.236.88(51852) -> a.b.137.173(80), 1
packet
05:41:14 denied tcp r.s.236.88(52259) -> a.b.137.201(80), 1
packet
05:41:20 denied tcp r.s.236.88(52697) -> a.b.138.1(80), 1
packet
05:41:23 denied tcp r.s.236.88(52700) -> a.b.138.4(80), 1
packet
05:41:25 denied tcp r.s.236.88(53081) -> a.b.138.51(80), 1
packet
05:41:29 denied tcp r.s.236.88(53081) -> a.b.138.51(80), 1
packet
05:41:31 denied tcp r.s.236.88(53459) -> a.b.138.101(80), 1
packet
05:41:34 denied tcp r.s.236.88(53462) -> a.b.138.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:41:36 denied tcp r.s.236.88(53863) -> a.b.138.151(80), 1
packet
05:41:40 denied tcp r.s.236.88(53866) -> a.b.138.154(80), 1
packet
05:41:42 denied tcp r.s.236.88(54256) -> a.b.138.201(80), 1
packet
05:41:45 denied tcp r.s.236.88(54259) -> a.b.138.204(80), 1
packet
05:41:48 denied tcp r.s.236.88(54671) -> a.b.139.1(80), 1
packet
05:41:51 denied tcp r.s.236.88(54674) -> a.b.139.4(80), 1
packet
05:41:54 denied tcp r.s.236.88(54996) -> a.b.139.51(80), 1
packet
05:41:56 denied tcp r.s.236.88(54996) -> a.b.139.51(80), 1
packet
05:41:58 denied tcp r.s.236.88(55145) -> a.b.139.73(80), 1
packet
05:42:00 denied tcp r.s.236.88(55368) -> a.b.139.101(80), 1
packet
05:42:04 denied tcp r.s.236.88(55371) -> a.b.139.104(80), 1
packet
05:42:06 denied tcp r.s.236.88(55695) -> a.b.139.151(80), 1
packet
05:42:14 denied tcp r.s.236.88(56096) -> a.b.139.204(80), 1
packet
05:42:18 denied tcp r.s.236.88(56645) -> a.b.140.45(80), 1
packet
05:42:20 denied tcp r.s.236.88(56471) -> a.b.140.1(80), 1
packet
05:42:21 denied tcp r.s.236.88(56545) -> a.b.140.25(80), 1
packet
05:42:22 denied tcp r.s.236.88(56493) -> a.b.140.23(80), 1
packet
05:42:23 denied tcp r.s.236.88(56911) -> a.b.140.51(80), 1
packet
05:42:26 denied tcp r.s.236.88(56914) -> a.b.140.54(80), 1
packet
05:42:29 denied tcp r.s.236.88(57323) -> a.b.140.101(80), 1
packet
05:42:34 denied tcp r.s.236.88(57727) -> a.b.140.151(80), 1
packet
05:42:38 denied tcp r.s.236.88(57730) -> a.b.140.154(80), 1
packet
05:42:40 denied tcp r.s.236.88(58154) -> a.b.140.201(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:42:43 denied tcp r.s.236.88(58157) -> a.b.140.204(80), 1
packet
05:42:45 denied tcp r.s.236.88(58543) -> a.b.141.1(80), 1
packet
05:42:49 denied tcp r.s.236.88(58546) -> a.b.141.4(80), 1
packet
05:42:51 denied tcp r.s.236.88(58943) -> a.b.141.51(80), 1
packet
05:42:54 denied tcp r.s.236.88(58946) -> a.b.141.54(80), 1
packet
05:42:57 denied tcp r.s.236.88(59381) -> a.b.141.101(80), 1
packet
05:42:59 denied tcp r.s.236.88(59381) -> a.b.141.101(80), 1
packet
05:43:00 denied tcp r.s.236.88(59427) -> a.b.141.127(80), 1
packet
05:43:02 denied tcp r.s.236.88(59759) -> a.b.141.151(80), 1
packet
05:43:05 denied tcp r.s.236.88(59762) -> a.b.141.154(80), 1
packet
05:43:07 denied tcp r.s.236.88(60184) -> a.b.141.201(80), 1
packet
05:43:11 denied tcp r.s.236.88(60186) -> a.b.141.203(80), 1
packet
05:43:17 denied tcp r.s.236.88(60578) -> a.b.142.4(80), 1
packet
05:43:19 denied tcp r.s.236.88(60975) -> a.b.142.51(80), 1
packet
05:43:22 denied tcp r.s.236.88(60978) -> a.b.142.54(80), 1
packet
05:43:28 denied tcp r.s.236.88(61390) -> a.b.142.104(80), 1
packet
05:43:30 denied tcp r.s.236.88(61762) -> a.b.142.151(80), 1
packet
05:43:33 denied tcp r.s.236.88(61764) -> a.b.142.153(80), 1
packet
05:43:34 denied tcp r.s.236.88(61762) -> a.b.142.151(80), 1
packet
05:43:36 denied tcp r.s.236.88(62145) -> a.b.142.201(80), 1
packet
05:43:39 denied tcp r.s.236.88(62148) -> a.b.142.204(80), 1
packet
05:43:42 denied tcp r.s.236.88(62633) -> a.b.143.1(80), 1
packet
05:43:45 denied tcp r.s.236.88(62636) -> a.b.143.4(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
05:43:47 denied tcp r.s.236.88(63016) -> a.b.143.60(80), 1
packet
05:43:52 denied tcp r.s.236.88(63073) -> a.b.143.77(80), 1
packet
05:43:54 denied tcp r.s.236.88(63441) -> a.b.143.101(80), 1
packet
05:43:57 denied tcp r.s.236.88(63443) -> a.b.143.103(80), 1
packet
05:44:00 denied tcp r.s.236.88(63833) -> a.b.143.151(80), 1
packet
05:44:02 denied tcp r.s.236.88(63833) -> a.b.143.151(80), 1
packet
05:44:03 denied tcp r.s.236.88(63839) -> a.b.143.157(80), 1
packet
05:44:05 denied tcp r.s.236.88(64248) -> a.b.143.201(80), 1
packet
05:44:09 denied tcp r.s.236.88(64251) -> a.b.143.204(80), 1
packet
05:44:10 denied tcp r.s.236.88(64335) -> a.b.143.241(80), 1
packet
05:44:16 denied tcp r.s.236.88(64760) -> a.b.144.1(80), 1
packet
05:44:21 denied tcp r.s.236.88(65146) -> a.b.144.54(80), 1
packet
05:44:27 denied tcp r.s.236.88(32811) -> a.b.144.101(80), 1
packet
05:44:28 denied tcp r.s.236.88(33045) -> a.b.144.151(80), 1
packet
05:44:31 denied tcp r.s.236.88(33045) -> a.b.144.151(80), 1
packet
05:44:32 denied tcp r.s.236.88(33146) -> a.b.144.196(80), 1
packet
05:44:34 denied tcp r.s.236.88(33494) -> a.b.144.201(80), 1
packet
05:44:37 denied tcp r.s.236.88(33494) -> a.b.144.201(80), 1
packet
05:44:38 denied tcp r.s.236.88(33659) -> a.b.144.228(80), 1
packet
05:44:44 denied tcp r.s.236.88(33965) -> a.b.145.4(80), 1
packet
05:44:47 denied tcp r.s.236.88(34282) -> a.b.145.51(80), 1
packet
05:44:49 denied tcp r.s.236.88(34282) -> a.b.145.51(80), 1
packet
05:44:50 denied tcp r.s.236.88(34422) -> a.b.145.77(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:44:52 denied tcp r.s.236.88(34690) -> a.b.145.101(80), 1
packet
05:44:55 denied tcp r.s.236.88(34690) -> a.b.145.101(80), 1
packet
05:44:56 denied tcp r.s.236.88(34812) -> a.b.145.127(80), 1
packet
05:45:02 denied tcp r.s.236.88(35101) -> a.b.145.153(80), 1
packet
05:45:05 denied tcp r.s.236.88(35505) -> a.b.145.201(80), 1
packet
05:45:07 denied tcp r.s.236.88(35505) -> a.b.145.201(80), 1
packet
05:45:08 denied tcp r.s.236.88(35576) -> a.b.145.234(80), 1
packet
05:45:08 denied tcp r.s.236.88(35719) -> a.b.145.253(80), 1
packet
05:45:11 denied tcp r.s.236.88(36042) -> a.b.146.1(80), 1
packet
05:45:15 denied tcp r.s.236.88(36042) -> a.b.146.1(80), 1
packet
05:45:17 denied tcp r.s.236.88(36384) -> a.b.146.51(80), 1
packet
05:45:20 denied tcp r.s.236.88(36387) -> a.b.146.54(80), 1
packet
05:45:20 denied tcp r.s.236.88(36538) -> a.b.146.95(80), 1
packet
05:45:26 denied tcp r.s.236.88(36758) -> a.b.146.104(80), 1
packet
05:45:28 denied tcp r.s.236.88(37159) -> a.b.146.151(80), 1
packet
05:45:32 denied tcp r.s.236.88(37162) -> a.b.146.154(80), 1
packet
05:45:36 denied tcp r.s.236.88(37567) -> a.b.146.201(80), 1
packet
05:45:38 denied tcp r.s.236.88(37702) -> a.b.146.248(80), 1
packet
05:45:40 denied tcp r.s.236.88(38075) -> a.b.147.1(80), 1
packet
05:45:43 denied tcp r.s.236.88(38077) -> a.b.147.3(80), 1
packet
05:45:48 denied tcp r.s.236.88(38475) -> a.b.147.51(80), 1
packet
05:45:49 denied tcp r.s.236.88(38566) -> a.b.147.100(80), 1
packet
05:45:51 denied tcp r.s.236.88(38891) -> a.b.147.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:45:54 denied tcp r.s.236.88(38891) -> a.b.147.101(80), 1
packet
05:45:55 denied tcp r.s.236.88(38938) -> a.b.147.127(80), 1
packet
05:45:57 denied tcp r.s.236.88(39291) -> a.b.147.151(80), 1
packet
05:45:59 denied tcp r.s.236.88(39291) -> a.b.147.151(80), 1
packet
05:46:00 denied tcp r.s.236.88(39333) -> a.b.147.173(80), 1
packet
05:46:03 denied tcp r.s.236.88(39726) -> a.b.147.201(80), 1
packet
05:46:06 denied tcp r.s.236.88(39729) -> a.b.147.204(80), 1
packet
05:46:07 denied tcp r.s.236.88(39726) -> a.b.147.201(80), 1
packet
05:46:09 denied tcp r.s.236.88(40160) -> a.b.148.1(80), 1
packet
05:46:12 denied tcp r.s.236.88(40163) -> a.b.148.4(80), 1
packet
05:46:15 denied tcp r.s.236.88(40544) -> a.b.148.51(80), 1
packet
05:46:17 denied tcp r.s.236.88(40544) -> a.b.148.51(80), 1
packet
05:46:18 denied tcp r.s.236.88(40617) -> a.b.148.78(80), 1
packet
05:46:24 denied tcp r.s.236.88(40978) -> a.b.148.103(80), 1
packet
05:46:26 denied tcp r.s.236.88(41349) -> a.b.148.151(80), 1
packet
05:46:29 denied tcp r.s.236.88(41349) -> a.b.148.151(80), 1
packet
05:46:30 denied tcp r.s.236.88(41517) -> a.b.148.198(80), 1
packet
05:46:33 denied tcp r.s.236.88(41752) -> a.b.148.201(80), 1
packet
05:46:35 denied tcp r.s.236.88(41752) -> a.b.148.201(80), 1
packet
05:46:36 denied tcp r.s.236.88(41773) -> a.b.148.222(80), 1
packet
05:46:38 denied tcp r.s.236.88(42158) -> a.b.149.1(80), 1
packet
05:46:42 denied tcp r.s.236.88(42161) -> a.b.149.4(80), 1
packet
05:46:44 denied tcp r.s.236.88(42589) -> a.b.149.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:46:46 denied tcp r.s.236.88(42589) -> a.b.149.51(80), 1
packet
05:46:47 denied tcp r.s.236.88(42633) -> a.b.149.95(80), 1
packet
05:46:49 denied tcp r.s.236.88(43005) -> a.b.149.101(80), 1
packet
05:46:53 denied tcp r.s.236.88(43008) -> a.b.149.104(80), 1
packet
05:46:53 denied tcp r.s.236.88(43038) -> a.b.149.134(80), 1
packet
05:46:55 denied tcp r.s.236.88(43430) -> a.b.149.151(80), 1
packet
05:46:58 denied tcp r.s.236.88(43431) -> a.b.149.152(80), 1
packet
05:47:01 denied tcp r.s.236.88(43857) -> a.b.149.201(80), 1
packet
05:47:04 denied tcp r.s.236.88(43860) -> a.b.149.204(80), 1
packet
05:47:05 denied tcp r.s.236.88(43857) -> a.b.149.201(80), 1
packet
05:47:07 denied tcp r.s.236.88(44296) -> a.b.150.1(80), 1
packet
05:47:10 denied tcp r.s.236.88(44296) -> a.b.150.1(80), 1
packet
05:47:11 denied tcp r.s.236.88(44414) -> a.b.150.44(80), 1
packet
05:47:12 denied tcp r.s.236.88(44468) -> a.b.150.48(80), 1
packet
05:47:13 denied tcp r.s.236.88(44666) -> a.b.150.51(80), 1
packet
05:47:16 denied tcp r.s.236.88(44669) -> a.b.150.54(80), 1
packet
05:47:18 denied tcp r.s.236.88(44666) -> a.b.150.51(80), 1
packet
05:47:19 denied tcp r.s.236.88(45037) -> a.b.150.101(80), 1
packet
05:47:23 denied tcp r.s.236.88(45040) -> a.b.150.104(80), 1
packet
05:47:25 denied tcp r.s.236.88(45441) -> a.b.150.151(80), 1
packet
05:47:28 denied tcp r.s.236.88(45443) -> a.b.150.153(80), 1
packet
05:47:30 denied tcp r.s.236.88(45845) -> a.b.150.201(80), 1
packet
05:47:34 denied tcp r.s.236.88(45848) -> a.b.150.204(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:47:39 denied tcp r.s.236.88(46256) -> a.b.151.4(80), 1
packet
05:47:41 denied tcp r.s.236.88(46653) -> a.b.151.51(80), 1
packet
05:47:44 denied tcp r.s.236.88(46656) -> a.b.151.54(80), 1
packet
05:47:46 denied tcp r.s.236.88(47069) -> a.b.151.101(80), 1
packet
05:47:49 denied tcp r.s.236.88(47072) -> a.b.151.104(80), 1
packet
05:47:52 denied tcp r.s.236.88(47248) -> a.b.151.151(80), 1
packet
05:47:55 denied tcp r.s.236.88(47269) -> a.b.151.172(80), 1
packet
05:47:56 denied tcp r.s.236.88(47264) -> a.b.151.167(80), 1
packet
05:47:58 denied tcp r.s.236.88(47753) -> a.b.151.201(80), 1
packet
05:48:01 denied tcp r.s.236.88(47756) -> a.b.151.204(80), 1
packet
05:48:01 denied tcp r.s.236.88(47859) -> a.b.151.243(80), 1
packet
05:48:04 denied tcp r.s.236.88(48209) -> a.b.152.1(80), 1
packet
05:48:07 denied tcp r.s.236.88(48212) -> a.b.152.4(80), 1
packet
05:48:08 denied tcp r.s.236.88(48209) -> a.b.152.1(80), 1
packet
05:48:09 denied tcp r.s.236.88(48506) -> a.b.152.51(80), 1
packet
05:48:13 denied tcp r.s.236.88(48508) -> a.b.152.53(80), 1
packet
05:48:14 denied tcp r.s.236.88(48506) -> a.b.152.51(80), 1
packet
05:48:16 denied tcp r.s.236.88(49017) -> a.b.152.101(80), 1
packet
05:48:19 denied tcp r.s.236.88(49020) -> a.b.152.104(80), 1
packet
05:48:22 denied tcp r.s.236.88(49326) -> a.b.152.151(80), 1
packet
05:48:25 denied tcp r.s.236.88(49328) -> a.b.152.153(80), 1
packet
