Kevin Cardwell

BLACK HAT BRIEFINGS

Toolkits: All-in-One Approach to Security

This talk will be on using toolkits for your pen-testing, vulnerability assessment etc. Configuring a plethora of the different tools out there can be quite time consuming, and challenging. The focus of this talk will be to look at an alternative solution that provides a suite of tools at boot. Until recently there was not very many toolkits, and the ones that were there did not work very well, that has changed and in this talk I will discuss the toolkits available, and demo one of the better ones. The toolkits that will be reviewed will all be open source, and free, there are commercial solutions available, but why pay when the free ones are more than adequate.

Kevin Cardwell *spent 22 years in the U.S. Navy, starting off in Sound Navigation and Ranging (SONAR). He began programming in 1987. He was fortunate enough to get on the Testing Team and got to test and evaluate Surveillance and Weapon system software including; Remote Mine-Hunting System, Multi-System Torpedo Recognition Alert Processor (MSTRAP), Advanced Radar Periscope Discrimination Detection System (ARPDD), Tactical Decision Support Subsystem (TDSS) and Computer Aided Dead Reckoning Tracer (CADRT). Shortly thereafter he became a software and systems engineer and was was selected to head the team that built a Network Operation Center (NOC) that provided services to the command ashore and ships at sea in the Norwegian Sea and Atlantic Ocean.*

In 2000, Cardwell formed his own Engineering Solutions company and has been providing consulting services for companies throughout the UK and Europe. He is also an Adjunct Associate Professor for the University of Maryland University College and is the European rep for the Information Assurance curriculum. He holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas.

Toolkits: All-in-one Approach to Security

Blackhat USA 2005

Speaker: Kevin Cardwell
computerguru63@yahoo.com

Agenda

- Tool Selection Methodology
- Tool Usage
  - Traditional
  - Alternative
- Available Toolkits
- Network Security Toolkit
  - Demo!
- Questions?

Tool Selection

- One of the most difficult things?
  - Finding security tools that
    - You are comfortable configuring
    - Have a reputation of being successful
    - Are FREE!
- Toolkit approach
  - The tool used is not a factor if
    - You are comfortable with the tool
    - The tool performs satisfactorily
    - The tool gets the job done

Tool Usage

- Two Approaches
  - Traditional
    - Download tool
    - README File
    - ./configure
    - make
    - make INSTALL
    - If all goes well! …. Run the tool

Traditional Approach Pitfalls

- Did you remember all the dependencies?
  - Libpcap, openssl etc
- Are all the libraries built?
- Is everything the right version?
- Are there specific steps to follow to get the tool running
  - ie: Nessus
- Does the tool work on your OS!

Tool Usage: Cont

- Alternative approach
  - **Tools Available at Boot!**
  - No build requirements
  - No hard drive impact
    - Can use on any machine, and then restore to its normal operation!
  - Use on virtually any Intel system
  - Web based GUI
  - SSL, ssh etc
  - Powerful Scripts!

Available Toolkits

- Knoppix
  - Father of the majority of the kits
- Helix
  - Forensic based
- PHLAK
  - Designed for “hacking”
- Auditor
  - Plethora of security tools
- Network Security Toolkit
  - Powerful scripts

Knoppix

- Most of the toolkits are based on Knoppix
- Hardware friendly
- Lots of choices:
  - Local Area Security
    - http://www.localareasecurity.com
  - Knoppix Security Tools Distribution
    - Kyle Rankin
      - *Knoppix Hacks* – ISBN: 0-595-00787-6

Helix

- Applications dedicated to Incident Response and Forensics.
- Will not auto mount swap space, or auto mount any attached devices
  - Forensically sound
- Special Windows autorun side for Incident Response and Forensics.
- Used by E-fense, SANS and others!

- http://www.e-fense.com/helix/

PHLAK

- Professional Hackers Linux Assault Kit
- Derivative of Morphix
  - by Alex de Landgraaf
- http://www.phlak.org

Auditor

- Very big
  - 600 MB+
- Tons of tools broken down into areas
  - Scanning
  - Footprinting etc
- Excellent at getting wireless working at boot!
- Tutorials available
  - http://new.remote-exploit.org/index.php/Tutorials
- http://www.remote-exploit.org

Network Security Toolkit

- My favorite
- The scripts are unbelievable
- From the GUI can run almost everything within clicks of a mouse
- http://www.networksecuritytoolkit.org

Introducing the Network Security Toolkit

- Created by:
  - Ronald W. Henderson and Paul Blankenbaker
- Distributed under the GPL (GNU Public License)
  - Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed
    - Change is allowed for your own personal use, but not for distribution to others

About the NST

- This bootable ISO CD is based on Fedora Core 2. The toolkit was designed to provide easy access to best-of-breed Open Source Network Security Applications and should run on most x86 platforms.
- When booted in the default manner, access to the running (NST) probe system can be accomplished in the following manner:
  - **Logging in directly to the probe using the console**
  - **logging in via a ssh client program: ssh root@IP**
  - **directing a SSL capable web browser to: https://IP/**

NST Info

- Boots from an ISO cd image
  - Works on virtually all x86 Intel Architectures
- Creates RAM disk
    - The more RAM the better
- X windows
  - Hit or miss
  - Start by typing *lx vwtm*
  - If problems
    - Run setup_x and choose hardware

NST Contents

- The majority of tools published in the article: Top 75 Security Tools by insecure.org are available in the toolkit.
  - Ettercap
    - Man-in-the-middle attacks
    - SSL sniffing
  - Nessus
    - Top 5 scanner
  - Kismet
    - Wireless WEP cracking

NST contents (cont)

- Snort
  - In 2 mouse clicks
    - Full blown with BASE or ACID display
  - **I have never seen an easier Snort setup!!**
- lots more
  - User guide
    - http://www.networksecuritytoolkit.org/nst/index.html
  - Man pages

Starting the Toolkit

- Insert CD-Rom
- Boot system
- During the initial boot, at the prompt press space bar for custom boot
  - Several options
    - 2 of note
      - Desktop
      - Laptop (loads all PCMCIA services)

Startup (cont)

- During boot
  - System stops and prompts for a password for root
  - On network interfaces the script looks for a DHCP server
    - If there is no DHCP this fails and the boot continues
- After boot
  - Login as user root with password supplied at boot
- Use ifconfig to setup network
  - ifconfig eth0 10.1.1.? (what ever ip you are assigning)
  - ifconfig eth0 netmask 255.255.255.0

Initial Setup

- Once x starts
  - Right-click on the desktop and select desktop applications
    - Select Firefox
- Firefox will load and prompt for a login
  - Login
    - User root
    - And password supplied at boot

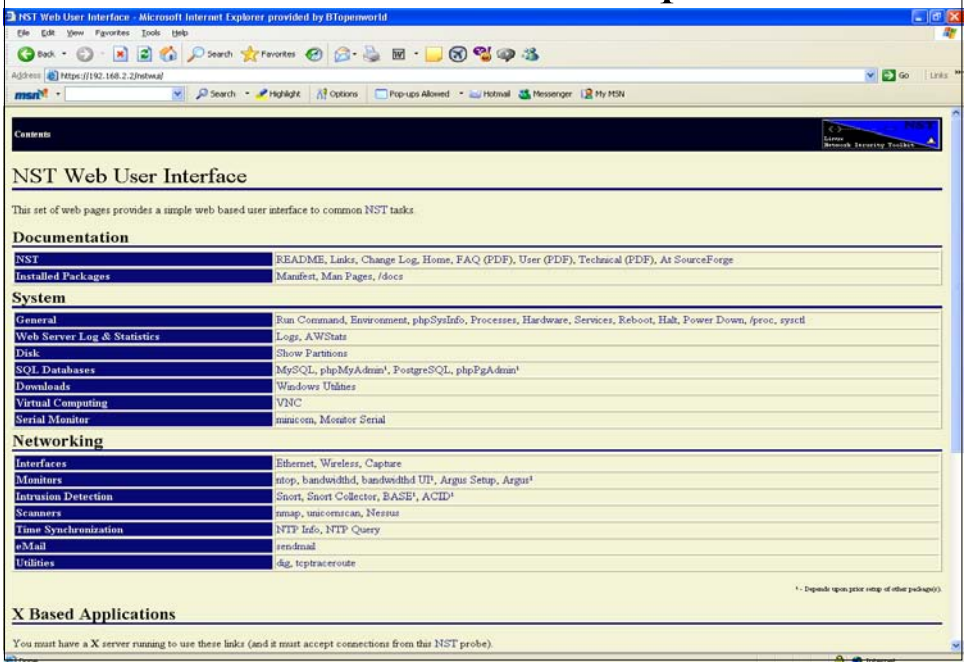
NST WUI
(Web User Interface)

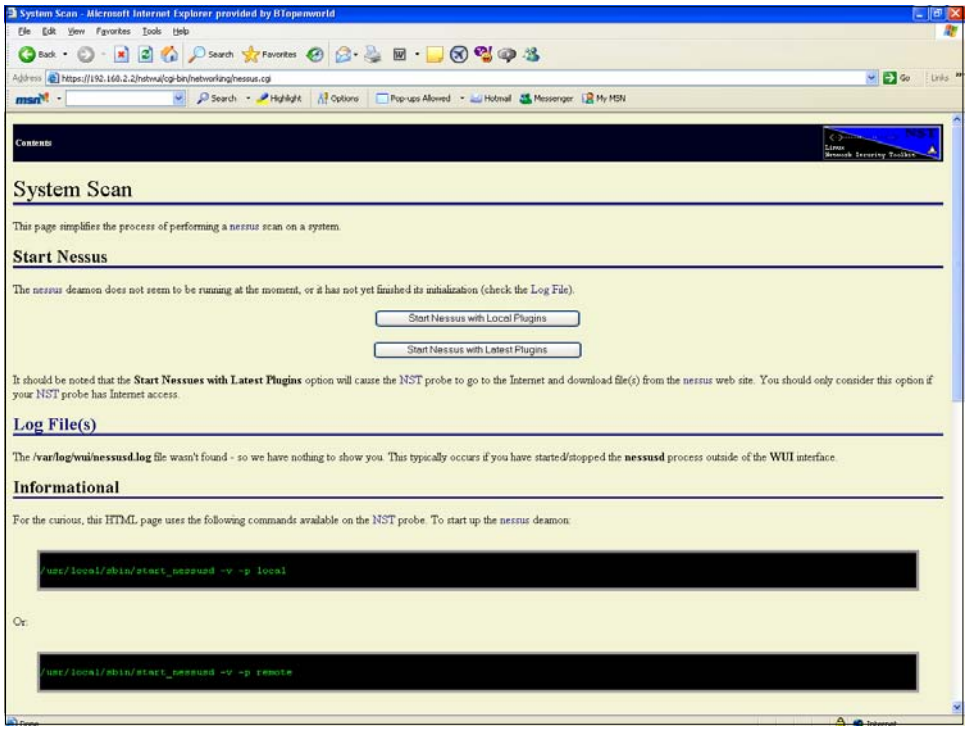
- There are 2 options
  - 1. Use the NST from the machine it is running on
  - 2. Connect to it from another machine
    - Open up browser and
      - Type https://IP ADDRESS/
      - **NOTE:**
        - » **HTTPS**
        - » **Cannot log in via HTTP due to clear text login**

