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.

Footprint Your Intranet

One of the basic precepts of cyber security is: you must know what assets you have, so you can find and define your vulnerabilities, and accurately assess what countermeasures you need to employ to protect those assets. Described in this paper are software tools to help maintain a current knowledge of the organization's intranet. They are demonstrated to be easy to use and manipulate, they do not demand special knowledge or skills, and they present the information in a usable manner. Going through the process of creati...

Copyright SANS Institute

Author Retains Full Rights

AD

Footprint Your Intranet

Bob Brown

August 30, 2001

Introduction

How well do you know your intranet? By that I mean: do you know what machines are connected to your intranet; do you know how they are configured to communicate and what services are available; and would you know if a new workstation or server was connected? Knowing the answers to these questions has been a quest that I have pursued time and again during my cyber security career of over 13 years. When I began, I used to practice computer security by walking around, observing, talking and asking questions, and demonstrating that computer security measures and procedures would not hamper operational concerns or progress. In today's information technology environment, that is no longer a viable method of fulfilling the responsibilities of a cyber security program manager.

Background

As cyber security practitioners, we have all experienced the delusion that our networks and systems are fully accounted for and described, that we have performed assessments of all systems with well documented risk analyses, and that we have tested and installed all reasonable mitigating safeguards. It is also very convenient to believe that we, as cooperating and knowledgeable co-workers, have the full confidence of our networking and systems staff, and that they always keep us informed as to what they have planned and what they have implemented.

With all the best intentions from the network and systems staff, I have found from personal and practical experience that this situation is almost certainly a myth. At my workplace, we have coordination meetings to plan and implement Information Technology upgrades and projects, we have one-line drawings and network maps aplenty, we have configuration and change control procedures in place, and I maintain cordial relationships with the network and operations staff personnel. In spite of all this, I find that I still have to seek out the network and systems people and ask specific questions about host machines and new workstations that I find are installed and operating on the company intranet and/or the DMZ (DeMilitarized Zone) of the Internet firewall.

Strategy

It became apparent that what was needed was a "footprint" of the local network; one that I could generate myself, edit and review at my convenience, and use to best advantage in order to keep myself informed about network developments. I must be able use the information acquired to maintain an accurate and current cyber security program plan and to report risk and vulnerability concerns to management and operations personnel. For this purpose, a footprint is a profile of the organization's network infrastructure, obtained with a combination of tools and techniques, and identifying machine functions and addresses.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

I came to realize that what I wanted was a current map of each segment of our Local Area Network (LAN) without having to rely on the systems people to provide up-to-date, accurate diagrams as often as I wanted them. The intent was to accomplish something like an on-the-spot audit of the Intranet resources. I researched the Internet to find and test software that would assist me to know more of what the intranet at my workplace was made of. I began without knowing exactly what it was that would be most useful to me, and not knowing what information would be relevant to my goal.

Choosing the Tools

I already knew that programs such as the Sun NetManager or HP OpenView would be too expensive, besides being to complex for what I wanted to do. At best, I could have a low end Windows NT machine assigned for this use, in addition to my standard Windows 98 workstation.

A search turned up NetworkView, an inexpensive shareware program from www.networkview.com that can be purchased over the Internet. NetworkView is a compact network discovery tool for the Windows NT, 2000, and Windows 9x platforms. It will discover all TCP/IP nodes in a network, using DNS, SNMP (available only for NT and 2000) and Ports information, and draw a high quality color map print to that can be saved a s a file for future use. It also resolves IP address to network names if possible.

Some of the capabilities of NetworkView are:

- three types of discovery: single address, range of addresses, full subnet.
- Node classification as a general type with corresponding icon. Eighteen icons are available including Server, Workstation, Router, PC, Printer, Unix station.
- Network nodes can be added manually.
- Routes can be added manually on devices for automatic discovery, without knowing the community name.
- Four types of reports are available: a node list with notes, a list of SNMP information, a list of addresses and routes on each device, and list of information from Ports.

After I had obtained the software to accomplish this task, and had obtained maps for each of the segments of the local Ethernet network, it occurred to me that although I now knew what was living on the network, I had no idea of what it was doing there. I wanted more detail about these machines than the drawings and diagrams could tell me. I started searching for a port scanning program that would be inexpensive and easy to use. A TCP/UDP port on a network device or computer is a network interface used for communications between network devices and/or computers. A port number is a logical rather than a physical assignment (i.e.; port 23 is used for telnet sessions, port 25 is Simple Mail Transfer Protocol, port 53 is used for Domain Name Services, etc.). Port scanning is the process of querying computers or devices connected to a network to find out which machines are listening for TCP or UDP connections – sort of like finding a modem in auto answer mode, which means it is just waiting for it's number to be dialed so it can automatically answer. Any ports that are in the active or listening state may permit an unauthorized user to gain access to that machine, creating a possible vulnerability to your systems or network. A complete list of port number assignments can be found at http://www.iana.org/assignments/port-numbers.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Going back to the Internet search, I found and tested WinDump, Ethereal, Tethereal, Fscan, and SuperScan. I finally settled on SuperScan for use as the port scanner for several reasons. It's free, very easy to use (unlike WinDump and Fscan it has a Windows interface), it has a complete and editable built-in port list, and options allow it to be set so it will scan as unobtrusively as possible. I found it detected several of the newer protocols that weren't available with the others. The software will also perform name resolution if at all possible. Superscan is downloadable from www.foundstone.com/tools.

SuperScan is a TCP port scanner, pinger, and hostname resolver. It can:

- Perform simple ping tests to tell whether a remote computer is alive.
- Resolve hostnames into IP addresses and reverse lookup IP addresses into hostnames.
- Attempt to connect to other computers on a TCP network to see what services they are running.
- Read responses from connected hosts.
- Scan from a range of addresses and ports.
- Scan from a list of ports.
- Scan from selected ports from a port list.
- Scan a list of hostnames contained in a text file.

The biggest difficulty, as always, is to have the time to periodically inspect or scan the network, and then to correlate the results into a meaningful and useful data. The resulting information files must be easily reviewable and any differences must be easy to identify. With the use of these software tools this task has become manageable without becoming an undue burden upon my other responsibilities.

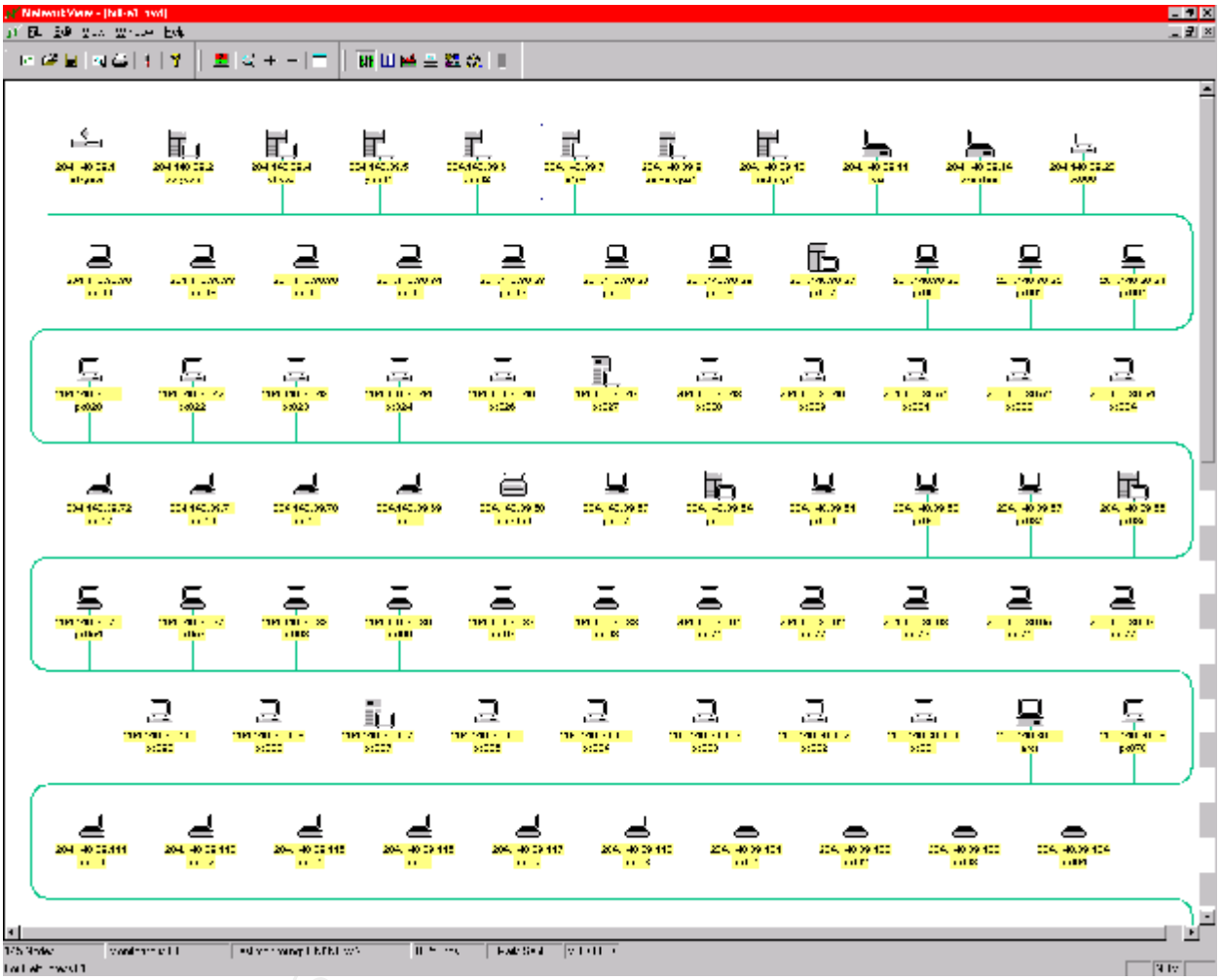
Using the Tools

It's entirely possible that both of these programs are not necessary to accomplish the discovery task. A list of IP addresses and discovered ports is usually enough of a presentation and will convince technical personnel that you are informed enough to warrant answers to your concerns. But I have found that for management presentations and reports, accompanying the information with corroborative drawings and diagrams saves much explanation time. In addition, the use of two complementing tools to screen for addressable devices on a network is desirable from a confidence point of view.

Shown below is a screen print of a NetworkView scan performed on a segment of our LAN. NetworkView allows you to select IP addresses by range, and can include domain ranges, segments, subnets, or even discover a particular address. The map can be customized so the display icons will identify the type and function of the discovered machine, whether desktop PC's, workstations, servers, routers, hubs, and printers.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

NetworkView does have it's own port scanning capability but it is not nearly as complete as it should be, including just a list of the traditional common TCP ports. Up to three additional ports may be added to the scan list. A very nice feature of NetworkView is that it will scan for any changes from a previously generated map, allowing you to keep track of any additions to or deletions from your network.



Shown below is the second piece of this "toolkit", a portion of the SuperScan report for the same LAN segment depicted above. Each asterisk identifies a new record with the IP address of the target machine followed by it's resolved hostname, and under that line is the responding port numbers from each of the machines with a short descriptor.

```
* + 204.140.39.4   dhcp2
        |___   21  File Transfer Protocol [Control]
                 |___ 220 dhcp2 FTP server (Version 6.00) ready...
        |___   25  Simple Mail Transfer
        |___   49  Login Host Protocol (TACACS)
        |___   53  Domain Name Server
        |___  111  SUN Remote Procedure Call
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
* + 204.140.39.5   ymnt1
        |___   139  NETBIOS Session Service
* + 204.140.39.6   ymnt2
        |___   139  NETBIOS Session Service
* + 204.140.39.7  a1s4
        |___    23  Telnet
                 |___ .........
* + 204.140.39.11   lois
        |___    25  Simple Mail Transfer
                 |___ 220 lois ESMTP Sendmail 8.9.3+Sun/8.9.1; Mon, 27 Aug 2001 10:40:52 -
0700 (PDT)..
        |___   111  SUN Remote Procedure Call
* + 204.140.39.27   pc007
        |___    80  World Wide Web HTTP
                 |___ HTTP/1.1 200 OK..Date: Mon, 27 Aug 2001 17:38:40 GMT..Server:
Apache/1.3.17 (Win32)..Last-Modified: Wed, 07 Feb 2001 19:15:22 G
        |___   139  NETBIOS Session Service
* + 204.140.39.29   pc009
        |___   139  NETBIOS Session Service
* + 204.140.39.55   pc035
        |___    21  File Transfer Protocol [Control]
                 |___ 220 B2Radio (Aironet AP4800E V7.22) ready..
        |___    23  Telnet
                 |___ ......
        |___    80  World Wide Web HTTP
                 |___ HTTP/1.0 200 OK.Content-type: text/html..
* + 204.140.39.56   pc036
        |___   139  NETBIOS Session Service
```

Putting the two together, annotating the NetworkView map with the discoveries from the port scanner, and then investigating anything unusual will certainly be an eye-opener. The good news is that it can confirm what you already think you know about your intranet and network configuration, but the bad news is that you may get a wakeup call and realize that complacency has no place in the cyber security profession we have chosen.

It can easily be seen that there are several items of interest in the information above: an open Telnet port on 204.140.39.6 (probably this is an NT server), a Sendmail service and a Remote Procedure Call service on 204.140.39.11 (could this be a Unix machine, and is the owner circumventing the company mail system?) and most alarmingly; an ftp port, telnet service, http port 80, and an 802.11b2 wireless access port on 204.140.39.55 (previously unknown at the time of the scan). Already, we can see that there's a lot to learn from this first scan. The identification of open port 139 (netBIOS session) on the PC's is of no concern on this network because we use Systems Management Server (SMS) software to push upgrades and patches to the user community.
The task now is to continue a regular routine of updating the NetworkView diagram, typically a monthly inspection of each Ethernet segment should be sufficient. The update will consist of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

opening an existing diagram and re-running the scan with the option to discover all differences. Over a short period of time all machines with network connections will be discovered, accounting for any that may be turned off due to employee absences and turnover. SuperScan will not discover differences between scans, but with experience the operator will learn which machines are running what services and will easily identify situations which need investigation.

Conclusion

One of the basic precepts of cyber security is: you must know what assets you have, so you can find and define your vulnerabilities, and accurately assess what countermeasures you need to employ to protect those assets. These software tools help me to maintain a current knowledge of the organization's intranet. They are demonstrated to be easy to use and manipulate, they do not demand special knowledge or skills, and they present the information in a usable manner.

This process, or one like it, is a great tool for the cyber security manager to use to stay up-to-date with network configurations and changes. It takes just a few sessions of asking specific questions about network changes, new machines, services, or ports for the network or systems people to realize that you must be included in their information circle for planning and implementation. As an additional benefit, a suitable presentation can be constructed for management that will illustrate the requirement for communication and coordination between cyber security and operations personnel to prevent unknown and untested vulnerabilities from threatening the organizational information resources. This will be especially helpful if you are in an adversarial relationship with the systems or network people.

It must be understood that this network mapping capability is just one part of an overall cyber security program. At my organization we have deployed a firewall and an Intrusion Detection System; we contract for periodic Internet point-of-presence scans; we do NT password cracking on a monthly basis, re-authenticate users annually, implement remote access controls and auditing; and we use internal modem controls. In short, we pay close attention to the myriad of other computer security practices and principles in order to protect our systems, data, and information resources.

References

Internet Assigned Numbers Authority, "Port Numbers." August 26, 2001. http://www.iana.org/assignments/port-numbers

Scambray, McClure, and Kurtz. "Hacking Exposed, Second Edition." Osborne/McGraw Hill, 2001.

F. R. Cooper, et al. "Implementing Internet Security." New Rider Publishing. 1995.

W. Timothy Polk. "Automated Tools for Testing Computer Systems Vulnerability." NIST Publication SP 800-6, Dec. 1992. http://csrc.nist.gov/publications/nistpubs

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Thomas R. Peltier, CISSP. “Information Protection Fundamentals.” Computer Security Institute, 1998. http://www.gocsi.com/ip.htm

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 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