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.

Snort Alert Collection and Analysis Suite

This document outlines separating Snort IDS Collection and Analysis Suite duties across a minimum of three servers (Snort sensor, MySQL database and an ACID web server) to gain optimal coverage and performance. The suggestion is to use Linux for all server components and Windows XP for management and viewing via a Management console. To effectively monitor and protect your network, you will need to understand what parts of your network are crucial to business operations and only then can you design your installation to...

Copyright SANS Institute
Author Retains Full Rights

AD

Chip Calhoun
September 14, 2003
GSEC Practical Assignment
Version 1.4b
Snort Alert Collection and Analysis Suite

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary 3
IDS Network Monitoring Design 3
Download the Software 3
Software Allocation per Server 4
Snort Sensor: 4
Acid Web Server: 4
MySQL Database Server: 4
Management Workstation: 4
Linux Installations 5
Installing the Software 5
Management Station Software Install – Windows XP 6
Snort Sensor Install – Red Hat 9 6
MySQL Server Install – Red Hat 9 7
ACID Web Server Install – Red Hat 9 11
Update the ACID Configuration File 11
Setup the ACID Console 12
Add Authentication to the ACID Website 14
Setup IDS Policy Manager to Control Snort's Configuration 16
Its Time to Start Snort 18
Success 19
Managing Snort Sensors 20
References 21

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary

This document outlines separating Snort IDS Collection and Analysis Suite duties across a minimum of three servers (Snort sensor, MySQL database and an ACID web server) to gain optimal coverage and performance. The suggestion is to use Linux for all server components and Windows XP for management and viewing via a Management console. To effectively monitor and protect your network, you will need to understand what parts of your network are crucial to business operations and only then can you design your installation to meet the business requirements. There will be a bit of discussion around Linux installations and the software required on each component. The goal is a scalable solution that can help to secure networks of varying designs and size.

Note: Though this document outlines how to perform the install of the server components on three separate servers, you can easily install all components onto a single machine.

IDS Network Monitoring Design

The IDS design is very dependant upon your network and should take into account critical server subnets, Internet gateways and other segments that are critical to operational integrity. The end design should include one to several Snort sensors strategically placed that report to a central MySQL database. The web server hosting the Analysis Console for Intrusion Detection (ACID) pulls and presents data from a MySQL database allowing easy viewing and correlation of events from all Snort sensors.

Download the Software

Now that we know the solution that we are after, it is time to collect all of the software needed to complete the Snort Intrusion Detection and Analysis suite setup. Create a directory on your Management workstation called 'snortsuite' and just below that, make directories for each of the pieces of software we need to install (i.e. acid, adodb, gd, idspolicymanager, jpgraph, mysql, mysqlcc, putty, redhat, snort, winscp). Be sure to use small case when naming the directories so the software will be easier to manage when we move the directories over to the respective Linux installations.

Your directory structure on your Management workstation should look like this:

- snortsuite
  - acid
  - adodb
  - gd
  - idspolicymanager

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- jpgraph
- mysql
- mysqlcc
- putty
- redhat
- snort
- winscp

Note: It is best to use the versions specified in the next section or you may find that you have difficulty during the installation process.

Software Allocation per Server

Snort Sensor:

Red Hat 9 http://www.redhat.com/download/howto_download.html
Snort http://www.snort.org/dl/snort-2.0.0.tar.gz
MySQL http://www.mysql.com/downloads/mysql-4.0.html

- Under 'Linux x86 RPM downloads' you will need the following:
  - Client programs
  - Libraries and header files

(These are required dependencies when compiling snort with MySQL support)

Acid Web Server:

Red Hat 9 http://www.redhat.com/download/howto_download.html
Acid http://www.andrew.cmu.edu/~rdanyliw/snort/acid-0.9.6b23.tar.gz
Adodb http://phplens.com/lens/dl/adodb350.tgz
GD http://www.boutell.com/gd/http/gd-2.0.15.tar.gz
JPGraph http://www.aditus.nu/jpgraph/downloads/jpgraph-1.12.2.tar.gz

MySQL Database Server:

Red Hat 9 http://www.redhat.com/download/howto_download.html
MySQL http://www.mysql.com/downloads/mysql-4.0.html

- Under 'Linux x86 RPM downloads' you will need the following:
  - Server
  - Client programs
  - Libraries and header files
  - Dynamic client libraries
    (including 3.23.x libraries)

Management Workstation:

IDSPolicy Manager http://www.activeworx.com/downloads/index.htm
MySQL Control Center http://www.mysql.com/downloads/mysqlcc.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Putty http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
WinSCP http://winscp.vse.cz/download2.php?file=winscp300setup.exe

Note: It would be a good idea to bookmark the above links. Each will come in handy for future reference.

Linux Installations

A quick word about Linux installations; everyone has their idea of what is best for the task at hand but for this setup, the simpler the better. You should leave off any software beyond the 'Server' installation option and specified add-ins during setup. The Snort sensor boxes are for sucking in packets and spitting out alerts, that's it. They have two interfaces, one for management (eth0 with a static IP address) and one for monitoring (eth1 with no IP address). If you want to add more functionality, that is up to you. Just remember that for every package you add, you will probably have to perform some upgrade in future. This is not intended to be a document explaining how to load Linux but rather how to build a low-cost IDS suite taking advantage of the efficiencies inherent in Linux. You should not have any problems during the setup process if you are using Red Hat 9, select 'Server' during setup, keep all the defaults and add in:

- Gnome Desktop
- Web Server
  - Add Php-mysql
- Development Tools
- Text Based Internet
  - Add Lynx
  - Add Pine
- Gnome Software Development
- System Tools
- Select to choose individual packages, Then choose the flat view
  - Add Sharutils

Choose your login type to be 'text' when prompted during X setup. It will be rare that you run the GUI from the console on the Snort sensors if hosting Snort is their only purpose. The collection of Snort sensors should not require monitors or keyboards and all management should be via SSH. After you complete the install of your systems, you will want to run 'ntsysv' at a shell prompt and turn off any services that are not needed.