05:48:26 denied tcp r.s.236.88(49326) -> a.b.152.151(80), 1
packet
05:48:29 denied tcp r.s.236.88(49952) -> a.b.152.235(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:48:32 denied tcp r.s.236.88(49737) -> a.b.152.204(80), 1
packet
05:48:33 denied tcp r.s.236.88(49734) -> a.b.152.201(80), 1
packet
05:48:35 denied tcp r.s.236.88(50295) -> a.b.153.1(80), 1
packet
05:48:37 denied tcp r.s.236.88(50295) -> a.b.153.1(80), 1
packet
05:48:38 denied tcp r.s.236.88(50302) -> a.b.153.8(80), 1
packet
05:48:38 denied tcp r.s.236.88(50357) -> a.b.153.21(80), 1
packet
05:48:41 denied tcp r.s.236.88(50634) -> a.b.153.51(80), 1
packet
05:48:44 denied tcp r.s.236.88(50636) -> a.b.153.53(80), 1
packet
05:48:50 denied tcp r.s.236.88(51039) -> a.b.153.104(80), 1
packet
05:48:52 denied tcp r.s.236.88(51036) -> a.b.153.101(80), 1
packet
05:48:56 denied tcp r.s.236.88(51435) -> a.b.153.151(80), 1
packet
05:48:57 denied tcp r.s.236.88(51526) -> a.b.153.178(80), 1
packet
05:49:02 denied tcp r.s.236.88(51855) -> a.b.153.201(80), 1
packet
05:49:03 denied tcp r.s.236.88(52011) -> a.b.153.226(80), 1
packet
05:49:07 denied tcp r.s.236.88(52401) -> a.b.154.1(80), 1
packet
05:49:10 denied tcp r.s.236.88(52475) -> a.b.154.28(80), 1
packet
05:49:12 denied tcp r.s.236.88(52667) -> a.b.154.51(80), 1
packet
05:49:15 denied tcp r.s.236.88(52667) -> a.b.154.51(80), 1
packet
05:49:16 denied tcp r.s.236.88(52828) -> a.b.154.77(80), 1
packet
05:49:19 denied tcp r.s.236.88(53105) -> a.b.154.101(80), 1
packet
05:49:22 denied tcp r.s.236.88(53255) -> a.b.154.139(80), 1
packet
05:49:23 denied tcp r.s.236.88(53240) -> a.b.154.124(80), 1
packet
05:49:25 denied tcp r.s.236.88(53471) -> a.b.154.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:49:29 denied tcp r.s.236.88(53474) -> a.b.154.154(80), 1
packet
05:49:31 denied tcp r.s.236.88(53996) -> a.b.154.201(80), 1
packet
05:49:34 denied tcp r.s.236.88(53996) -> a.b.154.201(80), 1
packet
05:49:35 denied tcp r.s.236.88(54141) -> a.b.154.226(80), 1
packet
05:49:38 denied tcp r.s.236.88(54567) -> a.b.155.1(80), 1
packet
05:49:42 denied tcp r.s.236.88(54570) -> a.b.155.4(80), 1
packet
05:49:44 denied tcp r.s.236.88(54804) -> a.b.155.51(80), 1
packet
05:49:47 denied tcp r.s.236.88(54807) -> a.b.155.54(80), 1
packet
05:49:49 denied tcp r.s.236.88(54804) -> a.b.155.51(80), 1
packet
05:49:51 denied tcp r.s.236.88(55498) -> a.b.155.147(80), 1
packet
05:49:53 denied tcp r.s.236.88(55240) -> a.b.155.101(80), 1
packet
05:49:54 denied tcp r.s.236.88(55375) -> a.b.155.146(80), 1
packet
05:49:55 denied tcp r.s.236.88(55499) -> a.b.155.148(80), 1
packet
05:49:56 denied tcp r.s.236.88(55603) -> a.b.155.151(80), 1
packet
05:49:59 denied tcp r.s.236.88(55603) -> a.b.155.151(80), 1
packet
05:50:00 denied tcp r.s.236.88(55884) -> a.b.155.200(80), 1
packet
05:50:02 denied tcp r.s.236.88(56057) -> a.b.155.201(80), 1
packet
05:50:05 denied tcp r.s.236.88(56057) -> a.b.155.201(80), 1
packet
05:50:06 denied tcp r.s.236.88(56277) -> a.b.155.247(80), 1
packet
05:50:09 denied tcp r.s.236.88(56668) -> a.b.156.23(80), 1
packet
05:50:12 denied tcp r.s.236.88(56626) -> a.b.156.4(80), 1
packet
05:50:14 denied tcp r.s.236.88(56995) -> a.b.156.51(80), 1
packet
05:50:18 denied tcp r.s.236.88(56998) -> a.b.156.54(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:50:20 denied tcp r.s.236.88(57382) -> a.b.156.101(80), 1
packet
05:50:23 denied tcp r.s.236.88(57385) -> a.b.156.104(80), 1
packet
05:50:25 denied tcp r.s.236.88(57739) -> a.b.156.151(80), 1
packet
05:50:28 denied tcp r.s.236.88(57739) -> a.b.156.151(80), 1
packet
05:50:29 denied tcp r.s.236.88(57844) -> a.b.156.200(80), 1
packet
05:50:34 denied tcp r.s.236.88(58142) -> a.b.156.204(80), 1
packet
05:50:35 denied tcp r.s.236.88(58139) -> a.b.156.201(80), 1
packet
05:50:42 denied tcp r.s.236.88(58747) -> a.b.157.1(80), 1
packet
05:50:43 denied tcp r.s.236.88(58977) -> a.b.157.51(80), 1
packet
05:50:46 denied tcp r.s.236.88(58977) -> a.b.157.51(80), 1
packet
05:50:47 denied tcp r.s.236.88(59127) -> a.b.157.78(80), 1
packet
05:50:49 denied tcp r.s.236.88(59363) -> a.b.157.101(80), 1
packet
05:50:53 denied tcp r.s.236.88(59366) -> a.b.157.104(80), 1
packet
05:50:55 denied tcp r.s.236.88(59771) -> a.b.157.151(80), 1
packet
05:50:58 denied tcp r.s.236.88(59774) -> a.b.157.154(80), 1
packet
05:51:00 denied tcp r.s.236.88(60171) -> a.b.157.201(80), 1
packet
05:51:04 denied tcp r.s.236.88(60174) -> a.b.157.204(80), 1
packet
05:51:09 denied tcp r.s.236.88(60582) -> a.b.158.4(80), 1
packet
05:51:11 denied tcp r.s.236.88(60983) -> a.b.158.51(80), 1
packet
05:51:14 denied tcp r.s.236.88(60986) -> a.b.158.54(80), 1
packet
05:51:22 denied tcp r.s.236.88(61804) -> a.b.158.151(80), 1
packet
05:51:25 denied tcp r.s.236.88(61807) -> a.b.158.154(80), 1
packet
05:51:27 denied tcp r.s.236.88(62100) -> a.b.158.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:51:31 denied tcp r.s.236.88(62103) -> a.b.158.204(80), 1
packet
05:51:33 denied tcp r.s.236.88(62529) -> a.b.159.1(80), 1
packet
05:51:36 denied tcp r.s.236.88(62529) -> a.b.159.1(80), 1
packet
05:51:37 denied tcp r.s.236.88(62550) -> a.b.159.22(80), 1
packet
05:51:38 denied tcp r.s.236.88(62550) -> a.b.159.22(80), 1
packet
05:51:39 denied tcp r.s.236.88(62873) -> a.b.159.51(80), 1
packet
05:51:43 denied tcp r.s.236.88(63014) -> a.b.159.84(80), 1
packet
05:51:48 denied tcp r.s.236.88(63227) -> a.b.159.104(80), 1
packet
05:51:53 denied tcp r.s.236.88(63528) -> a.b.159.151(80), 1
packet
05:51:54 denied tcp r.s.236.88(63656) -> a.b.159.196(80), 1
packet
05:51:56 denied tcp r.s.236.88(63957) -> a.b.159.201(80), 1
packet
05:51:59 denied tcp r.s.236.88(63957) -> a.b.159.201(80), 1
packet
05:52:00 denied tcp r.s.236.88(64050) -> a.b.159.240(80), 1
packet
05:52:02 denied tcp r.s.236.88(64453) -> a.b.160.1(80), 1
packet
05:52:05 denied tcp r.s.236.88(64453) -> a.b.160.1(80), 1
packet
05:52:06 denied tcp r.s.236.88(64539) -> a.b.160.25(80), 1
packet
05:52:08 denied tcp r.s.236.88(64850) -> a.b.160.51(80), 1
packet
05:52:11 denied tcp r.s.236.88(64850) -> a.b.160.51(80), 1
packet
05:52:12 denied tcp r.s.236.88(65032) -> a.b.160.100(80), 1
packet
05:52:13 denied tcp r.s.236.88(65032) -> a.b.160.100(80), 1
packet
05:52:14 denied tcp r.s.236.88(65329) -> a.b.160.101(80), 1
packet
05:52:18 denied tcp r.s.236.88(65332) -> a.b.160.104(80), 1
packet
05:52:20 denied tcp r.s.236.88(32924) -> a.b.160.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:52:23 denied tcp r.s.236.88(32927) -> a.b.160.154(80), 1
packet
05:52:26 denied tcp r.s.236.88(33358) -> a.b.160.201(80), 1
packet
05:52:29 denied tcp r.s.236.88(33361) -> a.b.160.204(80), 1
packet
05:52:30 denied tcp r.s.236.88(33358) -> a.b.160.201(80), 1
packet
05:52:33 denied tcp r.s.236.88(33867) -> a.b.161.1(80), 1
packet
05:52:35 denied tcp r.s.236.88(33867) -> a.b.161.1(80), 1
packet
05:52:36 denied tcp r.s.236.88(33952) -> a.b.161.35(80), 1
packet
05:52:37 denied tcp r.s.236.88(33953) -> a.b.161.36(80), 1
packet
05:52:41 denied tcp r.s.236.88(34260) -> a.b.161.51(80), 1
packet
05:52:42 denied tcp r.s.236.88(34390) -> a.b.161.78(80), 1
packet
05:52:44 denied tcp r.s.236.88(34628) -> a.b.161.101(80), 1
packet
05:52:47 denied tcp r.s.236.88(34628) -> a.b.161.101(80), 1
packet
05:52:48 denied tcp r.s.236.88(34748) -> a.b.161.146(80), 1
packet
05:52:51 denied tcp r.s.236.88(35176) -> a.b.161.173(80), 1
packet
05:52:53 denied tcp r.s.236.88(35083) -> a.b.161.151(80), 1
packet
05:52:54 denied tcp r.s.236.88(35193) -> a.b.161.190(80), 1
packet
05:52:57 denied tcp r.s.236.88(35567) -> a.b.161.229(80), 1
packet
05:52:59 denied tcp r.s.236.88(35479) -> a.b.161.201(80), 1
packet
05:53:00 denied tcp r.s.236.88(35572) -> a.b.161.234(80), 1
packet
05:53:03 denied tcp r.s.236.88(35948) -> a.b.162.1(80), 1
packet
05:53:06 denied tcp r.s.236.88(35951) -> a.b.162.4(80), 1
packet
05:53:08 denied tcp r.s.236.88(36296) -> a.b.162.51(80), 1
packet
05:53:12 denied tcp r.s.236.88(36298) -> a.b.162.53(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:53:14 denied tcp r.s.236.88(36681) -> a.b.162.101(80), 1
packet
05:53:17 denied tcp r.s.236.88(36684) -> a.b.162.104(80), 1
packet
05:53:19 denied tcp r.s.236.88(36681) -> a.b.162.101(80), 1
packet
05:53:20 denied tcp r.s.236.88(37068) -> a.b.162.151(80), 1
packet
05:53:23 denied tcp r.s.236.88(37071) -> a.b.162.154(80), 1
packet
05:53:25 denied tcp r.s.236.88(37068) -> a.b.162.151(80), 1
packet
05:53:29 denied tcp r.s.236.88(37495) -> a.b.162.203(80), 1
packet
05:53:31 denied tcp r.s.236.88(37493) -> a.b.162.201(80), 1
packet
05:53:32 denied tcp r.s.236.88(37953) -> a.b.163.1(80), 1
packet
05:53:37 denied tcp r.s.236.88(37953) -> a.b.163.1(80), 1
packet
05:53:38 denied tcp r.s.236.88(38352) -> a.b.163.51(80), 1
packet
05:53:42 denied tcp r.s.236.88(38508) -> a.b.163.98(80), 1
packet
05:53:44 denied tcp r.s.236.88(38792) -> a.b.163.101(80), 1
packet
05:53:47 denied tcp r.s.236.88(38795) -> a.b.163.104(80), 1
packet
05:53:50 denied tcp r.s.236.88(39200) -> a.b.163.151(80), 1
packet
05:53:53 denied tcp r.s.236.88(39203) -> a.b.163.154(80), 1
packet
05:53:55 denied tcp r.s.236.88(39608) -> a.b.163.201(80), 1
packet
05:53:58 denied tcp r.s.236.88(39611) -> a.b.163.204(80), 1
packet
05:54:04 denied tcp r.s.236.88(40019) -> a.b.164.4(80), 1
packet
05:54:06 denied tcp r.s.236.88(40416) -> a.b.164.51(80), 1
packet
05:54:09 denied tcp r.s.236.88(40419) -> a.b.164.54(80), 1
packet
05:54:11 denied tcp r.s.236.88(40824) -> a.b.164.101(80), 1
packet
05:54:14 denied tcp r.s.236.88(40827) -> a.b.164.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:54:16 denied tcp r.s.236.88(41232) -> a.b.164.151(80), 1
packet
05:54:20 denied tcp r.s.236.88(41235) -> a.b.164.154(80), 1
packet
05:54:22 denied tcp r.s.236.88(41640) -> a.b.164.201(80), 1
packet
05:54:24 denied tcp r.s.236.88(41640) -> a.b.164.201(80), 1
packet
05:54:25 denied tcp r.s.236.88(41667) -> a.b.164.228(80), 1
packet
05:54:28 denied tcp r.s.236.88(41951) -> a.b.165.1(80), 1
packet
05:54:30 denied tcp r.s.236.88(41951) -> a.b.165.1(80), 1
packet
05:54:31 denied tcp r.s.236.88(42088) -> a.b.165.23(80), 1
packet
05:54:34 denied tcp r.s.236.88(42398) -> a.b.165.51(80), 1
packet
05:54:37 denied tcp r.s.236.88(42401) -> a.b.165.54(80), 1
packet
05:54:37 denied tcp r.s.236.88(42582) -> a.b.165.97(80), 1
packet
05:54:40 denied tcp r.s.236.88(42802) -> a.b.165.101(80), 1
packet
05:54:43 denied tcp r.s.236.88(42805) -> a.b.165.104(80), 1
packet
05:54:46 denied tcp r.s.236.88(43218) -> a.b.165.151(80), 1
packet
05:54:49 denied tcp r.s.236.88(43221) -> a.b.165.154(80), 1
packet
05:54:51 denied tcp r.s.236.88(43594) -> a.b.165.201(80), 1
packet
05:54:54 denied tcp r.s.236.88(43597) -> a.b.165.204(80), 1
packet
05:54:57 denied tcp r.s.236.88(44030) -> a.b.166.1(80), 1
packet
05:55:00 denied tcp r.s.236.88(44033) -> a.b.166.4(80), 1
packet
05:55:00 denied tcp r.s.236.88(44207) -> a.b.166.49(80), 1
packet
05:55:03 denied tcp r.s.236.88(44480) -> a.b.166.51(80), 1
packet
05:55:06 denied tcp r.s.236.88(44483) -> a.b.166.54(80), 1
packet
05:55:12 denied tcp r.s.236.88(44938) -> a.b.166.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:55:13 denied tcp r.s.236.88(44935) -> a.b.166.101(80), 1
packet
05:55:15 denied tcp r.s.236.88(45300) -> a.b.166.151(80), 1
packet
05:55:19 denied tcp r.s.236.88(45303) -> a.b.166.154(80), 1
packet