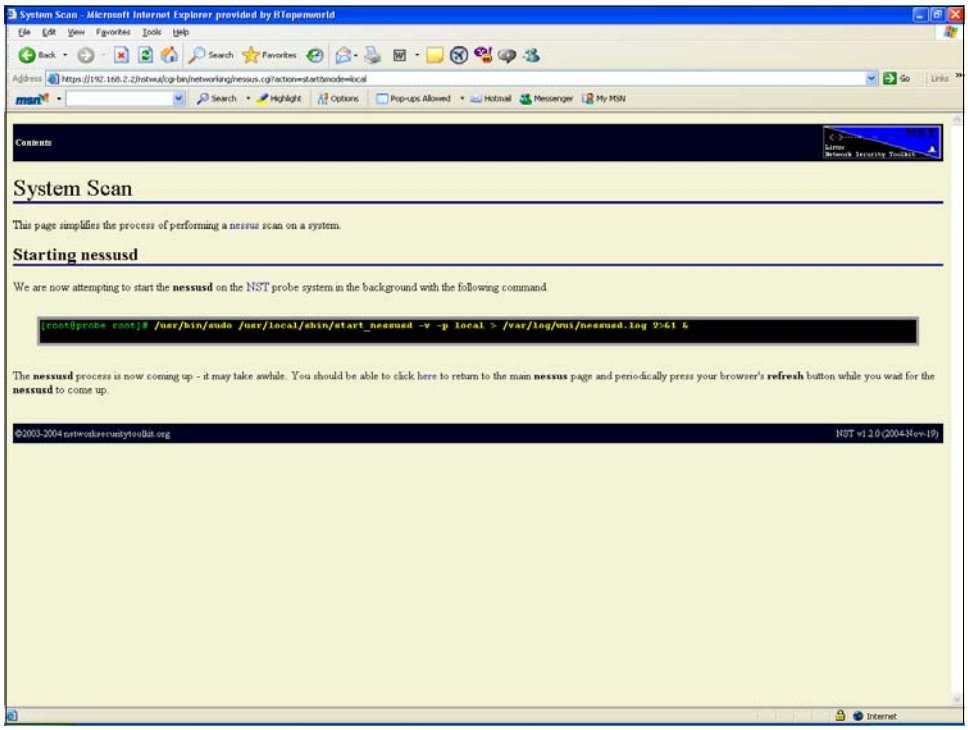
DEMO

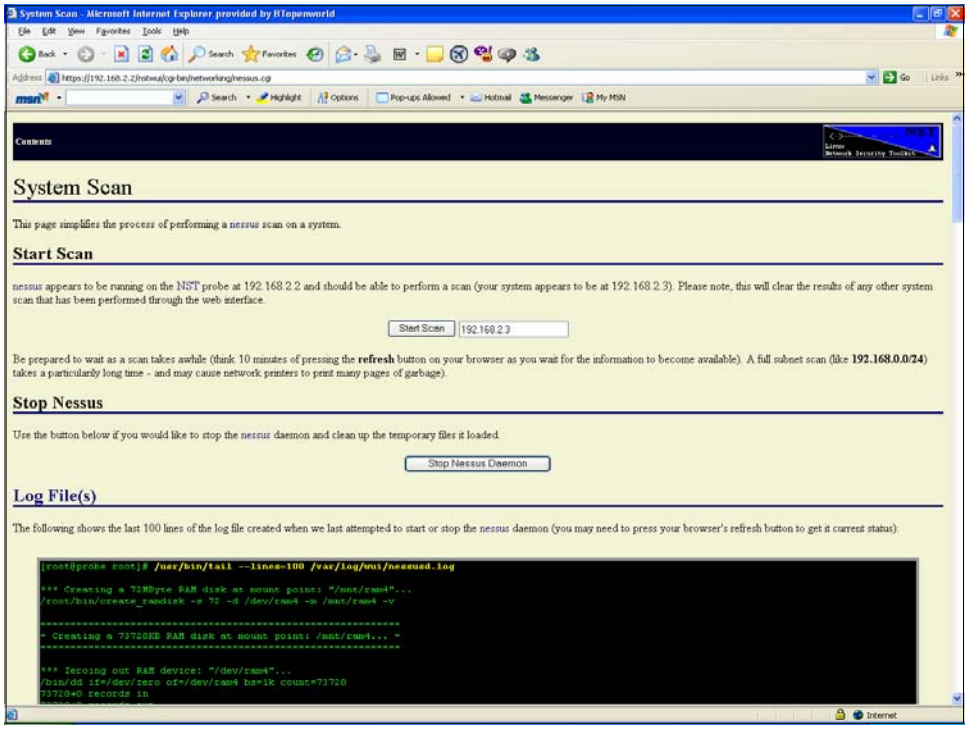
Questions?

