Kevin Cardwell



JU

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.

AOK **H** TING

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 Southerm 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!

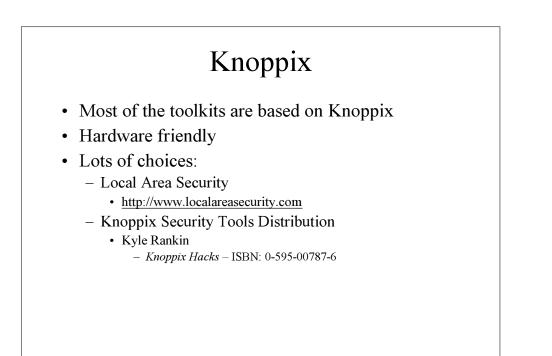
Tool Usage: Cont

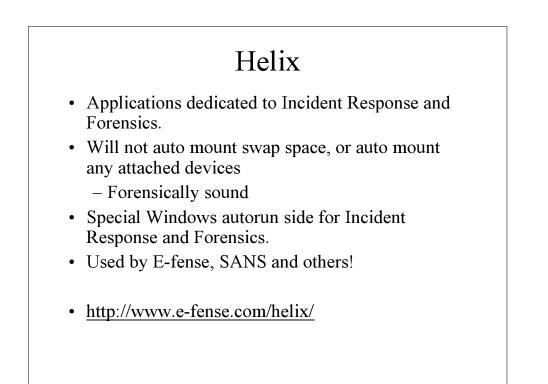
- Alternative approach
 - Tools Available at Boot!
 - No build requirements
 - No hard drive impact
 - Can use on any machine, and then restore to its normal operation!
 - Use on virtually any Intel system
 - Web based GUI
 - SSL, ssh etc
 - Powerful Scripts!



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





PHLAK

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

Auditor

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

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 <u>Fedora Core 2</u>. 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 (<u>NST</u>) 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: <u>Top 75</u> <u>Security Tools</u> by <u>insecure.org</u> 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
 - <u>http://www.networksecuritytoolkit.org/nst/index.ht</u>
 <u>ml</u>
 - 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 serverIf 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)

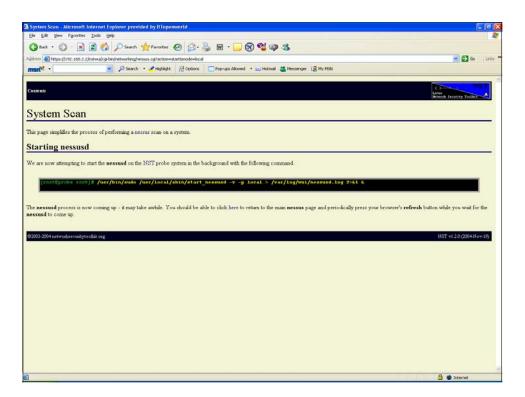
- There are 2 options
 - 1. Use the NST from the machine it is running on
 - 2. Connect to it from another machine
 - Open up browser and
 - Type https://IP ADDRESS/
 - NOTE:
 - » HTTPS
 - » Cannot log in via HTTP due to clear text login



NST WUI Screen Captures

Scheen all Mtps://192.168.2.2/nstwal	👻 🔂 🐼 🖄
nsn 🔨 💌 🔎	Search - 🥓 Highlight, 💦 Options. 📃 Pop-ups Allowed - 🛶 Hotmail 🍇 Messenger 😰 Hy HSN
ontents	Larger Largery Toulit
NST Web User Inter	face
his set of web names provides a simple we	b based user interface to common NST tasks.
	V ORIGINATION RECEIPTION OF CONTRAINING STOLE ARROWS
ocumentation	
ISI	README, Links, Change Log, Home, FAQ (PDF), User (PDF), Technical (PDF), At SourceForge
nstalled Packages	Manifest, Man Pages, /docs
ystem	
eneral	Run Command, Environment, phpSysInfo, Processes, Hardware, Services, Reboot, Halt, Power Down, /proc, syscil
Veb Server Log & Statistics	Logs, AWStata
Disk	Show Partitions
SQL Databases	MySQL, phpMyAdmin ¹ , PostgreSQL, phpPgAdmin ¹
Jownloads	Windows Unlines
/irtual Computing	VNC
Serial Monitor	minicom, Morator Serial
letworking	
nterfaces	Ethernet, Wireless, Capture
vIonitors .	ntop, bandwidthd, bandwidthd UT ¹ , Argus Setup, Argus ¹
intrusion Detection	Snort, Snort Collector, BASE ¹ , ACID ¹
Scanners	nmap, unicomacan, Nessua
Time Synchronization	NTP Info, NTP Query
Mail	rendmail
Julities	dig, teptraceroute
	*- Depender spon jetiter respect of other production

System Scan - Micro	soft Internet Explorer provided by BTopenworld	- Ø
	ontes Iools Help	
G Back • 🔘 •	🗷 🗟 🟠 🔎 Search 🧙 Favorites 🤣 🍰 🗟 🗧 😓 🚫 🕵 🧔 🖓	
Address 💽 https://192.1	(d).2.2/hshvul(cgi-bin/hetworking/hessus.cgi	🛩 🛃 Go 🛛 Lin
msn ^M ·	🖉 🔎 Search - 🥜 Highlight 🔥 Options 🔲 Pop-ups Allowed - 🔟 Hictmail 🚨 Messenger 😰 My MSN	
Contents		
System Sc	an	
This page simplifies th Start Nessus	ie process of performing a nessus scan on a system.	
	loes not seem to be running at the moment, or it has not yet finished its initialization (check the Log File). Stort Nersus with Local Plagins Stort Nersus with Latest Plugins option will cause the NST probe to go to the Latentt and download file(c) from the nersus web site. You should only o	ancider this antian if
your NST probe has		ounder and opposing
The /var/log/wui/nes	susd.log file wasn't found - so we have nothing to show you. This typically occurs if you have started/stopped the nessusd process outside of the WUI interface.	
Informationa	1	
For the curious, this I	TIML page uses the following commands available on the NST probe. To start up the neurus deamon.	
/usc/local/s	bin/start_bessund -v -p local	
Or:		
/use/iccal/s	bln/start_bessund -V -p remote	

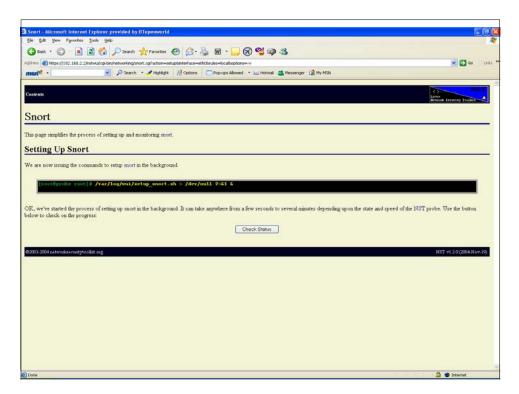


	ff Internet Explorer provided by BTopenworld	_ (B
Ele Edt Yew Favorite		
🕒 lack + 🔘 - 👱	👔 😰 🐔 🔎 Search 👷 Favorites 🛛 🔗 🐁 🗟 + 🥁 🔞 📽 🥨 🍪	
ģdress 🎒 https://192.168.1	2.2htmskg-bin/networking/nessus.cg	💌 🛃 Go 🔋 Lin
msn ^M ·	😕 🔎 Search 🔹 🥒 Highlight 🔥 Options 🔄 Pop-ups Allowed 🔹 🔤 Historial 🍱 Messenger 👔 My MSN	
Contents .	interest in the second se	everthy Toolbet
System Scar	n	
his page simplifies the p	process of performing a nessus scan on a system.	
Start Scan		
can that has been perfor le prepared to wait as a	ning on the NST probe at 192 168 2 3 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 a med through the web interface. Sinet Scan 192 168 2 3 a scan takes awhile (think 10 minutes of pressing the referesh button on your browser as you wait for the information to become available). A full subnet scan (like 19 time - and may cause network printers to pent many pages of garbage).	
se the button below if y	you would like to stop the nessue daemon and clean up the temporary files it loaded.	
	Stop Nessus Daemon	
Log File(s)		
he 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	it stabus):
[root@probe ro-	<pre>iot]# /usr/bin/taillines=100 /var/log/mui/nessusd.log</pre>	
	> T2HByre PAH disk at nount point: "/wmt/ram4" te_ramdisk =m 72 -d /dev/ram4 -m /wmt/ram4 -v	
	1972GERD FAR disk at mount point: /snt/can4	

	it RAM device: "/dev/ram4" v/zero of=/dev/ram4 bs=lk count=73720 te in	
		Internet

NST Web User Interface - Microsoft Intern	et Explorer provided by BTopenworld	
Ble Edit Yew Figworkes Iools Help		
🔇 Back + 🔘 · 🖹 🗟 🐔 🔎 Se	earch 👷 Favorites 🕢 😥 🍓 🖩 • 🔜 🕱 📽 🐢 🆓	
diress 1 https://192.160.2.2/nstwul/		Go Link
msn · .	search - 🖉 Highlight 🔣 Options 🦳 Pop-ups Allowed - 🔤 Historial 🌋 Messenger 😰 My MSN	
Contents	Lines	NINT Tolkit
NST Web User Interf	îace	
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, AWState	
Disk	Show Partitions	
SQL Databases	MySQL, phpMyAdmin ¹ , PostgreSQL, phpPgAdmin ¹	
Downloads	Windows Unlines	
Virtual Computing	VINC	
Serial Monitor	minicom, Monitor Serial	
Networking		
Interfaces	Ethernet, Wireless, Capture	
Monitors	ntop, bandwidthd, bandwidthd UT ¹ , Argus Setup, Argus ⁴	
Intrusion Detection	Snort, Snort Collector, BASE', ACID'	
Scanners	nmap, unicornscan, Nessus	
Time Synchronization	NTP Info, NTP Query	
eMail	sendmal	
Utilities	dig, toptraceroute	
	A - Depende open gebre entry o	f other package(i).
X Based Applications		
	The second s	-
Iou must have a X server running to use thes	se links (and it must accept connections from this NST probe).	
Dues	A	