05:55:21 denied tcp r.s.236.88(45955) -> a.b.166.254(80), 1
packet
05:55:24 denied tcp r.s.236.88(45784) -> a.b.166.228(80), 1
packet
05:55:27 denied tcp r.s.236.88(46312) -> a.b.167.1(80), 1
packet
05:55:30 denied tcp r.s.236.88(46315) -> a.b.167.4(80), 1
packet
05:55:35 denied tcp r.s.236.88(46712) -> a.b.167.51(80), 1
packet
05:55:36 denied tcp r.s.236.88(46721) -> a.b.167.60(80), 1
packet
05:55:38 denied tcp r.s.236.88(47060) -> a.b.167.101(80), 1
packet
05:55:41 denied tcp r.s.236.88(47063) -> a.b.167.104(80), 1
packet
05:55:47 denied tcp r.s.236.88(47484) -> a.b.167.153(80), 1
packet
05:55:47 denied tcp r.s.236.88(47537) -> a.b.167.180(80), 1
packet
05:55:50 denied tcp r.s.236.88(47924) -> a.b.167.201(80), 1
packet
05:55:52 denied tcp r.s.236.88(47924) -> a.b.167.201(80), 1
packet
05:55:53 denied tcp r.s.236.88(47985) -> a.b.167.224(80), 1
packet
05:55:56 denied tcp r.s.236.88(48394) -> a.b.168.1(80), 1
packet
05:55:59 denied tcp r.s.236.88(48397) -> a.b.168.4(80), 1
packet
05:56:01 denied tcp r.s.236.88(48814) -> a.b.168.83(80), 1
packet
05:56:04 denied tcp r.s.236.88(48694) -> a.b.168.51(80), 1
packet
05:56:05 denied tcp r.s.236.88(48819) -> a.b.168.88(80), 1
packet
05:56:07 denied tcp r.s.236.88(49157) -> a.b.168.101(80), 1
packet
05:56:11 denied tcp r.s.236.88(49234) -> a.b.168.146(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:56:12 denied tcp r.s.236.88(49319) -> a.b.168.148(80), 1
packet
05:56:13 denied tcp r.s.236.88(49537) -> a.b.168.151(80), 1
packet
05:56:16 denied tcp r.s.236.88(49537) -> a.b.168.151(80), 1
packet
05:56:17 denied tcp r.s.236.88(49710) -> a.b.168.197(80), 1
packet
05:56:19 denied tcp r.s.236.88(49918) -> a.b.168.201(80), 1
packet
05:56:22 denied tcp r.s.236.88(49918) -> a.b.168.201(80), 1
packet
05:56:23 denied tcp r.s.236.88(50125) -> a.b.168.245(80), 1
packet
05:56:26 denied tcp r.s.236.88(50578) -> a.b.169.1(80), 1
packet
05:56:29 denied tcp r.s.236.88(50580) -> a.b.169.3(80), 1
packet
05:56:32 denied tcp r.s.236.88(50891) -> a.b.169.51(80), 1
packet
05:56:35 denied tcp r.s.236.88(51044) -> a.b.169.82(80), 1
packet
05:56:42 denied tcp r.s.236.88(51312) -> a.b.169.128(80), 1
packet
05:56:44 denied tcp r.s.236.88(51617) -> a.b.169.151(80), 1
packet
05:56:47 denied tcp r.s.236.88(51618) -> a.b.169.152(80), 1
packet
05:56:49 denied tcp r.s.236.88(52000) -> a.b.169.201(80), 1
packet
05:56:53 denied tcp r.s.236.88(52002) -> a.b.169.203(80), 1
packet
05:56:56 denied tcp r.s.236.88(52619) -> a.b.170.1(80), 1
packet
05:56:59 denied tcp r.s.236.88(52622) -> a.b.170.4(80), 1
packet
05:57:02 denied tcp r.s.236.88(52986) -> a.b.170.51(80), 1
packet
05:57:04 denied tcp r.s.236.88(52986) -> a.b.170.51(80), 1
packet
05:57:06 denied tcp r.s.236.88(53108) -> a.b.170.77(80), 1
packet
05:57:09 denied tcp r.s.236.88(53470) -> a.b.170.123(80), 1
packet
05:57:11 denied tcp r.s.236.88(53345) -> a.b.170.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:57:12 denied tcp r.s.236.88(53595) -> a.b.170.149(80), 1
packet
05:57:13 denied tcp r.s.236.88(53596) -> a.b.170.150(80), 1
packet
05:57:14 denied tcp r.s.236.88(53738) -> a.b.170.151(80), 1
packet
05:57:17 denied tcp r.s.236.88(53738) -> a.b.170.151(80), 1
packet
05:57:18 denied tcp r.s.236.88(53963) -> a.b.170.188(80), 1
packet
05:57:21 denied tcp r.s.236.88(54181) -> a.b.170.201(80), 1
packet
05:57:23 denied tcp r.s.236.88(54181) -> a.b.170.201(80), 1
packet
05:57:24 denied tcp r.s.236.88(54202) -> a.b.170.222(80), 1
packet
05:57:27 denied tcp r.s.236.88(54735) -> a.b.171.1(80), 1
packet
05:57:33 denied tcp r.s.236.88(54995) -> a.b.171.51(80), 1
packet
05:57:36 denied tcp r.s.236.88(54998) -> a.b.171.54(80), 1
packet
05:57:37 denied tcp r.s.236.88(54995) -> a.b.171.51(80), 1
packet
05:57:38 denied tcp r.s.236.88(55356) -> a.b.171.101(80), 1
packet
05:57:42 denied tcp r.s.236.88(55358) -> a.b.171.103(80), 1
packet
05:57:44 denied tcp r.s.236.88(55760) -> a.b.171.151(80), 1
packet
05:57:47 denied tcp r.s.236.88(55763) -> a.b.171.154(80), 1
packet
05:57:49 denied tcp r.s.236.88(56164) -> a.b.171.201(80), 1
packet
05:57:52 denied tcp r.s.236.88(56166) -> a.b.171.203(80), 1
packet
05:57:54 denied tcp r.s.236.88(56572) -> a.b.172.1(80), 1
packet
05:57:58 denied tcp r.s.236.88(56575) -> a.b.172.4(80), 1
packet
05:58:00 denied tcp r.s.236.88(56984) -> a.b.172.51(80), 1
packet
05:58:03 denied tcp r.s.236.88(56987) -> a.b.172.54(80), 1
packet
05:58:05 denied tcp r.s.236.88(57388) -> a.b.172.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:58:13 denied tcp r.s.236.88(57592) -> a.b.172.151(80), 1
packet
05:58:14 denied tcp r.s.236.88(57833) -> a.b.172.200(80), 1
packet
05:58:16 denied tcp r.s.236.88(58021) -> a.b.172.201(80), 1
packet
05:58:19 denied tcp r.s.236.88(58021) -> a.b.172.201(80), 1
packet
05:58:20 denied tcp r.s.236.88(58162) -> a.b.172.244(80), 1
packet
05:58:21 denied tcp r.s.236.88(58163) -> a.b.172.245(80), 1
packet
05:58:23 denied tcp r.s.236.88(58486) -> a.b.173.1(80), 1
packet
05:58:25 denied tcp r.s.236.88(58486) -> a.b.173.1(80), 1
packet
05:58:26 denied tcp r.s.236.88(58579) -> a.b.173.12(80), 1
packet
05:58:31 denied tcp r.s.236.88(58856) -> a.b.173.51(80), 1
packet
05:58:32 denied tcp r.s.236.88(58865) -> a.b.173.60(80), 1
packet
05:58:32 denied tcp r.s.236.88(58945) -> a.b.173.65(80), 1
packet
05:58:35 denied tcp r.s.236.88(59216) -> a.b.173.101(80), 1
packet
05:58:39 denied tcp r.s.236.88(59216) -> a.b.173.101(80), 1
packet
05:58:44 denied tcp r.s.236.88(59709) -> a.b.173.154(80), 1
packet
05:58:46 denied tcp r.s.236.88(59706) -> a.b.173.151(80), 1
packet
05:58:47 denied tcp r.s.236.88(60121) -> a.b.173.201(80), 1
packet
05:58:50 denied tcp r.s.236.88(60261) -> a.b.173.229(80), 1
packet
05:58:51 denied tcp r.s.236.88(60369) -> a.b.173.249(80), 1
packet
05:58:52 denied tcp r.s.236.88(60367) -> a.b.173.247(80), 1
packet
05:58:54 denied tcp r.s.236.88(60771) -> a.b.174.23(80), 1
packet
05:58:57 denied tcp r.s.236.88(60623) -> a.b.174.4(80), 1
packet
05:58:58 denied tcp r.s.236.88(60620) -> a.b.174.1(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
05:59:00 denied tcp r.s.236.88(61008) -> a.b.174.51(80), 1
packet
05:59:03 denied tcp r.s.236.88(61008) -> a.b.174.51(80), 1
packet
05:59:08 denied tcp r.s.236.88(61301) -> a.b.174.104(80), 1
packet
05:59:11 denied tcp r.s.236.88(61801) -> a.b.174.197(80), 1
packet
05:59:14 denied tcp r.s.236.88(61754) -> a.b.174.178(80), 1
packet
05:59:16 denied tcp r.s.236.88(62110) -> a.b.174.201(80), 1
packet
05:59:22 denied tcp r.s.236.88(62561) -> a.b.175.23(80), 1
packet
05:59:25 denied tcp r.s.236.88(62521) -> a.b.175.4(80), 1
packet
05:59:26 denied tcp r.s.236.88(62518) -> a.b.175.1(80), 1
packet
05:59:27 denied tcp r.s.236.88(62922) -> a.b.175.51(80), 1
packet
05:59:30 denied tcp r.s.236.88(62925) -> a.b.175.54(80), 1
packet
05:59:32 denied tcp r.s.236.88(63330) -> a.b.175.101(80), 1
packet
05:59:35 denied tcp r.s.236.88(63330) -> a.b.175.101(80), 1
packet
05:59:36 denied tcp r.s.236.88(63377) -> a.b.175.133(80), 1
packet
05:59:38 denied tcp r.s.236.88(63738) -> a.b.175.151(80), 1
packet
05:59:41 denied tcp r.s.236.88(63741) -> a.b.175.154(80), 1
packet
05:59:43 denied tcp r.s.236.88(64142) -> a.b.175.201(80), 1
packet
05:59:47 denied tcp r.s.236.88(64145) -> a.b.175.204(80), 1
packet
05:59:49 denied tcp r.s.236.88(64550) -> a.b.176.1(80), 1
packet
05:59:52 denied tcp r.s.236.88(64550) -> a.b.176.1(80), 1
packet
05:59:56 denied tcp r.s.236.88(64700) -> a.b.176.51(80), 1
packet
05:59:57 denied tcp r.s.236.88(65028) -> a.b.176.100(80), 1
packet
05:59:59 denied tcp r.s.236.88(65158) -> a.b.176.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:00:02 denied tcp r.s.236.88(65161) -> a.b.176.104(80), 1
packet
06:00:04 denied tcp r.s.236.88(32806) -> a.b.176.151(80), 1
packet
06:00:07 denied tcp r.s.236.88(32806) -> a.b.176.151(80), 1
packet
06:00:10 denied tcp r.s.236.88(33214) -> a.b.176.201(80), 1
packet
06:00:13 denied tcp r.s.236.88(33216) -> a.b.176.203(80), 1
packet
06:00:15 denied tcp r.s.236.88(33618) -> a.b.177.1(80), 1
packet
06:00:19 denied tcp r.s.236.88(33625) -> a.b.177.8(80), 1
packet
06:00:21 denied tcp r.s.236.88(34022) -> a.b.177.51(80), 1
packet
06:00:24 denied tcp r.s.236.88(34025) -> a.b.177.54(80), 1
packet
06:00:30 denied tcp r.s.236.88(34432) -> a.b.177.103(80), 1
packet
06:00:35 denied tcp r.s.236.88(34841) -> a.b.177.154(80), 1
packet
06:00:37 denied tcp r.s.236.88(35246) -> a.b.177.201(80), 1
packet
06:00:40 denied tcp r.s.236.88(35249) -> a.b.177.204(80), 1
packet
06:00:43 denied tcp r.s.236.88(35650) -> a.b.178.1(80), 1
packet
06:00:46 denied tcp r.s.236.88(35653) -> a.b.178.4(80), 1
packet
06:00:49 denied tcp r.s.236.88(36054) -> a.b.178.51(80), 1
packet
06:00:51 denied tcp r.s.236.88(36054) -> a.b.178.51(80), 1
packet
06:00:52 denied tcp r.s.236.88(36103) -> a.b.178.100(80), 1
packet
06:00:54 denied tcp r.s.236.88(36102) -> a.b.178.99(80), 1
packet
06:00:58 denied tcp r.s.236.88(36830) -> a.b.178.188(80), 1
packet
06:01:02 denied tcp r.s.236.88(36766) -> a.b.178.151(80), 1
packet
06:01:03 denied tcp r.s.236.88(36914) -> a.b.178.199(80), 1
packet
06:01:04 denied tcp r.s.236.88(36913) -> a.b.178.198(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:01:05 denied tcp r.s.236.88(37074) -> a.b.178.201(80), 1
packet
06:01:09 denied tcp r.s.236.88(37077) -> a.b.178.204(80), 1
packet
06:01:14 denied tcp r.s.236.88(37687) -> a.b.179.1(80), 1
packet
06:01:15 denied tcp r.s.236.88(37690) -> a.b.179.4(80), 1
packet
06:01:17 denied tcp r.s.236.88(37989) -> a.b.179.51(80), 1
packet
06:01:21 denied tcp r.s.236.88(37992) -> a.b.179.54(80), 1
packet
06:01:21 denied tcp r.s.236.88(38004) -> a.b.179.66(80), 1
packet
06:01:23 denied tcp r.s.236.88(38386) -> a.b.179.101(80), 1
packet
06:01:29 denied tcp r.s.236.88(38799) -> a.b.179.151(80), 1
packet
06:01:32 denied tcp r.s.236.88(38800) -> a.b.179.152(80), 1
packet
06:01:34 denied tcp r.s.236.88(38799) -> a.b.179.151(80), 1
packet
06:01:35 denied tcp r.s.236.88(39248) -> a.b.179.201(80), 1
packet
06:01:38 denied tcp r.s.236.88(39251) -> a.b.179.204(80), 1
packet
06:01:41 denied tcp r.s.236.88(39753) -> a.b.180.1(80), 1
packet
06:01:45 denied tcp r.s.236.88(39755) -> a.b.180.3(80), 1
packet
06:01:47 denied tcp r.s.236.88(40019) -> a.b.180.51(80), 1
packet
06:01:49 denied tcp r.s.236.88(40019) -> a.b.180.51(80), 1
packet
06:01:50 denied tcp r.s.236.88(40107) -> a.b.180.78(80), 1
packet
06:01:51 denied tcp r.s.236.88(40102) -> a.b.180.73(80), 1
packet
06:01:53 denied tcp r.s.236.88(40427) -> a.b.180.101(80), 1
packet
06:01:56 denied tcp r.s.236.88(40523) -> a.b.180.123(80), 1
packet
06:01:57 denied tcp r.s.236.88(40623) -> a.b.180.146(80), 1
packet
06:01:59 denied tcp r.s.236.88(40881) -> a.b.180.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:02:02 denied tcp r.s.236.88(40884) -> a.b.180.154(80), 1
packet
06:02:04 denied tcp r.s.236.88(41286) -> a.b.180.201(80), 1
packet
06:02:07 denied tcp r.s.236.88(41286) -> a.b.180.201(80), 1
packet
06:02:08 denied tcp r.s.236.88(41343) -> a.b.180.251(80), 1
packet
06:02:10 denied tcp r.s.236.88(41697) -> a.b.181.1(80), 1
packet
06:02:13 denied tcp r.s.236.88(41699) -> a.b.181.3(80), 1
packet
06:02:14 denied tcp r.s.236.88(41697) -> a.b.181.1(80), 1
packet
06:02:16 denied tcp r.s.236.88(42101) -> a.b.181.51(80), 1
packet
06:02:18 denied tcp r.s.236.88(42101) -> a.b.181.51(80), 1
packet