Installing the Software

Now that you have a working version of Linux as the base, let's get started with installing the software that will drive the IDS solution:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For simplicity, our server host names will be:

SNORT001
MYSQL001
ACID001

The Management host name will be:

MGMT001

Management Station Software Install – Windows XP

Navigate to the directory where you downloaded the required software and copy both 'putty.exe' and 'winscp3.exe' to a directory that is in your path. I suggest creating a directory off the root of 'c:' called 'exe.' Then add 'c:\exe' to the path and place the executables there. The programs can then be executed directly from 'Start' > 'Run' by just typing in the program names. Install the MySQL Control Center program by running the installation package and accepting all of the defaults.

Snort Sensor Install – Red Hat 9

Use Putty to SSH to your Snort sensor (SNORT001) and load your Snort dependencies.

To keep the process consistent, copy the software to each server into '/usr/local/src' for each software package we have to install (i.e. /usr/local/src/snort). If you used your management workstation to download all of the software, just use WinSCP to copy over your MySQL RPMs and snort archive folders to your snort sensor.

You will end up with:

/usr/local/src/mysql/MySQL-client-4.0.15-0.i386.rpm
/usr/local/src/mysql/MySQL-devel-4.0.15-0.i386.rpm
/usr/local/src/snort/snort-2.0.0.tar.gz

Switch to the MySQL server directory and install the MySQL dependencies:

```
# cd ../../mysql
# rpm –Uvh MySQL-client-4.0.15-0.i386.rpm
# rpm –Uvh MySQL-devel-4.0.15-0.i386.rpm
```

Switch to the Snort directory and configure Snort using the '--with-mysql' option so we can log alerts to the MySQL server database and access it via the ACID web interface:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

cd ../../snort
tar –zxvf snort-2.0.0.tar.gz
cd snort-2.0.0
./configure -–with-mysql
make
make install

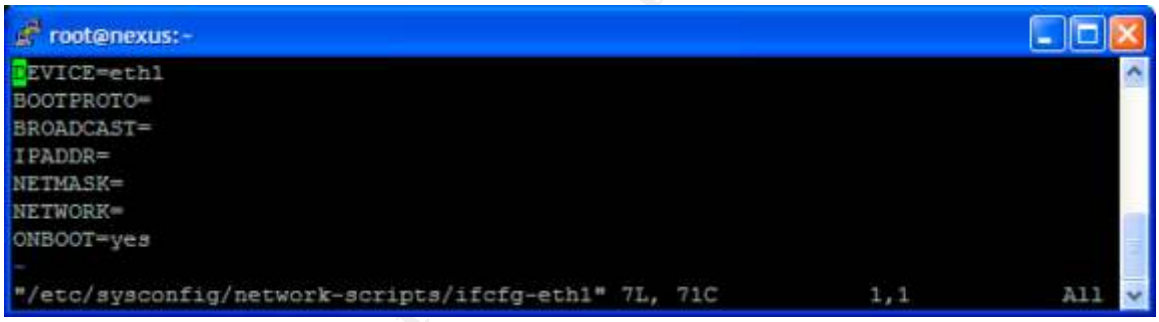
Switch to the /root directory and confirm the basic operation of Snort by typing the commands:

cd /root
snort –dvC

You should see packets, including their payload, scrolling rapidly across your terminal session. If you do, your sensor is in good shape.

Now set up eth1 to have a null IP address by editing the ifcfg-eth1 file.

vi /etc/sysconfig/network-scripts/ifcfg-eth1



Edit the file to reflect the settings above.

- hit escape
- type ':wq' (this quits and saves the file without any prompts)

/etc/rc.d/init.d/network restart

MySQL Server Install – Red Hat 9

Now on to the MySQL database server install. Open a WinSCP session from your Management station to your MySQL server. Copy the mysql folder containing the software for the server to '/usr/local/src' and you will end up with:

/usr/local/src/mysql/MySQL-client-4.0.15-0.i386.rpm
/usr/local/src/mysql/MySQL-devel-4.0.15-0.i386.rpm
/usr/local/src/mysql/MySQL-server-4.0.15-0.i386.rpm
/usr/local/src/mysql/MySQL-shared-compat-4.0.15-0.i386.rpm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(Note the version of Dynamic client libraries - MySQL-shared-compat-4.0.15-0.i386.rpm - which is required for using the existing RedHat 9 supplied Apache web server and associated php-mysql packages selected during the Red Hat install)

Use Putty to SSH to your MYSQL001 MySQL server and run the commands:

cd /usr/local/src/mysql
rpm –Uvh MySQL-*

All should install in the correct order.

Next we need to securely configure the MySQL server to accept Snort alerts by creating the Snort database, tables, username, and password. We will then assign the appropriate rights to the accounts. We will also want to secure the MySQL installation by changing the MySQL root password (this is blank by default) and removing any default anonymous accounts. This will be accomplished by following the instructions below:

Login to the MySQL server as root (not root on your Linux system but the MySQL root account):

mysql –u root -p
Enter password: (the password is blank, just hit enter)
mysql> set password for root@'localhost'=password('your*newrootpassword*');

