

Free And Open Source Security Tools

Agenda

- Firewalls
- Port Scanners
- Network Sniffers
- Vulnerability Assessment
- Intrusion Detection Systems
- Email Security

Bastille Linux

- Considered one of the most popular hardening tool
- User friendly and interactive
- Supports Linux, HP-UX and Mac OS-X
- Download from www.bastille-linux.org
- **Bastille Linux Installation**
 - rpm -ivh Bastille-a.b.c.rpm
 - rpm -ivh perl-TK-a.b.c.i386.rpm (for graphical interface)
 - rpm -ivh perl-Curses-a.b.c.i386.rpm (for console/text interface)
- **Run Bastille**
 - Bastille -x (graphical)
 - Bastille -c (Text)
 - Bastille -report (for assessment and reporting)

Turtle Firewall

- It's a web based interface to IPTables
- These are basically Perl Scripts that setup an IPTable Firewall
- Much easier to see rules and make order of the statements right
- Requirements:
 - Kernel 2.4 or higher
 - Iptables
 - Webmin Interface (www.webmin.org)
 - Perl with Expat Library

SmoothWall Express

- A Turnkey firewall solution
- Supports NAT, DHCP, SSH Admin, VPNs and a lot more
- Requires a dedicated system to install and run smoothwall
- Also comes in comercial version, Express version is free

- Smoothwall Requirements
 - Pentium 200 Mhz or higher
 - 32 MB RAM
 - 512 MB Disk space
 - CD-ROM and at least one NIC, but better to use two NIC

Smoothwall Corporate Features

- Enhanced IDS support
- Connection fail-over capabilities
- VPN roaming support (dynamic IPs)
- Additional graphs and reports
- Enhanced graphical user interface
- Certificate authentication support for VPN

Smoothwall Installation

- Download ISO image from www.smoothwall.org
- Make bootable CD of ISO and boot from CD-ROM
- Installation will ask about interfaces, IP addresses and DHCP
- After installation access from web browser

IPcop

- Ipcop is Another turnkey firewall solution which is created on smoothwall core
- Easy to manage through a simple to use web interface
- Require dedicated system
- Commercial support also available
- Download it from www.ipcop.org

IPcop Features

- **Interfaces**

- 4 interfaces with typical behavior
- GREEN : inside network
- RED : outside network (internet)
- ORANGE : DMZ (accessible from in and outside)
- BLUE : inside network for wifi (connect an Access point to this interface)

- **Hardware**

support i386 and alpha architecture (ppc will be available soon)

- memory size supported from 12 MB to 4 GB
- IDE, SCSI, SATA and RAID disk controller with 250 MB minimal hard disk size
- network cards from linux-2.4 kerne (ISA / PCI)
- smp kernel available on i386 for HT / multicore or multiples CPU
- indirect installation to flash device

IPcop Features

- **Core services**

- DHCP client / server

- Dynamic DNS

- Host list settable from web interface

- HTTP / FTP proxy (squid)

- IDS (snort) on all interfaces

- Log local or remote

- NTP client / server

- SSH server (PSK or password)

- Traffic shaping (red interface)

IPcop DHCP Server

IPCop - DHCP configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://192.168.1.200:445/cgi-bin/dhcp.cgi> Go Links >>

DHCP

Green Interface Enabled:

Start address: IP Address/Netmask: **192.168.1.200/255.255.255.0**

End address:

Default lease time (mins): Max lease time (mins):


Base IP for fixed lease creation:

Domain name suffix: Allow bootp clients:

Primary DNS: Secondary DNS:

Primary NTP Server: Secondary NTP Server:

Primary WINS Server address: Secondary WINS Server address:

This field may be blank. 

Additional DHCP Options

Add a DHCP Option

Option name: or Select

Option value:

Enabled: Option scope: GREEN BLUE

Global scope or limit scope to checked interfaces.

Option name	Option value	Option scope	Action
-------------	--------------	--------------	--------

IPcop Traffic Shapping

IPCop - Traffic Shaping Settings - Microsoft Internet Explorer

DU Meter
DL: 1.0 kbps UL: 1.2 kbps

Address: https://192.168.1.200:445/cgi-bin/shaping.cgi

SERVICES TRAFFIC SHAPING The bad packets stop here.