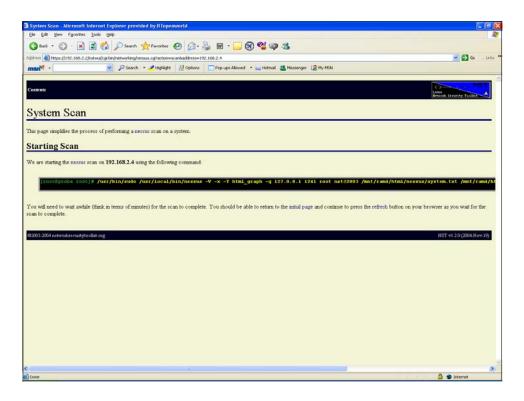
Snort - Microsoft Internet Explorer provided by BTopenworld	
Eine Edit Venn Fignanties Icals Help	
😮 hack + 🙄 - 🖹 🗟 🏠 🔎 Search 👷 Fararkes 🕖 🝰 - 🍑 🗟 + 🗍 🕄 🧐 🥵 🥥 🎎	
Ağdress 🝓 https://192.168.2.2/introdog-bin/networking/snort.cg	💌 🛃 Go 🔤 LH
man 🤄 🖉 Search 🔹 🥐 Highlight 👫 Cotions 🔲 Pop-ups Allowed 🔹 Wethmail 🌋 Messenger 👔 My MSN	
Concents. Snort	Arms Breatly Solitit
This page simplifies the process of setting up and monitoring mort. Setup Snort	
The following allows one to run an instance of snort on a particular interface.	
Interface eth0	
Rules O Local O Remote	
Other 😽	
Start Short	
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 mort web sit has Internet access.	e. You should only consider this option if your NST prob
It should also be noted that it is possible to start up multiple instances of most if your machine has more than one interface. For example, you could s interface.	tart mort twice, once on the eth0 and once on the eth1
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 fi	ield if desired).
[root8probe root]# /usr/incal/snort/setup snorthelp	
<pre>Mmage: setup_mnott -r <local <url;="" [-rs="" remote="" rules="" sis]="" =""> [- <interface>]</interface></local></pre>	
<pre>setup_anort -c [-rd <ram device="">] [-rds <ram (ru)5]="" <ram="" [-rup="" disk="" mount="" point="" size="">] [-rdir <runtime directory="">] [-v] [-h]</runtime></ram></ram></pre>	
The first form of this script "[-t]" is used to setup an instance of the Smort Hetwork Intrusion between [10] on a HST probe system. A Smort section can be used with any conjugated interface [-1 sinterface] and all associated aliert and log vertus redirected to a MySCL database server on host [-d database name]. The default setting is to create a 44MD FM bisk or bound point frame/came" for MySCL, ALLS, and Boost data bise.	
	🔒 🔮 Internet



3 Snort - Microsoft Internet Explorer provided by BTopenworld	- 6 8
Che Edit Yenn Fgrvates Iook Yelp	
🕝 Back + 🕑 - 🗷 🗟 🐔 🔎 Search 👷 Favorites 🥹 🎯 - 🌄 🔞 📲 - 🛄 🛞 🗳 🥥 🦓	
Ağdress 🔊 Mapsel/192.168.2.2/httmul/op/bin/hetmoning/snort.cgi?	🗙 🛃 Go 🛛 Links
msn 🕈 • 🖉 Search • 🥜 Highlight 🔥 Options 🔲 Pop-ups Allowed • 🔤 Hubmail 🍇 Messenger 👔 Hy MSH	
Cesarati	Latress Retwork Security Toubac
Snort	
This page simplifies the process of setting up and monitoring mort.	
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	
ADD Interface For Short	
The following shows the snort processes currently running on the probe:	
[rost]proke rost]# /bin/ps -E -C enert Uip P10 P10 C 577ME TTY TIME CMD root 1095 1 : 54510 7 00100100 /mst/sact/sact/sact -D -1 stab0 -C /stc/sact_stb0/sact.conf	
You should be able to use the button below to kall all of the snort processes running on the system: Kil All Snort Processes	
Setup Snort	
The following allows one to run an instance of snort on a particular interface.	
Interface ett0	
Rules OLocal ORemote	
Other	
Start Snort	
<mark>y</mark> (1997) - 1977) - 1	
0 Done	🔒 🔮 Internet

Basic Analysis and Security Engine (BASE) - Mic	osoft Internet Explorer provided by BTopenworld	
ije Edit Vjew Pgvorites Iools Help		4
🔇 Back + 🚫 + 🖹 📓 🏠 🔎 Search	🐈 Fevorites 🙆 🍰 🎍 🔟 📒 🐼 📽 🥥 🏂	
(dress) https://192.160.2.2/base/base_main.php?		💌 🛃 🐼 🕴 Unis
nsni ^N · 🖉 🔎 Search	* ZHighlight 👫 Options 🗔 Pop-ups Allowed * 🕁 Hotmail 🚳 Mess	senger 😰 My MSN
Basic Analysis and	Security Engine (BASE)	
 Most incent Aleris: any protocol. TCP. UDP: 10 Tody's alert unique, liteting. Perc / det Last 24 Hours: alert unique, liteting. Perc / det Last 22 Hours: alert unique, liteting. Perc / det Most recent 15 Unique Aleris Last Source Ports: any, TCP. UDP Last Source Ports: any, TCP, UDP Most Frequent O Aleris Most of the Aleris Aleris and any, TCP, UDP Most Frequent Destination Ports: any, TCP, UDP Most Frequent Destination Ports: any, TCP, UDP 	P	Queried on : Saf Fabroary (65, 2006 16, 60, 97 Database: strot(g)(scalboal: - Gabrona version: 105) Time wind(over no aberta defected Search Graph Alert data Graph alert data
Sensors: 0 Unique Alerts: 0 categories:0	Traffic Profile by Protocol TCP (0%)	
Total Number of Alerts: 0	UDP (0%)	
Src IP addrs: 0 Dest. IP addrs: 0 Unique IP links 0	ICMP (0%)	
 Source Ports: 0 TCP (0) UDP (0) Dest. Ports: 0 TCP (0) UDP (0) 	Portsoan Traffic (0%)	
Alert Group Maintenance Cache & Status SASE 0.9.9 (branna) (by Kevin Johnson Built on ACID by Roman Darryllw) Sustee (in tyuona)		
		a 🕲 itionat

System Scan - Microsoft 1	internet Explorer provided by BTopenworld	
Ele Edt Yew Favorites		
3 tock + 3 - 🗷	😰 🟠 🔎 Search 👷 Farcekes 🕢 🍰 💀 - 📴 🕱 🗳 🥥 🤹	
Address 🗿 https://192.168.2.2/	Instructiog-bin/networking/nessus.cgi	💌 🛃 Go 🛛 Links
man ^{**} ·	🖉 🔎 Search 🔹 🥒 Highlight 🔠 Options 🔄 Pop-ups Allowed 🔹 🔤 Historial 🍇 Messenger 😰 My MSN	
Contents		Come I NST
Contents		Betwork Security Toulast
System Scan		
System Sean		
This page simplifies the pro-	cess of performing a nessue scan on a system.	
Start Scan		
Start Scan		
	ig 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 ed through the web interface.	note, this will clear the results of any other system
	Start Scan 192 168 2 3	
	an takes awhile (think 10 minutes of pressing the refresh button on your browser as you wait for the information to become av	allable). A full subnet scan (like 192.168.0.0/24)
takes a particularity long tim	se - and may cause network printers to print many pages of garbage).	
Stop Nessus		
Use the button below if you	i would like to stop the nessus daemon and clean up the temporary files it loaded.	
	Stop Nessus Daemon	
Log File(s)		
annanan ar anna		An exception of the second second second
The following shows the las	t 100 lines of the log file created when we last attempted to start or stop the nessus daemon (you may need to press your brown	ser's refresh button to get it current status)
]# /usr/bin/taillines=100 /var/log/mui/nessusd.log	
	2HByte PAH disk at mount point: "/mnt/ram4" ramdisk -= 72 -d /dev/ram4 -m /mnt/ram4 -v	
	-	
	20KD RAN disk at mount point: /mnt/cam4 =	
	RAN device: "/dev/ram4" zero of=/dev/ram4 bs=1k count=73728	
73720+0 records		
		A A Internet

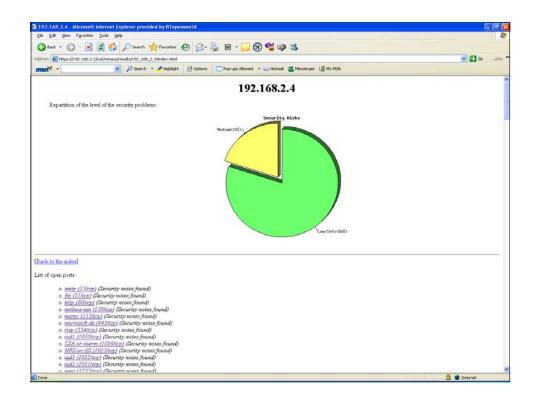


System Scan - Microsoft Internet Explorer provided by BToperworld	
Elle Edit view Figurates Icols Help	
🔇 bak + 🕐 - 🖹 🗟 🟠 🔎 Search 👷 Favorites 🤣 😥 - 🌄 🛞 🥞 🧐 🦓 🥥 🦓	
gåress 🜒 https://192.168.2.2/instwa/cgi-bin/networking/nessus.cgi	🗙 🔂 Go 🛛 Links
msn 🖣 🔹 🖉 Search 🔹 Z Highlight 🔥 Options 🔲 Pop-ups Allowed 🔹 🔤 Histmail 🙇 Messenger	L2 Hy MIN
Contents	Anno broat
System Scan	
This page simplifies the process of performing a neurous scan on a system. Scan In Progress	
It appears that a nerrors scan is already in progress. If you press the Refresh/Reload button on your browser, this message w show the end of the scan log (it should change as nersors continues its scan and you press the refresh button in your browser).	all dirappear once the results of the scan become available. The following should
<pre>[rootBgrOne root]# /usr/bin/tall /unt/rami/fitml/nrsmus/nessus_log.ixt attack[150.160.4.4]=15163 pottaema[150.460.4.4]=15163 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2440 pottaema[150.460.4.4]=100]2400 pottaema[150.460.4.4]=100]240 pottaema[150.460.4.4]=100]240 pottaema[150.460.4.4]=100]240</pre>	
The following should report the nessus processes currently running scans on the system:	
[root0probe root]# /bin/ps -f -C nessus -C suds DID DID PID C STIME TTY TIME CMD Foot 1063 1 7 16:41 7 00:00:06 /ust/local/bin/messus -V -x -T html graph	-q 127.0.0.1 1241 /mit/zam4/html/nedsus/system.t
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 n	ay need to press your browser's refresh button to get it current status).
Done	🙆 🔮 Internet