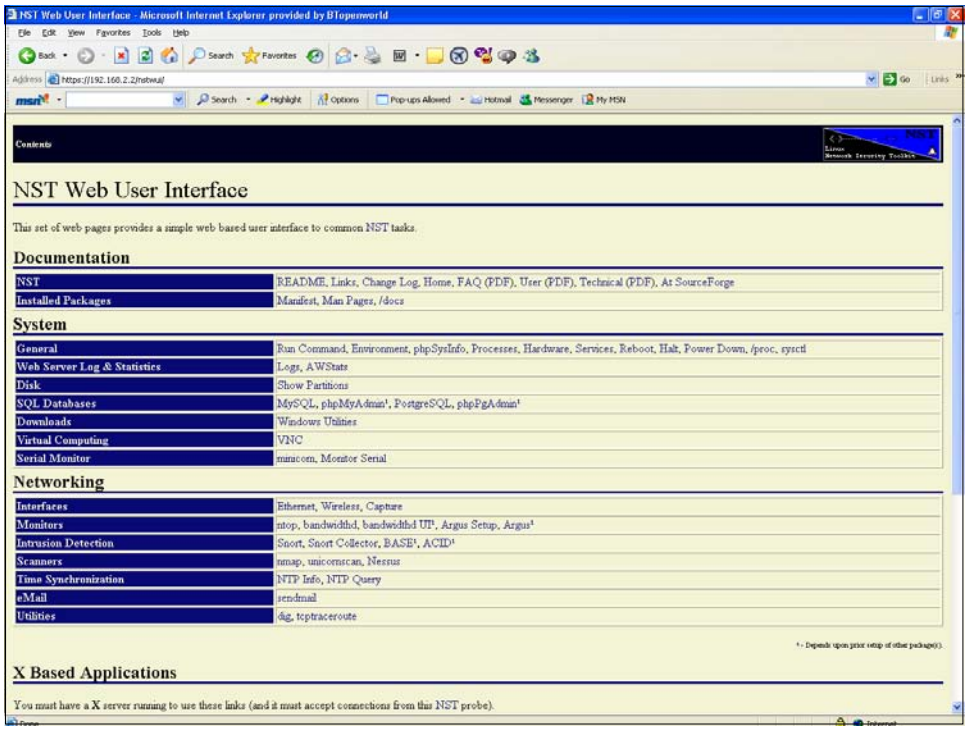
NST WUI Screen Captures

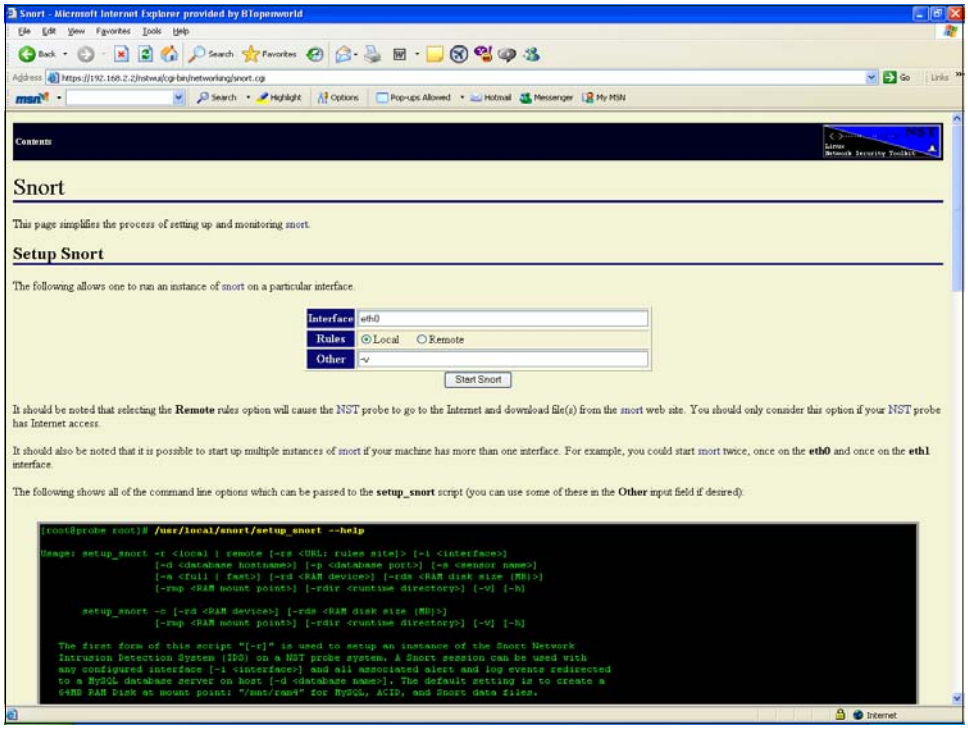


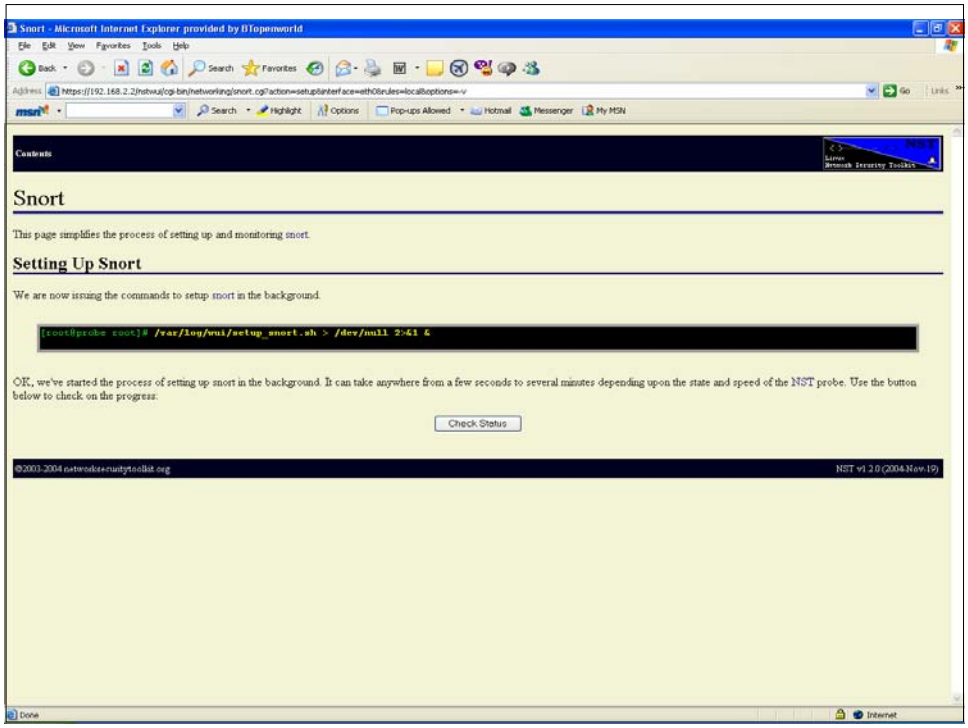


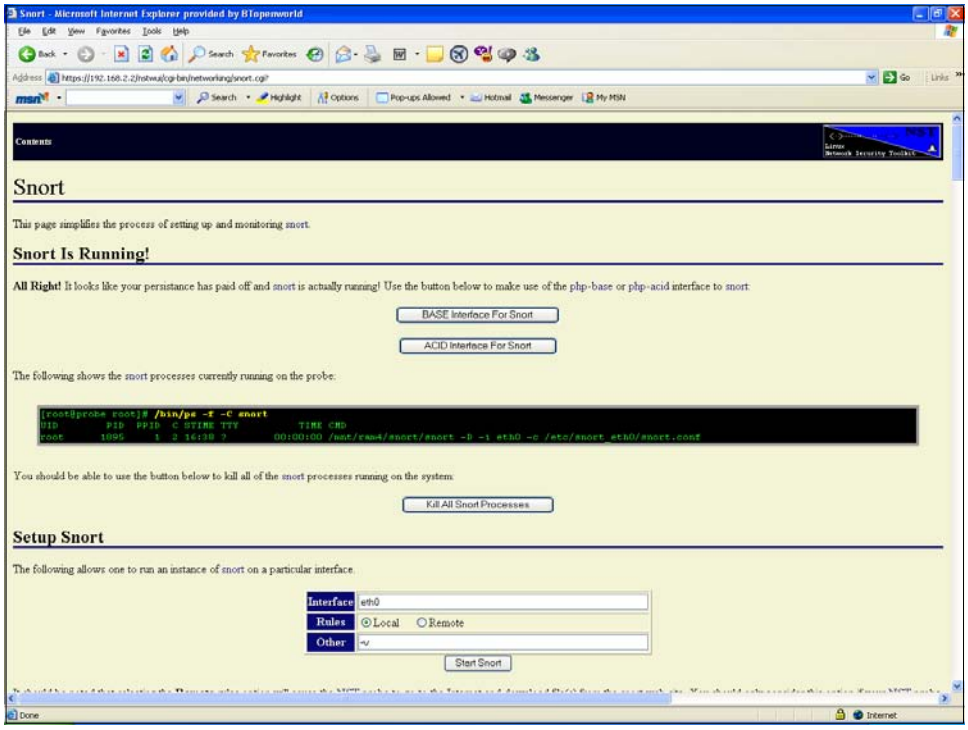

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Starting nessusd
We are now attempting to start the nessusd on the NST probe system in the background with the following command.
[root@probe root]# /usr/bin/sudo /usr/local/sbin/start_nessusd -v -p local > /var/log/nss/nessusd.log 2>&1 &
The nessusd process is now coming up - it may take awhile. You should be able to click here to return to the main nessus page and periodically press your browser's refresh button while you wait for the nessusd to come up.
©2003-2004 networksecuritytoolkit.org
NST v1.2.0 (2004-Nov-19)
Internet

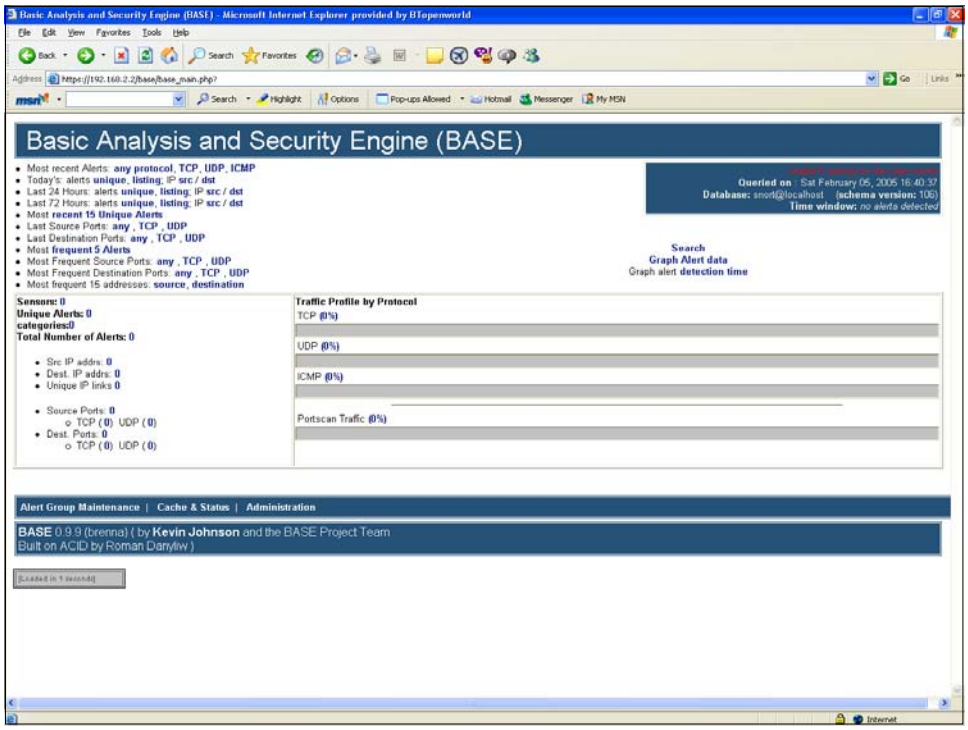

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Start Scan
nessus appears to be running on the NST probe at 192.168.2.2 and should be able to perform a scan (your system appears to be at 192.168.2.3). Please note, this will clear the results of any other system scan that has been performed through the web interface.
Start Scan
192.168.2.3
Be prepared to wait as a scan takes awhile (think 10 minutes of pressing the refresh button on your browser as you wait for the information to become available). A full subnet scan (like 192.168.0.0/24) takes a particularly long time - and may cause network printers to print many pages of garbage).
Stop Nessus
Use the button below if you would like to stop the nessus daemon and clean up the temporary files it loaded.
Stop Nessus Daemon
Log File(s)
The following shows the last 100 lines of the log file created when we last attempted to start or stop the nessus daemon (you may need to press your browser's refresh button to get it current status):
[root@probe root]# /usr/bin/tail --lines=100 /var/log/nss/nessusd.log
*** Creating a 70MByte RAM disk at mount point: "/mnt/ram4"...
/root/bin/create_ramdisk -s 72 -d /dev/ram4 -m /mnt/ram4 -v
* Creating a 73728KB RAM disk at mount point: /mnt/ram4... *
*** Zeroing out RAM device: "/dev/ram4"...
/bin/dd if=/dev/zero of=/dev/ram4 bs=1k count=73728
73728+0 records in
Internet

