

**Network Intrusion Detection Systems Lab  
(IDS)**

**Open Source Security Tools for Information  
Technology Professionals**

**School of Professional Studies (SPS)**

**The City University of New York (CUNY)**

Aron Trauring  
Adjunct Professor  
CEO, Zoteca

Class 10 November 28th, 2005

# Snort

- GPL licensed CLI tool
- Commercial company SourceFire provides tested rules, support and products
- Purchased by Check Point

# Other FOSS IDS

- Bro
- Prelude

# Invoking Snort

- `snort <options> <expression>`
- Expression similar to `tcpdump` selectors

## Snort Sniffer Mode

- similar to `tcpdump` or `tethereal`
- `-v` — displays TCP/IP headers
- `-d` — displays application layer data
- `-e` — displays link layer headers

## Snort Logging Mode

- logs all packets sniffed
- `-l <logpath directory>` — logs into subdirectories by IP address
- `-h <home network (local IP range)>` — logs into subdirectories by non-local IP address
- `-b` — logs into binary file that can be analyzed by `ethereal` or `tcpdump`

## Snort IDS Mode

- logs only packets that are suspicious or warrant further attention
- `-c <config file>` — configuration file sets parameters for logging
- In Ubuntu and others: `/etc/snort/snort.conf` is default config file
- `/var/log/snort` is default logging directory
- can leave off `-vde` switches which slows down and may cause packets to drop

## Snort Alert Modes

- `-A full` — full alert information. Default when nothing is specified
- `-A fast` — logs only packet header and alert type (useful on fast networks)
- `-M <workstation>` — use smb to send to Windows pop-up service
- `-s` — send to Unix syslog
- send to database for later analysis

## Example Snort Session

- `snort -A full -c /etc/snort/snort.conf -b`
- in other window run `nmapfe`
- `Control-C` after a while
- `ls -al /var/log/snort`
- `ethereal -r /var/log/snort/<logfile>`

# Snort Configuration — Home Network

- `var HOME_NET <addresses>`
- Addresses comma-separated list of local network e.g.  
`192.168.1.0/24`
- `var HOME_NET $<interface>`
- Takes IP and mask from interface configuration e.g. `eth0`
- `EXTERNAL_NET` can also be defined
- default for both is `any`

## Snort Configuration — Internal Servers

- Define servers you have running on your network
- Can specify ports so only registers attacks on open ports
- Limits false positives

# Snort Configuration — Decoders and Pre-processors

- Run on traffic before it passes through rule sets
- For proper formatting or types of traffic easier to deal with as a class
- Example: decoder to reassemble fragmented packets so properly formatted
- Example: pre-processor for port scanning traffic which is high-volume and better dealt with en masse
- Only change configuration as gain more experience with the tool

# Snort Configuration — Output Modules

- Used for managing output
- Three modules: `syslog`, `database`, `unified` (binary format)
- `output <module name>: <configuration options>`
- See documentation for details

## Snort Configuration — Rule Sets

- Rule sets are in `rules` directory
- In config file can turn on/off whole rule sets via deleting/adding comment #

## Snort Configuration — Individual Rules

- Go to rules directory and edit rules files
- Can turn on/off individual rule via deleting/adding comment #
- Better to work on individual rules than whole set if relevant in anyway

<b>Rule Classes</b>	<b>Descriptions</b>
attack-responses rules	These are alerts for common response packets after an attack is successful. They should rarely report false positives and should be left on in most cases.

<b>Rule Classes</b>	<b>Descriptions</b>
backdoor rules	These are common signs a backdoor or Trojan horse program is in use. They will rarely be false positive.
bad-traffic rules	These rules represent nonstandard network traffic that should not typically be seen on most networks.

<b>Rule Classes</b>	<b>Descriptions</b>
chat rules	<p>Look for standard sign-ons for many popular chat programs. If chat is allowed explicitly or implicitly, then these alerts should be turned off. Also, note that these are not silver bullets for chats and will not detect all types of chat traffic. Still, they can be helpful in ferreting out the worst offenders.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
ddos rules	<p>Look for standard distributed denial of service types of attacks. On a DMZ and WAN, these alerts don't serve much purpose, because if you are under a distributed denial of service you will probably know it right away. However, they can be very useful inside the LAN to see if you have zombie machine participating unknowingly in a DDOS attack on another network.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
dns rules	Look for some standard exploits against DNS servers. If you aren't running your own DNS, you can turn these off.
dos rules	Similar to the ddos.rule set above.
experimental rules	These are turned off by default. These are generally used only for testing new rules until they are moved into one of the other categories.
exploit rules	These are for standard exploit traffic and should always be enabled.

<b>Rule Classes</b>	<b>Descriptions</b>
finger rules	These rules flag traffic having to do with finger servers. If you are not running finger anywhere, you could probably turn these off. However, finger servers often are running hidden from the system administrator, so you could leave these on as they shouldn't generate false positives if you don't have any.

<b>Rule Classes</b>	<b>Descriptions</b>
ftp rules	Same as finger rules but looking for FTP exploits. Again, there is no harm in leaving them enabled even if you don't have FTP servers since it will alert you to any rogue FTP servers you may have.