SYSTEM STATUS NETWORK SERVICES FIREWALL VPNs LOGS

Settings:

Traffic Shaping

Downlink speed (kbit/sec):

Uplink speed (kbit/sec):

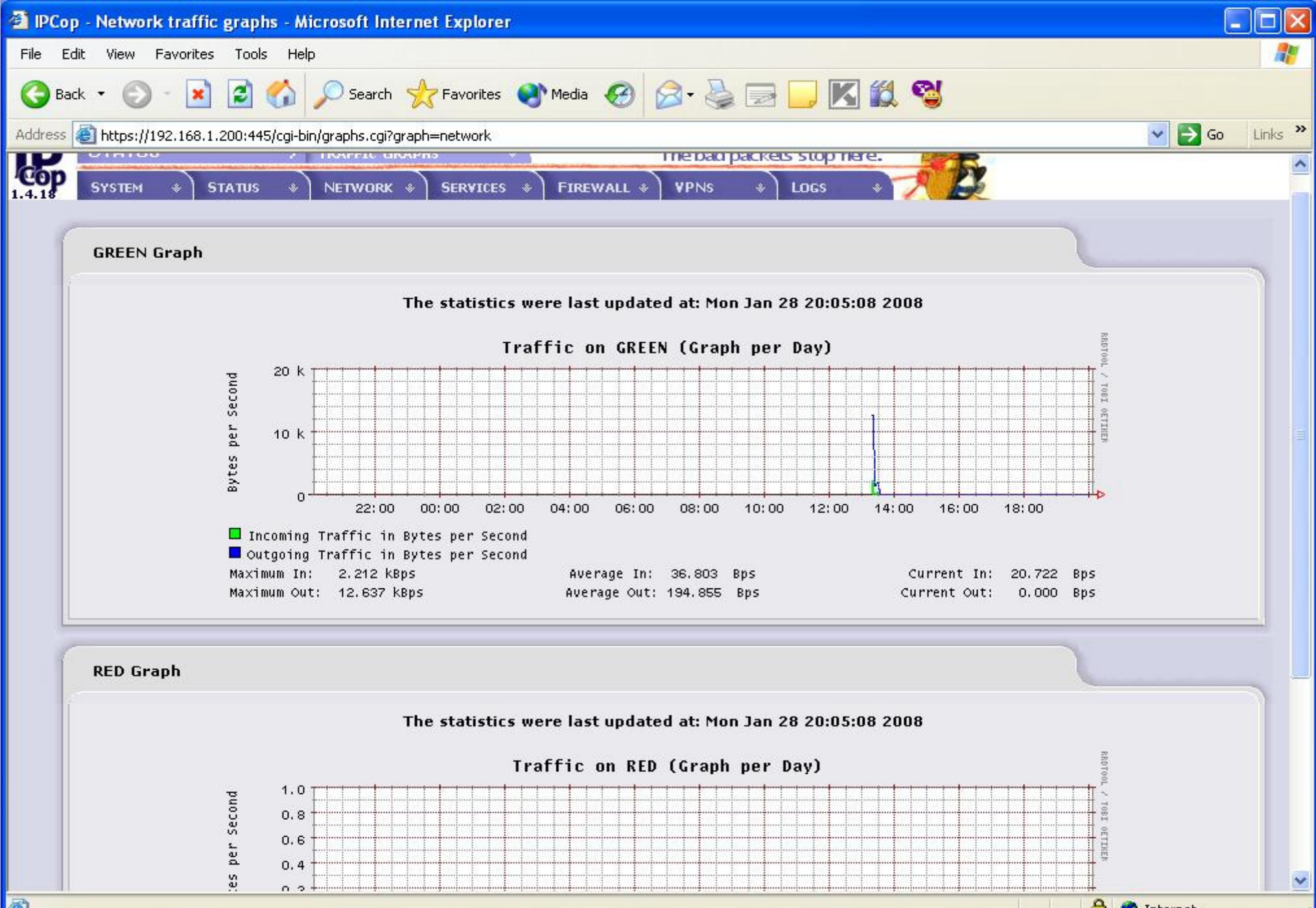
Add service

Priority: Port: Protocol: Enabled:

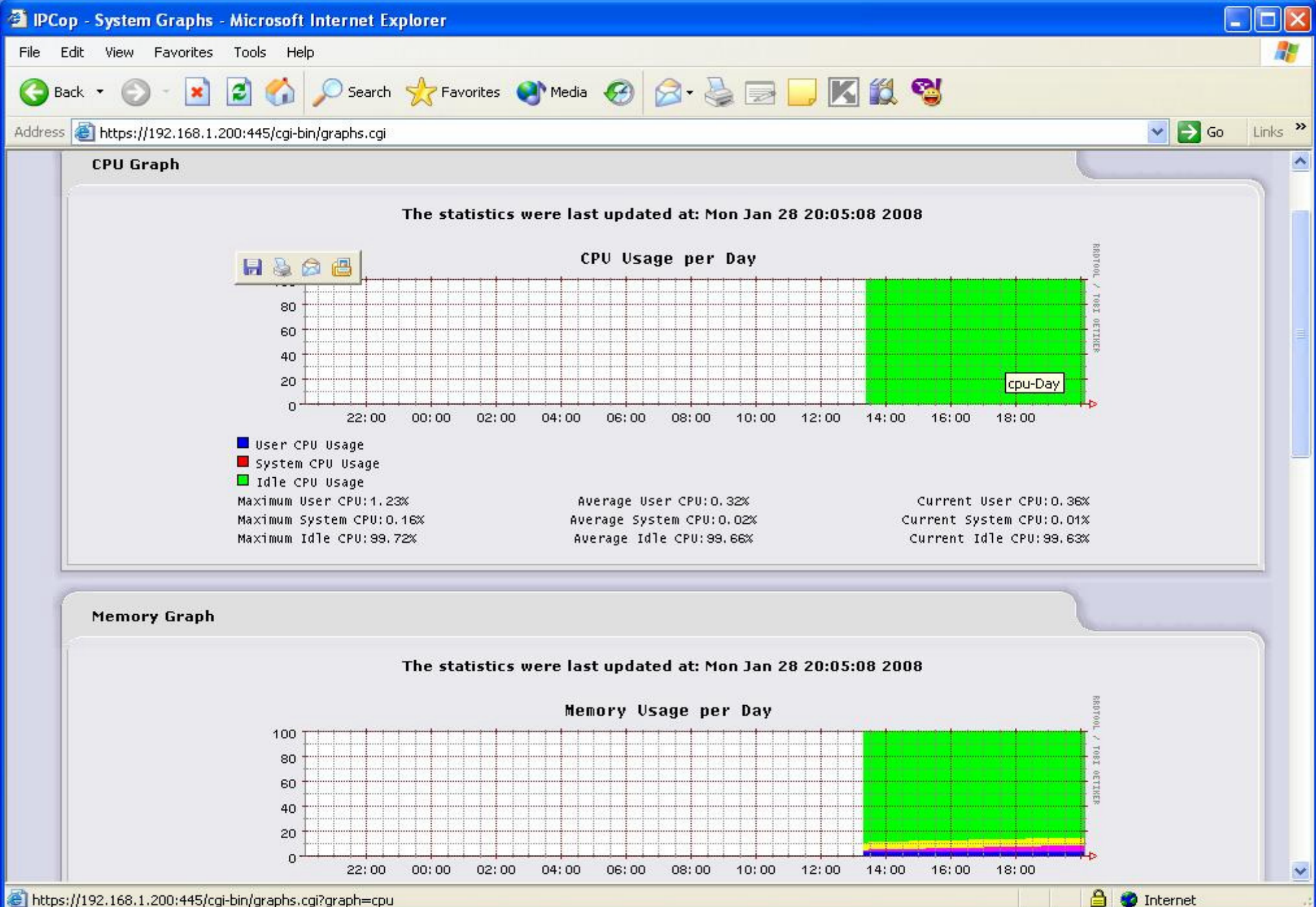
Traffic shaping services

Priority	Port	Protocol	Action
High	5060	udp	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Medium	80	tcp	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
High	22	tcp	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