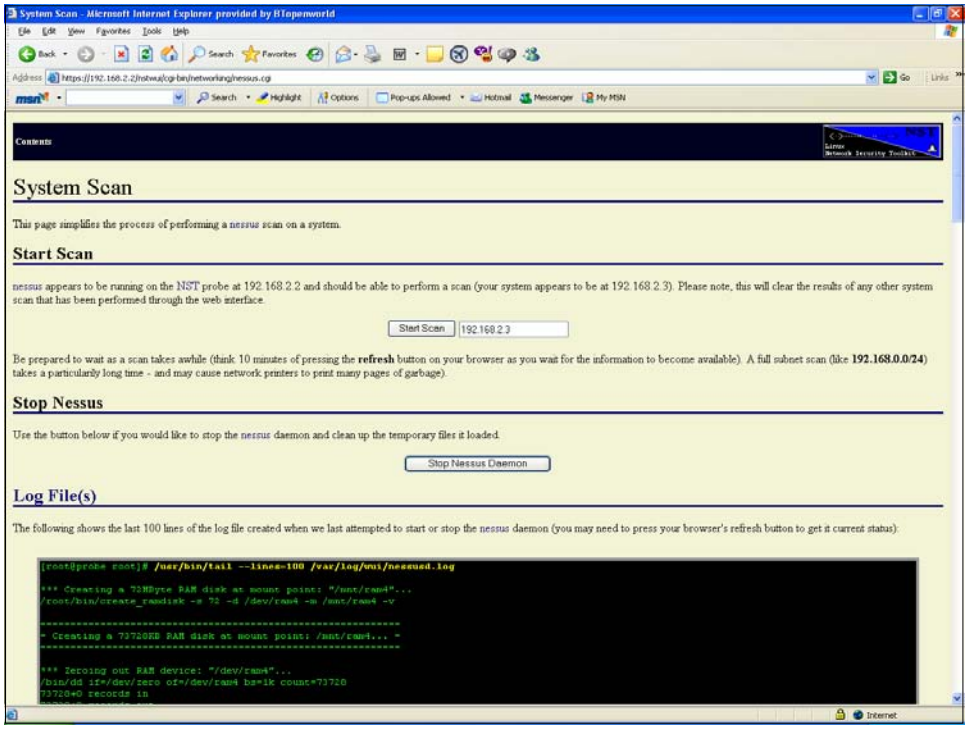

NST Web User Interface - Microsoft Internet Explorer provided by BTopenworld
Contents
NST Web User Interface
This set of web pages provides a simple web based user interface to common NST tasks.
Documentation
NST
README, Links, Change Log, Home, FAQ (PDF), User (PDF), Technical (PDF), At SourceForge
Installed Packages
Manifest, Man Pages, /docs
System
General
Run Command, Environment, phpSysInfo, Processes, Hardware, Services, Reboot, Halt, Power Down, /proc, sysctl
Web Server Log & Statistics
Logs, AWStats
Disk
Show Partitions
SQL Databases
MySQL, phpMyAdmin[1], PostgreSQL, phpPgAdmin[1]
Downloads
Windows Utilities
Virtual Computing
VNC
Serial Monitor
minicom, Monitor Serial
Networking
Interfaces
Ethernet, Wireless, Capture
Monitors
ntop, bandwidthd, bandwidthd UI[1], Argus Setup, Argus[1]
Intrusion Detection
Snort, Snort Collector, BASE[1], ACID[1]
Scanners
nmap, unicornscan, Nessus
Time Synchronization
NTP Info, NTP Query
eMail
sendmail
Utilities
dig, toptraceroute
X Based Applications
You must have a X server running to use these links (and it must accept connections from this NST probe).

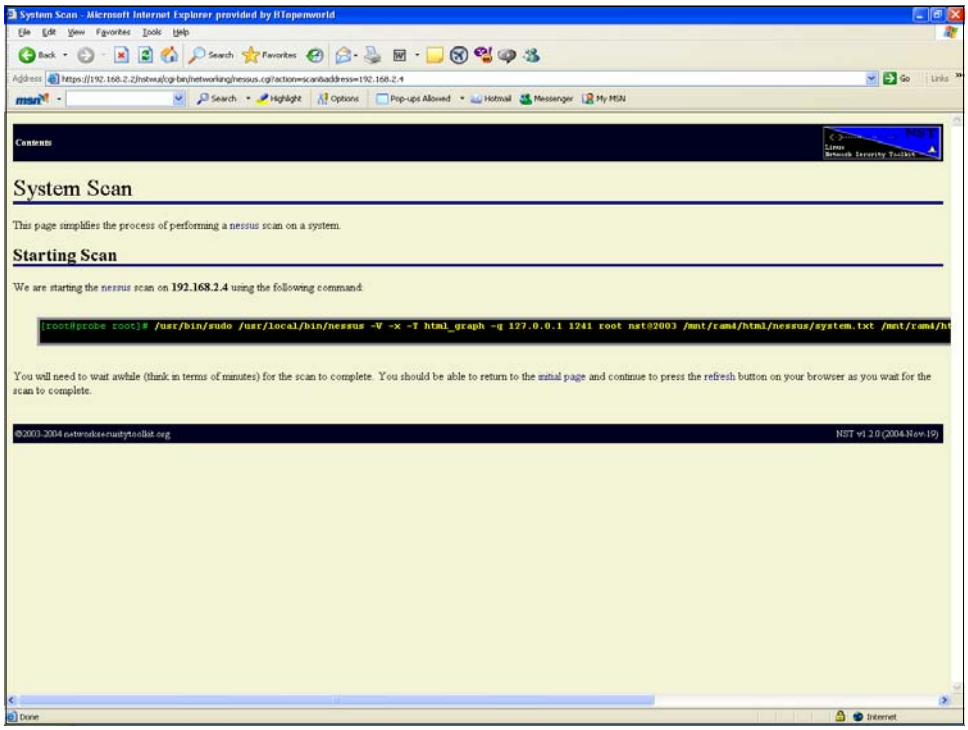

Snort - Microsoft Internet Explorer provided by BTopenworld
Contents
Snort
This page simplifies the process of setting up and monitoring snort.
Setup Snort
The following allows one to run an instance of snort on a particular interface.
Interface
eth0
Rules
Local
Remote
Other
-v
Start Snort
It should be noted that selecting the Remote rules option will cause the NST probe to go to the Internet and download file(s) from the snort web site. You should only consider this option if your NST probe has Internet access.
It should also be noted that it is possible to start up multiple instances of snort if your machine has more than one interface. For example, you could start snort twice, once on the eth0 and once on the eth1 interface.
The following shows all of the command line options which can be passed to the setup_snort script (you can use some of these in the Other input field if desired):
[root@probe root]# /usr/local/snort/setup_snort --help
Usage: setup_snort -r <local | remote [-rs <URL: rules site]> [-i <interface>]
[-d <database hostname>] [-p <database port>] [-s <sensor name>]
[-a <full | fast>] [-rd <RAM device>] [-rds <RAM disk size (MB)>]
[-rmp <RAM mount point>] [-rdir <runtime directory>] [-V] [-h]
setup_snort -c [-rd <RAM device>] [-rds <RAM disk size (MB)>]
[-rmp <RAM mount point>] [-rdir <runtime directory>] [-V] [-h]
The first form of this script "[-r]" is used to setup an instance of the Snort Network
Intrusion Detection System (IDS) on a NST probe system. A Snort session can be used with
any configured interface [-i <interface>] and all associated alert and log events redirected
to a MySQL database server on host [-d <database name>]. The default setting is to create a
64MB RAM Disk at mount point: "/mnt/ram4" for MySQL, ACID, and Snort data files.

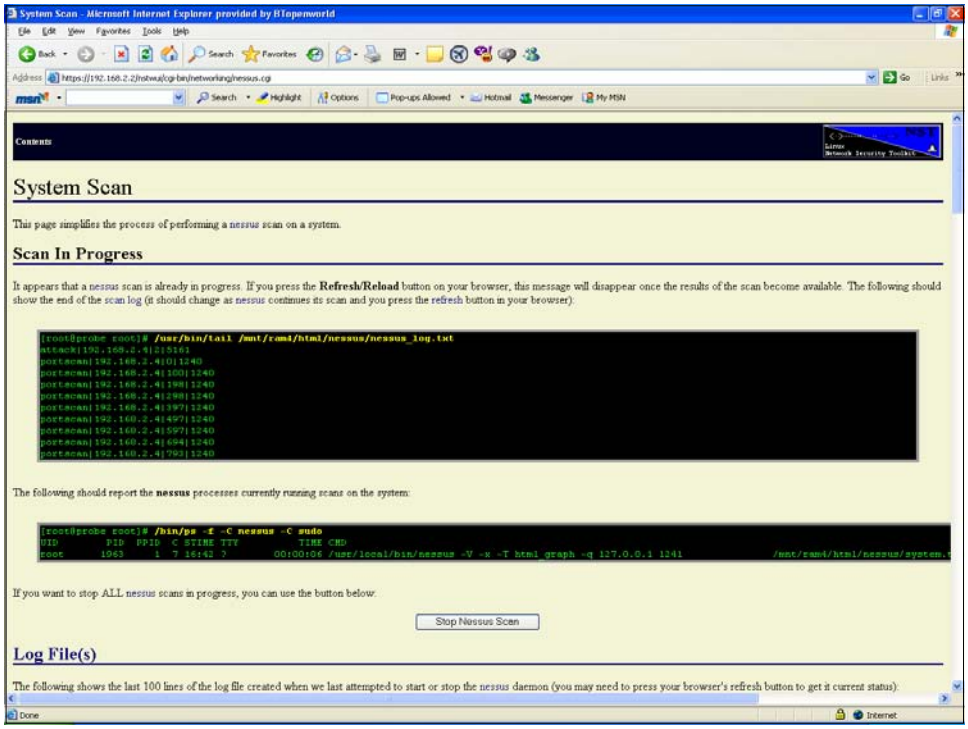

Snort - Microsoft Internet Explorer provided by BTopenworld
Contents
Snort
This page simplifies the process of setting up and monitoring snort.
Setting Up Snort
We are now issuing the commands to setup snort in the background.
[root@probe root]# /var/log/wui/setup_snort.sh > /dev/null 2>&1 &
OK, we've started the process of setting up snort in the background. It can take anywhere from a few seconds to several minutes depending upon the state and speed of the NST probe. Use the button below to check on the progress:
Check Status
©2003-2004 networks+unitytoolkit.org
NST v1.2.0 (2004.Nov.19)
Done
Internet