06:02:19 denied tcp r.s.236.88(42147) -> a.b.181.97(80), 1
packet
06:02:21 denied tcp r.s.236.88(42509) -> a.b.181.101(80), 1
packet
06:02:24 denied tcp r.s.236.88(42509) -> a.b.181.101(80), 1
packet
06:02:25 denied tcp r.s.236.88(42554) -> a.b.181.146(80), 1
packet
06:02:26 denied tcp r.s.236.88(42552) -> a.b.181.144(80), 1
packet
06:02:30 denied tcp r.s.236.88(42916) -> a.b.181.154(80), 1
packet
06:02:32 denied tcp r.s.236.88(43325) -> a.b.181.201(80), 1
packet
06:02:36 denied tcp r.s.236.88(43328) -> a.b.181.204(80), 1
packet
06:02:38 denied tcp r.s.236.88(43729) -> a.b.182.1(80), 1
packet
06:02:41 denied tcp r.s.236.88(43732) -> a.b.182.4(80), 1
packet
06:02:43 denied tcp r.s.236.88(44133) -> a.b.182.51(80), 1
packet
06:02:46 denied tcp r.s.236.88(44136) -> a.b.182.54(80), 1
packet
06:02:48 denied tcp r.s.236.88(44595) -> a.b.182.101(80), 1
packet
06:02:52 denied tcp r.s.236.88(44596) -> a.b.182.102(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:02:54 denied tcp r.s.236.88(44800) -> a.b.182.151(80), 1
packet
06:02:57 denied tcp r.s.236.88(44800) -> a.b.182.151(80), 1
packet
06:02:58 denied tcp r.s.236.88(44908) -> a.b.182.190(80), 1
packet
06:02:59 denied tcp r.s.236.88(45027) -> a.b.182.200(80), 1
packet
06:03:00 denied tcp r.s.236.88(45203) -> a.b.182.201(80), 1
packet
06:03:02 denied tcp r.s.236.88(45203) -> a.b.182.201(80), 1
packet
06:03:04 denied tcp r.s.236.88(45337) -> a.b.182.246(80), 1
packet
06:03:07 denied tcp r.s.236.88(45808) -> a.b.183.1(80), 1
packet
06:03:10 denied tcp r.s.236.88(45811) -> a.b.183.4(80), 1
packet
06:03:13 denied tcp r.s.236.88(46084) -> a.b.183.51(80), 1
packet
06:03:16 denied tcp r.s.236.88(46087) -> a.b.183.54(80), 1
packet
06:03:17 denied tcp r.s.236.88(46084) -> a.b.183.51(80), 1
packet
06:03:19 denied tcp r.s.236.88(46462) -> a.b.183.101(80), 1
packet
06:03:22 denied tcp r.s.236.88(46465) -> a.b.183.104(80), 1
packet
06:03:23 denied tcp r.s.236.88(46462) -> a.b.183.101(80), 1
packet
06:03:25 denied tcp r.s.236.88(46827) -> a.b.183.151(80), 1
packet
06:03:28 denied tcp r.s.236.88(46830) -> a.b.183.154(80), 1
packet
06:03:30 denied tcp r.s.236.88(47261) -> a.b.183.201(80), 1
packet
06:03:32 denied tcp r.s.236.88(47261) -> a.b.183.201(80), 1
packet
06:03:34 denied tcp r.s.236.88(47483) -> a.b.183.249(80), 1
packet
06:03:37 denied tcp r.s.236.88(47482) -> a.b.183.248(80), 1
packet
06:03:40 denied tcp r.s.236.88(47823) -> a.b.184.4(80), 1
packet
06:03:42 denied tcp r.s.236.88(48147) -> a.b.184.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:03:45 denied tcp r.s.236.88(48147) -> a.b.184.51(80), 1
packet
06:03:46 denied tcp r.s.236.88(48234) -> a.b.184.97(80), 1
packet
06:03:48 denied tcp r.s.236.88(48605) -> a.b.184.101(80), 1
packet
06:03:51 denied tcp r.s.236.88(48605) -> a.b.184.101(80), 1
packet
06:03:52 denied tcp r.s.236.88(48699) -> a.b.184.146(80), 1
packet
06:03:53 denied tcp r.s.236.88(48699) -> a.b.184.146(80), 1
packet
06:03:54 denied tcp r.s.236.88(49031) -> a.b.184.151(80), 1
packet
06:03:57 denied tcp r.s.236.88(49031) -> a.b.184.151(80), 1
packet
06:03:58 denied tcp r.s.236.88(49113) -> a.b.184.174(80), 1
packet
06:04:01 denied tcp r.s.236.88(49444) -> a.b.184.201(80), 1
packet
06:04:04 denied tcp r.s.236.88(49446) -> a.b.184.203(80), 1
packet
06:04:07 denied tcp r.s.236.88(49994) -> a.b.185.1(80), 1
packet
06:04:10 denied tcp r.s.236.88(49996) -> a.b.185.3(80), 1
packet
06:04:11 denied tcp r.s.236.88(50040) -> a.b.185.31(80), 1
packet
06:04:13 denied tcp r.s.236.88(50323) -> a.b.185.51(80), 1
packet
06:04:17 denied tcp r.s.236.88(50325) -> a.b.185.53(80), 1
packet
06:04:19 denied tcp r.s.236.88(50681) -> a.b.185.101(80), 1
packet
06:04:22 denied tcp r.s.236.88(50681) -> a.b.185.101(80), 1
packet
06:04:25 denied tcp r.s.236.88(51043) -> a.b.185.151(80), 1
packet
06:04:29 denied tcp r.s.236.88(51046) -> a.b.185.154(80), 1
packet
06:04:31 denied tcp r.s.236.88(51455) -> a.b.185.201(80), 1
packet
06:04:34 denied tcp r.s.236.88(51458) -> a.b.185.204(80), 1
packet
06:04:34 denied tcp r.s.236.88(51481) -> a.b.185.227(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:04:36 denied tcp r.s.236.88(51859) -> a.b.186.1(80), 1
packet
06:04:40 denied tcp r.s.236.88(51906) -> a.b.186.48(80), 1
packet
06:04:42 denied tcp r.s.236.88(52263) -> a.b.186.51(80), 1
packet
06:04:45 denied tcp r.s.236.88(52266) -> a.b.186.54(80), 1
packet
06:04:47 denied tcp r.s.236.88(52655) -> a.b.186.101(80), 1
packet
06:04:50 denied tcp r.s.236.88(52656) -> a.b.186.102(80), 1
packet
06:04:51 denied tcp r.s.236.88(52686) -> a.b.186.132(80), 1
packet
06:04:53 denied tcp r.s.236.88(52975) -> a.b.186.151(80), 1
packet
06:04:56 denied tcp r.s.236.88(52978) -> a.b.186.154(80), 1
packet
06:04:58 denied tcp r.s.236.88(53387) -> a.b.186.201(80), 1
packet
06:05:01 denied tcp r.s.236.88(53390) -> a.b.186.204(80), 1
packet
06:05:03 denied tcp r.s.236.88(53791) -> a.b.187.1(80), 1
packet
06:05:06 denied tcp r.s.236.88(53791) -> a.b.187.1(80), 1
packet
06:05:07 denied tcp r.s.236.88(54047) -> a.b.187.51(80), 1
packet
06:05:10 denied tcp r.s.236.88(54047) -> a.b.187.51(80), 1
packet
06:05:11 denied tcp r.s.236.88(54180) -> a.b.187.77(80), 1
packet
06:05:16 denied tcp r.s.236.88(54448) -> a.b.187.101(80), 1
packet
06:05:17 denied tcp r.s.236.88(54576) -> a.b.187.136(80), 1
packet
06:05:18 denied tcp r.s.236.88(54631) -> a.b.187.143(80), 1
packet
06:05:19 denied tcp r.s.236.88(54883) -> a.b.187.151(80), 1
packet
06:05:22 denied tcp r.s.236.88(54883) -> a.b.187.151(80), 1
packet
06:05:23 denied tcp r.s.236.88(55007) -> a.b.187.176(80), 1
packet
06:05:25 denied tcp r.s.236.88(55291) -> a.b.187.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:05:28 denied tcp r.s.236.88(55291) -> a.b.187.201(80), 1
packet
06:05:29 denied tcp r.s.236.88(55365) -> a.b.187.228(80), 1
packet
06:05:32 denied tcp r.s.236.88(55823) -> a.b.188.1(80), 1
packet
06:05:35 denied tcp r.s.236.88(55826) -> a.b.188.4(80), 1
packet
06:05:38 denied tcp r.s.236.88(56115) -> a.b.188.51(80), 1
packet
06:05:40 denied tcp r.s.236.88(56115) -> a.b.188.51(80), 1
packet
06:05:41 denied tcp r.s.236.88(56281) -> a.b.188.78(80), 1
packet
06:05:44 denied tcp r.s.236.88(56573) -> a.b.188.101(80), 1
packet
06:05:47 denied tcp r.s.236.88(56576) -> a.b.188.104(80), 1
packet
06:05:49 denied tcp r.s.236.88(56573) -> a.b.188.101(80), 1
packet
06:05:50 denied tcp r.s.236.88(56983) -> a.b.188.151(80), 1
packet
06:05:53 denied tcp r.s.236.88(56983) -> a.b.188.151(80), 1
packet
06:05:53 denied tcp r.s.236.88(57098) -> a.b.188.192(80), 1
packet
06:05:55 denied tcp r.s.236.88(57190) -> a.b.188.199(80), 1
packet
06:05:56 denied tcp r.s.236.88(57367) -> a.b.188.206(80), 1
packet
06:05:59 denied tcp r.s.236.88(57362) -> a.b.188.201(80), 1
packet
06:06:01 denied tcp r.s.236.88(57618) -> a.b.188.239(80), 1
packet
06:06:03 denied tcp r.s.236.88(57969) -> a.b.189.1(80), 1
packet
06:06:07 denied tcp r.s.236.88(57972) -> a.b.189.4(80), 1
packet
06:06:09 denied tcp r.s.236.88(58301) -> a.b.189.51(80), 1
packet
06:06:12 denied tcp r.s.236.88(58301) -> a.b.189.51(80), 1
packet
06:06:13 denied tcp r.s.236.88(58431) -> a.b.189.96(80), 1
packet
06:06:15 denied tcp r.s.236.88(58696) -> a.b.189.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:06:18 denied tcp r.s.236.88(58696) -> a.b.189.101(80), 1
packet
06:06:19 denied tcp r.s.236.88(58836) -> a.b.189.128(80), 1
packet
06:06:22 denied tcp r.s.236.88(59145) -> a.b.189.151(80), 1
packet
06:06:25 denied tcp r.s.236.88(59148) -> a.b.189.154(80), 1
packet
06:06:26 denied tcp r.s.236.88(59145) -> a.b.189.151(80), 1
packet
06:06:28 denied tcp r.s.236.88(59479) -> a.b.189.201(80), 1
packet
06:06:31 denied tcp r.s.236.88(59479) -> a.b.189.201(80), 1
packet
06:06:32 denied tcp r.s.236.88(59764) -> a.b.189.249(80), 1
packet
06:06:33 denied tcp r.s.236.88(59767) -> a.b.189.252(80), 1
packet
06:06:35 denied tcp r.s.236.88(60008) -> a.b.190.1(80), 1
packet
06:06:38 denied tcp r.s.236.88(60011) -> a.b.190.4(80), 1
packet
06:06:39 denied tcp r.s.236.88(60008) -> a.b.190.1(80), 1
packet
06:06:42 denied tcp r.s.236.88(60613) -> a.b.190.61(80), 1
packet
06:06:43 denied tcp r.s.236.88(60442) -> a.b.190.51(80), 1
packet
06:06:45 denied tcp r.s.236.88(60617) -> a.b.190.65(80), 1
packet
06:06:48 denied tcp r.s.236.88(60749) -> a.b.190.101(80), 1
packet
06:06:51 denied tcp r.s.236.88(60749) -> a.b.190.101(80), 1
packet
06:06:52 denied tcp r.s.236.88(61076) -> a.b.190.149(80), 1
packet
06:06:57 denied tcp r.s.236.88(61184) -> a.b.190.151(80), 1
packet
06:06:58 denied tcp r.s.236.88(61434) -> a.b.190.200(80), 1
packet
06:07:01 denied tcp r.s.236.88(61587) -> a.b.190.201(80), 1
packet
06:07:03 denied tcp r.s.236.88(61587) -> a.b.190.201(80), 1
packet
06:07:04 denied tcp r.s.236.88(61707) -> a.b.190.232(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:07:05 denied tcp r.s.236.88(61703) -> a.b.190.228(80), 1
packet
06:07:10 denied tcp r.s.236.88(62194) -> a.b.191.1(80), 1
packet
06:07:11 denied tcp r.s.236.88(62291) -> a.b.191.33(80), 1
packet
06:07:13 denied tcp r.s.236.88(62464) -> a.b.191.51(80), 1
packet
06:07:16 denied tcp r.s.236.88(62464) -> a.b.191.51(80), 1
packet
06:07:17 denied tcp r.s.236.88(62552) -> a.b.191.60(80), 1
packet
06:07:20 denied tcp r.s.236.88(62940) -> a.b.191.101(80), 1
packet
06:07:24 denied tcp r.s.236.88(62940) -> a.b.191.101(80), 1
packet
06:07:25 denied tcp r.s.236.88(63293) -> a.b.191.151(80), 1
packet
06:07:30 denied tcp r.s.236.88(63293) -> a.b.191.151(80), 1
packet
06:07:31 denied tcp r.s.236.88(63714) -> a.b.191.201(80), 1
packet
06:07:34 denied tcp r.s.236.88(63716) -> a.b.191.203(80), 1
packet
06:07:34 denied tcp r.s.236.88(63728) -> a.b.191.215(80), 1
packet
06:07:38 denied tcp r.s.236.88(64280) -> a.b.192.1(80), 1
packet
06:07:40 denied tcp r.s.236.88(64280) -> a.b.192.1(80), 1
packet
06:07:41 denied tcp r.s.236.88(64398) -> a.b.192.25(80), 1
packet
06:07:42 denied tcp r.s.236.88(64454) -> a.b.192.50(80), 1
packet
06:07:44 denied tcp r.s.236.88(64629) -> a.b.192.51(80), 1
packet
06:07:47 denied tcp r.s.236.88(64632) -> a.b.192.54(80), 1
packet
06:07:48 denied tcp r.s.236.88(64629) -> a.b.192.51(80), 1
packet
06:07:50 denied tcp r.s.236.88(65043) -> a.b.192.101(80), 1
packet
06:07:53 denied tcp r.s.236.88(65046) -> a.b.192.104(80), 1
packet
06:07:54 denied tcp r.s.236.88(65043) -> a.b.192.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:07:56 denied tcp r.s.236.88(65425) -> a.b.192.151(80), 1
packet
06:07:59 denied tcp r.s.236.88(65434) -> a.b.192.160(80), 1
packet
06:08:01 denied tcp r.s.236.88(33069) -> a.b.192.201(80), 1
packet
06:08:04 denied tcp r.s.236.88(33072) -> a.b.192.204(80), 1
packet
06:08:06 denied tcp r.s.236.88(33399) -> a.b.193.1(80), 1
packet
06:08:10 denied tcp r.s.236.88(33402) -> a.b.193.4(80), 1
packet
06:08:15 denied tcp r.s.236.88(33825) -> a.b.193.53(80), 1
packet
06:08:16 denied tcp r.s.236.88(33823) -> a.b.193.51(80), 1
packet
06:08:18 denied tcp r.s.236.88(34205) -> a.b.193.101(80), 1
packet
06:08:23 denied tcp r.s.236.88(34205) -> a.b.193.101(80), 1
packet
06:08:24 denied tcp r.s.236.88(34618) -> a.b.193.151(80), 1
packet
06:08:27 denied tcp r.s.236.88(34618) -> a.b.193.151(80), 1
packet
06:08:28 denied tcp r.s.236.88(34665) -> a.b.193.177(80), 1
packet
06:08:30 denied tcp r.s.236.88(35023) -> a.b.193.201(80), 1
packet
06:08:33 denied tcp r.s.236.88(35023) -> a.b.193.201(80), 1
packet