IPcop Traffic Graph



IPcop System Graph



Intrusion Detection Systems

- Programs that look for anomalous behavior on a system and alert operators
- Some systems provide for additional analysis / reporting capability
- This is CRUTIAL to the usability of the system
- A vital backup to your firewall and perimeter defenses.
- A strong defense against internal attacks which firewalls can't detect
stop

Types of IDS

- Network Intrusion Detection System(NIDS)
 - Monitors entire network
 - NIC operates in promiscuous mode
 - Complicated sniffers that check all packets against signatures
- Host Intrusion Detection System (HIDS)
 - Hids protects only the host system on which it resides
 - Network card operates in non-promiscuous mode
 - No need to interpret multiple rules designed to detect

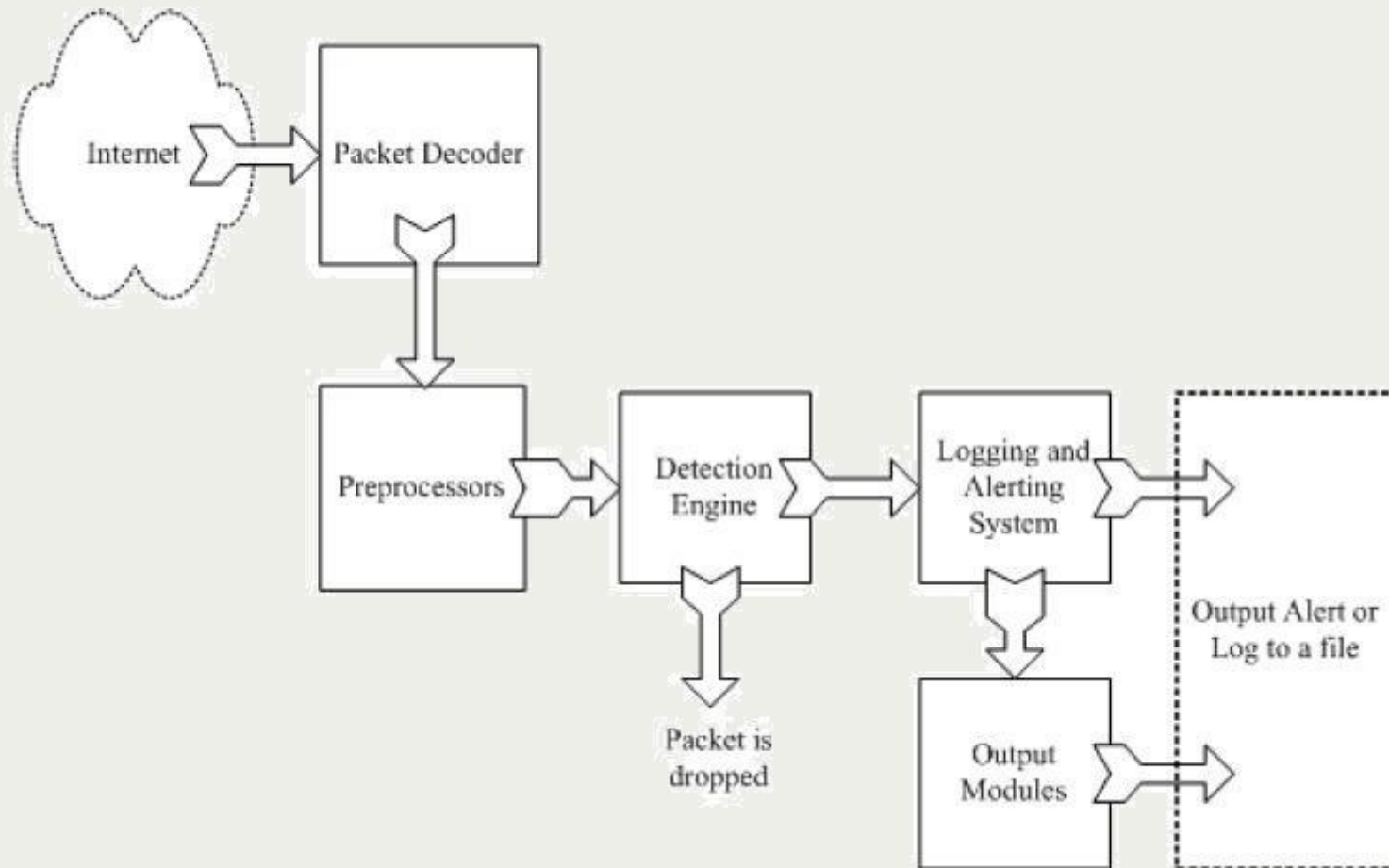


- Snort is a packet sniffer, a packet logger, and a network IDS.
- Snort runs on various operating systems and hardware platforms, including many UNIX systems and Windows. Hardware platforms include Intel-based systems, PA-RISC, PowerPC, and Sparc.
- Large default rule set (several thousand)
- Highly customizable and configurable
- Offers a scripting language to write custom rules to match your network

Components of Snort

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

How Components are arranged together



Description Of Components

- Packet Decoder
 - Prepares packets for processing.
- Preprocessors
 - Used to normalize protocol headers, detect anomalies, packet re-assembly and TCP stream re-assembly.
- Logging and Alerting System
 - Generates alert and log messages.
- Output Modules
 - Process alerts and logs and generate final output.

Snort Requirement

- Software Requirement
 - LibPcap Libraries
 - Linux Kernel 2.4 or greater
- Hardware Requirement
 - Network card capable of working in promiscuous mode
 - Intel 500 Ghz processor or greater (It also works on less)
 - 128MB of ram

Snort Installation

- Download snort from www.snort.org/dl/current/snort-2.8.0.1.tar.gz

```
tar -zxvf snort-2.8.0.1.tar.gz
```

```
cd snort-2.8.0.1
```

```
./configure --with mysql --enable-dynamicplugins
```

```
make
```

```
make install
```

- Install Snort Rules

Download from www.snort.org/dl/current/snortrules-pr-2.4.tar.gz

```