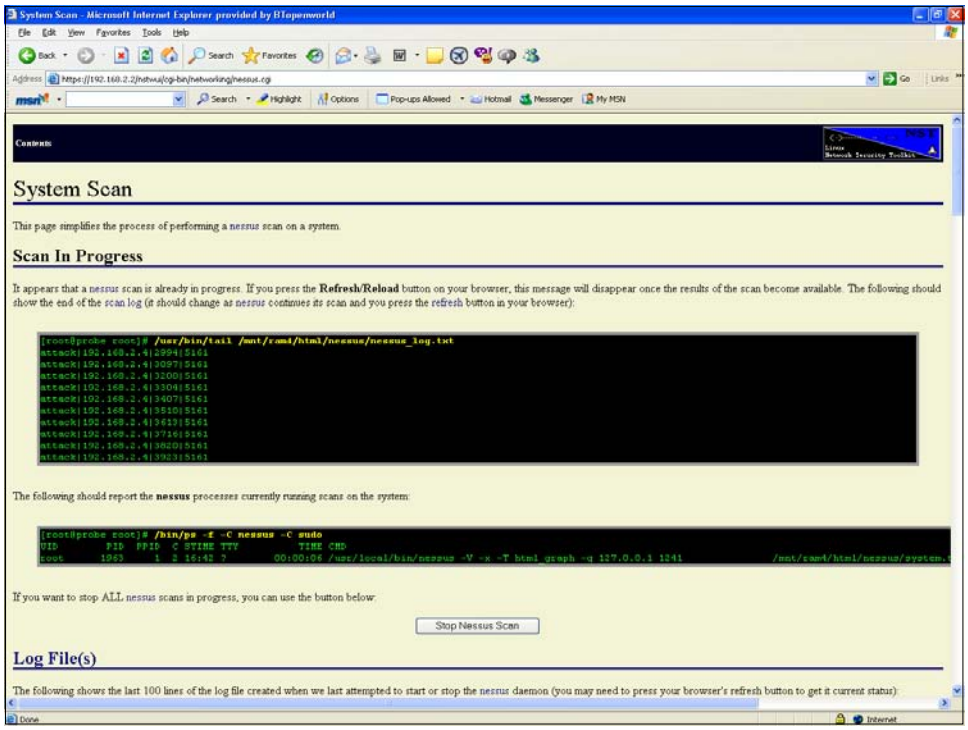

Snort - Microsoft Internet Explorer provided by BTopenworld
Contents
Snort
This page simplifies the process of setting up and monitoring snort.
Snort Is Running!
All Right! It looks like your persistance has paid off and snort is actually running! Use the button below to make use of the php-base or php-acid interface to snort:
BASE Interface For Snort
ACID Interface For Snort
The following shows the snort processes currently running on the probe:
[root@probe root]# /bin/ps -f -C snort
UID PID PPID C STIME TTY TIME CMD
root 1895 1 2 16:38 ? 00:00:00 /mnt/raw4/snort/snort -D -i eth0 -c /etc/snort_eth0/snort.conf
You should be able to use the button below to kill all of the snort processes running on the system:
Kill All Snort Processes
Setup Snort
The following allows one to run an instance of snort on a particular interface.
Interface eth0
Rules Local Remote
Other -v
Start Snort
Done
Internet

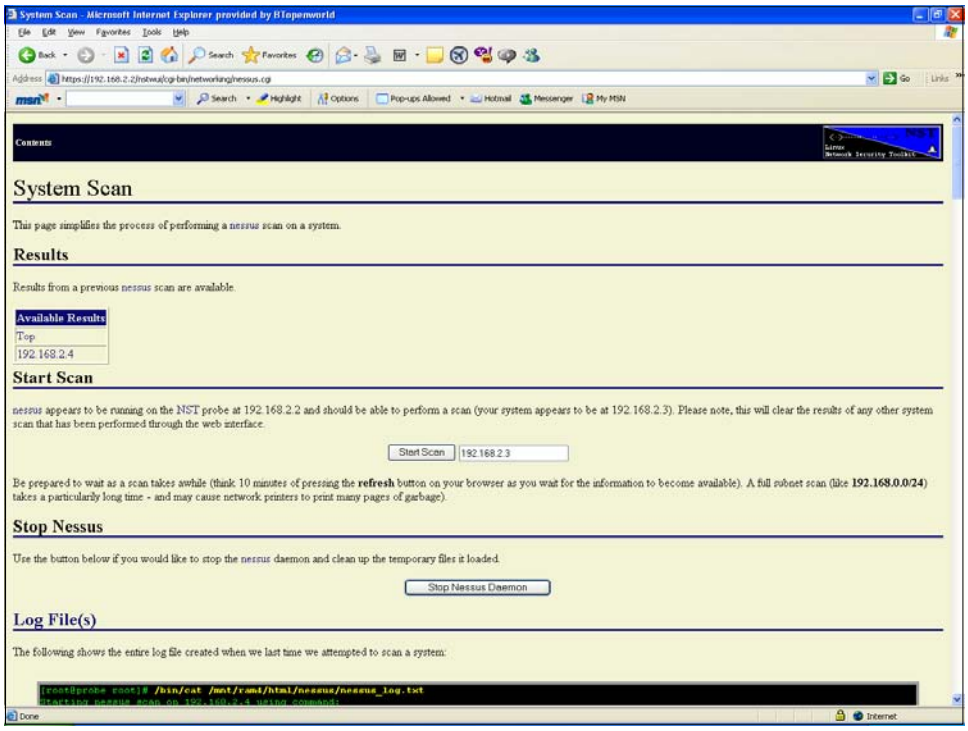

Basic Analysis and Security Engine (BASE) - Microsoft Internet Explorer provided by BTopenworld
Basic Analysis and Security Engine (BASE)
Most recent Alerts: any protocol, TCP, UDP, ICMP
Today's: alerts unique, listing, IP src / dst
Last 24 Hours: alerts unique, listing, IP src / dst
Last 72 Hours: alerts unique, listing, IP src / dst
Most recent 15 Unique Alerts
Last Source Ports: any , TCP , UDP
Last Destination Ports: any , TCP , UDP
Most frequent 5 Alerts
Most Frequent Source Ports: any , TCP , UDP
Most Frequent Destination Ports: any , TCP , UDP
Most frequent 15 addresses: source, destination
Queried on : Sat February 05, 2005 16:40:37
Database: snort@localhost (schema version: 106)
Time window: no alerts detected
Search
Graph Alert data
Graph alert detection time
Sensors: 0
Unique Alerts: 0
categories:0
Total Number of Alerts: 0
Src IP addrs: 0
Dest. IP addrs: 0
Unique IP links 0
Source Ports: 0
TCP (0) UDP (0)
Dest. Ports: 0
TCP (0) UDP (0)
Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)
Alert Group Maintenance | Cache & Status | Administration
BASE 0.9.9 (brenna) (by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw)

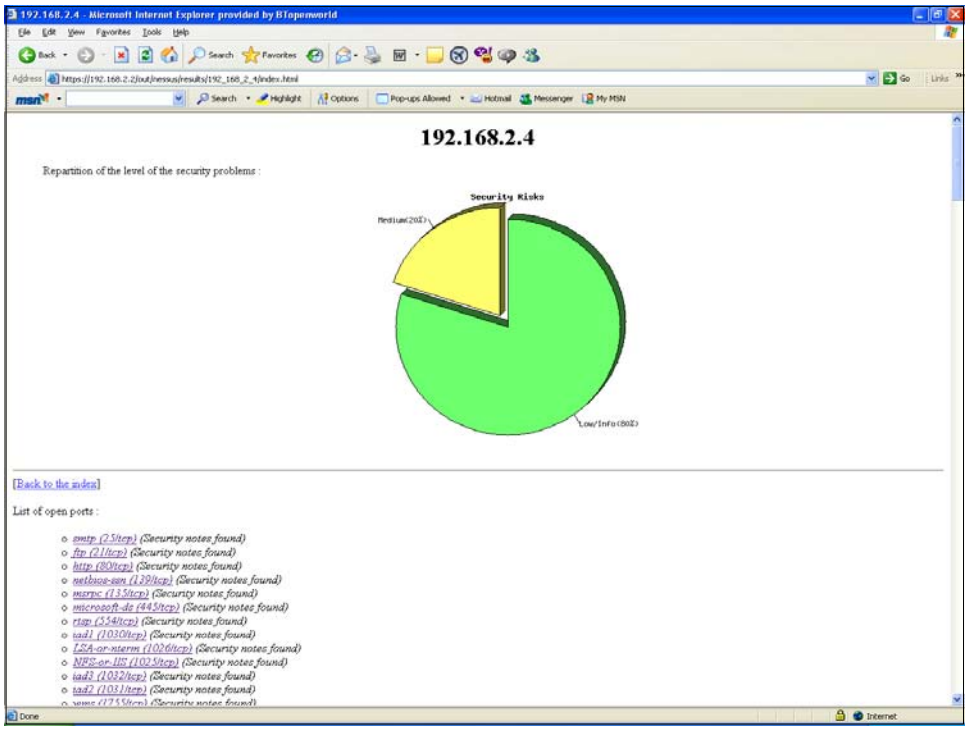

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Start Scan
nessus appears to be running on the NST probe at 192.168.2.2 and should be able to perform a scan (your system appears to be at 192.168.2.3). Please note, this will clear the results of any other system scan that has been performed through the web interface.
Start Scan
192.168.2.3
Be prepared to wait as a scan takes awhile (think 10 minutes of pressing the refresh button on your browser as you wait for the information to become available). A full subnet scan (like 192.168.0.0/24) takes a particularly long time - and may cause network printers to print many pages of garbage).
Stop Nessus
Use the button below if you would like to stop the nessus daemon and clean up the temporary files it loaded.
Stop Nessus Daemon
Log File(s)
The following shows the last 100 lines of the log file created when we last attempted to start or stop the nessus daemon (you may need to press your browser's refresh button to get it current status):
[root@probe root]# /usr/bin/tail --lines=100 /var/log/nms/nessusd.log
*** Creating a 72MByte RAM disk at mount point: "/mnt/ram4"...
/root/bin/create_ramdisk -s 72 -d /dev/ram4 -m /mnt/ram4 -v
= Creating a 73728KB RAM disk at mount point: /mnt/ram4... =
*** Zeroing out RAM device: "/dev/ram4"...
/bin/dd if=/dev/zero of=/dev/ram4 bs=1k count=73728
73728+0 records in