06:08:34 denied tcp r.s.236.88(35110) -> a.b.193.246(80), 1
packet
06:08:35 denied tcp r.s.236.88(35134) -> a.b.193.248(80), 1
packet
06:08:37 denied tcp r.s.236.88(35490) -> a.b.194.1(80), 1
packet
06:08:40 denied tcp r.s.236.88(35493) -> a.b.194.4(80), 1
packet
06:08:42 denied tcp r.s.236.88(35809) -> a.b.194.51(80), 1
packet
06:08:45 denied tcp r.s.236.88(35809) -> a.b.194.51(80), 1
packet
06:08:46 denied tcp r.s.236.88(35923) -> a.b.194.71(80), 1
packet
06:08:46 denied tcp r.s.236.88(35932) -> a.b.194.80(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:08:49 denied tcp r.s.236.88(36217) -> a.b.194.101(80), 1
packet
06:08:52 denied tcp r.s.236.88(36233) -> a.b.194.117(80), 1
packet
06:08:53 denied tcp r.s.236.88(36604) -> a.b.194.150(80), 1
packet
06:08:58 denied tcp r.s.236.88(36699) -> a.b.194.151(80), 1
packet
06:08:59 denied tcp r.s.236.88(36790) -> a.b.194.196(80), 1
packet
06:09:01 denied tcp r.s.236.88(36851) -> a.b.194.200(80), 1
packet
06:09:04 denied tcp r.s.236.88(37099) -> a.b.194.201(80), 1
packet
06:09:05 denied tcp r.s.236.88(37315) -> a.b.194.251(80), 1
packet
06:09:07 denied tcp r.s.236.88(37591) -> a.b.195.1(80), 1
packet
06:09:11 denied tcp r.s.236.88(37594) -> a.b.195.4(80), 1
packet
06:09:16 denied tcp r.s.236.88(38047) -> a.b.195.54(80), 1
packet
06:09:19 denied tcp r.s.236.88(38521) -> a.b.195.101(80), 1
packet
06:09:23 denied tcp r.s.236.88(38521) -> a.b.195.101(80), 1
packet
06:09:25 denied tcp r.s.236.88(38911) -> a.b.195.151(80), 1
packet
06:09:29 denied tcp r.s.236.88(38914) -> a.b.195.154(80), 1
packet
06:09:30 denied tcp r.s.236.88(39005) -> a.b.195.200(80), 1
packet
06:09:31 denied tcp r.s.236.88(39315) -> a.b.195.201(80), 1
packet
06:09:34 denied tcp r.s.236.88(39318) -> a.b.195.204(80), 1
packet
06:09:37 denied tcp r.s.236.88(39823) -> a.b.196.1(80), 1
packet
06:09:40 denied tcp r.s.236.88(39826) -> a.b.196.4(80), 1
packet
06:09:42 denied tcp r.s.236.88(40141) -> a.b.196.51(80), 1
packet
06:09:45 denied tcp r.s.236.88(40141) -> a.b.196.51(80), 1
packet
06:09:46 denied tcp r.s.236.88(40194) -> a.b.196.66(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:09:48 denied tcp r.s.236.88(40578) -> a.b.196.101(80), 1
packet
06:09:51 denied tcp r.s.236.88(40578) -> a.b.196.101(80), 1
packet
06:09:54 denied tcp r.s.236.88(40993) -> a.b.196.151(80), 1
packet
06:09:58 denied tcp r.s.236.88(40996) -> a.b.196.154(80), 1
packet
06:10:03 denied tcp r.s.236.88(41399) -> a.b.196.203(80), 1
packet
06:10:06 denied tcp r.s.236.88(41859) -> a.b.197.1(80), 1
packet
06:10:11 denied tcp r.s.236.88(42237) -> a.b.197.51(80), 1
packet
06:10:15 denied tcp r.s.236.88(42289) -> a.b.197.84(80), 1
packet
06:10:17 denied tcp r.s.236.88(42638) -> a.b.197.101(80), 1
packet
06:10:20 denied tcp r.s.236.88(42638) -> a.b.197.101(80), 1
packet
06:10:21 denied tcp r.s.236.88(42732) -> a.b.197.147(80), 1
packet
06:10:27 denied tcp r.s.236.88(43047) -> a.b.197.153(80), 1
packet
06:10:29 denied tcp r.s.236.88(43556) -> a.b.197.201(80), 1
packet
06:10:33 denied tcp r.s.236.88(43559) -> a.b.197.204(80), 1
packet
06:10:34 denied tcp r.s.236.88(43556) -> a.b.197.201(80), 1
packet
06:10:35 denied tcp r.s.236.88(43998) -> a.b.198.1(80), 1
packet
06:10:40 denied tcp r.s.236.88(43998) -> a.b.198.1(80), 1
packet
06:10:45 denied tcp r.s.236.88(44364) -> a.b.198.54(80), 1
packet
06:10:47 denied tcp r.s.236.88(44891) -> a.b.198.128(80), 1
packet
06:10:50 denied tcp r.s.236.88(44903) -> a.b.198.140(80), 1
packet
06:10:57 denied tcp r.s.236.88(45284) -> a.b.198.196(80), 1
packet
06:10:58 denied tcp r.s.236.88(45360) -> a.b.198.200(80), 1
packet
06:10:59 denied tcp r.s.236.88(45715) -> a.b.198.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:11:09 denied tcp r.s.236.88(46224) -> a.b.199.1(80), 1
packet
06:11:10 denied tcp r.s.236.88(46603) -> a.b.199.51(80), 1
packet
06:11:14 denied tcp r.s.236.88(46606) -> a.b.199.54(80), 1
packet
06:11:16 denied tcp r.s.236.88(47036) -> a.b.199.101(80), 1
packet
06:11:19 denied tcp r.s.236.88(47039) -> a.b.199.104(80), 1
packet
06:11:21 denied tcp r.s.236.88(47448) -> a.b.199.151(80), 1
packet
06:11:24 denied tcp r.s.236.88(47467) -> a.b.199.170(80), 1
packet
06:11:26 denied tcp r.s.236.88(47852) -> a.b.199.201(80), 1
packet
06:11:35 denied tcp r.s.236.88(48387) -> a.b.200.28(80), 1
packet
06:11:37 denied tcp r.s.236.88(48764) -> a.b.200.51(80), 1
packet
06:11:40 denied tcp r.s.236.88(48767) -> a.b.200.54(80), 1
packet
06:11:42 denied tcp r.s.236.88(49059) -> a.b.200.101(80), 1
packet
06:11:45 denied tcp r.s.236.88(49059) -> a.b.200.101(80), 1
packet
06:11:46 denied tcp r.s.236.88(49086) -> a.b.200.128(80), 1
packet
06:11:51 denied tcp r.s.236.88(49485) -> a.b.200.151(80), 1
packet
06:11:52 denied tcp r.s.236.88(49600) -> a.b.200.199(80), 1
packet
06:11:54 denied tcp r.s.236.88(49930) -> a.b.200.201(80), 1
packet
06:11:57 denied tcp r.s.236.88(49932) -> a.b.200.203(80), 1
packet
06:11:58 denied tcp r.s.236.88(49930) -> a.b.200.201(80), 1
packet
06:12:05 denied tcp r.s.236.88(50454) -> a.b.201.1(80), 1
packet
06:12:06 denied tcp r.s.236.88(50848) -> a.b.201.51(80), 1
packet
06:12:09 denied tcp r.s.236.88(50851) -> a.b.201.54(80), 1
packet
06:12:10 denied tcp r.s.236.88(50968) -> a.b.201.82(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:12:16 denied tcp r.s.236.88(51330) -> a.b.201.101(80), 1
packet
06:12:18 denied tcp r.s.236.88(51735) -> a.b.201.151(80), 1
packet
06:12:24 denied tcp r.s.236.88(52306) -> a.b.201.246(80), 1
packet
06:12:33 denied tcp r.s.236.88(52598) -> a.b.202.3(80), 1
packet
06:12:34 denied tcp r.s.236.88(52596) -> a.b.202.1(80), 1
packet
06:12:36 denied tcp r.s.236.88(52982) -> a.b.202.51(80), 1
packet
06:12:39 denied tcp r.s.236.88(52985) -> a.b.202.54(80), 1
packet
06:12:40 denied tcp r.s.236.88(52982) -> a.b.202.51(80), 1
packet
06:12:42 denied tcp r.s.236.88(53440) -> a.b.202.101(80), 1
packet
06:12:45 denied tcp r.s.236.88(53443) -> a.b.202.104(80), 1
packet
06:12:45 denied tcp r.s.236.88(53522) -> a.b.202.133(80), 1
packet
06:12:48 denied tcp r.s.236.88(53848) -> a.b.202.151(80), 1
packet
06:12:52 denied tcp r.s.236.88(53851) -> a.b.202.154(80), 1
packet
06:12:54 denied tcp r.s.236.88(54324) -> a.b.202.201(80), 1
packet
06:12:57 denied tcp r.s.236.88(54327) -> a.b.202.204(80), 1
packet
06:12:59 denied tcp r.s.236.88(54760) -> a.b.203.1(80), 1
packet
06:13:02 denied tcp r.s.236.88(54760) -> a.b.203.1(80), 1
packet
06:13:03 denied tcp r.s.236.88(54809) -> a.b.203.50(80), 1
packet
06:13:05 denied tcp r.s.236.88(55141) -> a.b.203.51(80), 1
packet
06:13:07 denied tcp r.s.236.88(55141) -> a.b.203.51(80), 1
packet
06:13:09 denied tcp r.s.236.88(55191) -> a.b.203.76(80), 1
packet
06:13:11 denied tcp r.s.236.88(55522) -> a.b.203.101(80), 1
packet
06:13:13 denied tcp r.s.236.88(55522) -> a.b.203.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:13:15 denied tcp r.s.236.88(55572) -> a.b.203.128(80), 1
packet
06:13:16 denied tcp r.s.236.88(55934) -> a.b.203.151(80), 1
packet
06:13:19 denied tcp r.s.236.88(55934) -> a.b.203.151(80), 1
packet
06:13:20 denied tcp r.s.236.88(55981) -> a.b.203.178(80), 1
packet
06:13:22 denied tcp r.s.236.88(56334) -> a.b.203.201(80), 1
packet
06:13:25 denied tcp r.s.236.88(56334) -> a.b.203.201(80), 1
packet
06:13:26 denied tcp r.s.236.88(56412) -> a.b.203.245(80), 1
packet
06:13:28 denied tcp r.s.236.88(56792) -> a.b.204.1(80), 1
packet
06:13:32 denied tcp r.s.236.88(56794) -> a.b.204.3(80), 1
packet
06:13:38 denied tcp r.s.236.88(57242) -> a.b.204.93(80), 1
packet
06:13:42 denied tcp r.s.236.88(57557) -> a.b.204.104(80), 1
packet
06:13:44 denied tcp r.s.236.88(57966) -> a.b.204.151(80), 1
packet
06:13:47 denied tcp r.s.236.88(57969) -> a.b.204.154(80), 1
packet
06:13:49 denied tcp r.s.236.88(58366) -> a.b.204.201(80), 1
packet
06:13:53 denied tcp r.s.236.88(58369) -> a.b.204.204(80), 1
packet
06:13:55 denied tcp r.s.236.88(58774) -> a.b.205.1(80), 1
packet
06:13:58 denied tcp r.s.236.88(58777) -> a.b.205.4(80), 1
packet
06:14:00 denied tcp r.s.236.88(59178) -> a.b.205.51(80), 1
packet
06:14:04 denied tcp r.s.236.88(59181) -> a.b.205.54(80), 1
packet
06:14:05 denied tcp r.s.236.88(59586) -> a.b.205.101(80), 1
packet
06:14:09 denied tcp r.s.236.88(59589) -> a.b.205.104(80), 1
packet
06:14:14 denied tcp r.s.236.88(59958) -> a.b.205.153(80), 1
packet
06:14:17 denied tcp r.s.236.88(60298) -> a.b.205.201(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:14:21 denied tcp r.s.236.88(60298) -> a.b.205.201(80), 1
packet
06:14:23 denied tcp r.s.236.88(60728) -> a.b.206.1(80), 1
packet
06:14:27 denied tcp r.s.236.88(60728) -> a.b.206.1(80), 1
packet
06:14:29 denied tcp r.s.236.88(61244) -> a.b.206.51(80), 1
packet
06:14:32 denied tcp r.s.236.88(61247) -> a.b.206.54(80), 1
packet
06:14:35 denied tcp r.s.236.88(61636) -> a.b.206.101(80), 1
packet
06:14:38 denied tcp r.s.236.88(61639) -> a.b.206.104(80), 1
packet
06:14:44 denied tcp r.s.236.88(62033) -> a.b.206.154(80), 1
packet
06:14:45 denied tcp r.s.236.88(62044) -> a.b.206.165(80), 1
packet
06:14:46 denied tcp r.s.236.88(62480) -> a.b.206.201(80), 1
packet
06:14:49 denied tcp r.s.236.88(62480) -> a.b.206.201(80), 1
packet
06:14:50 denied tcp r.s.236.88(62596) -> a.b.206.251(80), 1
packet
06:14:51 denied tcp r.s.236.88(62597) -> a.b.206.252(80), 1
packet
06:14:53 denied tcp r.s.236.88(62992) -> a.b.207.1(80), 1
packet
06:14:56 denied tcp r.s.236.88(62995) -> a.b.207.4(80), 1
packet
06:14:59 denied tcp r.s.236.88(63359) -> a.b.207.51(80), 1
packet
06:15:02 denied tcp r.s.236.88(63438) -> a.b.207.78(80), 1
packet
06:15:08 denied tcp r.s.236.88(63707) -> a.b.207.104(80), 1
packet
06:15:11 denied tcp r.s.236.88(64206) -> a.b.207.151(80), 1
packet
06:15:14 denied tcp r.s.236.88(64208) -> a.b.207.153(80), 1
packet
06:15:15 denied tcp r.s.236.88(64206) -> a.b.207.151(80), 1
packet
06:15:17 denied tcp r.s.236.88(64612) -> a.b.207.201(80), 1
packet
06:15:20 denied tcp r.s.236.88(64615) -> a.b.207.204(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:15:23 denied tcp r.s.236.88(65144) -> a.b.208.1(80), 1
packet
06:15:27 denied tcp r.s.236.88(65147) -> a.b.208.4(80), 1
packet
06:15:31 denied tcp r.s.236.88(32768) -> a.b.208.51(80), 1
packet
06:15:32 denied tcp r.s.236.88(32782) -> a.b.208.60(80), 1
packet
06:15:34 denied tcp r.s.236.88(33102) -> a.b.208.101(80), 1
packet
06:15:38 denied tcp r.s.236.88(33104) -> a.b.208.103(80), 1
packet
06:15:40 denied tcp r.s.236.88(33510) -> a.b.208.151(80), 1
packet
06:15:44 denied tcp r.s.236.88(33513) -> a.b.208.154(80), 1
packet
06:15:44 denied tcp r.s.236.88(33522) -> a.b.208.163(80), 1
packet
06:15:46 denied tcp r.s.236.88(33989) -> a.b.208.201(80), 1
packet
06:15:50 denied tcp r.s.236.88(33992) -> a.b.208.204(80), 1
packet
06:15:52 denied tcp r.s.236.88(34446) -> a.b.209.1(80), 1
packet
06:15:56 denied tcp r.s.236.88(34450) -> a.b.209.5(80), 1
packet
06:15:58 denied tcp r.s.236.88(34858) -> a.b.209.51(80), 1
packet
06:16:03 denied tcp r.s.236.88(35208) -> a.b.209.101(80), 1
packet
06:16:06 denied tcp r.s.236.88(35211) -> a.b.209.104(80), 1
packet
06:16:09 denied tcp r.s.236.88(35639) -> a.b.209.151(80), 1
packet
06:16:12 denied tcp r.s.236.88(35642) -> a.b.209.154(80), 1
packet
06:16:14 denied tcp r.s.236.88(36020) -> a.b.209.201(80), 1
packet
06:16:17 denied tcp r.s.236.88(36020) -> a.b.209.201(80), 1
packet
06:16:18 denied tcp r.s.236.88(36169) -> a.b.209.250(80), 1