System Scan - Microsoft Internet Explorer provided by BTopernworld	
(He Edit Yew Provintes Icols Help	4
🔾 Back + 🔘 - 🖹 🗟 🖚 🔎 Search 👷 Ferrorites 🤣 😥 + 🍑 🗟 - 💆 🐼 🗳 🥥 🎉	
Agdress 👔 https://142.160.2.2/nstwa/og-bin/networking/nessus.cg	💌 🔁 Go 🔤 Links
man ^N · PSearch · Phylicit 🖓 Options 🔽 Pop-ups Alowed · Withmail 🖏 Messenger 😰 Hy MSN	
Сантик	Little Based Security Perilat
System Scan	
This page simplifies the process of performing a nearus scan on a system. Scan In Progress	
It appears that a nersus scan is already in progress. If you press the Refresh/Reload button on your browser, this message will disappea show the end of the scan log (it should change as nersus continues its scan and you press the refirsh button in your browser):	ar once the results of the scan become available. The following should
[root@proke toot]# /usr/bin/tail /mst/romi/him}/nessus/nessus_log.twt attacks[102.468.4.1]2591[364 attacks] 102.468.4.1]200[364] attacks] 102.468.4.1]200[364] attacks] 102.468.4.1]300[364] attacks] 102.468.4.1]3500[365] attacks] 102.468.4.1]3500[365] attacks] 102.468.4.1]3500[365] attacks] 102.468.4.1]3500[365] attacks] 102.468.4.1]3500[365] attacks] 102.468.4.1]3500[365]	
The following should report the nexsus processes currently running scans on the system:	
[costBprobe cost]# /bin/ps -# -C negsus -C sudo ULD F1D F1D C STIME TTY TIME CMD cost 1965 1 2 16:42 ? Ob:00:06 /wsc/local/bin/nessus -V -x -T html_graph -q 127.0.	.0.1 1241 /mst/cam4/html/nssua/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 neurus daemon (you may need to	press your browser's refresh button to get it current status)
Done	🚔 🐲 Internet

3 System Scan - Microsoft Internet Explorer provided by 8Topenworld	
Elle Edit View Figurantes Icolis Unit	4
🔇 Back + 🙄 - 🖹 🗟 🟠 🔎 Search 👷 Ferrarkes 🤣 🎯 - 🍑 🗃 + 🔂 🕄 🥥 🤹	
Address 👩 https://192.168-2.2/notwolog-be/networking/nessus.cg	😴 🛃 Go 🛛 Links
man 🕅 • 🖉 🖉 Search • 🥒 Highlight 👫 Options 🔤 Pop-ups Allowed • 🔤 Histonal 🦉 Messenger 👔 My MSN	
Салила	Linne Minimità Jacobility Zonikit
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 192 163 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 16 scan that has been performed through the web interface. [Start Scan] [122 168 2.3	68.2.3). Please note, this will clear the results of any other system
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 takes a particularly long time - and may cause network printers to print many pages of garbage).	n to become available). A full subnet scan (like $192.168.0.0/24$)
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:	
[rootBprobe root]# /bin/cat /mnt/rami/html/nessus/nessus_log.txt	
HEALASIN MANNU AGAN ON 122 INU-24 MAINE COMMANDE	🔒 🔮 Internet

BLACK HAT BRIEFINGS



		S 🖸 😒
nan 🔍 🖌 🖌 Soar	ch 🔹 🥜 Highlight 🛛 👬 Options 📄 Pop-ups Allowed 🔹 🐸 Hotmail	🚜 Messenger 👔 Hy MSN
Basic Analysis an	d Security Engine (BASE)
Most recent Alerts: any protocol TCP UDP Tody's alerts unique, limits, Pare / Art Latt 24 Most and the second second second Latt 24 Most and the second second second second Latt 30 works Ports: any, TCP, UDP Last Generation Ports: any, TCP, UDP Most Frequent 5 Alerts Most Frequent Second second second second Most Frequent Second second second second Most Frequent Second second second second Most Frequent Second second second second second Most Frequent Second second second second second Most Frequent Second second second second second second Most Frequent Second second second second second second Most Frequent Second second second second second second second second	ICMP dat dat DIP	Queried on . Saf February 05, 2005 16.43 Database: trentgile::about Time window: (2005/02/06 16.43 17) - (2005/02/06 16.47 1 Search Graph Alart data Graph Alart data Graph Alart data
ensors: 1 nique Alerts: 28 stegories:7	Traffic Profile by Protocol TCP (39%)	
stal Number of Alerts: 269	UDP (59%)	
Src IP addrs: 2 Dest. IP addrs: 2 Unique IP links 4	ICMP (25)	
 Source Ports: 113 TCP (55) UDP (58) Dest. Ports: 60 TCP (49) UDP (13) 	Portscan Traffic (0%)	
lert Group Maintenance Cache & Status		
ASE 0.9.9 (brenna) (by Kevin Johnso uit on ACID by Roman Darwliw)	n and the BASE Project Team	
raded in Q seconds		