Tar -zxvf snortrules-pr-2.4.tar.gz
```

```
Cd snortrules-pr-2.4
```

```
Cp * /etc/snort/rules
```

Snort Modes

- Packet Sniffer Mode

- In Packet Sniffer Mode Snort act like tcpdump program and is used for testing.
- Type “snort -v” at command prompt to start snort in sniffer mode
- Other switches
 - -d displays application layer -e displays data link layer

- Packet Logger Mode

- Same as Packet Sniffing Mode but it also logs the output.
- Type “snort -dev -l /var/log/snort” where -l is switch for logging and /var/log/snort is directory to save output.

- Intrusion Detection Mode

- In this mode snort applies signature rules on all captured packets
- If packet matches rules, it is logged or an alert is generated. If no match

Snort Addons

- Webmin Snort Module – Configuration tool
- BASE/ACID – Alerts Analysis
- Barnyard – A fast output system for Snort
- Loghog- log analyzer and block traffic by configuring IPTables
- SneakyMan- A GNOME-based Snort rules Configurator

Basic Analysis and Security Engine (BASE)

Formerly Analysis Console for Intrusion Detection (ACID)

Web front end created in PHP and database interface for Snort

Imports alerts into a database and allows viewing through a web-based interface

This allows analysis of your Snort data and helps with tuning your Snort sensors

BASE Requirements

- MySQL, PostgreSQL or Oracle database
- PHP-enabled web server
- One or more snort sensors to gather data from
- Must build snort with “—with-mysql” parameter if using mysql as database
- Download BASE from: <http://secureideas.sourceforge.net/>

BASE Demo

Basic Analysis and Security Engine (BASE) 1.2.6 (christine) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://203.215.161.166/base/base_main.php Go Links

Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Added 0 alert(s) to the Alert cache
Queried on : Tue January 29, 2008 03:46:45
Database: snort@localhost (Schema Version: 107)
Time Window: [2008-01-23 09:01:29] - [2008-01-29 03:46:02]

[Search](#)
[Graph Alert Data](#)
[Graph Alert Detection Time](#)

Sensors/Total: 1 / 1
Unique Alerts: 14
Categories: 6
Total Number of Alerts: 963

- Src IP addr: **169**
- Dest. IP addr: **122**
- Unique IP links **305**

- Source Ports: **41**
 - TCP (3) UDP (38)
- Dest Ports: **8**
 - TCP (5) UDP (3)