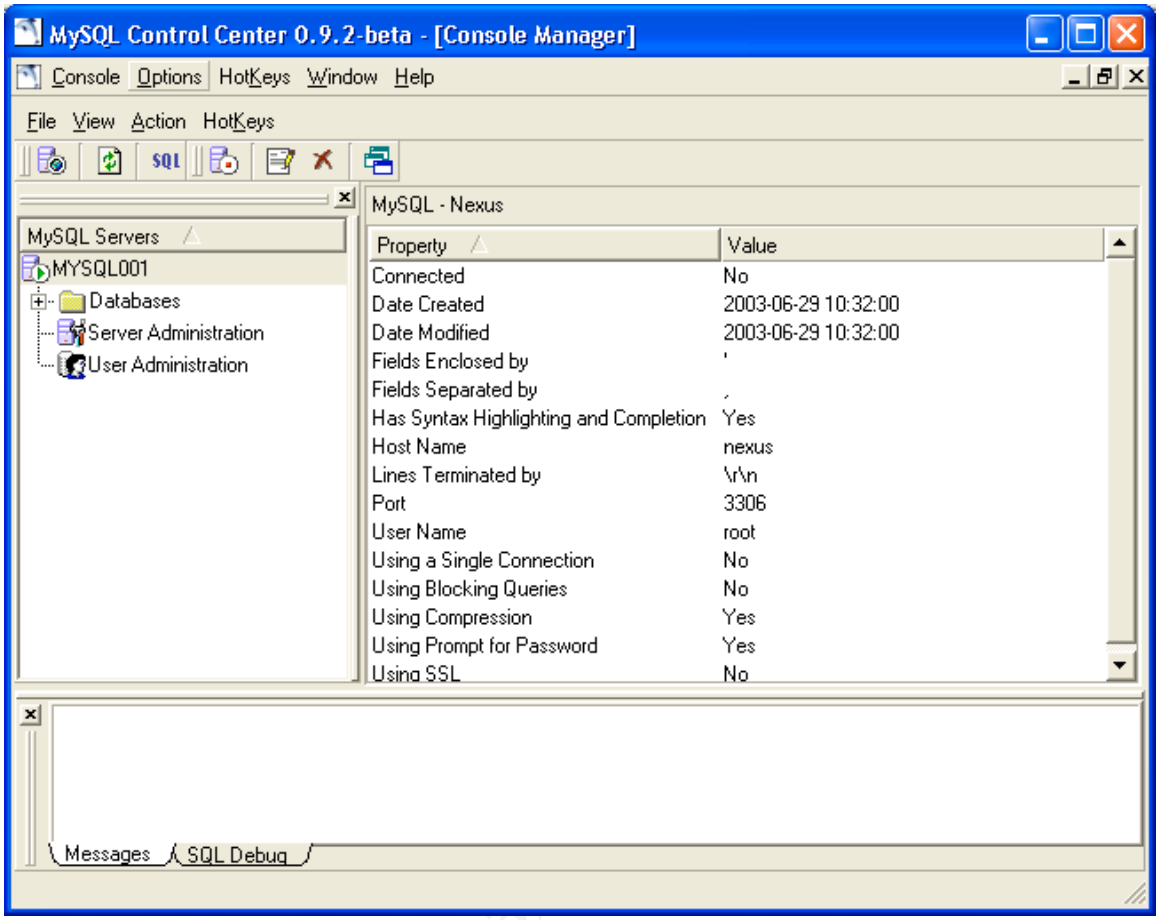
To give access from the Management station to the MySQL server installation, issue the following command:

mysql> grant all on *.* to root@'*youriporsubnet*' identified by 'your*newrootpassword*' with grant option;

Note: If you use a subnet address to support DHCP address assignments for '*youriporsubnet*' you should specify the address portion of the command like this: root@'10.0.0.%' otherwise just put your Management station's static IP address.

Now configure the MySQL Control Center GUI on the Management station to connect to the MySQL installation on MYSQL001 and make your connection.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Remove unwanted anonymous users by double-clicking on 'User Administration' then right clicking on users that have no name before the '@' sign and selecting 'Delete User'.

Create your Snort database by right-clicking on the 'Databases' folder and selecting 'New Database', type in 'snortalert' and hit enter. Double-click on the 'Databases' folder to show that your 'snortalert' database now exists.

Connect to your 'snortalert' database by double-clicking on 'snortalert'. Create the database tables by using the 'create_mysql' source file supplied with your Snort archive. It can be found in the 'contrib' directory after it has been extracted. Click on the 'SQL' icon in the toolbar and click on 'File' then 'Open'. Navigate to where you extracted the snort-2.0.0.tar.gz archive and locate the 'create_mysql' file in the 'contrib' directory under the snort-2.0.0 directory. You will have to change the 'Files of type' to be (*.*) then double-click on the 'create_mysql' file.

Note: Be sure to use the 'create_mysql' file and not the 'create_mssql' file which is for Microsoft SQL server. Microsoft SQL scripts do not work very well with MySQL…

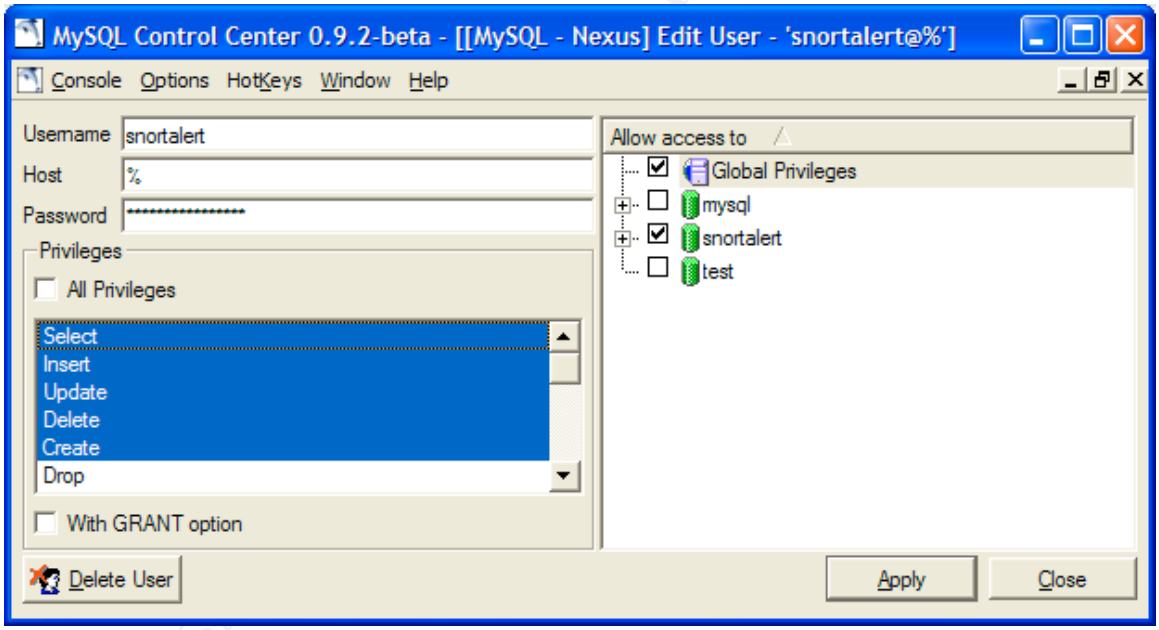
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Now click on the red exclamation point icon in the toolbar to execute the script. You will hear a few 'dings' if your sound is on and should see something like 'Query OK, 1 row affected (0.01) sec' in the last line of your 'Messages' window. Close your query window and you should be back to the console manager.