packet
06:16:20 denied tcp r.s.236.88(36449) -> a.b.210.1(80), 1
packet
06:16:23 denied tcp r.s.236.88(36451) -> a.b.210.3(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:16:26 denied tcp r.s.236.88(36858) -> a.b.210.51(80), 1
packet
06:16:29 denied tcp r.s.236.88(36861) -> a.b.210.54(80), 1
packet
06:16:31 denied tcp r.s.236.88(37290) -> a.b.210.101(80), 1
packet
06:16:34 denied tcp r.s.236.88(37290) -> a.b.210.101(80), 1
packet
06:16:35 denied tcp r.s.236.88(37429) -> a.b.210.145(80), 1
packet
06:16:38 denied tcp r.s.236.88(37721) -> a.b.210.151(80), 1
packet
06:16:40 denied tcp r.s.236.88(37721) -> a.b.210.151(80), 1
packet
06:16:41 denied tcp r.s.236.88(37792) -> a.b.210.178(80), 1
packet
06:16:44 denied tcp r.s.236.88(38192) -> a.b.210.201(80), 1
packet
06:16:47 denied tcp r.s.236.88(38195) -> a.b.210.204(80), 1
packet
06:16:48 denied tcp r.s.236.88(38281) -> a.b.210.238(80), 1
packet
06:16:50 denied tcp r.s.236.88(38635) -> a.b.211.1(80), 1
packet
06:16:53 denied tcp r.s.236.88(38637) -> a.b.211.3(80), 1
packet
06:16:56 denied tcp r.s.236.88(39042) -> a.b.211.51(80), 1
packet
06:16:59 denied tcp r.s.236.88(39045) -> a.b.211.54(80), 1
packet
06:17:01 denied tcp r.s.236.88(39452) -> a.b.211.101(80), 1
packet
06:17:03 denied tcp r.s.236.88(39452) -> a.b.211.101(80), 1
packet
06:17:05 denied tcp r.s.236.88(39522) -> a.b.211.134(80), 1
packet
06:17:07 denied tcp r.s.236.88(39830) -> a.b.211.151(80), 1
packet
06:17:10 denied tcp r.s.236.88(39833) -> a.b.211.154(80), 1
packet
06:17:10 denied tcp r.s.236.88(39830) -> a.b.211.151(80), 1
packet
06:17:13 denied tcp r.s.236.88(40234) -> a.b.211.201(80), 1
packet
06:17:15 denied tcp r.s.236.88(40234) -> a.b.211.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:17:16 denied tcp r.s.236.88(40268) -> a.b.211.235(80), 1
packet
06:17:18 denied tcp r.s.236.88(40646) -> a.b.212.1(80), 1
packet
06:17:22 denied tcp r.s.236.88(40646) -> a.b.212.1(80), 1
packet
06:17:23 denied tcp r.s.236.88(41054) -> a.b.212.51(80), 1
packet
06:17:27 denied tcp r.s.236.88(41063) -> a.b.212.60(80), 1
packet
06:17:28 denied tcp r.s.236.88(41063) -> a.b.212.60(80), 1
packet
06:17:29 denied tcp r.s.236.88(41458) -> a.b.212.101(80), 1
packet
06:17:32 denied tcp r.s.236.88(41460) -> a.b.212.103(80), 1
packet
06:17:34 denied tcp r.s.236.88(41862) -> a.b.212.151(80), 1
packet
06:17:38 denied tcp r.s.236.88(41911) -> a.b.212.200(80), 1
packet
06:17:39 denied tcp r.s.236.88(42266) -> a.b.212.201(80), 1
packet
06:17:42 denied tcp r.s.236.88(42266) -> a.b.212.201(80), 1
packet
06:17:43 denied tcp r.s.236.88(42295) -> a.b.212.230(80), 1
packet
06:17:45 denied tcp r.s.236.88(42728) -> a.b.213.1(80), 1
packet
06:17:49 denied tcp r.s.236.88(42728) -> a.b.213.1(80), 1
packet
06:17:51 denied tcp r.s.236.88(43136) -> a.b.213.51(80), 1
packet
06:17:55 denied tcp r.s.236.88(43136) -> a.b.213.51(80), 1
packet
06:17:57 denied tcp r.s.236.88(43540) -> a.b.213.101(80), 1
packet
06:17:59 denied tcp r.s.236.88(43540) -> a.b.213.101(80), 1
packet
06:18:00 denied tcp r.s.236.88(43555) -> a.b.213.116(80), 1
packet
06:18:02 denied tcp r.s.236.88(43948) -> a.b.213.151(80), 1
packet
06:18:05 denied tcp r.s.236.88(43950) -> a.b.213.153(80), 1
packet
06:18:07 denied tcp r.s.236.88(44271) -> a.b.213.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:18:10 denied tcp r.s.236.88(44271) -> a.b.213.201(80), 1
packet
06:18:11 denied tcp r.s.236.88(44376) -> a.b.213.245(80), 1
packet
06:18:12 denied tcp r.s.236.88(44374) -> a.b.213.243(80), 1
packet
06:18:13 denied tcp r.s.236.88(44629) -> a.b.214.1(80), 1
packet
06:18:16 denied tcp r.s.236.88(44629) -> a.b.214.1(80), 1
packet
06:18:17 denied tcp r.s.236.88(44790) -> a.b.214.26(80), 1
packet
06:18:19 denied tcp r.s.236.88(45070) -> a.b.214.51(80), 1
packet
06:18:23 denied tcp r.s.236.88(45072) -> a.b.214.53(80), 1
packet
06:18:25 denied tcp r.s.236.88(45422) -> a.b.214.101(80), 1
packet
06:18:28 denied tcp r.s.236.88(45425) -> a.b.214.104(80), 1
packet
06:18:30 denied tcp r.s.236.88(45830) -> a.b.214.151(80), 1
packet
06:18:36 denied tcp r.s.236.88(46230) -> a.b.214.201(80), 1
packet
06:18:39 denied tcp r.s.236.88(46233) -> a.b.214.204(80), 1
packet
06:18:42 denied tcp r.s.236.88(46684) -> a.b.215.1(80), 1
packet
06:18:46 denied tcp r.s.236.88(46684) -> a.b.215.1(80), 1
packet
06:18:47 denied tcp r.s.236.88(47096) -> a.b.215.51(80), 1
packet
06:18:51 denied tcp r.s.236.88(47099) -> a.b.215.54(80), 1
packet
06:18:57 denied tcp r.s.236.88(47510) -> a.b.215.101(80), 1
packet
06:18:58 denied tcp r.s.236.88(47914) -> a.b.215.151(80), 1
packet
06:19:01 denied tcp r.s.236.88(47914) -> a.b.215.151(80), 1
packet
06:19:06 denied tcp r.s.236.88(48317) -> a.b.215.204(80), 1
packet
06:19:08 denied tcp r.s.236.88(48768) -> a.b.216.1(80), 1
packet
06:19:12 denied tcp r.s.236.88(48771) -> a.b.216.4(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:19:18 denied tcp r.s.236.88(49184) -> a.b.216.51(80), 1
packet
06:19:22 denied tcp r.s.236.88(49572) -> a.b.216.104(80), 1
packet
06:19:28 denied tcp r.s.236.88(49899) -> a.b.216.154(80), 1
packet
06:19:28 denied tcp r.s.236.88(50084) -> a.b.216.198(80), 1
packet
06:19:31 denied tcp r.s.236.88(50339) -> a.b.216.201(80), 1
packet
06:19:33 denied tcp r.s.236.88(50342) -> a.b.216.204(80), 1
packet
06:19:35 denied tcp r.s.236.88(50347) -> a.b.216.209(80), 1
packet
06:19:40 denied tcp r.s.236.88(50803) -> a.b.217.4(80), 1
packet
06:19:43 denied tcp r.s.236.88(51254) -> a.b.217.73(80), 1
packet
06:19:46 denied tcp r.s.236.88(51209) -> a.b.217.72(80), 1
packet
06:19:47 denied tcp r.s.236.88(51188) -> a.b.217.51(80), 1
packet
06:19:49 denied tcp r.s.236.88(51595) -> a.b.217.101(80), 1
packet
06:19:53 denied tcp r.s.236.88(51595) -> a.b.217.101(80), 1
packet
06:19:57 denied tcp r.s.236.88(51981) -> a.b.217.154(80), 1
packet
06:20:00 denied tcp r.s.236.88(52378) -> a.b.217.201(80), 1
packet
06:20:02 denied tcp r.s.236.88(52378) -> a.b.217.201(80), 1
packet
06:20:03 denied tcp r.s.236.88(52397) -> a.b.217.220(80), 1
packet
06:20:05 denied tcp r.s.236.88(52782) -> a.b.218.1(80), 1
packet
06:20:09 denied tcp r.s.236.88(52785) -> a.b.218.4(80), 1
packet
06:20:11 denied tcp r.s.236.88(53220) -> a.b.218.51(80), 1
packet
06:20:14 denied tcp r.s.236.88(53222) -> a.b.218.53(80), 1
packet
06:20:16 denied tcp r.s.236.88(53506) -> a.b.218.101(80), 1
packet
06:20:20 denied tcp r.s.236.88(53509) -> a.b.218.104(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:20:22 denied tcp r.s.236.88(53910) -> a.b.218.151(80), 1
packet
06:20:27 denied tcp r.s.236.88(54310) -> a.b.218.201(80), 1
packet
06:20:30 denied tcp r.s.236.88(54313) -> a.b.218.204(80), 1
packet
06:20:33 denied tcp r.s.236.88(54764) -> a.b.219.1(80), 1
packet
06:20:35 denied tcp r.s.236.88(54764) -> a.b.219.1(80), 1
packet
06:20:36 denied tcp r.s.236.88(54791) -> a.b.219.28(80), 1
packet
06:20:41 denied tcp r.s.236.88(55171) -> a.b.219.54(80), 1
packet
06:20:43 denied tcp r.s.236.88(55592) -> a.b.219.101(80), 1
packet
06:20:47 denied tcp r.s.236.88(55599) -> a.b.219.108(80), 1
packet
06:20:48 denied tcp r.s.236.88(55992) -> a.b.219.151(80), 1
packet
06:20:53 denied tcp r.s.236.88(56368) -> a.b.219.241(80), 1
packet
06:20:55 denied tcp r.s.236.88(56223) -> a.b.219.201(80), 1
packet
06:20:56 denied tcp r.s.236.88(56373) -> a.b.219.246(80), 1
packet
06:21:02 denied tcp r.s.236.88(56781) -> a.b.220.36(80), 1
packet
06:21:03 denied tcp r.s.236.88(56782) -> a.b.220.37(80), 1
packet
06:21:08 denied tcp r.s.236.88(57150) -> a.b.220.51(80), 1
packet
06:21:09 denied tcp r.s.236.88(57570) -> a.b.220.101(80), 1
packet
06:21:12 denied tcp r.s.236.88(57573) -> a.b.220.104(80), 1
packet
06:21:15 denied tcp r.s.236.88(57913) -> a.b.220.169(80), 1
packet
06:21:18 denied tcp r.s.236.88(57879) -> a.b.220.156(80), 1
packet
06:21:19 denied tcp r.s.236.88(57877) -> a.b.220.154(80), 1
packet
06:21:20 denied tcp r.s.236.88(58325) -> a.b.220.201(80), 1
packet
06:21:23 denied tcp r.s.236.88(58325) -> a.b.220.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:21:24 denied tcp r.s.236.88(58471) -> a.b.220.247(80), 1
packet
06:21:26 denied tcp r.s.236.88(58473) -> a.b.220.249(80), 1
packet
06:21:30 denied tcp r.s.236.88(58827) -> a.b.221.1(80), 1
packet
06:21:32 denied tcp r.s.236.88(59205) -> a.b.221.51(80), 1
packet
06:21:35 denied tcp r.s.236.88(59208) -> a.b.221.54(80), 1
packet
06:21:38 denied tcp r.s.236.88(59688) -> a.b.221.101(80), 1
packet
06:21:41 denied tcp r.s.236.88(59691) -> a.b.221.104(80), 1
packet
06:21:44 denied tcp r.s.236.88(60057) -> a.b.221.151(80), 1
packet
06:21:47 denied tcp r.s.236.88(60060) -> a.b.221.154(80), 1
packet
06:21:49 denied tcp r.s.236.88(60457) -> a.b.221.201(80), 1
packet
06:21:54 denied tcp r.s.236.88(60861) -> a.b.222.1(80), 1
packet
06:21:58 denied tcp r.s.236.88(60907) -> a.b.222.47(80), 1
packet
06:22:00 denied tcp r.s.236.88(61273) -> a.b.222.51(80), 1
packet
06:22:03 denied tcp r.s.236.88(61276) -> a.b.222.54(80), 1
packet
06:22:05 denied tcp r.s.236.88(61681) -> a.b.222.101(80), 1
packet
06:22:09 denied tcp r.s.236.88(61681) -> a.b.222.101(80), 1
packet
06:22:10 denied tcp r.s.236.88(61930) -> a.b.222.151(80), 1
packet
06:22:13 denied tcp r.s.236.88(61930) -> a.b.222.151(80), 1
packet
06:22:14 denied tcp r.s.236.88(62048) -> a.b.222.196(80), 1
packet
06:22:16 denied tcp r.s.236.88(62125) -> a.b.222.199(80), 1
packet
06:22:17 denied tcp r.s.236.88(62438) -> a.b.222.223(80), 1
packet
06:22:19 denied tcp r.s.236.88(62365) -> a.b.222.201(80), 1
packet
06:22:20 denied tcp r.s.236.88(62442) -> a.b.222.227(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:22:23 denied tcp r.s.236.88(62803) -> a.b.223.1(80), 1
packet
06:22:26 denied tcp r.s.236.88(62804) -> a.b.223.2(80), 1
packet
06:22:27 denied tcp r.s.236.88(62803) -> a.b.223.1(80), 1
packet
06:22:29 denied tcp r.s.236.88(63255) -> a.b.223.51(80), 1
packet
06:22:32 denied tcp r.s.236.88(63258) -> a.b.223.54(80), 1
packet
06:22:32 denied tcp r.s.236.88(63259) -> a.b.223.55(80), 1
packet
06:22:35 denied tcp r.s.236.88(63655) -> a.b.223.101(80), 1
packet
06:22:38 denied tcp r.s.236.88(63656) -> a.b.223.102(80), 1
packet
06:22:41 denied tcp r.s.236.88(64071) -> a.b.223.151(80), 1
packet
06:22:50 denied tcp r.s.236.88(64474) -> a.b.223.204(80), 1
packet
06:22:55 denied tcp r.s.236.88(64881) -> a.b.224.3(80), 1
packet
06:22:57 denied tcp r.s.236.88(65287) -> a.b.224.51(80), 1
packet
06:23:00 denied tcp r.s.236.88(65287) -> a.b.224.51(80), 1
packet
06:23:01 denied tcp r.s.236.88(65305) -> a.b.224.69(80), 1
packet
06:23:03 denied tcp r.s.236.88(32927) -> a.b.224.101(80), 1
packet
06:23:06 denied tcp r.s.236.88(32930) -> a.b.224.104(80), 1
packet
06:23:13 denied tcp r.s.236.88(33743) -> a.b.224.201(80), 1
packet
06:23:17 denied tcp r.s.236.88(33743) -> a.b.224.201(80), 1
packet
06:23:19 denied tcp r.s.236.88(34151) -> a.b.225.1(80), 1
packet
06:23:22 denied tcp r.s.236.88(34168) -> a.b.225.18(80), 1
packet
06:23:24 denied tcp r.s.236.88(34559) -> a.b.225.51(80), 1
packet
06:23:28 denied tcp r.s.236.88(34562) -> a.b.225.54(80), 1
packet
06:23:30 denied tcp r.s.236.88(35009) -> a.b.225.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:23:33 denied tcp r.s.236.88(35009) -> a.b.225.101(80), 1
packet
06:23:35 denied tcp r.s.236.88(35379) -> a.b.225.151(80), 1
packet
06:23:38 denied tcp r.s.236.88(35382) -> a.b.225.154(80), 1
packet