Traffic Profile by Protocol

TCP (1%)	
UDP (6%)	
ICMP (15%)	
Portscan Traffic (78%)	

Done Internet

Tripwire

- Tripwire is host based IDS
- Originally Tripwire was purely open source. Eventually founders form a company to sell and support it commercially
- Significant differences between commercial and open source
 - Open source tripwire supports only Linux while commercial supports more platforms including windows
 - Commercial version comes with a program called twagent, which is utility for managing multiple installations of tripwire

Tripwire installation

- Download from <http://sourceforge.net/projects/tripwire/>
tar -zxvf tripwire.tar.gz
cd tripwire
make all
open install.cfg to make sure all paths are correct
type ./install.sh

Tripwire Configuration

- Set policy file, it tells tripwire what file to keep an eye on and what level of details to go into.
- Policy file can be found in policy directory in main tripwire directory and named as twpol.txt
- Initializing Baseline database
 - Type “tripwire –m –i –v” to establish initial file database
 - Switches
 - m denotes mode
 - i denotes initialize
 - v denotes verbose
- Checking file integrity
 - Type “tripwire –m c file.txt” where as file.txt is file to be checked

Network Sniffers

- These programs capture data packets off the network for examination/analysis, detecting bottlenecks and problems.
- Network sniffing, or just “sniffing,” is using a computer to read all network traffic, of which some may not be destined for that system.
- To perform sniffing, a network interface must be put into promiscuous mode so that it forwards, to the application layer, all network traffic, not just network traffic destined for it.

Wireshark

- Wireshark is a free, open source network sniffer with many features
- Graphic Interface
- Formerly known as Ethereal
- Requirements
 - Latest LibPcap (4.0) Libraries
 - Network card capable of working in promiscuous mode

Devices from Which Wireshark Can Capture Data

- Ethernet
- Token-Ring
- FDDI
- Serial i.e PPP and SLIP (if os allows wireshark to do so)
- 802.11 wireless LAN (commercial Add-on)
- ATM ((if os allows wireshark to do so)
- Any device supported on Linux by recent versions of libpcap.

Wireshark Demo

The screenshot displays the Wireshark application window. The title bar reads "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, capture, and analysis. Below the toolbar is a filter field with a dropdown arrow and buttons for "Expression...", "Clear", and "Apply".

No. .	Time	Source	Destination	Protocol	Info
20	8.346626	203.215.167.91	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
21	9.325342	203.215.167.91	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
22	9.332226	203.215.167.91	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
23	9.339139	203.215.167.91	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
24	9.345815	203.215.167.91	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	9.578868	HonHaiPr_2e:02:5d	Broadcast	ARP	Who has 203.215.167.92? Tell 203.215.167.84
26	10.305110	221.254.41.233	203.215.167.88	ICMP	Echo (ping) request
27	10.788438	203.215.172.13	203.215.161.166	DNS	Standard query response PTR 221x254x41x233.ap221.fttl
28	11.800849	64.74.133.28	203.215.167.87	UDP	Source port: 11479 Destination port: 33439
29	11.823914	64.74.133.16	203.215.167.87	UDP	Source port: 11479 Destination port: 33442
30	12.627678	Cisco_5e:04:43	Broadcast	ARP	Who has 203.215.161.162? Tell 203.215.161.161
31	14.593346	Intel_5b:b3:ce	Broadcast	ARP	Who has 203.215.167.92? Tell 203.215.167.82
32	15.421065	Cisco_5e:04:43	Broadcast	ARP	Who has 203.215.161.162? Tell 203.215.161.161

The detailed view of the selected packet (No. 28) shows the following structure:

- Frame 1 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Cisco_5e:04:43 (00:e0:1e:5e:04:43), Dst: Intel_fa:29:ff (00:19:d1:fa:29:ff)
- Internet Protocol, Src: 64.74.133.28 (64.74.133.28), Dst: 203.215.167.87 (203.215.167.87)
- User Datagram Protocol, Src Port: 11479 (11479), Dst Port: 33439 (33439)
- Data (4 bytes)