To see the new tables, disconnect from your 'snortalert' database and reconnect. You disconnect by right-clicking on 'snortalert' and selecting 'Disconnect'. Reconnect by double-clicking on 'snortalert'. Now can expand the tables and see where Snort will store alert data.

Add the user account that will access the 'snortalert' database and grant it the required privileges. Double-click on 'snortalert' to connect to the database. Right-click on 'User Administration' and select 'New User' and you will see the 'Add User' screen. Fill in the boxes as shown below:

'Username' should be 'snortalert' (or whatever you choose).
'Host' should be '%' without the quotes.
'Password' should be whatever you choose.



Click on 'Add' and select the checkbox next to the 'snortalert' database. Now de-select 'All Privileges' and select the first five privileges before clicking on 'Apply' to complete the addition of the 'snortalert' user it's associated privileges to the 'snortalert' database. Click on 'Close' and you should be back at the MySQL Control Center Manger.

Note: You may want to create a 'view' account that will not have the privilege of 'Delete' on the 'snortalert' database. Follow the same procedure as outlined above if you want to provide this non-administrative, view-only access to your ACID console simply leaving off 'Delete' during the privilege assignment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

At the MySQL Control Center Manger, right-click on 'Server Administration' select 'Flush' and 'Privileges' to activate the rights for the users you've just created.

Note: If you want an archive database, follow the same steps above to create a database called 'snortarchive', run the script to create the tables, assign the 'snortalert' user rights, and then flush the privileges.

ACID Web Server Install – Red Hat 9

Open a WinSCP session from your Management station to your ACID Web server. Copy the folders containing the software for the ACID web server to '/usr/local/src' and the directory structure on the web server will look like this:

/usr/local/src/acid/acid-0.9.6b23.tar.gz
/usr/local/src/adodb/adodb350.tgz
/usr/local/src/gd/gd-2.0.15.tar.gz
/usr/local/src/jpgraph/jpgraph-1.12.2.tar.gz

Run the following commands to prepare all of the software for use:

```
# cd ../../acid
# tar -zxvf acid-0.9.6b23.tar.gz -C /var/www/html
# cd ../adodb
# tar -zxvf adodb350.tgz -C /var/www/html
# cd ../gd
# tar -zxvf gd-2.0.15.tar.gz -C /var/www/html
# mv /var/www/html/gd-2.0.15 /var/www/html/gd
# cd ../jpgraph
# tar -zxvf jpgraph-1.12.2.tar.gz -C /var/www/html
# mv /var/www/html/jpgraph-1.12.2 /var/www/html/jpgraph
```

Update the ACID Configuration File

On the ACID001 web server, Update the ACID configuration file to use the account created on the MySQL database server, point it to the correct database host and tweak the timeout configuration for large queries.

Use Putty to SSH to the ACID001 web server. Type the following commands to edit the 'acid_conf.php' file using 'vi' as your editor:

```
# vi /var/www/html/acid/acid_conf.php
# /DBlib
# i
```

- change the line to read >> $DBlib_path="../adodb";

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- scroll down to $alert_dbname=”snort_log”;
- change the following lines to read
  - $alert_dbname=”snortalert”;
  - $alert_host = "MYSQL001"; (if you do not have DNS or Host resolution, use an IP address here)
  - $alert_port = "";
  - $alert_user = "snortalert";
  - $alert_password = "*yournewpassword*";
- hit escape

/ChartLib
i

- change the line to read >> $ChartLib_path=”../jpgraph/src”;
- hit escape

/max_script_runtime
i

- change the line to read >> $max_script_runtime = 1800;
- hit escape
- type ‘:wq’ (this quits and saves the file without any prompts)

If you created an archive database and want to create an archive website as well, use the following commands to make a copy of the ACID website calling it ‘acidarchive’:

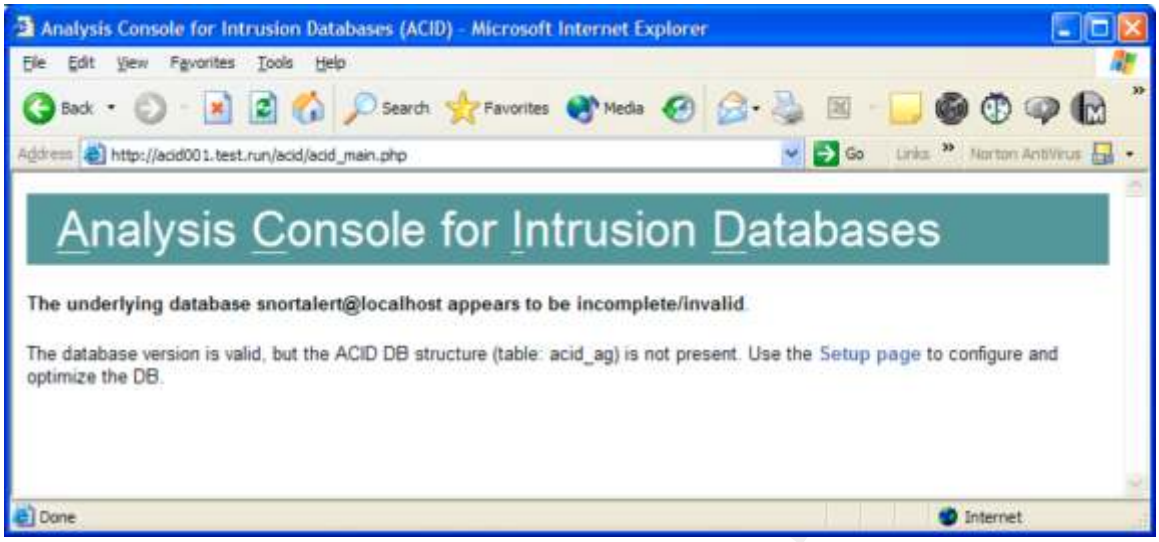
cp –R /var/www/html/acid /var/www/html/acidarchive