<b>Rule Classes</b>	<b>Descriptions</b>
icmp-info rules	<p>These rules track the use of ICMP messages crossing your network, for example, pings. These are often the cause of false positives, and you may want to disable the whole lot unless you want to keep a close eye on ICMP traffic on your network. Another class for known bad ICMP traffic, icmp rules catches ports scans and the like.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
icmp rules	Cover bad or suspicious ICMP traffic such as port scans, and are less likely to generate false positives. However, it is possible they will be triggered often on a busy network with lots of diagnostic services running.
imap rules	Rules regarding the use of Internet Message Access Protocol (IMAP) on your network.
info rules	Trap miscellaneous error messages on your network from Web, FTP, and other servers.

<b>Rule Classes</b>	<b>Descriptions</b>
local rules	You add your own custom signatures for your network in this file. This file is empty by default. See the documentation for information on writing a custom Snort rule.
misc rules	Rules that don't fit under one of the other categories or don't warrant their own sections are in this file. An example would be older alerts like Gopher server exploits.

<b>Rule Classes</b>	<b>Descriptions</b>
multimedia rules	Track usage of streaming video type software. If you allow streaming video applications or use video conferencing on your network, then you will want to disable these rules.

<b>Rule Classes</b>	<b>Descriptions</b>
mysql rules	<p>Watch for administrator access and other important files in a MySQL database. If you don't run MySQL, then you can probably disable these alerts. Also, if your MySQL database is under development, these might trigger a lot of false positives.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
Netbios rules	<p>This class of rules alerts you to various NetBIOS activity on your LAN. Some of them are obvious exploits. However, others, such as the NULL session alerts, may happen normally on a Windows LAN. You will have to play with this section to figure out the rules that are appropriate for your LAN.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
nntp rules	News server-related rules. If you don't run network news on your servers, you can probably turn these off.
oracle rules	Oracle database server rules. Again, if you don't run it, turn it off.
other-ids rules	These rules are related to exploits on other IDS manufacturers' boxes. Chances are that you don't have any NIDS on your LAN, but if you do, leave these on.

<b>Rule Classes</b>	<b>Descriptions</b>
p2p rules	Rules governing peer-to-peer file sharing software use. These rules will create alerts during normal use of these products, so if you allow this software then you will need to turn these off.

<b>Rule Classes</b>	<b>Descriptions</b>
policy rules	This file contains various alerts relating to allowed activity on the LAN, such as Go-to-my-pc and other programs. You should review these and enable only the ones that apply to your internal policies.

<b>Rule Classes</b>	<b>Descriptions</b>
pop2 / pop3 rules	Both files to mail servers. Most companies, if using POP, will be using a POP3 server. If you have either of these types of servers, leave these rules on; if not, disable them.

<b>Rule Classes</b>	<b>Descriptions</b>
porn rules	These are some rudimentary traps for pornography-related Web surfing. These are by no means a replacement for a good content-filtering system, but can catch some of the more egregious violators.

<b>Rule Classes</b>	<b>Descriptions</b>
rpc rules	<p>This class handles remote procedure call (RPC) alerts. Even though you may not think you are running any of these services, they often run as part of other programs, so it is important to be aware when this is happening on your LAN. RPC can enable remote code execution and is often used in Trojans and exploits.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
rservices rules	Track use of various remote services programs, such as rlogin and rsh. These are insecure services in general, but if you have to use them, they can be tracked closely with this rule set.

<b>Rule Classes</b>	<b>Descriptions</b>
scan rules	Alert you to use of port scanning programs. Ports scans are a good indication of illicit activity. If you use port scanners, you will want to either turn off Snort during those times or disable the particular rule for your scanner machine.

<b>Rule Classes</b>	<b>Descriptions</b>
shellcode rules	<p>This class looks for packets containing assembly code, low-level commands also known as shell code. These commands are often integral to many exploits such as buffer overflows. Catching a chunk of shell code flying by is often a pretty good indication that an attack is underway.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
smtp rules	Govern alerts for mail server use on the LAN. This section will need some fine-tuning, as many normal mail server activities will set off rules in this section.

<b>Rule Classes</b>	<b>Descriptions</b>
sql rules	Rules for various SQL database programs. If you don't run any databases you can turn these off, but it's not a bad idea to leave them on just in case there are SQL databases running that you don't know about.

<b>Rule Classes</b>	<b>Descriptions</b>
telnet rules	Track Telnet use on the network. Telnet is often used on routers or other command line devices, so it is a good thing to track even if you don't run Telnet on your servers.
tftp rules	TFTP (trivial FTP) is an alternate FTP server often run on routers. It can be used to upload new configurations and therefore is worth keeping an eye on.

<b>Rule Classes</b>	<b>Descriptions</b>
virus rules	Contain signatures of some common worms and viruses. This list is not complete and is not maintained regularly. It is not a replacement for virus scanning software but can catch some network-aware worms.

<p><b>Rule Classes</b></p>	<p><b>Descriptions</b></p>
<p>web-attacks rules web-cgi rules web-client rules web-coldfusion rules web-frontpage</p>	<p>All these classes refer to various kinds of suspicious Web activity. Some are generic, such as the web-attacks class. Others, like web-iis and web-frontpage, are specific to a particular Web server platform. However, even if you don't think you run a Microsoft Web server or use PHP, it is worth leaving them all running to uncover any of this kind of activity on your LAN you may be unaware of. You will have to do some fine-tuning of the rule sets, especially if your Web servers are in active development.</p>

<b>Rule Classes</b>	<b>Descriptions</b>
X11 rules	Track the use of the X11 graphical environment on your network.

# Webmin Snort