The packet bytes are displayed in hexadecimal and ASCII:

```
0000 00 19 d1 fa 29 ff 00 e0 1e 5e 04 43 08 00 45 00  ....).... ^..C..E.
0010 00 20 04 15 00 00 01 11 7d 23 40 4a 85 1c cb d7  . . . . . }#@J....
0020 a7 57 2c d7 82 9f 00 0c 61 2c 69 56 4d 47 00 04  .W,.... a,iVMG..
0030 03 73 6d 77 a0 1e 02 04 02 03 0f f7             .smw.... . . . .
```

At the bottom of the window, the status bar shows: File: "/tmp/etherXXXX17Saud" 5520 Bytes 00:00:15 Packets: 32 Displayed: 32 Marked: 0 Dropped: 0

Wireshark Voip Calls

- Supported Protocols
 - SIP
 - H323
 - ISUP
 - MGCP
 - UNISTIM
- Filtering A Call
 - Can filter particular call
- Playing A Call
 - Can play call only for G.711 A-Law and G.711 U-law RTP streams

Port Scanners

- A port scanner is a program which attempts to connect to a list or range of TCP/UDP ports on a list or range of IP addresses and determine the state of TCP/UDP ports.
- Nmap(Network Mapper) is the most popular port scanner.
- **Purpose of Port Scanners**
 - Determine number of answering machines on the network (Ping Sweep)
 - OS Identification (TCP Fingerprinting)
 - Identify unnecessary or rogue services running on

Nmap

- Powerful light weight port scanner
- Runs on Unix or Windows
- Command Line or GUI
- Zenmap is GUI package for Nmap
- Easy to run but also deep in functionality

- Nmap Requirements:
 - LibPcap libraries (www.tcpdump.org)
 - GTK+ is required by Zenmap

- Download Nmap from www.insecure.org

Nmap Requirement

- Nmap Requirements:
 - LibPcap libraries (www.tcpdump.org)
 - GTK+ is required by Zenmap
- Download Nmap from www.insecure.org

Zenmap demo

Zenmap

Scan Tools Profile Help

New Scan Command Wizard Save Scan Open Scan Report a bug Help

Intense Scan on 192.168.1.1 X

Target: 192.168.1.1 Profile: Intense Scan Scan

Command: nmap -T Aggressive -A -v 192.168.1.1

Hosts Services

OS	Host
3	192.168.1.1

Ports / Hosts Nmap Output Host Details Scan Details

```
-----
Scanning 3 services on 192.168.1.1
Service scan Timing: About 33.33% done; ETC: 10:58 (0:04:02 remaining)
Completed Service scan at 10:54, 121.14s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.1
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 10:54
SCRIPT ENGINE Timing: About 40.00% done; ETC: 10:56 (0:00:45 remaining)
SCRIPT ENGINE Timing: About 80.00% done; ETC: 10:57 (0:00:30 remaining)
Completed SCRIPT ENGINE at 10:57, 150.53s elapsed
Host 192.168.1.1 appears to be up ... good.
Interesting ports on 192.168.1.1:
Not shown: 1711 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet?
80/tcp    open  http?
|_ HTML title: Site doesn't have a title.
5190/tcp  open  aol?
MAC Address: 00:15:EB:D3:00:A2 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.18 (x86_64, SMP)
Uptime: 0.187 days (since Wed Jan 30 06:28:43 2008)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: D:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 277.312 seconds
Raw packets sent: 1737 (78.040KB) | Rcvd: 1729 (79.864KB)
|
```

Enable Nmap output highlight

Preferences Refresh

SuperScan

- Port Scanner for Windows
- Not as powerful as Nmap but nice graphic interface and quick
- Good for fast network host discovery
- Download SuperScan at
www.foundstone.com/resources/proddesc/superscan.htm
- No Source code provided; just free

Vulnerability Scanners

- These programs take port scanning a bit farther and try to run exploits against open ports
- These scripts replicate the actions of hackers or other malware such as viruses or worms
- Can be very useful to show how good your defenses are from the outside or inside

Vulnerability Scanner Options

- Nessus was the state of the art, but closed source after version 3.0.

Still available for free with registration for latest plugin feed.