06:23:41 denied tcp r.s.236.88(35659) -> a.b.225.201(80), 1
packet
06:23:43 denied tcp r.s.236.88(35659) -> a.b.225.201(80), 1
packet
06:23:44 denied tcp r.s.236.88(35678) -> a.b.225.220(80), 1
packet
06:23:50 denied tcp r.s.236.88(36186) -> a.b.226.4(80), 1
packet
06:23:52 denied tcp r.s.236.88(36683) -> a.b.226.96(80), 1
packet
06:23:55 denied tcp r.s.236.88(36544) -> a.b.226.54(80), 1
packet
06:24:01 denied tcp r.s.236.88(36866) -> a.b.226.104(80), 1
packet
06:24:04 denied tcp r.s.236.88(37217) -> a.b.226.151(80), 1
packet
06:24:08 denied tcp r.s.236.88(37395) -> a.b.226.176(80), 1
packet
06:24:10 denied tcp r.s.236.88(37661) -> a.b.226.201(80), 1
packet
06:24:16 denied tcp r.s.236.88(37664) -> a.b.226.204(80), 1
packet
06:24:20 denied tcp r.s.236.88(38065) -> a.b.227.1(80), 1
packet
06:24:21 denied tcp r.s.236.88(38465) -> a.b.227.51(80), 1
packet
06:24:25 denied tcp r.s.236.88(38465) -> a.b.227.51(80), 1
packet
06:24:26 denied tcp r.s.236.88(38877) -> a.b.227.101(80), 1
packet
06:24:29 denied tcp r.s.236.88(38880) -> a.b.227.104(80), 1
packet
06:24:35 denied tcp r.s.236.88(39280) -> a.b.227.153(80), 1
packet
06:24:40 denied tcp r.s.236.88(39697) -> a.b.227.204(80), 1
packet
06:24:41 denied tcp r.s.236.88(39694) -> a.b.227.201(80), 1
packet
06:24:41 denied tcp r.s.236.88(40098) -> a.b.228.1(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:24:46 denied tcp r.s.236.88(40101) -> a.b.228.4(80), 1
packet
06:24:50 denied tcp r.s.236.88(40498) -> a.b.228.51(80), 1
packet
06:24:51 denied tcp r.s.236.88(40544) -> a.b.228.97(80), 1
packet
06:24:51 denied tcp r.s.236.88(40542) -> a.b.228.95(80), 1
packet
06:24:53 denied tcp r.s.236.88(40910) -> a.b.228.101(80), 1
packet
06:24:58 denied tcp r.s.236.88(41310) -> a.b.228.151(80), 1
packet
06:25:01 denied tcp r.s.236.88(41333) -> a.b.228.174(80), 1
packet
06:25:03 denied tcp r.s.236.88(41726) -> a.b.228.201(80), 1
packet
06:25:07 denied tcp r.s.236.88(41763) -> a.b.228.238(80), 1
packet
06:25:09 denied tcp r.s.236.88(42171) -> a.b.229.42(80), 1
packet
06:25:11 denied tcp r.s.236.88(42133) -> a.b.229.4(80), 1
packet
06:25:14 denied tcp r.s.236.88(42403) -> a.b.229.51(80), 1
packet
06:25:18 denied tcp r.s.236.88(42472) -> a.b.229.77(80), 1
packet
06:25:20 denied tcp r.s.236.88(42932) -> a.b.229.123(80), 1
packet
06:25:23 denied tcp r.s.236.88(42793) -> a.b.229.101(80), 1
packet
06:25:24 denied tcp r.s.236.88(42937) -> a.b.229.128(80), 1
packet
06:25:25 denied tcp r.s.236.88(42932) -> a.b.229.123(80), 1
packet
06:25:30 denied tcp r.s.236.88(43244) -> a.b.229.154(80), 1
packet
06:25:33 denied tcp r.s.236.88(43554) -> a.b.229.201(80), 1
packet
06:25:35 denied tcp r.s.236.88(43554) -> a.b.229.201(80), 1
packet
06:25:36 denied tcp r.s.236.88(43686) -> a.b.229.221(80), 1
packet
06:25:39 denied tcp r.s.236.88(44098) -> a.b.230.1(80), 1
packet
06:25:43 denied tcp r.s.236.88(44254) -> a.b.230.47(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:25:45 denied tcp r.s.236.88(44462) -> a.b.230.51(80), 1
packet
06:25:48 denied tcp r.s.236.88(44465) -> a.b.230.54(80), 1
packet
06:25:54 denied tcp r.s.236.88(44914) -> a.b.230.149(80), 1
packet
06:25:56 denied tcp r.s.236.88(45278) -> a.b.230.151(80), 1
packet
06:25:58 denied tcp r.s.236.88(45278) -> a.b.230.151(80), 1
packet
06:25:59 denied tcp r.s.236.88(45292) -> a.b.230.165(80), 1
packet
06:26:01 denied tcp r.s.236.88(45686) -> a.b.230.201(80), 1
packet
06:26:05 denied tcp r.s.236.88(45689) -> a.b.230.204(80), 1
packet
06:26:07 denied tcp r.s.236.88(46094) -> a.b.231.1(80), 1
packet
06:26:10 denied tcp r.s.236.88(46096) -> a.b.231.3(80), 1
packet
06:26:16 denied tcp r.s.236.88(46497) -> a.b.231.54(80), 1
packet
06:26:18 denied tcp r.s.236.88(46898) -> a.b.231.101(80), 1
packet
06:26:21 denied tcp r.s.236.88(46900) -> a.b.231.103(80), 1
packet
06:26:26 denied tcp r.s.236.88(47313) -> a.b.231.154(80), 1
packet
06:26:28 denied tcp r.s.236.88(47718) -> a.b.231.201(80), 1
packet
06:26:31 denied tcp r.s.236.88(47721) -> a.b.231.204(80), 1
packet
06:26:37 denied tcp r.s.236.88(48129) -> a.b.232.4(80), 1
packet
06:26:43 denied tcp r.s.236.88(48529) -> a.b.232.54(80), 1
packet
06:26:44 denied tcp r.s.236.88(48984) -> a.b.232.101(80), 1
packet
06:26:48 denied tcp r.s.236.88(48987) -> a.b.232.104(80), 1
packet
06:26:50 denied tcp r.s.236.88(49366) -> a.b.232.151(80), 1
packet
06:26:54 denied tcp r.s.236.88(49366) -> a.b.232.151(80), 1
packet
06:26:59 denied tcp r.s.236.88(49589) -> a.b.232.201(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:27:00 denied tcp r.s.236.88(49732) -> a.b.232.242(80), 1
packet
06:27:02 denied tcp r.s.236.88(50111) -> a.b.233.1(80), 1
packet
06:27:06 denied tcp r.s.236.88(50114) -> a.b.233.4(80), 1
packet
06:27:11 denied tcp r.s.236.88(50461) -> a.b.233.54(80), 1
packet
06:27:13 denied tcp r.s.236.88(50865) -> a.b.233.101(80), 1
packet
06:27:16 denied tcp r.s.236.88(50866) -> a.b.233.102(80), 1
packet
06:27:19 denied tcp r.s.236.88(51246) -> a.b.233.151(80), 1
packet
06:27:21 denied tcp r.s.236.88(51246) -> a.b.233.151(80), 1
packet
06:27:22 denied tcp r.s.236.88(51267) -> a.b.233.172(80), 1
packet
06:27:24 denied tcp r.s.236.88(51678) -> a.b.233.201(80), 1
packet
06:27:28 denied tcp r.s.236.88(52076) -> a.b.234.1(80), 1
packet
06:27:31 denied tcp r.s.236.88(52079) -> a.b.234.4(80), 1
packet
06:27:34 denied tcp r.s.236.88(52391) -> a.b.234.51(80), 1
packet
06:27:37 denied tcp r.s.236.88(52394) -> a.b.234.54(80), 1
packet
06:27:39 denied tcp r.s.236.88(52795) -> a.b.234.101(80), 1
packet
06:27:42 denied tcp r.s.236.88(52798) -> a.b.234.104(80), 1
packet
06:27:44 denied tcp r.s.236.88(53153) -> a.b.234.151(80), 1
packet
06:27:48 denied tcp r.s.236.88(53156) -> a.b.234.154(80), 1
packet
06:27:50 denied tcp r.s.236.88(53557) -> a.b.234.201(80), 1
packet
06:27:53 denied tcp r.s.236.88(53560) -> a.b.234.204(80), 1
packet
06:27:54 denied tcp r.s.236.88(53557) -> a.b.234.201(80), 1
packet
06:27:56 denied tcp r.s.236.88(54069) -> a.b.235.1(80), 1
packet
06:27:58 denied tcp r.s.236.88(54072) -> a.b.235.4(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:28:01 denied tcp r.s.236.88(54423) -> a.b.235.51(80), 1
packet
06:28:04 denied tcp r.s.236.88(54425) -> a.b.235.53(80), 1
packet
06:28:06 denied tcp r.s.236.88(54827) -> a.b.235.101(80), 1
packet
06:28:09 denied tcp r.s.236.88(54827) -> a.b.235.101(80), 1
packet
06:28:10 denied tcp r.s.236.88(55085) -> a.b.235.151(80), 1
packet
06:28:14 denied tcp r.s.236.88(55085) -> a.b.235.151(80), 1
packet
06:28:16 denied tcp r.s.236.88(55589) -> a.b.235.201(80), 1
packet
06:28:19 denied tcp r.s.236.88(55592) -> a.b.235.204(80), 1
packet
06:28:22 denied tcp r.s.236.88(56101) -> a.b.236.1(80), 1
packet
06:28:26 denied tcp r.s.236.88(56104) -> a.b.236.4(80), 1
packet
06:28:31 denied tcp r.s.236.88(56532) -> a.b.236.78(80), 1
packet
06:28:34 denied tcp r.s.236.88(56913) -> a.b.236.101(80), 1
packet
06:28:36 denied tcp r.s.236.88(56913) -> a.b.236.101(80), 1
packet
06:28:37 denied tcp r.s.236.88(56926) -> a.b.236.114(80), 1
packet
06:28:42 denied tcp r.s.236.88(57320) -> a.b.236.154(80), 1
packet
06:28:44 denied tcp r.s.236.88(57621) -> a.b.236.201(80), 1
packet
06:28:48 denied tcp r.s.236.88(57624) -> a.b.236.204(80), 1
packet
06:28:50 denied tcp r.s.236.88(58133) -> a.b.237.1(80), 1
packet
06:28:53 denied tcp r.s.236.88(58135) -> a.b.237.3(80), 1
packet
06:28:55 denied tcp r.s.236.88(58505) -> a.b.237.51(80), 1
packet
06:28:58 denied tcp r.s.236.88(58508) -> a.b.237.54(80), 1
packet
06:29:01 denied tcp r.s.236.88(58895) -> a.b.237.101(80), 1
packet
06:29:04 denied tcp r.s.236.88(58897) -> a.b.237.103(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:29:06 denied tcp r.s.236.88(59309) -> a.b.237.151(80), 1
packet
06:29:09 denied tcp r.s.236.88(59311) -> a.b.237.153(80), 1
packet
06:29:11 denied tcp r.s.236.88(59799) -> a.b.237.247(80), 1
packet
06:29:14 denied tcp r.s.236.88(59725) -> a.b.237.201(80), 1
packet
06:29:15 denied tcp r.s.236.88(60038) -> a.b.238.1(80), 1
packet
06:29:18 denied tcp r.s.236.88(60038) -> a.b.238.1(80), 1
packet
06:29:19 denied tcp r.s.236.88(60146) -> a.b.238.47(80), 1
packet
06:29:20 denied tcp r.s.236.88(60142) -> a.b.238.43(80), 1
packet
06:29:21 denied tcp r.s.236.88(60461) -> a.b.238.51(80), 1
packet
06:29:24 denied tcp r.s.236.88(60461) -> a.b.238.51(80), 1
packet
06:29:25 denied tcp r.s.236.88(60514) -> a.b.238.78(80), 1
packet
06:29:27 denied tcp r.s.236.88(60848) -> a.b.238.101(80), 1
packet
06:29:30 denied tcp r.s.236.88(60848) -> a.b.238.101(80), 1
packet
06:29:31 denied tcp r.s.236.88(60941) -> a.b.238.150(80), 1
packet
06:29:33 denied tcp r.s.236.88(61328) -> a.b.238.151(80), 1
packet
06:29:37 denied tcp r.s.236.88(61328) -> a.b.238.151(80), 1
packet
06:29:42 denied tcp r.s.236.88(61727) -> a.b.238.204(80), 1
packet
06:29:45 denied tcp r.s.236.88(62147) -> a.b.239.1(80), 1
packet
06:29:48 denied tcp r.s.236.88(62147) -> a.b.239.1(80), 1
packet
06:29:49 denied tcp r.s.236.88(62213) -> a.b.239.46(80), 1
packet
06:29:51 denied tcp r.s.236.88(62551) -> a.b.239.51(80), 1
packet
06:29:55 denied tcp r.s.236.88(62551) -> a.b.239.51(80), 1
packet
06:29:56 denied tcp r.s.236.88(62755) -> a.b.239.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:29:59 denied tcp r.s.236.88(62755) -> a.b.239.101(80), 1
packet
06:30:00 denied tcp r.s.236.88(62920) -> a.b.239.124(80), 1
packet
06:30:03 denied tcp r.s.236.88(63145) -> a.b.239.151(80), 1
packet
06:30:06 denied tcp r.s.236.88(63148) -> a.b.239.154(80), 1
packet
06:30:07 denied tcp r.s.236.88(63145) -> a.b.239.151(80), 1
packet
06:30:10 denied tcp r.s.236.88(63850) -> a.b.239.248(80), 1
packet
06:30:12 denied tcp r.s.236.88(63606) -> a.b.239.201(80), 1
packet
06:30:13 denied tcp r.s.236.88(63852) -> a.b.239.250(80), 1
packet
06:30:19 denied tcp r.s.236.88(64122) -> a.b.240.4(80), 1
packet
06:30:19 denied tcp r.s.236.88(64195) -> a.b.240.24(80), 1
packet
06:30:25 denied tcp r.s.236.88(64453) -> a.b.240.53(80), 1
packet
06:30:26 denied tcp r.s.236.88(64451) -> a.b.240.51(80), 1
packet
06:30:28 denied tcp r.s.236.88(64837) -> a.b.240.101(80), 1
packet
06:30:31 denied tcp r.s.236.88(64839) -> a.b.240.103(80), 1
packet
06:30:32 denied tcp r.s.236.88(64837) -> a.b.240.101(80), 1
packet
06:30:34 denied tcp r.s.236.88(65286) -> a.b.240.151(80), 1
packet
06:30:37 denied tcp r.s.236.88(65288) -> a.b.240.153(80), 1
packet
06:30:40 denied tcp r.s.236.88(32885) -> a.b.240.201(80), 1
packet
06:30:43 denied tcp r.s.236.88(32888) -> a.b.240.204(80), 1
packet
06:30:45 denied tcp r.s.236.88(33297) -> a.b.241.1(80), 1
packet
06:30:49 denied tcp r.s.236.88(33300) -> a.b.241.4(80), 1
packet
06:30:51 denied tcp r.s.236.88(33701) -> a.b.241.51(80), 1
packet
06:30:53 denied tcp r.s.236.88(33701) -> a.b.241.51(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:30:54 denied tcp r.s.236.88(33728) -> a.b.241.78(80), 1
packet
06:30:56 denied tcp r.s.236.88(34109) -> a.b.241.101(80), 1
packet
06:31:00 denied tcp r.s.236.88(34112) -> a.b.241.104(80), 1
packet
06:31:02 denied tcp r.s.236.88(34517) -> a.b.241.151(80), 1
packet
06:31:05 denied tcp r.s.236.88(34520) -> a.b.241.154(80), 1
packet
06:31:10 denied tcp r.s.236.88(34920) -> a.b.241.204(80), 1
packet
06:31:12 denied tcp r.s.236.88(35329) -> a.b.242.1(80), 1
packet
06:31:15 denied tcp r.s.236.88(35329) -> a.b.242.1(80), 1
packet
06:31:16 denied tcp r.s.236.88(35368) -> a.b.242.40(80), 1