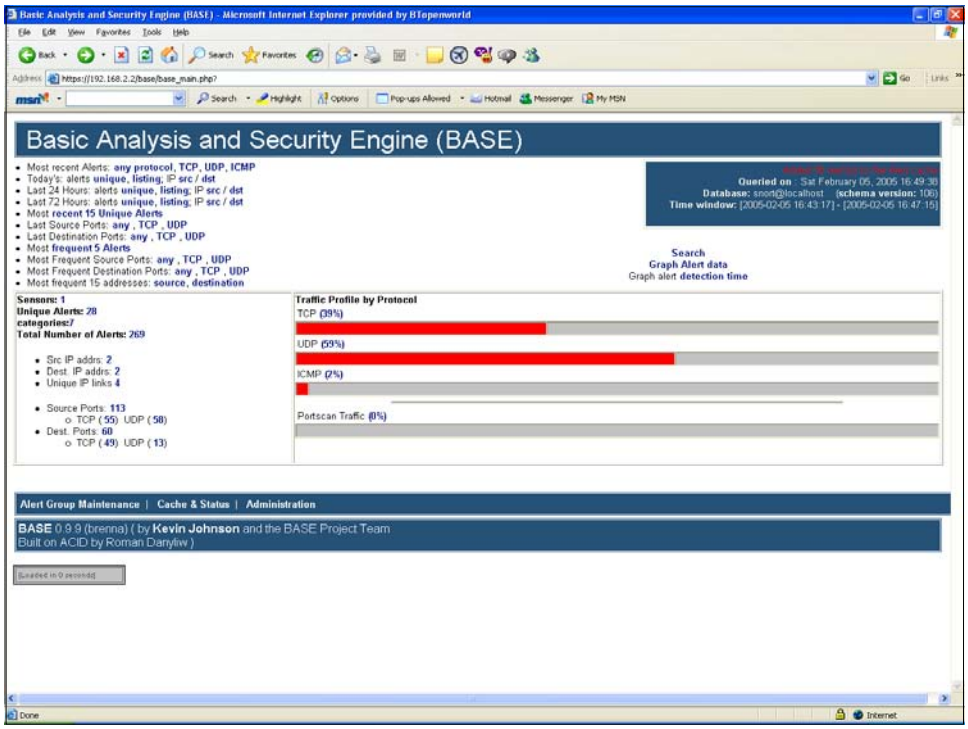

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Starting Scan
We are starting the nessus scan on 192.168.2.4 using the following command:
[root@probe root]# /usr/bin/sudo /usr/local/bin/nessus -V -x -T html_graph -q 127.0.0.1 1241 root nst@2003 /mnt/ram4/html/nessus/system.txt /mnt/ram4/ht
You will need to wait awhile (think in terms of minutes) for the scan to complete. You should be able to return to the initial page and continue to press the refresh button on your browser as you wait for the scan to complete.
©2003-2004 netwokxe-cuntytoolkit.org
NST v1.2.0 (2004-Nov-19)
Done
Internet

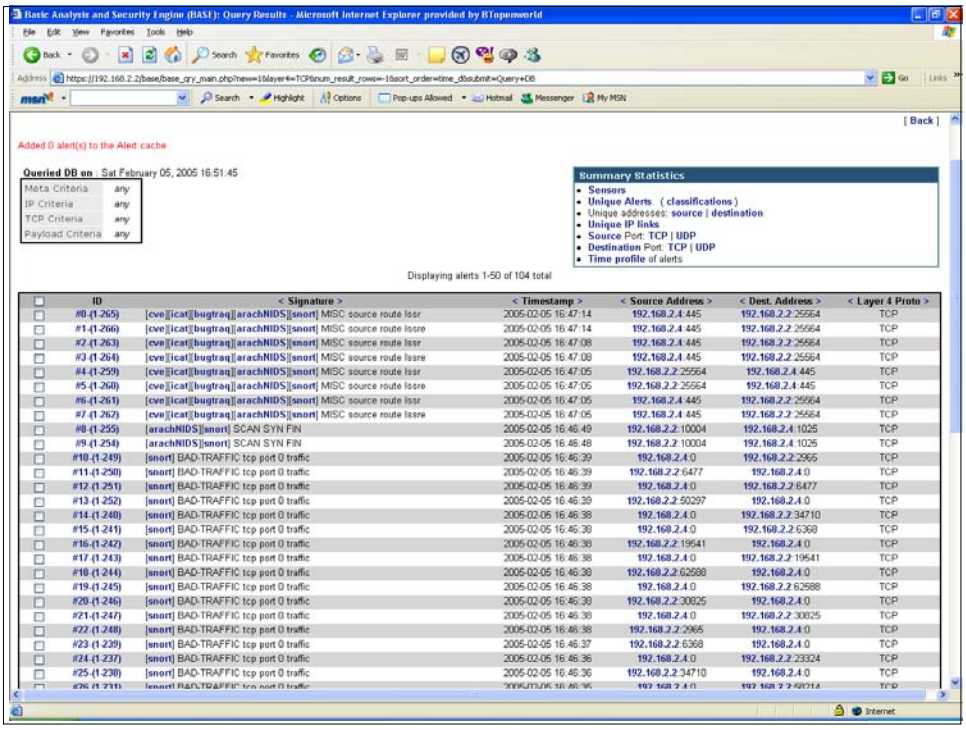

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Scan In Progress
It appears that a nessus scan is already in progress. If you press the Refresh/Reload button on your browser, this message will disappear once the results of the scan become available. The following should show the end of the scan log (it should change as nessus continues its scan and you press the refresh button in your browser):
[root@probe root]# /usr/bin/tail /mnt/ram4/html/nessus/nessus_log.txt
attack|192.168.2.4|2|5161
portscan|192.168.2.4|0|1240
portscan|192.168.2.4|100|1240
portscan|192.168.2.4|198|1240
portscan|192.168.2.4|298|1240
portscan|192.168.2.4|397|1240
portscan|192.168.2.4|497|1240
portscan|192.168.2.4|597|1240
portscan|192.168.2.4|694|1240
portscan|192.168.2.4|793|1240
The following should report the nessus processes currently running scans on the system:
[root@probe root]# /bin/ps -f -C nessus -C sudo
UID PID PPID C STIME TTY TIME CMD
root 1063 1 7 16:42 ? 00:00:06 /usr/local/bin/nessus -V -x -T html_graph -q 127.0.0.1 1241 /mnt/ram4/html/nessus/system.
If you want to stop ALL nessus scans in progress, you can use the button below:
Stop Nessus Scan
Log File(s)
The following shows the last 100 lines of the log file created when we last attempted to start or stop the nessus daemon (you may need to press your browser's refresh button to get it current status):
Done
Internet

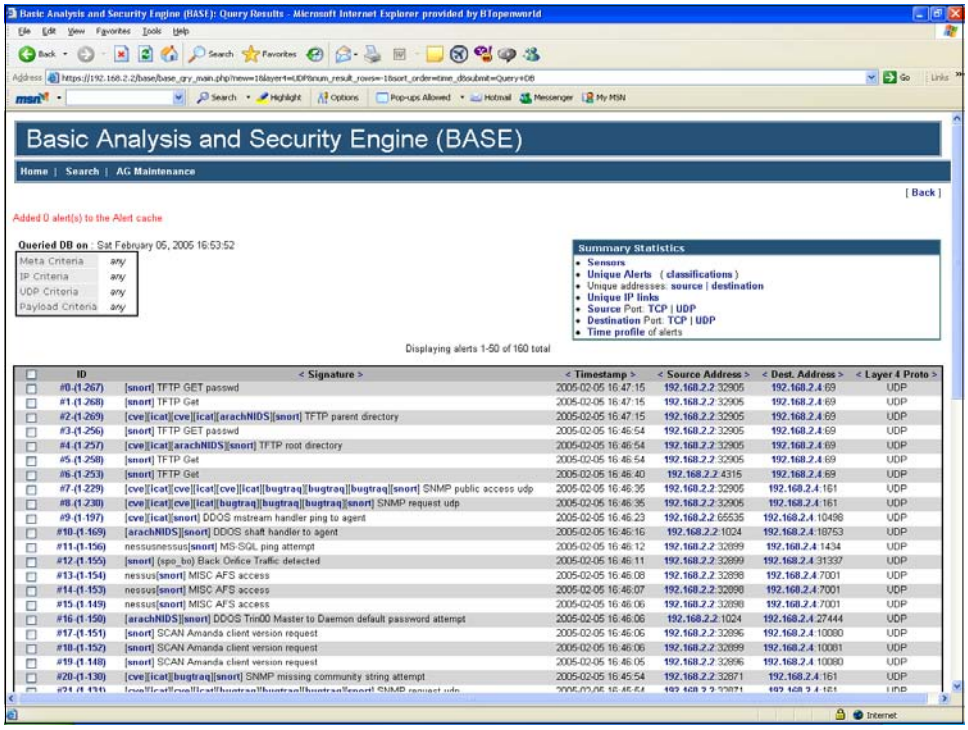

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Scan In Progress
It appears that a nessus scan is already in progress. If you press the Refresh/Reload button on your browser, this message will disappear once the results of the scan become available. The following should show the end of the scan log (it should change as nessus continues its scan and you press the refresh button in your browser):
[root@probe root]# /usr/bin/tail /mnt/ram4/html/nessus/nessus_log.txt
attack|192.168.2.4|2994|5161
attack|192.168.2.4|3097|5161
attack|192.168.2.4|3200|5161
attack|192.168.2.4|3304|5161
attack|192.168.2.4|3407|5161
attack|192.168.2.4|3510|5161
attack|192.168.2.4|3613|5161
attack|192.168.2.4|3716|5161
attack|192.168.2.4|3820|5161
attack|192.168.2.4|3923|5161
The following should report the nessus processes currently running scans on the system:
[root@probe root]# /bin/ps -f -C nessus -C suto
UID PID PPID C STIME TTY TIME CMD
root 1963 1 2 16:48 ? 00:00:06 /usr/local/bin/nessus -V -x -T html_graph -q 127.0.0.1 1241 /mnt/ram4/html/nessus/system.
If you want to stop ALL nessus scans in progress, you can use the button below:
Stop Nessus Scan
Log File(s)
The following shows the last 100 lines of the log file created when we last attempted to start or stop the nessus daemon (you may need to press your browser's refresh button to get it current status):
Done
Internet

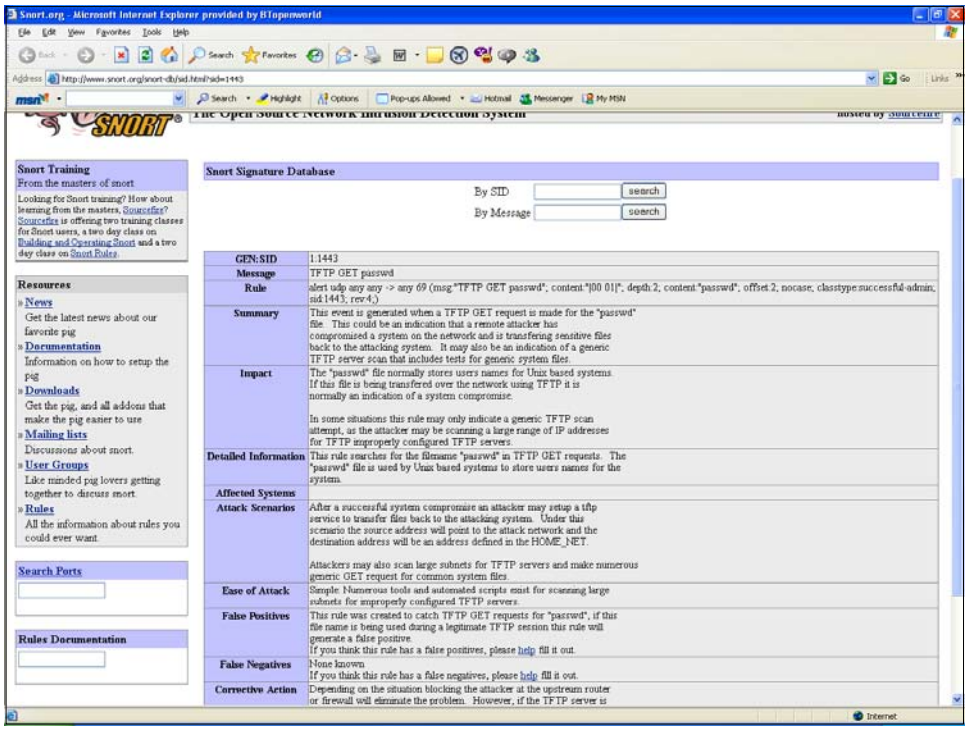

System Scan - Microsoft Internet Explorer provided by BTopenworld
Contents
System Scan
This page simplifies the process of performing a nessus scan on a system.
Results
Results from a previous nessus scan are available.
Available Results
Top
192.168.2.4
Start Scan
nessus appears to be running on the NST probe at 192.168.2.2 and should be able to perform a scan (your system appears to be at 192.168.2.3). Please note, this will clear the results of any other system scan that has been performed through the web interface.
Start Scan
192.168.2.3
Be prepared to wait as a scan takes awhile (think 10 minutes of pressing the refresh button on your browser as you wait for the information to become available). A full subnet scan (like 192.168.0.0/24) takes a particularly long time - and may cause network printers to print many pages of garbage).
Stop Nessus
Use the button below if you would like to stop the nessus daemon and clean up the temporary files it loaded.
Stop Nessus Daemon
Log File(s)
The following shows the entire log file created when we last time we attempted to scan a system:
[root@probe root]# /bin/cat /mnt/ram4/html/nessus/nessus_log.txt
Done
Internet

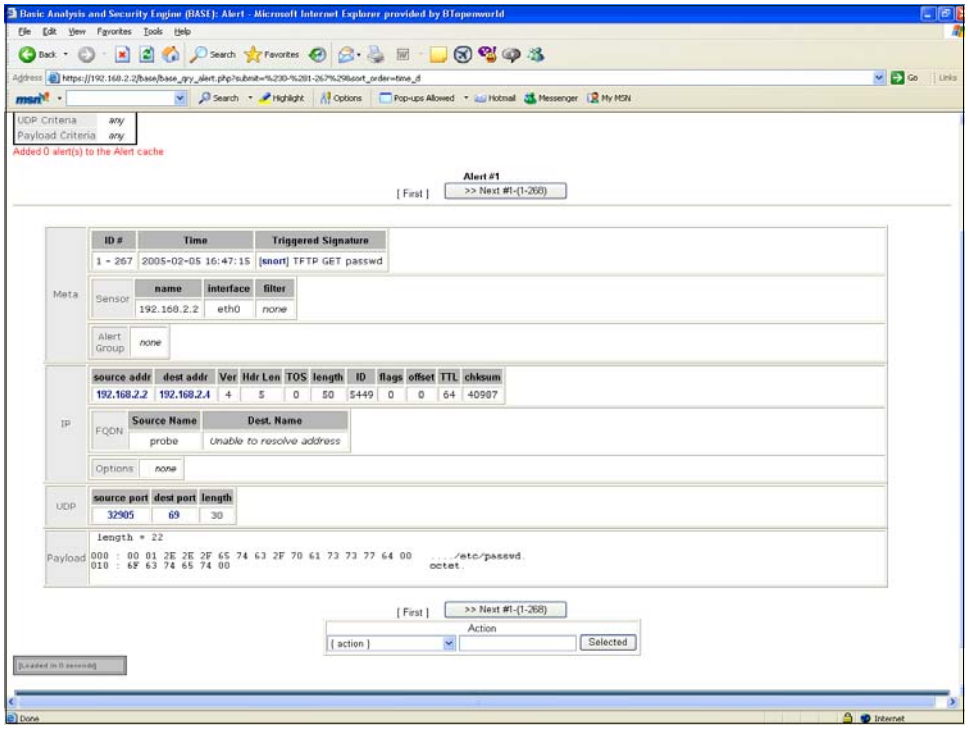

192.168.2.4 - Microsoft Internet Explorer provided by BTopenworld
192.168.2.4
Repartition of the level of the security problems :
Security Risks
Medium(20%)
Low/Info(80%)
[Back to the index]
List of open ports :
smtp (25/tcp) (Security notes found)
ftp (21/tcp) (Security notes found)
http (80/tcp) (Security notes found)
netbios-ssn (139/tcp) (Security notes found)
msrpc (135/tcp) (Security notes found)
microsoft-ds (445/tcp) (Security notes found)
rtsp (554/tcp) (Security notes found)
iad1 (1030/tcp) (Security notes found)
LSA-or-nterm (1026/tcp) (Security notes found)
NFS-or-IIS (1025/tcp) (Security notes found)
iad3 (1032/tcp) (Security notes found)
iad2 (1031/tcp) (Security notes found)

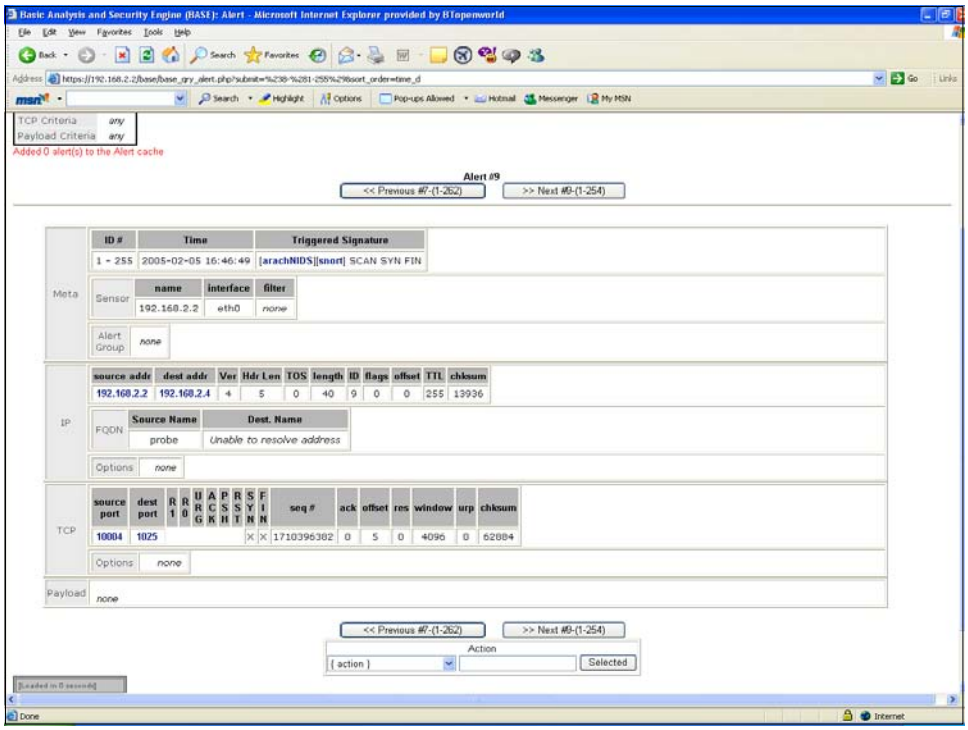

Basic Analysis and Security Engine (BASE) - Microsoft Internet Explorer provided by BTopenworld
Basic Analysis and Security Engine (BASE)
Most recent Alerts: any protocol, TCP, UDP, ICMP
Today's: alerts unique, listing, IP src / dst
Last 24 Hours: alerts unique, listing, IP src / dst
Last 72 Hours: alerts unique, listing, IP src / dst
Most recent 15 Unique Alerts
Last Source Ports: any , TCP , UDP
Last Destination Ports: any , TCP , UDP
Most frequent 5 Alerts
Most Frequent Source Ports: any , TCP , UDP
Most Frequent Destination Ports: any , TCP , UDP
Most frequent 15 addresses: source, destination
Queried on : Sat February 05, 2005 16:49:38
Database: snort@localhost (schema version: 106)
Time window: [2005-02-05 16:43:17] - [2005-02-05 16:47:15]
Search
Graph Alert data
Graph alert detection time
Sensors: 1
Unique Alerts: 28
categories:7
Total Number of Alerts: 269
Src IP addrs: 2
Dest. IP addrs: 2
Unique IP links 4
Source Ports: 113
TCP (55) UDP (58)
Dest. Ports: 60
TCP (49) UDP (13)
Traffic Profile by Protocol
TCP (39%)
UDP (59%)
ICMP (2%)
Portscan Traffic (0%)
Alert Group Maintenance | Cache & Status | Administration
BASE 0.9.9 (brenna) (by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw)