in file		rity Engine (BASE): Query Results - Microsoft Internet Explorer provided	by BTopenworld			
	: Yew Pavorites					
Back	· O · *	📓 🏠 🔎 Search 👷 Favortes 🚱 🔗 - 🍡 🔟 😓 🗑) 🐒 🚳 🚳			
	biter-1/102 160 2	2/base/base grv main.php?mew=18/aver#=TOPtinum result rows=-18/sort order=time d	hadentu Cuerva CB			🗸 🛃 Go
	and the second se			1		
IS/N	•L	🖌 🔎 Search 🔹 🥒 Highlight 👫 Options 🔲 Pop-ups Allowed	• Wessenger	My MSN		
						[Bac
ded 0 a	alert(s) to the Aler	trache				
ueried	DB on : Sat Feb	muary 05, 2005 16:51:45	Sur	mmary Statistics		
leta C	ritoria any		• S	ensors	210X-1	
P Crite	ria any			nique Alerts (classification		
CP Cri	itena any			nique addresses: source der nique IP links	stination	
ayload	d Criteria any			ource Port: TCP UDP		
		7 (f)	• D	estination Port: TCP UDP		
			• TI	ime profile of alerts		
		Displaying all	erts 1-50 of 104 total			
	ID	< Sinnature >	< Timestamp >	< Source Address >	< Dest, Address >	< Layer 4 Proto 3
õ	#0-(1-265)	[cve][icat][bugtrag][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 Issre	2005-02-05 16:47:14	192.168.2.4:445	192.168.2.2 25564	TCP
D.	#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 25554	TCP
	#3-(1-264)	[cve][icat][bugtrag][arachNIDS][snort] MISC source route Issre	2005-02-05 16:47:08	192.168.2.4.445	192.168.2.2 25564	TCP
	#3-(1-264) #4-(1-259)	[cve][icat][bugtraq][arachNIDS[[snort] MISC source route Issre [cve][icat][bugtraq][arachNIDS[[snort] MISC source route Issr	2005-02-05 16 47:08 2005-02-05 16:47:05	192.168.2.4.445 192.168.2.2.25564	192.168.2.2 25564 192.168.2.4.445	TCP TCP
	#4-(1-259)	[cve][icat][bugtraq][arachNIDS][smort] MISC source route lssr	2005-02-05 16:47:05	192.168.2.2.25564	192.168.2.4.445	TCP
	#4-(1-259) #5-(1-260)	[cve][icat][bugtraq][arachNIDS][snort] MISC source route issr [cve][icat][bugtraq]]arachNIDS][snort] MISC source route issre	2005-02-05 16:47:05 2005-02-05 16:47:05	192.168.2.2 25564 192.168.2.2 25564	192.168.2.4:445 192.168.2.4:445	TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261)	[cve][icat][bugtreq][erachNIDS][snort] MISC source route issr [cve][icat][bugtreq][erachNIDS][snort] MISC source route issre [cve][icat][bugtreq][erachNIDS][snort] MISC source route issr	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05	192.168.2.2 25554 192.168.2.2 25554 192.168.2.4 445	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25564	TCP TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262)	[cve][icat][bugtraq][arachNIDS][snort] MISC source route issr [cve][icat][bugtraq][arachNIDS][snort] MISC source route issr [cve][icat][bugtraq][arachNIDS][snort] MISC source route issr [cve][icat][bugtraq][arachNIDS][snort] MISC source route issre	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05	192.168.2.2 25554 192.168.2.2 25554 192.168.2.4 445 192.168.2.4 445	192.168.2.4.445 192.168.2.4.445 192.168.2.2.29564 192.168.2.2 25564	TCP TCP TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262) #8-(1-255)	[cve][icat][bugtan][arachNIDS][snort] MISC source route lists [cve][icat][bugtan][arachNIDS][snort] MISC source route lists [cve][icat][bugtan][arachNIDS][snort] MISC source route lists [cve][icat][bugtan][arachNIDS][snort] MISC source route lists [arachNIDS][snort] SCAN SYN FIN	2005-02-05 16 47 05 2005-02-05 16 46 49	192.168.2.2 25554 192.168.2.2 25554 192.168.2.4 445 192.168.2.4 445 192.168.2.4 445 192.168.2.2 10004	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25664 192.168.2.2.25564 192.168.2.4.1025	TCP TCP TCP TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262) #8-(1-255) #9-(1-254)	[cve][icat][bugtaq][arachNDS][snot] MSC source route iss [cve][icat][bugtaq][arachNDS[snot] MSC source route iss [cve][icat][bugtaq][arachNDS[snot] MSC source route iss [cve][icat][bugtaq][arachNDS[snot] MSC source route isse [arachNDS][snot] SCAN SYN FN [arachNDS][snot] SCAN SYN FN	2005-02-05 16:47.05 2005-02-05 16:47.05 2005-02-05 16:47.05 2005-02-05 16:47.05 2005-02-05 16:46:49 2005-02-05 16:46:48	192.168.2.2 25564 192.168.2.2 25564 192.168.2.4 245 192.168.2.4 245 192.168.2.4 245 192.168.2.2 10004	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25564 192.168.2.4.1025 192.168.2.4.1025	TCP TCP TCP TCP TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262) #8-(1-255) #9-(1-254) #10-(1-249)	Iver_itcat[bingtrag]arachNUS]smont MSS source route har [cve_itcat]bingtrag]arachNUS_sound MSS cource code hare [cve_itcat]bingtrag]arachNUS_[cond] MSS source route hare [arachNUS]spingt SCAN STVF FN [arachNUS]spingt SCAN STVF FN [arachNUS]spingt SCAN STVF FN	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:45:48 2005-02-05 16:45:48 2005-02-05 16:46:39	192.168.2.2 25554 192.168.2.2 25554 192.168.2.4 445 192.168.2.4 445 192.168.2.2 10004 192.168.2.2 10004 192.168.2.4 10	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25564 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.1025 192.168.2.2.2565	TCP TCP TCP TCP TCP TCP TCP
	#4.(1-259) #5-(1-260) #6-(1-261) #7-(1-267) #8-(1-255) #9-(1-254) #10-(1-259) #11-(1-259)	Icve jicatijbugtanajjarachNIDS jisnoni / MSC souce roude issr [cve]icatijbugtanajjarachNIDS jisnoni / MSC souce roude issr [cve]icatijbugtanajjarachNIDS jisnoni / MSC souce roude issr [cve]icatijbugtanajjarachNIDS jisnoni / MSC souce roude issr [arachNIDS jisnoni / SCAN SYN FN [arachNIDS jisnoni / SCAN SYN FN [anachNIDS jisnoni / SCAN SYN FN [anachNIDS jisnoni / SCAN SYN FN [anachNIDS jisnoni / SCAN SYN FN	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:46:49 2005-02-05 16:46:39 2005-02-05 16:46:39	192.168.2.2 25564 192.168.2.2 25554 192.168.2.4 25554 192.168.2.4 445 192.168.2.4 1004 192.168.2.2 10004 192.168.2.4 1001 192.168.2.4 10	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25664 192.168.2.2.25664 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.10	TCP TCP TCP TCP TCP TCP TCP TCP
	#4.(1.259) #5-(1.260) #6-(1.261) #7-(1.262) #8-(1.255) #9-(1.254) #10-(1.254) #10-(1.249) #11-(1.250) #12-(1.251)	Icveficat[bingtrag](archMDS](smort) MSO source route hisr [cveficat[bingtrag](archMDS)(smort) MSO source code hisre (cveficat[bingtrag](archMDS)(smort) MSO source route hisr [archMDS](smort) SCAN STN FRI [archMDS](smort) SCAN STN FRI [archMDS](smort) SCAN STN FRI [archMDS](smort) SCAN STN FRI [anort] BAD-TRAFFIC top por 0 traffic [smort] BAD-TRAFFIC top por 0 traffic	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:46:49 2005-02-05 16:46:49 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39	192.168.2.2 25564 192.168.2.2 25564 192.168.2.4 445 192.168.2.4 445 192.168.2.2 10004 192.168.2.2 10004 192.168.2.4.0 192.168.2.4.0	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25664 192.168.2.2.25664 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.0 192.168.2.4.0 192.168.2.4.0	TCP TCP TCP TCP TCP TCP TCP TCP TCP
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262) #8-(1-255) #9-(1-254) #10-(1-254) #10-(1-254) #11-(1-250) #12-(1-251) #13-(1-252)	Icve Ticcal Disptragil archNUDS [smoth MSC source route hisr [cve]Ticcal[bugtragi]archNUDS[smoth MSC source route isre [cve]Ticcal[bugtragi]archNUDS[smoth MSC source route isre [archNUDS[smoth]SCAN SYN FN arachNUDS[smoth SCAN SYN FN smoth] BAD-TRAFFIC ktp pol 0 traffic [smoth] BAD-TRAFFIC ktp pol 0 traffic [smoth] BAD-TRAFFIC ktp pol 0 traffic	2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:47:05 2005-02-05 16:46:49 2005-02-05 16:46:49 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39	192.168.2.2 25564 192.168.2.4 25564 192.168.2.4 445 192.168.2.4 445 192.168.2.2 0004 192.168.2.2 0004 192.168.2.2 0024 192.168.2.4 0 192.168.2.4 0 192.168.2.4 0	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25664 192.168.2.2.25564 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.025 192.168.2.4.0 192.168.2.4.0	тср тср тср тср тср тср тср тср тср тср
	#4-(1-259) #5-(1-260) #6-(1-261) #7-(1-262) #8-(1-255) #9-(1-254) #10-(1-249) #11-(1-250) #12-(1-251) #13-(1-252) #14-(1-240)	Iver EradIbiogram] and MIDS [smort] MISS source route hisr [cver] iscal[biogram] and MIDS [smort] MISS source code hisre (cver] iscal[biogram] and MIDS [smort] MISS source route hisr [cver] iscal[biogram] and MIDS [smort] MISS source route hisr [and MIDS [smort] SCAN SYN FRI [and BAD-TRAFFIC to pard that [smort] BAD-TRAFFIC to pard that [smort] BAD that [2005-02205 16.47 05 2005-02305 16.47 05 2005-02305 16.47 05 2005-02205 16.47 05 2005-02205 16.46.48 2005-02205 16.46.48 2005-02205 16.46.48 2005-02205 16.46.48 2005-02205 16.46.39 2005-02205 16.46.39	192, 168, 2, 2, 25564 192, 168, 2, 2, 25564 192, 168, 2, 4, 445 192, 168, 2, 4, 445 192, 168, 2, 2, 10004 192, 168, 2, 2, 10004 192, 168, 2, 4, 0 192, 168, 2, 4, 0 192, 168, 2, 2, 50297 192, 168, 2, 4, 0	192.168.2.4.445 192.168.2.4.445 192.168.2.4.445 192.168.2.4.25564 192.168.2.4.1025 192.168.2.4.1025 192.168.2.2.2565 192.168.2.2.2567 192.168.2.2.26477 192.168.2.4.0 192.168.2.4.0	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР
	#4.(1.259) #5.(1.260) #6.(1.261) #7.(1.262) #8.(1.255) #9.(1.254) #10.(1.249) #11.(1.250) #12.(1.251) #13.(1.252) #14.(1.240) #15.(1.241)	Icve Ticat[Ibugitaq][arachNU5][smot] MSC source route hisr [cve][cat[Ibugitaq][arachNU5][smot] MSC source route hisr [cve][cat][bugitaq][arachNU5][smot] MSC source route hisr [cve][cat][bugitaq][arachNU5][smot] MSC source route hisr [arachNU5][smot] SCAN SYN FN [arachNU5][smot] SCAN SYN FN [smot] BAD-TRAFFIC top port 0 traffic [smot] BAD-TRAFFIC top port 0 traffic	2005-02-05 16: 47: 05 2005-02-05 16: 47: 05 2005-02-05 16: 47: 05 2005-02-05 16: 47: 05 2005-02-05 16: 46: 47: 05 2005-02-05 16: 46: 39 2005-02-05 16: 46: 39 2005-02-05 16: 46: 39 2005-02-05 16: 46: 39 2005-02-05 16: 46: 38 2005-02-05 16: 46: 38 2005-02-05 16: 46: 38	192.168.2.2 25564 192.168.2.2 25564 192.168.2.4 445 192.168.2.4 445 192.168.2.4 145 192.168.2.2 10004 192.168.2.2 10004 192.168.2.4 0 192.168.2.4 0 192.168.2.4 0 192.168.2.4 0	192.168.2.4.445 192.168.2.4.445 192.168.2.2.4.445 192.168.2.2.26564 192.168.2.2.26564 192.168.2.4.1025 192.168.2.4.1025 192.168.2.2.366 192.168.2.2.6470 192.168.2.2.6471 192.168.2.2.63710	тср тср тср тср тср тср тср тср тср тср
	#4-(1-259) #5-(1-261) #7-(1-262) #8-(1-263) #9-(1-254) #10-(1-249) #11-(1-250) #12-(1-251) #13-(1-252) #14-(1-240) #15-(1-241) #16-(1-242)	Iver EradhangtanglaranhUDS janon) MSC source route has Iver jizad janganglaranhUDS janon) MSC source code has Iver jizad janganglaranhUDS janon) MSC source route has Iver jizad janganglaranhUDS janon) MSC source route has IarachNUS janon i SCAN SYN FM janon) BACHTARFIC top pod tradic janoni BACHTARFIC top pod tradic	2005-02-05 16 4/16 2005-02-05 16 4/16 2005-02-05 16 4/16 2005-02-05 16 4/16 2005-02-05 16 4/16 2005-02-05 16 46 19 2005-02-05 16 46 19	192, 168, 2, 2, 25554 192, 169, 2, 25554 192, 169, 2, 4, 545 192, 169, 2, 4, 25554 192, 169, 2, 4, 245 192, 169, 2, 2, 10004 192, 169, 2, 4, 0 192, 169, 2, 4, 0\\192, 169, 2, 4, 0\\192, 169, 2, 4, 0\\192, 169, 2, 169, 2, 0\\192, 169, 2, 169, 2, 0\\192, 169, 2, 169, 2, 0\\192, 169, 169, 2	192.168.2.4.445 192.168.2.4.445 192.168.2.2.25564 192.168.2.2.25564 192.168.2.4.1025 192.168.2.4.1025 192.168.2.4.1025 192.168.2.2.25677 192.168.2.2.26477 192.168.2.2.6477 192.168.2.4.0 192.168.2.4.0	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
	#4-(1-259) #5-(1-261) #6-(1-261) #7-(1-262) #8-(1-262) #9-(1-262) #10-(1-249) #11-(1-250) #12-(1-251) #12-(1-252) #14-(1-240) #15-(1-242) #15-(1-242)	Icve Ticat[Ibigitag][arachNIDS][smoth MSC source route hisr [cve][icat[Ibigitag][arachNIDS][smoth MSC source route hisr [cve][icat][bigitag][arachNIDS][smoth MSC source route hisr [arachNIDS][smoth] SCAN SYN FN [arachNIDS][smoth] SCAN SYN FN [arachNIDS][smoth] SCAN SYN FN [amoth] BAD-TRAFFIC top pard 0 traffic [smoth] BAD-TRAFFIC top pard 0 traffic	2005-02-05 16:47/05 2006-02-05 16:47/05 2005-02-05 16:47/05 2005-02-05 16:46:49 2005-02-05 16:46:49 2005-02-05 16:46:49 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39 2005-02-05 16:46:39	192, 168, 2, 2, 25564 192, 168, 2, 2, 5564 192, 168, 2, 4, 445 192, 168, 2, 4, 445 192, 168, 2, 4, 445 192, 168, 2, 2, 10004 192, 168, 2, 2, 10004 192, 168, 2, 2, 1004 192, 168, 2, 4, 0 192, 168, 2, 4, 0 192, 168, 2, 4, 0 192, 168, 2, 4, 0 192, 168, 2, 4, 0	192,168,2,4,445 192,169,2,4,445 192,169,2,2,25564 192,168,2,2,25564 192,168,2,4,1025 192,168,2,4,1025 192,168,2,4,1025 192,168,2,4,0 192,168,2,4,0 192,168,2,4,0 192,168,2,2,34710 192,168,2,2,10541	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР
	#4-(1-259) #5-(1-261) #7-(1-262) #8-(1-262) #8-(1-262) #9-(1-254) #10-(1-259) #11-(1-259) #11-(1-259) #12-(1-254) #13-(1-252) #14-(1-246) #15-(1-244) #16-(1-243) #18-(1-244)	Iver EradhangtanglaranhUtoSismont MRS source route hisr Iver EradhangtanglaranhUtoSismont MRS bauer code hisre Iver AnnothutoSismont SCAN SYN FAN Iment BAD-TRAFFIC top perit 0 traffic Iment BAD-TRAFFIC top perit 0 traffic	2005-02-05 16 4/16 2005-02-05 16	192, 168, 2, 2, 25554 192, 169, 2, 2, 5554 192, 169, 2, 4, 645 192, 169, 2, 4, 465 192, 169, 2, 4, 465 192, 169, 2, 2, 10004 192, 169, 2, 2, 10004 192, 169, 2, 4, 0 192, 169, 2, 2, 0055	192,168,2,4,45 192,168,2,4,45 192,168,2,2,2664 192,168,2,2,2664 192,168,2,4,1025 192,168,2,4,1025 192,168,2,4,102 192,168,2,2,2650 192,168,2,2,670 192,168,2,2,670 192,168,2,2,670 192,168,2,2,670 192,168,2,2,670 192,168,2,2,01951 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,01952 192,168,2,019	10P 10P 10P 10P 10P 10P 10P 10P 10P 10P
	#4.(1.259) #5.(1.260) #6.(1.261) #7.(1.262) #8.(1.253) #9.(1.254) #10.(1.254) #10.(1.254) #12.(1.254) #12.(1.254) #13.(1.252) #14.(1.254) #14.(1.254) #14.(1.254) #16.(1.242) #17.(1.243) #18.(1.244)	Iver Eact Things and in a child shared MIOS is source route his r (ove Eact Things and Each MIOS is source route his re- (ove Eact Things and Each MIOS is source route his re- (ove Eact Things and Each MIOS is source route his re- larach MIOS is primer is Sock STVF FN and RAD TRAFFIC top period traffic shared BAD TRAFFIC t	2005-02-05 16.47/15 2006-02-05 16.47/15 2005-02-05 16.47/15 2005-02-05 16.46.49 2005-02-05 16.46.49 2005-02-05 16.46.49 2005-02-05 16.46.49 2005-02-05 16.46.39 2005-02-05 16.46.39 2005-02-05 16.46.39 2005-02-05 16.46.39 2005-02-05 16.46.39 2005-02-05 16.46.39	192, 168, 2, 2, 25554 192, 168, 2, 2, 5554 192, 168, 2, 4, 445 192, 168, 2, 4, 445 192, 168, 2, 4, 1004 192, 168, 2, 4, 1004 192, 168, 2, 4, 1004 192, 168, 2, 4, 0 192, 168, 2, 4, 0	192, 168, 2, 4, 465 192, 168, 2, 2, 465 192, 168, 2, 2, 25564 192, 168, 2, 2, 25564 192, 168, 2, 4, 1025 192, 168, 2, 4, 1025 192, 168, 2, 4, 1025 192, 168, 2, 4, 1025 192, 168, 2, 2, 256 192, 168, 2, 2, 2, 257 192, 168, 2, 2, 10541 192, 168, 2, 2, 10541 192, 168, 2, 2, 10541 192, 168, 2, 2, 10541	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР
	44-(1-259) #5-(1-261) #7-(1-262) #7-(1-262) #0-(1-259) #12-(1-259) #12-(1-259) #12-(1-259) #13-(1-259) #13-(1-259) #14-(1-259	Iver EractIbingtragilarabilitySianoti MRS issuer order biss Iver EractIbingtragilarabilitySianoti MRS bauec order biss Iver EractIbingtragilarabilitySianoti MRS Iver IdeA TRAFFIC top per 0 tradic Iver IdeA	2005-02-05 16 4716 2005-02-05 16 4716 2005-02-05 16 4716 2005-02-05 16 4716 2005-02-05 16 46 49 2005-02-05 16	192, 168, 2, 2, 25554 192, 169, 2, 2, 25554 192, 169, 2, 4, 845 192, 169, 2, 4, 845 192, 169, 2, 4, 845 192, 169, 2, 4, 82, 2, 10004 192, 169, 2, 4, 1004 192, 169, 2, 4, 1004 192, 169, 2, 4, 0, 192, 169, 2, 4, 0 192, 169, 2, 20055 192, 169, 2, 20055	$\begin{array}{c} 192, 182, 24, 445\\ 192, 160, 22, 4264\\ 192, 160, 22, 25564\\ 192, 160, 24, 2656\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 2057\\$	1029 1029 1029 1029 1029 1029 1029 1029
	#4.(1.259) #5.(1.260) #6.(1.261) #7.(1.261) #7.(1.262) #10.(1.254) #10.(1.254) #10.(1.254) #11.(1.254) #12.(1.254) #12.(1.254) #13.(1.254) #14.(1.240) #15.(1.244) #16.(1.244) #19.(1.244) #19.(1.244)	Iver Eact Things and in a child shared MIOS (secre route his r (cve) [act Things and [area MIOS (secre route his re (cve) [act Things and [area MIOS (secre route his re [area MIOS (secre) and a child shared MIOS (secre route his re [area MIOS (secre) Secret Secret Secret and secre (secre) [act Things (SecR STM FR) [area MIOS (secret Secret Sec	2005-02-05 16.47/16 2006-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.46.49 2005-02-05 16.46.39 2005-02-05 16.46.39	192, 168, 2, 2, 25554 192, 168, 2, 2, 5554 192, 168, 2, 4, 445 192, 168, 2, 4, 445 192, 168, 2, 4, 1004 192, 168, 2, 4, 1004 192, 168, 2, 4, 1004 192, 168, 2, 4, 0 192, 168, 2, 4, 0	192,198,24,445 192,193,24,445 192,193,22,2554 192,193,22,2554 192,193,24,1025 192,198,24,1025 192,198,24,1025 192,198,24,2555 192,193,24,2567 192,193,24,240 192,193,24,240 192,193,24,25589 192,193,24,25589	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР
	44-(1-259) #5-(1-261) #7-(1-262) #7-(1-262) #0-(1-259) #12-(1-259) #12-(1-259) #12-(1-259) #13-(1-259) #13-(1-259) #14-(1-259	Iver EractIbingtragilarabilitySianoti MRS issuer order biss Iver EractIbingtragilarabilitySianoti MRS bauec order biss Iver EractIbingtragilarabilitySianoti MRS Iver IdeA TRAFFIC top per 0 tradic Iver IdeA	2005-02-05 16 4/16 2005-02-05 16	192, 168, 2, 2, 25554 192, 169, 2, 2, 25554 192, 169, 2, 4, 845 192, 169, 2, 4, 845 192, 169, 2, 4, 845 192, 169, 2, 4, 82, 2, 10004 192, 169, 2, 4, 1004 192, 169, 2, 4, 1004 192, 169, 2, 4, 0, 192, 169, 2, 4, 0 192, 169, 2, 20055 192, 169, 2, 20055	$\begin{array}{c} 192, 182, 24, 445\\ 192, 160, 22, 4264\\ 192, 160, 22, 25564\\ 192, 160, 24, 2656\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2055\\ 192, 160, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 24, 2057\\ 102, 100, 2057\\$	1029 1029 1029 1029 1029 1029 1029 1029
	44 (1 259) #5 (1 260) #6 (1 261) #7 (1 262) #9 (1 255) #9 (1 254) #10 (1 249) #11 (1 250) #12 (1 251) #13 (1 252) #14 (1 240) #15 (1 241) #16 (1 242) #17 (1 241) #16 (1 242) #17 (1 243) #18 (1 244) #22 (1 246) #22 (1 246)	Iver Tracellinging all area MHDS Steamer MHS course route hisr (cw)Tracellinging all area MHDS Steamer MHS course code hisre (cw)Tracellinging all area MHDS Steamer MHS course route hisr (cw)Tracellinging all area MHDS Steamer MHS course route hisr (area MHDS Steamer) SCAN STM FM Trace MHDS Steamer) SCAN STM FM (area MHS STM STM STM STM STM (area MHS STM STM STM STM (area MHS STM STM STM (area	2005-02-05 16.47/16 2006-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.47/16 2005-02-05 16.46.49 2005-02-05 16.46.39 2005-02-05 16.46.39	192, 168, 2, 2, 25554 192, 168, 2, 2, 5554 192, 168, 2, 4, 455 192, 168, 2, 2, 160, 4, 445 192, 168, 2, 2, 10004 192, 168, 2, 2, 10004 192, 168, 2, 2, 10004 192, 168, 2, 2, 10004 192, 168, 2, 4, 0 192, 168, 2, 2, 2, 5680	192,168,24,445 192,169,27,2554 192,169,27,2554 192,169,27,2554 192,169,27,2554 192,169,27,102,24 192,169,27,2555 192,169,24,102 192,169,22,2555 192,169,22,67 192,169,22,67 192,169,22,67 192,169,22,67 192,169,22,002 192,169,22,002 192,169,22,002 192,169,22,002 192,169,22,002 192,169,24,00 192,169,24,00	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР

	St Yow Favo	upea Tooja Reib				
Bac	x · () ·	🖹 😰 🐔 🔎 Search 👷 Favorites 🤪 🔗 - 🌉 🔟 - 🛄 🛞 🗳 🥥 🦓				
	al brossiliter 16	8.2.2/base/base_gry_main.php?mew=18/ayer1=UDP8num_result_rows==18sor1_order=time_d8submt=Query+D8				✓ 53 60
			10 to 100			
n ^{NI}	14	🖉 🔎 Search 🔹 🥭 Highlight 🛛 All Options 🔤 Pop-ups Allowed 🔹 🔤 Hotmail 🌋 Mi	issenger La My MSN			
3a	asic A	nalysis and Security Engine (BASE)				
me	Search	AG Maintenance				
						[Ba
40	alert(s) to the A	Alert cache				
	d DB on : Cat	February 05, 2005 16:53:52				
		ne proviny 05, 2005 16:53:52	Summary Ste Sensors	tistics		
		79 70		(classifications)		
		79 79	 Unique addres 	ses: source destination	on	
			 Unique IP lini 			
10-0	ad Criteria a	14	Source Port Destination P			
		Displaying alerts 1-50 of 160 tot	Time profile of all	or dimits		
_		Displaying alerts 1-50 of 160 tot	al			
	ID	< Signature >	al < Timestamp >	< Source Address >	< Dest. Address >	
	#0-(1-267)	< Signature > [snort] TFTP GET passwd	al < Timestamp > 2005-02-05 16:47:15	< Source Address > 192.168.2.2 32905	192.168.2.4:69	UDP
	#0-(1-267) #1-(1-268)	< Signature > [snort] TFTP GET passwd [snort] TFTP Get	al < Timestamp > 2005-02-05 16:47:15 2005-02-05 16:47:15	< Source Address > 192.168.2.2 32905 192.168.2.2 32905	192.168.2.4:69 192.168.2.4:69	UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269)	<pre></pre>	al Timestamp > 2005-02-05 16:47:15 2005-02-05 16:47:15 2005-02-05 16:47:15	< Source Address > 192.168.2.2.32905 192.168.2.2.32905 192.168.2.2.32905	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69	UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269) #3-(1-256)	< Signature > [snort] TFTP GET passwd [snort] TFTP Get [cve][icat][cve][icat][arachNIDS[[snort] TFTP parent directory [snort] TFTP GET passwd	al	< Source Address > 192.168.2.2.32905 192.168.2.2.32905 192.168.2.2.32905 192.168.2.2.32905	192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69	
	#0-(1-267) #1-(1-268) #2-(1-269) #3-(1-256) #4-(1-257)	Signature > [snort] IFTP GET passwd [snort] IFTP Get [cve][icat][cve][icat][arachNIDS[]snort] IFTP parent directory [anelt] IFTP GET passwd [cve][icat][arachNIDS[]snort] IFTP pot directory	al < Timestamp >2005:02:05:16:47:152005:02:05:16:47:152005:02:05:16:47:152005:02:05:16:47:152005:02:05:16:46:542005:02:05:16:46:54	< Source Address > 192.168.2.2 32905 192.168.2.2 32905 192.168.2.2 32905 192.168.2.2 32905 192.168.2.2 32905	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69	UDP UDP UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269) #3-(1-256) #4-(1-257) #5-(1-258)	<pre></pre>	al < Timestamp > 2005/02/05 16:47:15 2005/02/05 16:47:15 2005/02/05 16:47:15 2005/02/05 16:46:54 2005/02/05 16:46:54 2005/02/05 16:46:54 2005/02/05 16:46:54 2005/02/05 16:46:54	Source Address > 192,468.2,2 32905 192,468.2,2 32905 192,468.2,2 32905 192,468.2,2 32905 192,468.2,2 32905 192,468.2,2 32905	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69	UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269) #3-(1-256) #4-(1-257) #5-(1-258) #6-(1-253)	<pre></pre>	al Constants > 2005/02/05/16/47/15 2005/02/05/16/47/15 2005/02/05/16/47/15 2005/02/05/16/46/54 2005/02/05/16/46/40	< Source Address > 192,468,2,2 32905 192,168,2,2 32905 192,168,2,2 32905 192,168,2,2 32905 192,168,2,2 32905 192,168,2,2 32905 192,168,2,2 32905 192,168,2,2 4315	192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69	UDP UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269) #3-(1-256) #4-(1-257) #5-(1-258) #6-(1-253) #7-(1-229)	<pre>< Signature > [snort] TETP GET passed [nort] TETP Get [cove[icat[cove[icat[larachNIDS]snort] TETP parent directory [snort] TETP GET passed [cove[icat[larachNIDS]snort] TETP not directory [snort] TETP Get [snort] TETP Get [cove[icat[love][icat[love][icat[lbugtraq]bugtraq]snort] SNMP public access udp</pre>	al < Timestamp > 2005/02.05 16:47:15 2005/02.05 16:47:15 2005/02.05 16:47:15 2005/02.05 16:45:54 2005/02.05 16:46:54 2005/02.05 16:46:54 2005/02.05 16:46:36	< Source Address > 192,160.2,2 32905 192,160.2,2 32905 192,160.2,2 32905 192,160.2,2 32905 192,160.2,2 32905 192,160.2,2 32905 192,160.2,2 32905	192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69 192.168.2.4.69	UDP UDP UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1 (1-268) #2-(1-269) #3-(1-256) #4 (1-257) #5 (1-258) #6-(1-253) #7-(1-229) #8 (1-230)	<pre></pre>	al < Timestamp > 2005-02-05-16-47-15 2005-02-05-16-47-15 2005-02-05-16-47-15 2005-02-05-16-48-54 2005-02-05-16-48-54 2005-02-05-16-48-54 2005-02-05-16-48-36 2005-02-05-16-48-38	< Source Address > 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 3205 192,168.2,2 3205 192,168.2,2 3205 192,168.2,2 3305 192,168.2,2 3305 192,168.2,2 3305	192.168.2.4 69 192.168.2.4 69 192.168.2.4 69 192.168.2.4 69 192.168.2.4 69 192.168.2.4 69 192.168.2.4 69 192.168.2.4 59 192.168.2.4 161	UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0.(1.267) #1.(1.268) #2.(1.269) #3.(1.256) #4.(1.257) #5.(1.258) #6.(1.253) #7.(1.229) #8.(1.230) #9.(1.197)	<pre></pre>	al < Timestamp > 2005 02 05 16 47 16 2005 02 05 16 47 16 2005 02 05 16 47 15 2005 02 05 16 45 15 2005 02 05 16 46 54 2005 02 05 16 46 54 2005 02 05 16 48 58 2005 02 05	Source Address > 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 32905 192,168.2,2 4315 192,168.2,2 4315 192,168.2,2 4305 192,168.2,2 4305	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,161 192,168,2,4,161 192,168,2,4,164	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0.(1.267) #1.(1.268) #2.(1.269) #3.(1.256) #4.(1.257) #5.(1.258) #6.(1.253) #7.(1.229) #8.(1.230) #9.(1.197) #10.(1.169)	Signature > [snent] IFTP: GET passwd [snent] IFTP: Get [cve][icat](archHi05[snent] IFTP parent directory [snent] IFTP: GET passwd [cve][icat](archHi05[snent] IFTP root directory [snent] IFTP: Get [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq[inent] SNMP public access udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snent] SNMP request udp	al < Timestamp > 2005:02:05:16:47:15 2005:02:05:16:47:15 2005:02:05:16:47:15 2005:02:05:16:46:54 2005:02:05:16:46:54 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:35 2005:02:05:16:46:16	< Source Address > 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,23205 192,168.2,2505 192,168.2,21024	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,161 192,168,2,4,164 192,168,2,4,10496	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-268) #3-(1-256) #4-(1-257) #5-(1-258) #6-(1-253) #7-(1-259) #8-(1-253) #7-(1-259) #8-(1-259)	Signature > [snort] IFTP GET passwd [snort] IFTP Get [cve]icat[cve]icat[arachNIDS[snort] IFTP parent directory [anert] IFTP Get [cve]icat[arachNIDS[snort] IFTP not directory [snort] IFTP Get [snort] IFTP Get [cve]icat[cve]icat[Nuptraq][bugtraq[bugtraq[snort] SNMP public sccess udp [cve]icat[cve]icat[lbugtraq][bugtraq][bugtraq[snort] SNMP public sccess udp [cve]icat[cve]icat[lbugtraq][bugtraq][bugtraq][bugtraq][snort] SNMP public sccess udp [cve]icat[cve]icat[cve]icat][bugtraq][bugtraq][snort] SNMP public sccess udp [cve]icat[cve]icat][cve]icat][bugtraq][bugtraq][snort] SNMP public sccess udp [cve]icat[cve]icat][cve]icat][cve]icat][bugtraq][snort] SNMP public sccess udp [cve]icat[cve]icat][cve]icat][cve]icat][bugtraq][snort] SNMP public sccess udp [cve]icat[cve]icat][cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][cve]icat][bugtraq][snort] SNMP request udp [cve]icat[cve]icat][cve]icat][cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat[cve]icat][cve]icat[cve]icat][cve]icat[cve]icat][cve	al < Timestamp > 2005/02/05/16/47/15 2005/02/05/16/47/15 2005/02/05/16/47/15 2005/02/05/16/45/14 2005/02/05/16/46/54 2005/02/05/16/46/54 2005/02/05/16/46/54 2005/02/05/16/46/54 2005/02/05/16/46/54 2005/02/05/16/46/12 2005/02/05/16/46/12	< Source Address > 192,160.2,2 32905 192,160.2,2 32905	192,160,2,4,69 192,168,2,4,69 192,168,2,4,69 192,160,2,4,69 192,160,2,4,69 192,160,2,4,69 192,168,2,4,161 192,168,2,4,161 192,168,2,4,10496 192,168,2,4,10496 192,160,2,4,10496	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0.(1.267) #1.(1.268) #2.(1.268) #3.(1.256) #4.(1.257) #5.(1.258) #6.(1.253) #7.(1.229) #8.(1.230) #9.(1.127) #10.(1.169) #11.(1.156) #12.(1.155)	Signature > [snert] IFTP: GET_passwd [snert] IFTP: Get [cve][icat](archH05[snert] IFTP parent directory [snert] IFTP: Get [cve][icat](archH05][snert] IFTP root directory [snert] IFTP: Get [cve][icat](cve][icat](bugtrat][bugtrat][bugtrat][snert] SNMP public access udp [cve][icat](cve][icat](bugtrat][bugtrat][bugtrat][bugtrat][snert] [snert] [cve][icat](bugtrat][bugtrat][bugtrat][bugtrat][snert] [snert] [cve][icat](bugtrat][bugtrat][bugtrat][bugtrat][snert] [snert] [cve][icat](block] that direct to gent ensetUncessus[snert] MSS GR, ping attempt [snert] [cve][icat](block that direct dedet direct][snert] [cve][icat](block] that direct to gent ensetUncessus[snert] MSS GR, ping attempt [snert] [cve][icat](block that direct dedet direct][snert] [cve][icat](block] that direct dedet	al 1 2005/02/65 (16.47.16) 2005/02/65 (16.47.16) 2005/02/65 (16.47.16) 2005/02/65 (16.47.16) 2005/02/65 (16.46.16) 200	 Source Address > 192,168,2,2 32005 192,168,2,2 32005 192,168,2,2 32005 192,168,2,2 32005 192,168,2,2 32005 192,168,2,2 4315 192,168,2,2 4315 192,168,2,2 4315 192,168,2,2 3205 192,168,2,2 3205 192,168,2,2 3205 192,168,2,2 1024 192,168,2,2 3205 192,168,2,2 3205 192,168,2,2 3205 192,168,2,2 3209 192,168,2,2 3209 192,168,2,2 3209 192,168,2,2 3209 	192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,69 192,168,2,4,161 192,168,2,4,161 192,168,2,4,163 192,168,2,4,163 192,168,2,4,163	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1-(1-268) #2-(1-269) #4-(1-256) #4-(1-257) #5-(1-258) #6-(1-253) #7-(1-229) #7-(1-229) #10-(1-197) #10-(1-197) #10-(1-196) #11-(1-156) #13-(1-154)	Signature > [snort] IFTP GET passwd [snort] IFTP Get [cve][icat[cve][icat[cred][icat[snort] IFTP parent directory [snort] IFTP Get [snort] IFTP Get [snort] IFTP Get [snort] IFTP Get [snort] IFTP Get [snort] IFTP Get [cve][icat[cve][icat[bugthat][bugtrad][bugtrad][snort] SNMP public access udp [cve][icat[snort][icat][bugthat][bugtrad][bugtrad][snort] SNMP request udp [cve][icat[snort] DDDS sharb hardwe ping to agent [arachNIDS][snort] DDDS sharb madder to agent [arachNIDS][snort] DDDS sharb madder to agent [sessurpressurption] MS SGL ping attempt [smort] (ping bb] Bick Orders Trafic detected nessurpressurption] MS CAFS access	al - Timestamp 5 2005 (2/2 6) (6.47) (5 2005 (2/2 6) (6.47) (5 2005 (2/2 6) (6.47) (5 2005 (2/2 6) (6.47) (5 2005 (2/2 6) (6.46) (5 2005 (2/2 6) (6) (6) (6) (6) (6) (6) (6) (6) (6)	Source Address > 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,3205 192,160,22,1024 192,160,22,1024 192,160,22,32059	192,160,2,4,69 192,168,2,4,69 192,168,2,4,69 192,160,2,4,69 192,160,2,4,69 192,160,2,4,69 192,168,2,4,69 192,168,2,4,161 192,168,2,4,161 192,168,2,4,1045 192,168,2,4,1035 192,168,2,4,1337 192,168,2,4,7001	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0.