packet
06:31:21 denied tcp r.s.236.88(35737) -> a.b.242.54(80), 1
packet
06:31:23 denied tcp r.s.236.88(36116) -> a.b.242.101(80), 1
packet
06:31:26 denied tcp r.s.236.88(36116) -> a.b.242.101(80), 1
packet
06:31:27 denied tcp r.s.236.88(36137) -> a.b.242.122(80), 1
packet
06:31:29 denied tcp r.s.236.88(36500) -> a.b.242.151(80), 1
packet
06:31:33 denied tcp r.s.236.88(36503) -> a.b.242.154(80), 1
packet
06:31:35 denied tcp r.s.236.88(36850) -> a.b.242.201(80), 1
packet
06:31:38 denied tcp r.s.236.88(36853) -> a.b.242.204(80), 1
packet
06:31:39 denied tcp r.s.236.88(36920) -> a.b.242.249(80), 1
packet
06:31:41 denied tcp r.s.236.88(37362) -> a.b.243.1(80), 1
packet
06:31:44 denied tcp r.s.236.88(37365) -> a.b.243.4(80), 1
packet
06:31:49 denied tcp r.s.236.88(37725) -> a.b.243.60(80), 1
packet
06:31:56 denied tcp r.s.236.88(38070) -> a.b.243.101(80), 1
packet
06:31:58 denied tcp r.s.236.88(38451) -> a.b.243.151(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

```
06:32:01 denied tcp r.s.236.88(38451) -> a.b.243.151(80), 1
packet
06:32:02 denied tcp r.s.236.88(38603) -> a.b.243.177(80), 1
packet
06:32:03 denied tcp r.s.236.88(38615) -> a.b.243.189(80), 1
packet
06:32:04 denied tcp r.s.236.88(38869) -> a.b.243.201(80), 1
packet
06:32:07 denied tcp r.s.236.88(38869) -> a.b.243.201(80), 1
packet
06:32:08 denied tcp r.s.236.88(38907) -> a.b.243.226(80), 1
packet
06:32:09 denied tcp r.s.236.88(38872) -> a.b.243.204(80), 1
packet
06:32:11 denied tcp r.s.236.88(39359) -> a.b.244.1(80), 1
packet
06:32:14 denied tcp r.s.236.88(39362) -> a.b.244.4(80), 1
packet
06:32:15 denied tcp r.s.236.88(39359) -> a.b.244.1(80), 1
packet
06:32:17 denied tcp r.s.236.88(39809) -> a.b.244.51(80), 1
packet
06:32:20 denied tcp r.s.236.88(39811) -> a.b.244.53(80), 1
packet
06:32:23 denied tcp r.s.236.88(40272) -> a.b.244.101(80), 1
packet
06:32:26 denied tcp r.s.236.88(40275) -> a.b.244.104(80), 1
packet
06:32:29 denied tcp r.s.236.88(40632) -> a.b.244.151(80), 1
packet
06:32:32 denied tcp r.s.236.88(40635) -> a.b.244.154(80), 1
packet
06:32:33 denied tcp r.s.236.88(40632) -> a.b.244.151(80), 1
packet
06:32:34 denied tcp r.s.236.88(41032) -> a.b.244.201(80), 1
packet
06:32:38 denied tcp r.s.236.88(41035) -> a.b.244.204(80), 1
packet
06:32:39 denied tcp r.s.236.88(41032) -> a.b.244.201(80), 1
packet
06:32:41 denied tcp r.s.236.88(41529) -> a.b.245.1(80), 1
packet
06:32:45 denied tcp r.s.236.88(41529) -> a.b.245.1(80), 1
packet
06:32:47 denied tcp r.s.236.88(42076) -> a.b.245.96(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:32:50 denied tcp r.s.236.88(41874) -> a.b.245.54(80), 1
packet
06:32:51 denied tcp r.s.236.88(41871) -> a.b.245.51(80), 1
packet
06:32:53 denied tcp r.s.236.88(42296) -> a.b.245.101(80), 1
packet
06:32:56 denied tcp r.s.236.88(42296) -> a.b.245.101(80), 1
packet
06:32:57 denied tcp r.s.236.88(42413) -> a.b.245.133(80), 1
packet
06:32:59 denied tcp r.s.236.88(42671) -> a.b.245.151(80), 1
packet
06:33:02 denied tcp r.s.236.88(42671) -> a.b.245.151(80), 1
packet
06:33:03 denied tcp r.s.236.88(42698) -> a.b.245.178(80), 1
packet
06:33:05 denied tcp r.s.236.88(43046) -> a.b.245.201(80), 1
packet
06:33:08 denied tcp r.s.236.88(43049) -> a.b.245.204(80), 1
packet
06:33:11 denied tcp r.s.236.88(43555) -> a.b.246.19(80), 1
packet
06:33:13 denied tcp r.s.236.88(43458) -> a.b.246.1(80), 1
packet
06:33:14 denied tcp r.s.236.88(43560) -> a.b.246.24(80), 1
packet
06:33:17 denied tcp r.s.236.88(43916) -> a.b.246.51(80), 1
packet
06:33:20 denied tcp r.s.236.88(43919) -> a.b.246.54(80), 1
packet
06:33:20 denied tcp r.s.236.88(43932) -> a.b.246.67(80), 1
packet
06:33:23 denied tcp r.s.236.88(44324) -> a.b.246.101(80), 1
packet
06:33:26 denied tcp r.s.236.88(44327) -> a.b.246.104(80), 1
packet
06:33:27 denied tcp r.s.236.88(44324) -> a.b.246.101(80), 1
packet
06:33:29 denied tcp r.s.236.88(44741) -> a.b.246.151(80), 1
packet
06:33:32 denied tcp r.s.236.88(44741) -> a.b.246.151(80), 1
packet
06:33:33 denied tcp r.s.236.88(44920) -> a.b.246.177(80), 1
packet
06:33:36 denied tcp r.s.236.88(45466) -> a.b.246.247(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:33:38 denied tcp r.s.236.88(45232) -> a.b.246.201(80), 1
packet
06:33:39 denied tcp r.s.236.88(45338) -> a.b.246.227(80), 1
packet
06:33:42 denied tcp r.s.236.88(45841) -> a.b.247.1(80), 1
packet
06:33:45 denied tcp r.s.236.88(45844) -> a.b.247.4(80), 1
packet
06:33:48 denied tcp r.s.236.88(46202) -> a.b.247.51(80), 1
packet
06:33:51 denied tcp r.s.236.88(46205) -> a.b.247.54(80), 1
packet
06:33:52 denied tcp r.s.236.88(46202) -> a.b.247.51(80), 1
packet
06:33:54 denied tcp r.s.236.88(46679) -> a.b.247.101(80), 1
packet
06:33:56 denied tcp r.s.236.88(46681) -> a.b.247.103(80), 1
packet
06:34:03 denied tcp r.s.236.88(47089) -> a.b.247.154(80), 1
packet
06:34:05 denied tcp r.s.236.88(47466) -> a.b.247.201(80), 1
packet
06:34:08 denied tcp r.s.236.88(47466) -> a.b.247.201(80), 1
packet
06:34:09 denied tcp r.s.236.88(47559) -> a.b.247.246(80), 1
packet
06:34:11 denied tcp r.s.236.88(47932) -> a.b.248.1(80), 1
packet
06:34:14 denied tcp r.s.236.88(47932) -> a.b.248.1(80), 1
packet
06:34:15 denied tcp r.s.236.88(47954) -> a.b.248.23(80), 1
packet
06:34:17 denied tcp r.s.236.88(48340) -> a.b.248.51(80), 1
packet
06:34:20 denied tcp r.s.236.88(48343) -> a.b.248.54(80), 1
packet
06:34:22 denied tcp r.s.236.88(48740) -> a.b.248.101(80), 1
packet
06:34:25 denied tcp r.s.236.88(48740) -> a.b.248.101(80), 1
packet
06:34:26 denied tcp r.s.236.88(48835) -> a.b.248.150(80), 1
packet
06:34:28 denied tcp r.s.236.88(49148) -> a.b.248.151(80), 1
packet
06:34:31 denied tcp r.s.236.88(49151) -> a.b.248.154(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:34:34 denied tcp r.s.236.88(49548) -> a.b.248.201(80), 1
packet
06:34:37 denied tcp r.s.236.88(49551) -> a.b.248.204(80), 1
packet
06:34:40 denied tcp r.s.236.88(50014) -> a.b.249.1(80), 1
packet
06:34:43 denied tcp r.s.236.88(50016) -> a.b.249.3(80), 1
packet
06:34:45 denied tcp r.s.236.88(50422) -> a.b.249.51(80), 1
packet
06:34:47 denied tcp r.s.236.88(50422) -> a.b.249.51(80), 1
packet
06:34:49 denied tcp r.s.236.88(50470) -> a.b.249.78(80), 1
packet
06:34:51 denied tcp r.s.236.88(50826) -> a.b.249.101(80), 1
packet
06:34:54 denied tcp r.s.236.88(50829) -> a.b.249.104(80), 1
packet
06:34:57 denied tcp r.s.236.88(51250) -> a.b.249.151(80), 1
packet
06:35:00 denied tcp r.s.236.88(51253) -> a.b.249.154(80), 1
packet
06:35:00 denied tcp r.s.236.88(51339) -> a.b.249.191(80), 1
packet
06:35:02 denied tcp r.s.236.88(51630) -> a.b.249.201(80), 1
packet
06:35:05 denied tcp r.s.236.88(51630) -> a.b.249.201(80), 1
packet
06:35:06 denied tcp r.s.236.88(51716) -> a.b.249.227(80), 1
packet
06:35:09 denied tcp r.s.236.88(52046) -> a.b.250.1(80), 1
packet
06:35:11 denied tcp r.s.236.88(52046) -> a.b.250.1(80), 1
packet
06:35:13 denied tcp r.s.236.88(52231) -> a.b.250.49(80), 1
packet
06:35:15 denied tcp r.s.236.88(52504) -> a.b.250.51(80), 1
packet
06:35:18 denied tcp r.s.236.88(52507) -> a.b.250.54(80), 1
packet
06:35:20 denied tcp r.s.236.88(52928) -> a.b.250.101(80), 1
packet
06:35:24 denied tcp r.s.236.88(52929) -> a.b.250.102(80), 1
packet
06:35:26 denied tcp r.s.236.88(53333) -> a.b.250.151(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:35:29 denied tcp r.s.236.88(53335) -> a.b.250.153(80), 1
packet
06:35:30 denied tcp r.s.236.88(53333) -> a.b.250.151(80), 1
packet
06:35:32 denied tcp r.s.236.88(53716) -> a.b.250.201(80), 1
packet
06:35:35 denied tcp r.s.236.88(53719) -> a.b.250.204(80), 1
packet
06:35:36 denied tcp r.s.236.88(53716) -> a.b.250.201(80), 1
packet
06:35:38 denied tcp r.s.236.88(54336) -> a.b.251.1(80), 1
packet
06:35:42 denied tcp r.s.236.88(54339) -> a.b.251.4(80), 1
packet
06:35:44 denied tcp r.s.236.88(54740) -> a.b.251.51(80), 1
packet
06:35:47 denied tcp r.s.236.88(54743) -> a.b.251.54(80), 1
packet
06:35:49 denied tcp r.s.236.88(55004) -> a.b.251.101(80), 1
packet
06:35:52 denied tcp r.s.236.88(55006) -> a.b.251.103(80), 1
packet
06:35:53 denied tcp r.s.236.88(55115) -> a.b.251.140(80), 1
packet
06:35:55 denied tcp r.s.236.88(55393) -> a.b.251.151(80), 1
packet
06:35:58 denied tcp r.s.236.88(55395) -> a.b.251.153(80), 1
packet
06:36:01 denied tcp r.s.236.88(55827) -> a.b.251.201(80), 1
packet
06:36:04 denied tcp r.s.236.88(55827) -> a.b.251.201(80), 1
packet
06:36:05 denied tcp r.s.236.88(56077) -> a.b.251.238(80), 1
packet
06:36:08 denied tcp r.s.236.88(56341) -> a.b.252.1(80), 1
packet
06:36:11 denied tcp r.s.236.88(56344) -> a.b.252.4(80), 1
packet
06:36:14 denied tcp r.s.236.88(56722) -> a.b.252.51(80), 1
packet
06:36:17 denied tcp r.s.236.88(56725) -> a.b.252.54(80), 1
packet
06:36:18 denied tcp r.s.236.88(56722) -> a.b.252.51(80), 1
packet
06:36:20 denied tcp r.s.236.88(57183) -> a.b.252.101(80), 1
packet
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:36:23 denied tcp r.s.236.88(57186) -> a.b.252.104(80), 1
packet
06:36:26 denied tcp r.s.236.88(57623) -> a.b.252.151(80), 1
packet
06:36:29 denied tcp r.s.236.88(57626) -> a.b.252.154(80), 1
packet
06:36:31 denied tcp r.s.236.88(58052) -> a.b.252.201(80), 1
packet
06:36:35 denied tcp r.s.236.88(58055) -> a.b.252.204(80), 1
packet
06:36:38 denied tcp r.s.236.88(58454) -> a.b.253.1(80), 1
packet
06:36:41 denied tcp r.s.236.88(58457) -> a.b.253.4(80), 1
packet
06:36:43 denied tcp r.s.236.88(58854) -> a.b.253.51(80), 1
packet
06:36:47 denied tcp r.s.236.88(58854) -> a.b.253.51(80), 1
packet
06:36:49 denied tcp r.s.236.88(59258) -> a.b.253.101(80), 1
packet
06:36:52 denied tcp r.s.236.88(59261) -> a.b.253.104(80), 1
packet
06:36:54 denied tcp r.s.236.88(59658) -> a.b.253.151(80), 1
packet
06:36:58 denied tcp r.s.236.88(59661) -> a.b.253.154(80), 1
packet
06:37:02 denied tcp r.s.236.88(60062) -> a.b.253.201(80), 1
packet
06:37:03 denied tcp r.s.236.88(60093) -> a.b.253.232(80), 1
packet
06:37:05 denied tcp r.s.236.88(60486) -> a.b.254.1(80), 1
packet
06:37:08 denied tcp r.s.236.88(60488) -> a.b.254.3(80), 1
packet
06:37:11 denied tcp r.s.236.88(60886) -> a.b.254.51(80), 1
packet
06:37:14 denied tcp r.s.236.88(60889) -> a.b.254.54(80), 1
packet
06:37:16 denied tcp r.s.236.88(61290) -> a.b.254.101(80), 1
packet
06:37:19 denied tcp r.s.236.88(61293) -> a.b.254.104(80), 1
packet
06:37:21 denied tcp r.s.236.88(61740) -> a.b.254.151(80), 1
packet
06:37:25 denied tcp r.s.236.88(61743) -> a.b.254.154(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
06:37:27 denied tcp r.s.236.88(62148) -> a.b.254.201(80), 1
packet
06:37:30 denied tcp r.s.236.88(62149) -> a.b.254.202(80), 1
packet
06:37:33 denied tcp r.s.236.88(62568) -> a.b.255.1(80), 1
packet
06:37:36 denied tcp r.s.236.88(62571) -> a.b.255.4(80), 1
packet
06:37:37 denied tcp r.s.236.88(62568) -> a.b.255.1(80), 1
packet
06:37:39 denied tcp r.s.236.88(62968) -> a.b.255.51(80), 1
packet
06:37:42 denied tcp r.s.236.88(62971) -> a.b.255.54(80), 1
packet
06:37:44 denied tcp r.s.236.88(63372) -> a.b.255.101(80), 1
packet
06:37:48 denied tcp r.s.236.88(63375) -> a.b.255.104(80), 1 packet
06:37:49 denied tcp r.s.236.88(63772) -> a.b.255.151(80), 1
packet
06:37:53 denied tcp r.s.236.88(63775) -> a.b.255.154(80), 1
packet
06:37:55 denied tcp r.s.236.88(64180) -> a.b.255.201(80), 1
packet
06:37:58 denied tcp r.s.236.88(64182) -> a.b.255.203(80), 1
packet
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced