

Intrusion Detection Tool Workshop



Nick Savvides

nicks@physics.unimelb.edu.au

Tools To Be Used

- Snort
- www.snort.org
- Snort is a powerful network sniffer and realtime intrusion detection system.
- Notes + Demo
- Cross platform
- GPL
- Ethereal
- www.ethereal.com
- Ethereal is a powerful graphical network sniffer and traffic analyser.
- Demo only
- Cross platform
- GPL



- Common Command Line options:
 - **-?** , displays help.
 - **-F <filename>** , reads filters from filename
 - **-l <directory>**, logs to directory
 - **-d**, dump application layer
 - **-e**, dump second layer header info
 - **-b**, log in tcpdump format (fastest mode)
 - **-c <filename>**, use filename for configuration



- Launch snort as packet logger:
 - `snort -dev -l /var/log/snort`
 - Packets dumped to screen and logged to `/var/log/snort`
 - `snort -l /var/log/snort`
 - Packets logged to `/var/log/snort`
- Log in binary mode
 - `snort -b -l /var/log/snort`
 - Packets logged to `/var/log/snort` in tcpdump format



- Launch Snort as a network IDS.
 - `snort -b -l /var/log/snort -c snort.conf`
 - Config file must exist
- Snort uses rules to match traffic patterns against known attacks.
 - Rules can be in `snort.conf` or included from other files.



- Snort rules
- Example, Subseven rule
- alert tcp \$EXTERNAL_NET 27374 -> \$HOME_NET any
(msg:"BACKDOOR subseven 22"; flags: A+; content: "|
0d0a5b52504c5d3030320d0a|"; reference:arachnids,485; sid:103;
classtype:misc-activity; rev:3;)



- Snort rules are classified by action type. Valid action types are:
 - Alert – generate alert
 - Log – log packet
 - Pass – ignore packer
 - activate/dynamic – being phased out



- Snort rules then specify protocol, IP addresses, ports and direction of travel. Variables can be used to make life easier. Eg
- `alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any`

Here the protocol is TCP, EXTERNAL_NET is the src IP with src port 27374 and HOME_NET is the dest IP with dest port of any



- Beyond this comes the important part. The rule options.
- Rule options tell snort what to lookout for and how to behave on a match. Eg.
- `msg:"BACKDOOR subseven 22"; flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485; sid:103; classtype:misc-activity; rev:3;`

This says the alert message is “BACKDOOR subseven 22”. Snort matches on the packet contents of “|0d0a5b52504c5d3030320d0a|”.



- **Snort Pre-processors**
- Snort preprocessors were introduced in Snort 1.5. Preprocessors can be thought of as plugins that act on the packets after they have been decoded but before they are matched against rules.
- Useful preprocessors include HTTP decode, Portscan detectors, Stream4.
- Stream4 is a powerful preprocessor that provides TCP stream reassembly and allows stateful analysis.



- Snort demo.
- Ethereal demo.
- End Of Presentation