(1.267) #1.(1.268) #2.(1.269) #3.(1.256) #4.(1.257) #5.(1.258) #6.(1.253) #7.(1.229) #8.(1.230) #9.(1.197) #10.(1.169) #11.(1.156) #11.(1.155) #14.(1.154)	Signature > [snert] IFTP: GET_passwd [snert] IFTP: Get [cve][icat](archH05[snert] IFTP parent directory [snert] IFTP: Get [cve][icat](archH05[snert] IFTP root directory [snert] IFTP: Get [cve][icat](archH05[snert] IFTP root directory [snert] IFTP: Get [cve][icat](archH05[snert][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat](archH05[snert] Itat][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat](archH05[snert] Itat][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat](snert] Itat][bugtrat][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat][snert] [bugtrat][bugtrat][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat][snert] [bugtrat][bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat][snert] [bugtrat][bugtrat][bugtrat][snert] SNMP report upp [cve][icat][snert] [bugtrat][bugtrat][bugtrat][snert] [cve][icat][snert] [bugtrat][snert] [bugtrat][snert	4 * Timestamp > 2056/02/65 (64.71:5) 2005/02/05 (64.71:5) 2005/02/05 (64.71:5) 2005/02/05 (64.75:5) 2005/02/05 (64.75:5) 2005/02/05 (64.85:5) 2005/02/05 (64.85:5) 2005/02/05 (64.85:5) 2005/02/05 (64.85:16) 2005/02/05 (64.85:16) 2005/02/05 (64.85:16) 2005/02/05 (64.86:11) 2005/02/05 (C Source Address > 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32056 192,168,2,2,32059 192,168,2,2,32059 192,168,2,2,32059	192,160,2,4,63 192,162,2,4,63 192,162,2,4,63 192,162,2,4,63 192,160,2,4,63 192,160,2,4,63 192,160,2,4,63 192,160,2,4,161 192,160,2,4,161 192,160,2,4,164 192,160,2,4,164 192,160,2,4,163 192,160,2,4,163 192,160,2,4,163	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0-(1-267) #1.(1-268) #2-(1-269) #4.(1-257) #5.(1-253) #6.(1-253) #7.(1-229) #8.(1-233) #9.(1-177) #10-(1-169) #11.(1-156) #12.(1-155) #13.(1-154) #15.(1-149)	Signature > [snent] ITTP GET passwd [snent] ITTP GET [cve][icat[archHIDS[snent] TFTP parent directory [snent] ITTP GET passwd [cve][icat[archHIDS[snent] TFTP root directory [snent] ITTP Get [snent] ITTP Get [snent] ITTP Get [cve][icat[cve][icat][bugtan][bugtan][bugtan][snent] SNMP public access udp [cve][icat[snent] DOOS sntteam handler ing to agent [archHIDS[snent] DDOS shtt handler to agent [srachHIDS[snent] DDOS shtt handler to agent [srachHIDS[snent] DDOS shtt handler to agent [srachHIDS[snent] MSC AFS access neessus[snent] MSC AFS access	4 Timestamp > 2005/02/06 (64.7*15 2005/02/06 (64.7*15 2005/02/06 (64.7*15 2005/02/06 (64.7*15 2005/02/06 (64.6*17) 2005/02/06 (64.6*17) 2005/02/06 (64.6*2) 2005/02/06 (64.6*2)	Source Address > 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32015 192,160,2,2 32015 192,160,2,2 32015 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005	192, 168, 2, 4, 69 192, 168, 2, 4, 164 192, 168, 2, 4, 164 192, 168, 2, 4, 110 192, 168, 2, 4, 7001	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	#0.(1.267) #1.(1.268) #2.(1.268) #3.(1.256) #4.(1.257) #5.(1.258) #6.(1.253) #7.(1.253) #7.(1.229) #8.(1.230) #9.(1.197) #10.(1.169) #11.(1.156) #13.(1.154) #13.(1.154) #14.(1.453) #15.(1.1459)	Signature > [snert] ITETP. GET_passwed [snert] ITETP. Get [cve][icat](archIDS[snert] ITETP parent directory [snert] ITETP. Get [cve][icat](archIDS[snert] ITETP parent directory [snert] ITETP. Get [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snert] SNMP request udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snert] SNMP request udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snert] SNMP request udp [cve][icat](cve][icat](bugtraq][bugtraq][bugtraq][snert] SNMP request udp [cve][icat](snert] BodS Core in a factor in a facto	4 Timestimp 5 2005/02/06 (56/47):15 2005/02/06 (56/47):15 2005/02/06 (56/47):15 2005/02/06 (56/47):15 2005/02/06 (56/46):16 2005/02/06 (56/46) 2005/02/06 (56/46) 2005/02/06 (56/46):10 2005/02/06 (56/46):11 2005/02/06	C Source Address > 192, 681, 2, 2 2096 192, 681, 2, 2 2096 192, 681, 2, 2 2095 192, 681, 2, 2 2099 192, 681, 2, 2 2099	192, 162, 24, 69 192, 162, 24, 69 192, 163, 24, 163 192, 163, 24, 1163 192, 163, 24, 1163 192, 163, 24, 1163 192, 163, 24, 1163 192, 163, 24, 1103 192, 163, 24, 7001 192, 163, 24, 7001	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	10.1(267) #1 (1268) #2 (1269) #2 (1269) #3 (1259) #4 (1257) #5 (1258) #7 (1229) #8 (1230) #7 (1229) #8 (1230) #9 (1197) #10.[1469] #11.[1.56] #14.[1.55] #14.[1.453] #15 (149) #15 (149) #16 (1459) #17 (1.55]	Signature > [snen] TFTP GET passwd [snen] TFTP Get [cve][icat[archNH05[[snen]] TFTP parent directory [snen] TFTP GET passwd [cve][icat[archNH05][snen]] TFTP not directory [snen] TFTP Get [snen] TFTP Get [snen] (TFTP Get [icat[archNH05[icat][cve][icat][bugtraq][bugtraq][snen] SNMP request udp [cve][icat[archNH05[snen] DOOS shat handler to agent [srachNH05[snen] DOOS shat handler to agent ensourcessus[snen] MSS GAP saccess merous[snen] MSS GAP saccess merous[snen] MSS GAP saccess [srachNH05][snen] MSS GAP saccess [sractNH05][snen] MSS GAP saccess [sractNH05][snen] MSS GAP saccess [sractNH05][snen] MSS GAP saccess [sractNH05][snen] DSS TricO Naster to Daemon default password attempt [snen] SGAN Jamada client version request]	4 Timestamp > 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.48.15 2005/02/06 16.48.15 2005/02/06 16.48.15 2005/02/06 16.48.12 2005/02/06 16.48.12 2005/02/06 16.48.12 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10 2005/02/06 16.48.10	Source Address > 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 32005 192,160,2,2 4305 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205 192,160,2,2 3205	192, 162, 24, 69 192, 162, 24, 162 192, 162, 24, 162 192, 162, 24, 162 192, 162, 24, 1107 192, 162, 24, 1107 192, 162, 24, 1107 192, 162, 24, 1107 192, 162, 24, 24, 1107 192, 162, 24, 24, 1107 192, 162, 24, 27001 192, 162, 24, 27001	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	$\begin{array}{c} 0.(1267)\\ \pm 1.(1268)\\ \pm 2.(1268)\\ \pm 3.(1256)\\ \pm 3.(1256)\\ \pm 4.(1257)\\ \pm 5.(1258)\\ \pm 6.(1253)\\ \pm 7.(1229)\\ \pm 8.(1229)\\ \pm 8.(1229)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 19.(1153)\\ \pm 19.(1,153)\\ $	Signature > [snert] TFTP: GET_passwed [snert] TFTP: Get [cve][icat](archIDS[snert] TFTP parent directory [snert] TFTP Get [cve][icat](archIDS[snert] TFTP parent directory [snert] TFTP Get [cve][icat](snert][bugtraq][bugtraq][bugtraq][snert] SNAP request udp [cve][icat](snert][DDOS matients handler in given [cve][icat](snert][DDOS matients handler in given [snert][snert][DDOS matients handler in given [snert][snert][NSC AFS access messus[[snert]] MSC AFS access messus[[snert]] MSC AFS access messus[[snert]] DDOS findD Matier to Diemon default password attempt [snert] SCAN Amada Cient version request] [snert] SCAN Amada Scient version request]	4 * Timestamp 5 2005/02/06 (616/7):5 2005/02/06 (616/7):5 2005/02/06 (616/7):5 2005/02/05 (616/7):5 2005	C Source Address > 192, 161, 2, 2 2005 192, 161, 2, 2 2009 192, 161, 2, 2 2009	192, 168, 24, 463 192, 168, 24, 165 192, 168, 24, 1001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 10001	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	$\begin{array}{c} 0.(1267)\\ \pm 1.(1280)\\ \pm 2.(1280)\\ \pm 2.(1280)\\ \pm 3.(2250)\\ \pm 4.(1250)\\ \pm 4.(1250)\\ \pm 4.(1250)\\ \pm 6.(1280)\\ \pm 6.(1,180)\\ $	Signature > [snent] ITTP GET passwd [snent] ITTP Get [cve][icat](archH05[[snent] TFTP parent directory [snent] TFTP Get [cve][icat](archH05[[snent] TFTP root directory [snent] TFTP Get [cve][icat](cve][icat][cve][icat][bugtraq][bugtraq][snent] SNMP public access udp [cve][icat](cve][icat][cve][icat][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat][cve][icat][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat][cve][icat][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat][cve][icat][bugtraq][bugtraq][snent] SNMP request udp [cve][icat](cve][icat][cve][ica	4 Timestamp > 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.47.15 2005/02/06 16.48.15 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.62 2005/02/06 16.48.63 2005/02/06 16.48.63 2005/02/06 16.48.63 2005/02/06 16.48.63 2005/02/06 16.48.63 2005/02/06 16.48.65 2005/02/06 16.48.55 2005/02/06 16.48.55 2005/02/06 16.48.55 2005/02/06 16.48.55 2005/02/05 2	Source Address > 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32005 193,160.2,2 32005 192,160.2,2 4315 192,160.2,2 4315 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32005 192,160.2,2 32055 192,160.2,2 32055 192,160.2,2 32055 192,160.2,2 32055	192, 168, 24, 493 192, 168, 24, 463 192, 168, 24, 169 192, 168, 24, 161 192, 168, 24, 161 192, 168, 24, 101 192, 168, 24, 2701 192, 168, 24, 2704	UDP UDP UDP UDP UDP UDP UDP UDP UDP UDP
	$\begin{array}{c} 0.(1267)\\ \pm 1.(1268)\\ \pm 2.(1268)\\ \pm 3.(1256)\\ \pm 3.(1256)\\ \pm 4.(1257)\\ \pm 5.(1258)\\ \pm 6.(1253)\\ \pm 7.(1229)\\ \pm 8.(1229)\\ \pm 8.(1229)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 9.(1197)\\ \pm 19.(1153)\\ \pm 19.(1,153)\\ $	Signature > [snert] TFTP: GET_passwed [snert] TFTP: Get [cve][icat](archIDS[snert] TFTP parent directory [snert] TFTP Get [cve][icat](archIDS[snert] TFTP parent directory [snert] TFTP Get [cve][icat](snert][bugtraq][bugtraq][bugtraq][snert] SNAP request udp [cve][icat](snert][DOS] snarteram handler ping to agent [archIDS[snert] DDSS mathematic bagent [snert][snert][DDSS mathematic bagent [snert][snert][DDSS mathematic bagent [snert][snert][DDSS mathematic bagent [snert][snert][DDSS mathematic bagent [snert][snert][DDSS mathematic bagent [snert][snert][NSC AFS access messus[[snert][NSC AFS access messus[[snert]][NSC AFS access messus[[snert]][DSC] FindD Matter to Daemon default password attempt [snert] SCAN Amada Clent version request] [snert] SCAN Amada Scient version request]	4 * Timestamp 5 2005/02/06 (616/7):5 2005/02/06 (616/7):5 2005/02/06 (616/7):5 2005/02/05 (616/7):5 2005	C Source Address > 192, 161, 2, 2 2005 192, 161, 2, 2 2009 192, 161, 2, 2 2009	192, 168, 24, 463 192, 168, 24, 165 192, 168, 24, 1001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 7001 192, 168, 24, 10001	00P 00P 00P 00P 00P 00P 00P 00P 00P 00P