- OpenVAS – A fork of older open source Nessus code; still has yet to release a new version

- Sara – An improved version of the SATAN Scanner; minimal functionality

Benefits of OpenVAS and other Nessus Forks

- Client-Server architecture. Supports multiple platforms for clients (Linux, Windows, Web-based, Java)
- Has a built in scripting language (NASL) for writing custom security tests
- Well documented and supported from legacy
- For now, we use Nessus 2.2.5, the last open source version

Nessus / OpenVAS Requirements

- LibPcap Libraries (www.tcpdump.org)
- Gimp Tool Kit (GTK) [ftp.gimp.org/pub/gtk/v1.2](ftp://ftp.gimp.org/pub/gtk/v1.2)
- Nmap (if you want to use it as your port scanner)
- OpenSSL (www.openssl.org)

Installing Nessus 2.2.10

- Download the software package from www.nessus.org
- If its not available on that site, look on mirrors or from the CD in the book
- There are four separate tar files
 - Nessus-libraries
 - Libnasl
 - Nessus-core
 - Nessus-plug-ins
- You must untar and install each module in the order above

Using the following commands:

```
./configure
```

```
make
```

```
make install
```

Installing Nessus 2.2.10

- Put the following in your path statement:
 - `/usr/local/sbin:/usr/local/bin`
- Edit a file called `ld.so.conf` in `/etc` and add the following line
 - `/usr/local/lib`

Then type “`ldconfig`”

Installing Nessus 2.2.10

Creating the certificates and initializing the installation

- Type “nessus-mkcert”
 - This creates a certificate for your Nessus installation
- Type “nessus-adduser”
 - This will create an initial user to give you access to the Nessus server

Using Nessus 2.2.10

- Start the Nessus server by typing

`./nessusd &` to run it as a daemon
- start the Unix Client by typing “./nessus”
- Or
- Use NessusWX, the window client to access the server
- Use one of the web clients out there (NCC which is next)

Netscan Command Console (NCC)

- A web based interface and database backend for managing multiple .nsr-based vulnerability scans
- Allows for scheduling of future scans, recurrence and storing of results in a database
- Web based analysis tool for results

Netscan Command Console (NCC)

- Written using Perl and PHP
- Based on the LAMP platform (Linux, Apache, MySQL and PHP (Perl too!))
- Backwards compatible with OS Nessus Requirements:
 - **MySQL:** **Version 3.2352 or higher**
 - **PHP:** **Version 4.32 or higher**
 - **Perl:** **Version 5.8 or higher**
 - **OpenVAS/Nessus:** **Version 2.07 or higher**
 - **Apache:** **Version 2.0.47 or higher**

Get it at www.netsecuritysvcs.com/ncc

Nikto

- Nikto is webserver scanner
- Conduct series of tests against a webserver and report known vulnerabilities in the server and its applications
- An important tool for web server administrator
- Test for more than 2600 vulnerabilities
- Based on popular whiskers scanner, still uses LibWhiskers perl module.
- Download from <http://www.cirt.net>

Nikto

- Requirements
 - Basic PERL installation
- Installation
 - Download from <http://www.cirt.net>
 - Tar `–zxvf nikto-current.tar.gz`
- Basic Testing
 - Type `“perl nikto.pl –h 192.168.1.100”`
 - Where `–h` stands for host

Email Security

- Anti spam (SpamAssassin)
- Anti virus (ClamAV)

AntiSpam Tools

- SpamAssassin
 - Perl based Spam filter
 - Works with Sendmail/Postfix
 - Filters spam based on signature matching, location, attributes (futures date, internal addresses) or Bayesian logic.
- Part of many commercial anti-spam Solutions
- Get it at <http://spamassassin.apache.org/>

ClamAV

- Open Source Anti-virus Toolkit project
- Works at the mail server rather than on desktops
- Upsides:
 - Takes processing job off of the desktops
 - Free!
- Downsides
 - Mainly for Email Attachment scanning;
 - Doesn't catch Viruses on CDs or downloaded via other means (web)
- Best used as a additional protection not sole
- Download at: <http://www.clamav.net/>

References

- “Open Source Security Tools” by Tony Howlett
- “Linux Toronto 2007” Presentation on “Open Source Security Tools” by Tony Howlett
- “Intrusion Detection Systems with Snort” by Rafeeq Ur Rehman
- “Linux Network Security” by Peter G. Smith
- Documentation of every tool