Update the ‘Archive DB connection parameters’ section of the ‘acid_conf.php’ file in ‘/var/www/html/acid’ to reflect the name of the archive database (‘snortarchive’) and update the alert_host, alert_user and alert_password in kind. Switch to the ‘/var/www/html/acidarchive/acid_conf.php’ file and update the ‘Alert DB connections parameters’ changing the ‘alert_dbname’ to be ‘snortarchive’ and the rest of the parameters should match your settings from the ‘/var/www/html/acid/acid_conf.php’ file. Leave the ‘Archive DB connection parameters’ section as default.

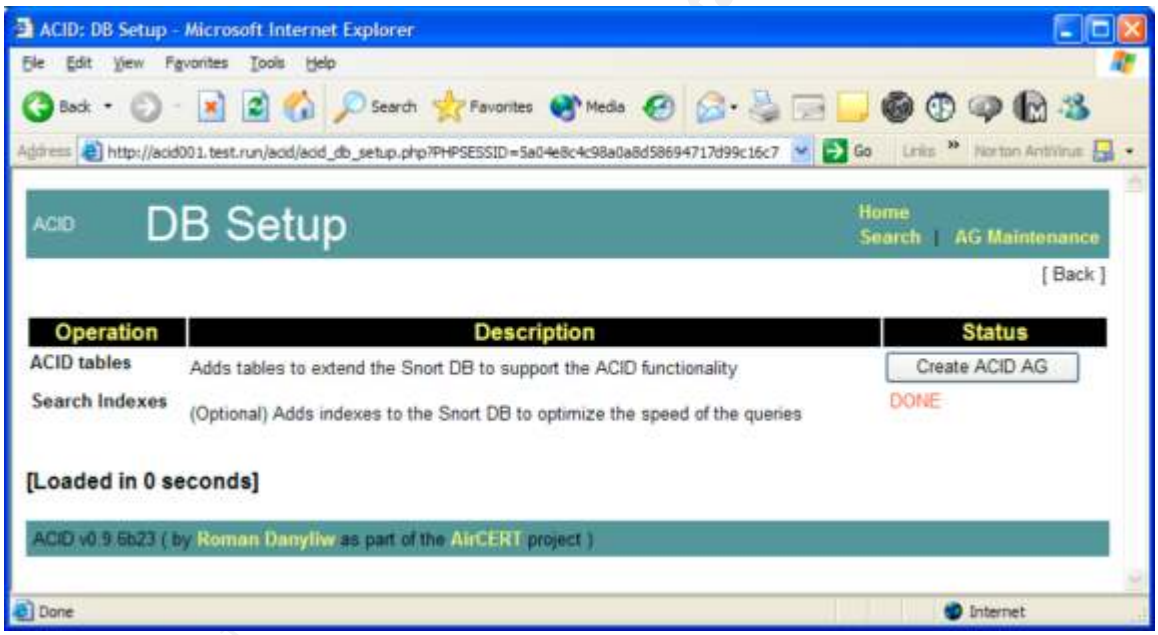
Setup the ACID Console

First access the new ACID console from the Management station. Open the web browser and point it to http://ACID001/acid to see the following web page:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

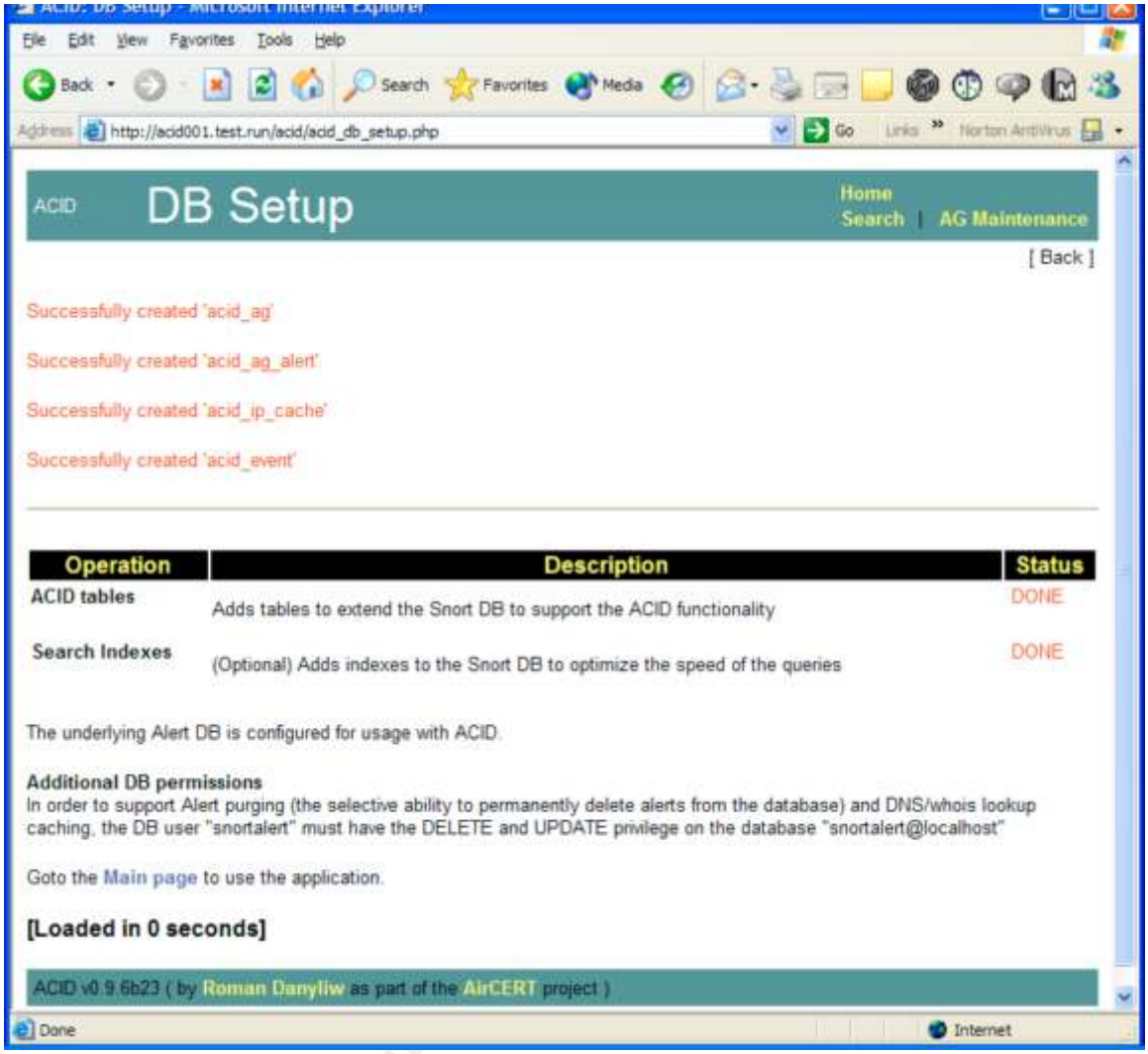


Click on 'Setup page' to configure the 'snortalert' database to work with ACID.



Now click on the 'Create ACID AG' button to build the tables on the 'snortalert' database on MYSQL001. If everything works correctly, you will see this web page:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Now click on 'Main page' near the bottom of the screen to see what your console will look like when it begins to collect alerts.

Add Authentication to the ACID Website

Using the 'Directory' section of the Apache configuration file, you can set up authorized usernames and passwords for basic authenticated access to your ACID web console. You can do this by updating the '<Directory>' section of the httpd.conf file located at '/etc/httpd/conf/httpd.conf' with the following commands:

vi /etc/httpd/conf/httpd.conf
/<Directory>
i

- <Directory "/var/www/html/acid/">
- AuthType Basic
- AuthName "Your Realm Name"
- AuthUserFile /etc/httpd/passwd/passwords

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Require user admin
- AllowOverride None
- </Directory>
-
- <Directory "/var/www/html/acidarchive/">
- AuthType Basic
- AuthName "Your Realm Name"
- AuthUserFile /etc/httpd/passwd/passwords
- Require user admin
- AllowOverride None
- </Directory>
- hit escape
- type ':wq' (this quits and saves the file without any prompts)

If you want to allow the 'view' account discussed earlier which does not have the right to delete alerts, give this account permissions to the web site by adding the 'view' account behind 'admin' account in the 'Require user' '<Directory>' section.

Now you need to create the password file you specified in the settings above, add the user 'admin' and give it a password. Do this by issuing the following commands:

Note: A word of caution, you only use the '-c' portion of the following commands when creating the passwords file. If you use it when adding other users in the future, you will overwrite the contents of the passwords file. If you already have a password file that Apache uses, just change the configuration to meet your needs.

```
# mkdir /etc/httpd/passwd
# htpasswd –c /etc/httpd/passwd/passwords admin
New password: ******************
Re-type new password: ******************
```

To allow the web server to read the new password file, issue the following commands:

```
# chown root.apache /etc/httpd/passwd/passwords
# chmod 640 /etc/httpd/passwd/passwords
# service httpd restart
```

Now when you access the ACID console you will be challenged for authentication based on the credentials provided in commands above.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Setup IDS Policy Manager to Control Snort's Configuration

On the Management station, open the folder where you stored the IDS Policy Manger installation archive. Extract the installation files to the same directory and double-click on 'IDSPM1.3.EXE' which will start the installation process. Keep all defaults and next we will configure the software to manage your Snort sensor.

Set up a new policy and sensor by doing the following:

- 'Start' – 'All Programs' – 'Activeworx' – 'IDS Policy Manager'.
- Click on the 'Policy Manager' tab
- Highlight 'Official Policy'
- Right-click and select 'Copy Policy'
- Assign the name 'SNORT001' in the 'New Policy Name' box
- Click on 'Browse' and navigate to the location of the Activeworx install and select the folder you created (c:\Program Files\Activeworx\SNORT001\)
- Select 'Copy'
- When the copy finishes, right-click on the 'SNORT001' policy and select 'Edit Policy Settings'
- Select 'Quick Policy Update Check'
- Click 'OK'
- Double-click on the 'SNORT001' policy and accept any updates that are found by the 'Quick Policy Update Check' by clicking 'Save' then 'OK'
- Now click 'File' then 'Save and Exit'

Use Putty to SSH to SNORT001 and make a directory under '/usr/local/src/snort/' called 'rules'

```
# mkdir /usr/local/src/snort/rules
```

Now back to IDS Policy Manager

- Click on the 'Sensor Manager' tab
- Click on 'Sensor' and 'Add Sensor'
- Type in the name for your sensor (SNORT001)
- Type in the IP of your sensor
- Choose the policy 'SNORT001' from the drop down menu
- Type in your SSH username and password for SNORT001
- Type in the path that exists on SNORT001 to your rules directory (/usr/local/src/snort/rules)
- Click 'OK'
- Click 'OK' when it asks you to set up SCP
- Click 'OK' when it says the setup has succeeded
- Put a checkmark next to 'SNORT001'

Now you need to customize the configuration file for your network.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Click on the 'Policy Manager' tab to view your current policy
- Double-click on 'SNORT001'

You will see the policy file and activated rules in a graphic format.

- Click on the 'Settings' tab to edit the configuration file
- De-select the 'HOME_NET' variable with 'any' listed
- Select the 'HOME_NET' variable with a single subnet listed (this is an example, use what best suits your network)
- Highlight the variable and click 'Edit'
- Add your address range you would like to monitor
- Leave the 'EXTERNAL_NET' set to 'any' (you can change it later if you get too many alerts)
- Scroll down to 'RULE_PATH' and edit it to read '/usr/local/src/snort/rules'
- Leave the rest of the 'Settings' section as default for now
- Click 'File' and 'Save Policy'

Now you need to configure the Snort sensor to report alerts to your MySQL server at MYSQL001.

- Click 'Logging' in the left pane
- Put a checkmark in 'TCPDump'
- Put a checkmark in 'Database'
- Type in 'SNORT001' in the 'Sensor Name' box
- Type in 'snortalert' in the 'DB Name' box
- Set the 'Log Rule Type' to 'alert'
- Change user to 'snortalert'
- Enter '*yournewpassword*' in 'User Pass'
- Enter 'MYSQL001' (or the IP) in 'DB Host'
- Leave the rest of the 'Logging' section as default for now
- Click 'File' and 'Save Policy'

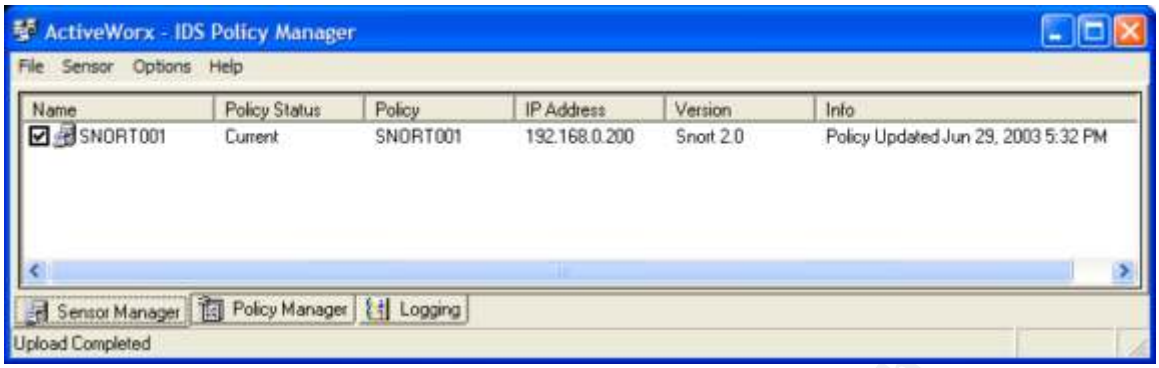
Tune the PreProcessors to suit your needs but I would suggest the following to start.

- Click 'PreProcessors' in the left pane
- Delete the bogus entry in 'Arp Spoof' (even though it is not checked, it can cause errors during Snort's initialization)
- Leave the rest of the 'PreProcessors' section as default for now
- Click 'File' and 'Save and Exit'

Upload your new policy file to SNORT001.

- Click on the 'Sensor Manager' tab
- Right-click on 'SNORT001' and select 'Upload Policy to Sensor'

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Its Time to Start Snort

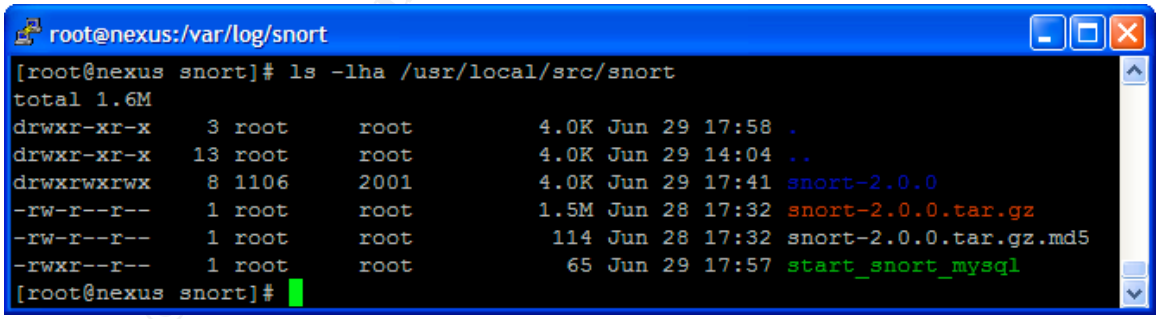
Now it is time to create a 'start_snort_mysql' executable file on your Snort sensor to reflect any special commands that you need to pass to Snort at runtime.