digital self defense

BLACK HAT BRIEFINGS

Snort.org - Microsoft Internet Explore	r provided by BTopenwo				
Ele Edt Yew Favorites Look Help	2				
Q tot + Q + 🗷 🗟 🟠 🔎	🔎 Search 🔶 Pavorites 🕠	🕹 😓 📓 · 📴 🕲 🗳 🥥 🎕			
Address 🜒 http://www.snort.org/snort-db/sid.h	itmil/sid=1443	S Co Links			
msn ^M ·	🔎 Search 🔹 🥒 Highlight	👫 Options 🔲 Pop-ups Allowed 🔹 🔤 Hotmail 📲 Messenger [🔒 My MSN			
	The open source i	ческогк шилимон рессссион зумени — — — — — — — — — — — — — — — — — — —			
Snort Training From the masters of snort	Snort Signature Dat	abase			
From the masters of snort Looking for Snort training? How about		By SID search			
learning from the masters, Sourcefire?		By Message seench			
Sourcefice is offering two training classes for Snort users, a two day class on					
Building and Operating Snort and a two					
day class on Snort Rules	GEN: SID	1.1443			
Resources	Message	TFTP GET passwd			
» News	Rule	alert udp any any >> any 69 (msg *TFTP GET passwd*; content* 00 01 *; depth.2; content*passwd*; offset.2; nocase; classtype successful-admin; sid:1443; rev.4;)			
Get the latest news about our	Summary	This event is generated when a TFTP GET request is made for the "passwd"			
favorite pig		file. This could be an indication that a remote attacker has			
» Documentation	compromised a system on the network and is transfering sensitive files back to the attacking system. It may also be an indication of a generic				
Information on how to setup the		TFTP server scan that includes tests for generic system files.			
pig	Impact	The "passwd" file normally stores users names for Unix based systems. If this file is being transfered over the network using TFTP it is			
» Downloads	normally an indication of a system compromise.				
Get the pig, and all addons that make the pig easier to use		In some situations this rule may only indicate a generic TFTP scan			
a Mailing lists		attempt, as the attacker may be scanning a large range of IP addresses			
Discussions about snort.		for TFTP improperty configured TFTP servers			
» User Groups	Detailed Information	This rule searches for the filename "parswd" in TFTP GET requests. The "parswd" file is used by Unix based systems to store users names for the			
Like minded pig lovers getting		rystem			
together to discuss snort.	Affected Systems				
» <u>Rules</u>	Attack Scenarios	After a successful system compromise an attacker may setup a thp service to transfer files back to the attacking system. Under this			
All the information about rules you could ever want		scenario the source address will point to the attack network and the			
could ever want		destination address will be an address defined in the HOME_NET.			
Search Ports		Attackers may also scan large subnets for TFTP servers and make numerous generic GET request for common system files.			
	Ease of Attack	Simple Numerous tools and automated scripts east for scanning large submets for improperly configured TFTP servers.			
	False Positives	This rule was created to catch TFTP GET requests for "passwd", if this			
Rules Documentation		file name is being used during a legitimate TFTP session this rule will generate a faise positive.			
		If you think this rule has a false positives, please help fill it out			
		None known			
		If you think this rule has a false negatives, please help fill it out. Depending on the situation blocking the attacker at the upstream router			
		or freewall will eignmate the problem. However, if the TFTP server is			

1 to 1		aht 👫 Options 🔽 Pop-ups Allowed 👻 Hotmail 🌋 Messenger 😰 My MSN	
Criteria ad Criter	any ia any		
0 alert(s)	to the Alert cache		
		Alert #1 [First] >> Next #1-(1-260)	
	and the second s	gered Signature	
	1 - 267 2005-02-05 16:47:15 [snort]	TFTP GET passwd	
Meta	Sensor name interface filter 192.168.2.2 eth0 none		
	Alect Group none		
	and the property of the proper	OS length ID flags offset TTL chksum 0 50 5449 0 0 64 40997	
Ib	Source Name Dest, Nam		
	FQDN probe Unable to resolve	e address	
	Options none		
UDP	source port dest port length 32905 69 30		
	length = 22		
Payload	000 : 00 01 2E 2E 2F 65 74 63 2F 7 010 : 6F 63 74 65 74 00	70 61 73 73 77 64 00/etc/passvd. octet.	
			-
		[First] >> Next #1-(1-268)	
<u>}-</u>		Action	

• • • • • • • • • • • • •				Microsoft Internet Explorer provided by BTopenworld	
Introductive Trippered Signature Introductive Introd					
• • • • • • • • • • • • •	sk • E	> 💌	📓 🞧 🔎 Search 🥱	🖓 Favorkes 🚱 😂 🍓 🔟 - 🔜 🕲 📽 🥥 🤹	
Toria arry Criteria arry Verteria arry Ve		192.168.2.2	🛩 🛃 Go		
Image: series Image: series Image: series Image: series <t< td=""><td></td><td></td><td>Search •</td><td>Highlight 🕂 Options 🔲 Pop-ups Allowed 🔹 🔤 Hotmail 🍱 Messenger 😰 My MSN</td><td></td></t<>			Search •	Highlight 🕂 Options 🔲 Pop-ups Allowed 🔹 🔤 Hotmail 🍱 Messenger 😰 My MSN	
< Previous #ft-(1-252) >> Next #6-(1-254) ID # Time Triggered Signature II - 255 2005-02-05 16-46-49 [arachtHDS][snort] SCAN SVN FIN Bernsor Insertice Alert Anne Alert Anne Provide addr dest addr		a any	cache		
1 - 255 2005-02-05 16-46-49 [arachtIDS](monet] SCAN SYN FIN Sensor 1902-160-2.2 eth0 none Abert none 1922-160-2.2 eth0 none 100 Feedow 192.160-2.2 eth0 none 100 Feedow 192.160-2.4 4 5 0 0 255 192.60 100 Feedow Feedow Topolo 0 0 255 192.60 100 Feedow					
Weta Earsor name interface filter Allert none Allert none 102 102.160.2.2 eth0 none 102 FQON Saurce addi dest addr. 4 5 0 0 255 15936 102 FQON Saurce Name Dest. Name Dest. Name Dest. Name Dest. Name 102 FQON Saurce Name Dest. Name Dest. Name Dest. Name 102 FQON Saurce Name Dest. Name Dest. Name Dest. Name 102 FQON Saurce Name Dest. Name Dest. Name Saurce 103 102.5 X X 17.0396302 0 62004 102 FX X 17.0396302 0 0 62004 102 Coptons none Saurce Saurce Saurce Saurce at/odd rone Saurce Sau		ID #	Time	Triggered Signature	
Virial Sensor 192.168.2.2 eth0 none Alert Coolp Alert Coolp Alert Alert Coolp none IP FQON Sence addi dest addi probe Veri Har Lon TOS Inengh 0 0 0 255 19396 IP FQON Sence Name probe Dest. Name (Inable to resolve address - - - - Sence dest 1004 R R 1025 K R 10304 R R 1025 K R 1710396302 0		1 - 255	2005-02-05 16:46:49	[arachNIDS][snort] SCAN SYN FIN	
Image: Index: Index: Image:	Meta	Francis	name interface	filter	
None Burces addr. dei addr. Ver Hdr. Len TOS Nength ID Rags affert TTL chlowm P Exacts addr. dei addr. Ver Hdr. Len TOS Nength ID Rags affert TTL chlowm P FQDN Sources Name Deet. Name probe Unable for resolve address Options none		Sensor	192.160.2.2 eth0	none	
192.169.2.2 192.169.2.4 4 5 0 40 9 0 255 19996 P PORN Seurce Name Dest. Hame Porto			none		
FOON probe Unable to resolve address Cptions none securce dest R R V R S F seg # ack offset res window urp chkoum TCP 10004 1025 X X 1710396382 0 0 0.0004 Violation none Coptions Next #6(1254) violation Address #7(1-252) >> Next #6(1254) colspan="2">Coptions Next #6(1254) colspan="2">Coptions Next #6(1254)					
PCQN probe Unable to resolve address Options none TOP	tP	S	ource Name (est. Name	
Image: solution of the		FQDN ==	probe Unable t	o resolve address	
TCP 10004 1025 ix ix i1710396362 0 5 0 4096 0 62004 Options none		Options	none		
10004 10/25 x x 1/103/95/302 0 5 0 40/36 0 52/804 Options none		source port	dest R R U A P R S port 1 0 G K H T M	F I seq# ack offset res window urp chksum N	
ayload none <pre></pre>	TCP	10084 1	1025	× 1710396382 0 5 0 4096 0 62884	
<		Options	none.		
(action)	Payload	none			
(5) second (Action	
	d in D second	M			🔒 🗶 internet