Basic Analysis and Security Engine (BASE): Query Results - Microsoft Internet Explorer provided by BTopenworld
[Back]
Added 0 alert(s) to the Alert cache
Queried DB on : Sat February 05, 2005 16:51:45
Meta Criteria any
IP Criteria any
TCP Criteria any
Payload Criteria any
Summary Statistics
Sensors
Unique Alerts (classifications)
Unique addresses: source | destination
Unique IP links
Source Port: TCP | UDP
Destination Port: TCP | UDP
Time profile of alerts
Displaying alerts 1-50 of 104 total
ID | < Signature > | < Timestamp > | < Source Address > | < Dest. Address > | < Layer 4 Proto >
#0-(1-265) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssr 2005-02-05 16:47:14 192.168.2.4:445 192.168.2.2:25564 TCP
#1-(1-266) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssre 2005-02-05 16:47:14 192.168.2.4:445 192.168.2.2:25564 TCP
#2-(1-263) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssr 2005-02-05 16:47:08 192.168.2.4:445 192.168.2.2:25564 TCP
#3-(1-264) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssre 2005-02-05 16:47:08 192.168.2.4:445 192.168.2.2:25564 TCP
#4-(1-259) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssr 2005-02-05 16:47:05 192.168.2.2:25564 192.168.2.4:445 TCP
#5-(1-260) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssre 2005-02-05 16:47:05 192.168.2.2:25564 192.168.2.4:445 TCP
#6-(1-261) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssr 2005-02-05 16:47:05 192.168.2.4:445 192.168.2.2:25564 TCP
#7-(1-262) [cve][icat][bugtraq][arachNIDS][snort] MISC source route lssre 2005-02-05 16:47:05 192.168.2.4:445 192.168.2.2:25564 TCP
#8-(1-255) [arachNIDS][snort] SCAN SYN FIN 2005-02-05 16:46:49 192.168.2.2:10004 192.168.2.4:1025 TCP
#9-(1-254) [arachNIDS][snort] SCAN SYN FIN 2005-02-05 16:46:48 192.168.2.2:10004 192.168.2.4:1025 TCP
#10-(1-249) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:39 192.168.2.4:0 192.168.2.2:2965 TCP
#11-(1-250) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:39 192.168.2.2:6477 192.168.2.4:0 TCP
#12-(1-251) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:39 192.168.2.4:0 192.168.2.2:6477 TCP
#13-(1-252) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:39 192.168.2.2:50297 192.168.2.4:0 TCP
#14-(1-248) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.4:0 192.168.2.2:34710 TCP
#15-(1-241) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.4:0 192.168.2.2:6368 TCP
#16-(1-242) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.2:19541 192.168.2.4:0 TCP
#17-(1-243) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.4:0 192.168.2.2:19541 TCP
#18-(1-244) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.2:62588 192.168.2.4:0 TCP
#19-(1-245) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.4:0 192.168.2.2:62588 TCP
#20-(1-246) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.2:30825 192.168.2.4:0 TCP
#21-(1-247) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.4:0 192.168.2.2:30825 TCP
#22-(1-248) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:38 192.168.2.2:2965 192.168.2.4:0 TCP
#23-(1-239) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:37 192.168.2.2:6368 192.168.2.4:0 TCP
#24-(1-237) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:36 192.168.2.4:0 192.168.2.2:23324 TCP
#25-(1-238) [snort] BAD-TRAFFIC tcp port 0 traffic 2005-02-05 16:46:36 192.168.2.2:34710 192.168.2.4:0 TCP


Basic Analysis and Security Engine (BASE): Query Results - Microsoft Internet Explorer provided by BTopenworld
Basic Analysis and Security Engine (BASE)
Home | Search | AG Maintenance
[Back]
Added 0 alert(s) to the Alert cache
Queried DB on : Sat February 05, 2005 16:53:52
Meta Criteria any
IP Criteria any
UDP Criteria any
Payload Criteria any
Summary Statistics
Sensors
Unique Alerts (classifications)
Unique addresses: source | destination
Unique IP links
Source Port: TCP | UDP
Destination Port: TCP | UDP
Time profile of alerts
Displaying alerts 1-50 of 160 total
ID | < Signature > | < Timestamp > | < Source Address > | < Dest. Address > | < Layer 4 Proto >
#0-(1-267) [snort] TFTP GET passwd 2005-02-05 16:47:15 192.168.2.2:32905 192.168.2.4:69 UDP
#1-(1-268) [snort] TFTP Get 2005-02-05 16:47:15 192.168.2.2:32905 192.168.2.4:69 UDP
#2-(1-269) [cve][icat][cve][icat][arachNIDS][snort] TFTP parent directory 2005-02-05 16:47:15 192.168.2.2:32905 192.168.2.4:69 UDP
#3-(1-256) [snort] TFTP GET passwd 2005-02-05 16:46:54 192.168.2.2:32905 192.168.2.4:69 UDP
#4-(1-257) [cve][icat][arachNIDS][snort] TFTP root directory 2005-02-05 16:46:54 192.168.2.2:32905 192.168.2.4:69 UDP
#5-(1-258) [snort] TFTP Get 2005-02-05 16:46:54 192.168.2.2:32905 192.168.2.4:69 UDP
#6-(1-253) [snort] TFTP Get 2005-02-05 16:46:40 192.168.2.2:4315 192.168.2.4:69 UDP
#7-(1-229) [cve][icat][cve][icat][cve][icat][bugtraq][bugtraq][bugtraq][snort] SNMP public access udp 2005-02-05 16:46:35 192.168.2.2:32905 192.168.2.4:161 UDP
#8-(1-230) [cve][icat][cve][icat][bugtraq][bugtraq][bugtraq][snort] SNMP request udp 2005-02-05 16:46:35 192.168.2.2:32905 192.168.2.4:161 UDP
#9-(1-197) [cve][icat][snort] DDOS mstream handler ping to agent 2005-02-05 16:46:23 192.168.2.2:65535 192.168.2.4:10498 UDP
#10-(1-169) [arachNIDS][snort] DDOS shaft handler to agent 2005-02-05 16:46:16 192.168.2.2:1024 192.168.2.4:18753 UDP
#11-(1-156) nessusnessus[snort] MS-SQL ping attempt 2005-02-05 16:46:12 192.168.2.2:32899 192.168.2.4:1434 UDP
#12-(1-155) [snort] (spo_bo) Back Orifice Traffic detected 2005-02-05 16:46:11 192.168.2.2:32899 192.168.2.4:31337 UDP
#13-(1-154) nessus[snort] MISC AFS access 2005-02-05 16:46:08 192.168.2.2:32898 192.168.2.4:7001 UDP
#14-(1-153) nessus[snort] MISC AFS access 2005-02-05 16:46:07 192.168.2.2:32898 192.168.2.4:7001 UDP
#15-(1-149) nessus[snort] MISC AFS access 2005-02-05 16:46:06 192.168.2.2:32898 192.168.2.4:7001 UDP
#16-(1-150) [arachNIDS][snort] DDOS Trin00 Master to Daemon default password attempt 2005-02-05 16:46:06 192.168.2.2:1024 192.168.2.4:27444 UDP
#17-(1-151) [snort] SCAN Amanda client version request 2005-02-05 16:46:06 192.168.2.2:32896 192.168.2.4:10080 UDP
#18-(1-152) [snort] SCAN Amanda client version request 2005-02-05 16:46:06 192.168.2.2:32899 192.168.2.4:10081 UDP
#19-(1-148) [snort] SCAN Amanda client version request 2005-02-05 16:46:05 192.168.2.2:32896 192.168.2.4:10080 UDP
#20-(1-130) [cve][icat][bugtraq][snort] SNMP missing community string attempt 2005-02-05 16:45:54 192.168.2.2:32871 192.168.2.4:161 UDP


Snort.org - Microsoft Internet Explorer provided by BTopenworld
Snort Training
From the masters of snort
Resources
News
Documentation
Downloads
Mailing lists
User Groups
Rules
Search Ports
Rules Documentation
Snort Signature Database
By SID
By Message
search
GEN:SID
1:1443
Message
TFTP GET passwd
Rule
Summary
Impact
Detailed Information
Affected Systems
Attack Scenarios
Ease of Attack
False Positives
False Negatives
Corrective Action


Basic Analysis and Security Engine (BASE): Alert - Microsoft Internet Explorer provided by BTopenworld
UDP Criteria any
Payload Criteria any
Added 0 alert(s) to the Alert cache
Alert #1
[First]
>> Next #1-(1-268)
ID #
Time
Triggered Signature
1 - 267
2005-02-05 16:47:15
[snort] TFTP GET passwd
Meta
Sensor
name
interface
filter
192.168.2.2
eth0
none
Alert Group
none
source addr
dest addr
Ver
Hdr Len
TOS
length
ID
flags
offset
TTL
chksum
192.168.2.2
192.168.2.4
4
5
0
50
5449
0
0
64
40987
IP
FQDN
Source Name
Dest. Name
probe
Unable to resolve address
Options
none
UDP
source port
dest port
length
32905
69
30
Payload
length = 22
000 : 00 01 2E 2E 2F 65 74 63 2F 70 61 73 73 77 64 00
010 : 6F 63 74 65 74 00
../etc/passwd.
octet.
[First]
>> Next #1-(1-268)
Action
[action]
Selected


Basic Analysis and Security Engine (BASE): Alert - Microsoft Internet Explorer provided by BTopenworld
TCP Criteria any
Payload Criteria any
Added 0 alert(s) to the Alert cache
Alert #9
<< Previous #7-(1-262)
>> Next #9-(1-254)
ID #
Time
Triggered Signature
1 - 255
2005-02-05 16:46:49
[arachNIDS][snort] SCAN SYN FIN
Meta
Sensor
name
interface
filter
192.168.2.2
eth0
none
Alert Group
none
IP
source addr
dest addr
Ver
Hdr Len
TOS
length
ID
flags
offset
TTL
chksum
192.168.2.2
192.168.2.4
4
5
0
40
9
0
0
255
13936
FQDN
Source Name
Dest. Name
probe
Unable to resolve address
Options
none
TCP
source port
dest port
R 1
R 0
URG
ACK
PSH
RST
SYN
FIN
seq #
ack
offset
res
window
urp
chksum
10004
1025
X
X
1710396382
0
5
0
4096
0
62084
Options
none
Payload
none
<< Previous #7-(1-262)
>> Next #9-(1-254)
Action
(action)
Selected
Done
Internet