Use Putty to SSH to SNORT001, create a local log directory for snort and create a 'start_snort_mysql' executable file with the following commands:

mkdir /var/log/snort
vi /usr/local/src/snort/start_snort_mysql
i

- snort -i eth1 -c /usr/local/src/snort/rules/snort.conf –D (this tells Snort to listen on eth1, use the listed configuration file and run as daemon)
- hit escape
- type ':wq' (this quits and saves the file without any prompts)

chmod 700 /usr/local/src/snort/start_snort_mysql
ls –lha /usr/local/src/snort



You will see that 'start_snort_mysql' is green representing an executable file. Now Snort can be started with the following command:

/usr/local/src/snort/start_snort_mysql

The parameters from the file will be passed to Snort at runtime. After you have started Snort and there are no obvious errors, run a port scan from your

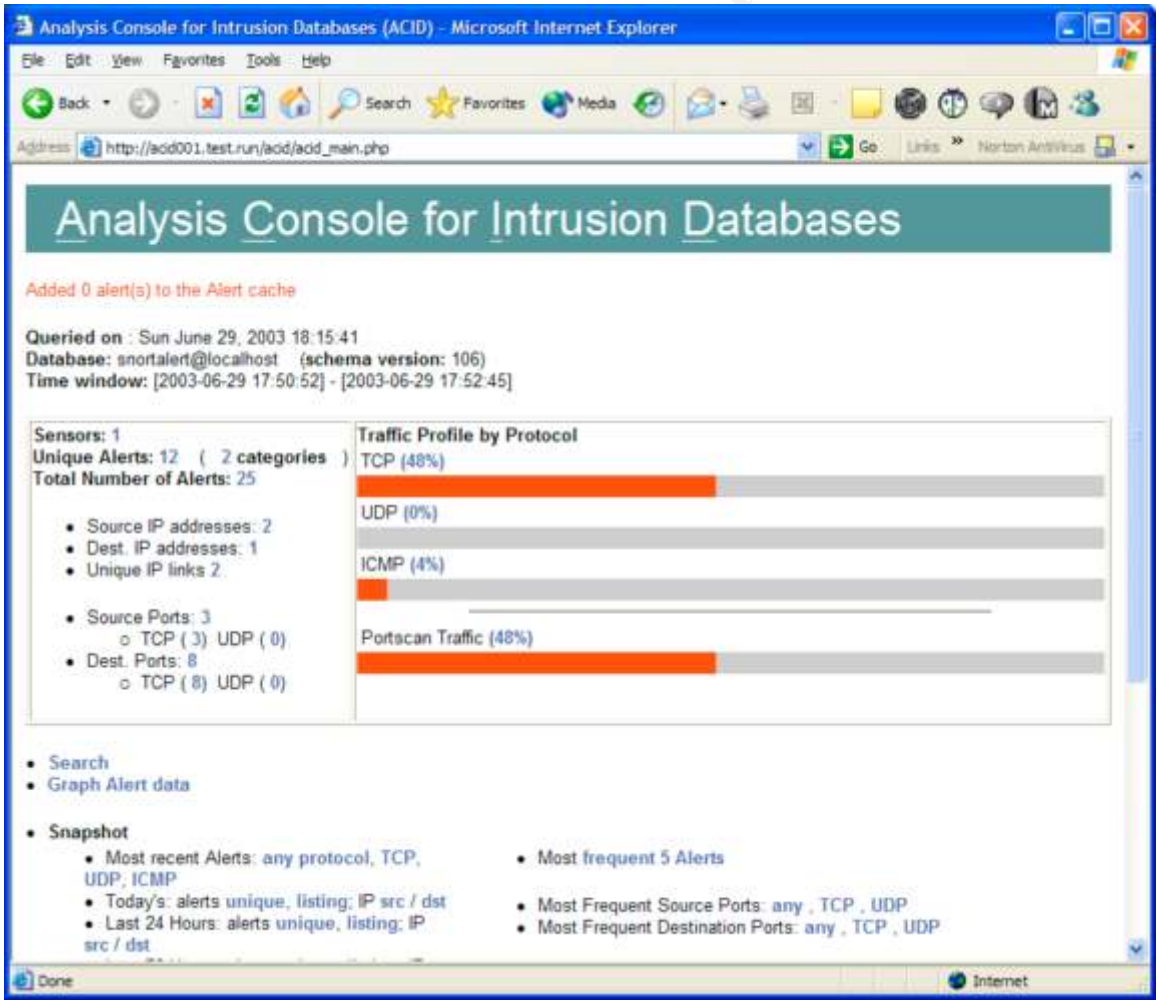
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Management console against a device on a network segment where eth1 is listening to confirm alerts are working.

Note: If you are having problems getting Snort to run or you are not receiving any alerts to your ACID console, remove the '-D' from the 'start_snort_mysql' file temporarily and any errors will be reported to your shell. Simply switch this back and Snort off to daemon mode when your troubleshooting is complete.

Success

Now open up a browser on your Management Console and type in the web server address: http://ACID001/acid. If everything has gone as planned, you will get prompted for the credentials you set up under Apache and after successful authentication, you will see evidence of the port scan you just ran against your Snort sensor.



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Managing Snort Sensors

Managing Snort sensors includes tuning the sensors so they do not give you too many false-alerts. We have started with a near-default set of rules and parameters supplied from snort.org. I would suggest that you use ACID to monitor your network over time and tune the sensors reduce false-alerts. For IDS to be effective, it must be configured to produce good information about real threats and ignore normal network traffic. Using IDS Policy Center, it is quite easy to enable, disable, create new or modify existing rules and create an optimum configuration file.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Roesch, Martin. Green, Chris. Sourcefire, Inc. Snort Users Manual: 2.0.1
URL: http://www.snort.org/docs/SnortUsersManual-2.0.1.pdf

Danyliw, Roman. ACID: Installation and Configuration
URL: http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html

Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook
Indianapolis: New Riders, 1999

Scott, J. Steven. Snort, MySQL, SnortCenter and ACID on Redhat 9.0
URL: http://www.superhac.com/docs/snort_enterprise.pdf

MySQL AB MySQL Reference Manual
URL: http://mysql.oregonstate.edu/Downloads/Manual/manual.pdf

Dell, Jeff. IDS Policy Manager Help
URL: http://www.activeworx.com/downloads/IDSPolMan-1.3.1.build45.zip

Sanchez, C. Scott. IDS Zone Theory Diagram
URL: http://www.snort.org/docs/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf

Bace, Rebecca. Mell, Peter. NIST Special Publication on Intrusion Detection Systems
URL: http://www.snort.org/docs/nist-ids.pdf

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 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