

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort

www.snort.org



- **Network Intrusion Detection System (NIDS)**
- Inspects/sniffs all network traffic passing thru it for any abnormal content
- Provides a layer of defense which monitors network traffic for predefined suspicious activity or patterns
- Has built in signature-base and anomaly detection, providing the capability to look for set "patterns" in packets
- String search signature (i.e. look for confidential), logging and TCP reset features
- Provides worthwhile information about malicious network traffic
- Help identify the source of the incoming probes, scans or attacks
- Alert sys admins when potential hostile traffic is detected
- Similar to a security "camera" or a "burglar alarm"
- Alerts security personnel that a Network Invasion maybe in progress

Network Management Workshop – APRICOT 2004, Kuala Lumpur

◆ Snort Features

- a cross-platform, lightweight network intrusion detection tool
- rules based logging to perform content pattern matching
- detect a variety of attacks and probes
- buffer overflows [ALE96], stealth port scans, CGI attacks, SMB probes, and much more
- has real-time alerting capability - syslog, SMB "WinPopup" messages, or a separate "alert" file
- detection engine is programmed using a simple language that describes per packet tests and actions
- Ease of use simplifies and expedites the development of new exploit detection rules
- detect a wide variety of suspicious network traffic as well as outright attacks
- is useful when it is not cost efficient to deploy commercial NIDS sensors
- Architecture is focused on performance, simplicity, and flexibility
- is available under the GNU General Public License, and is free for use

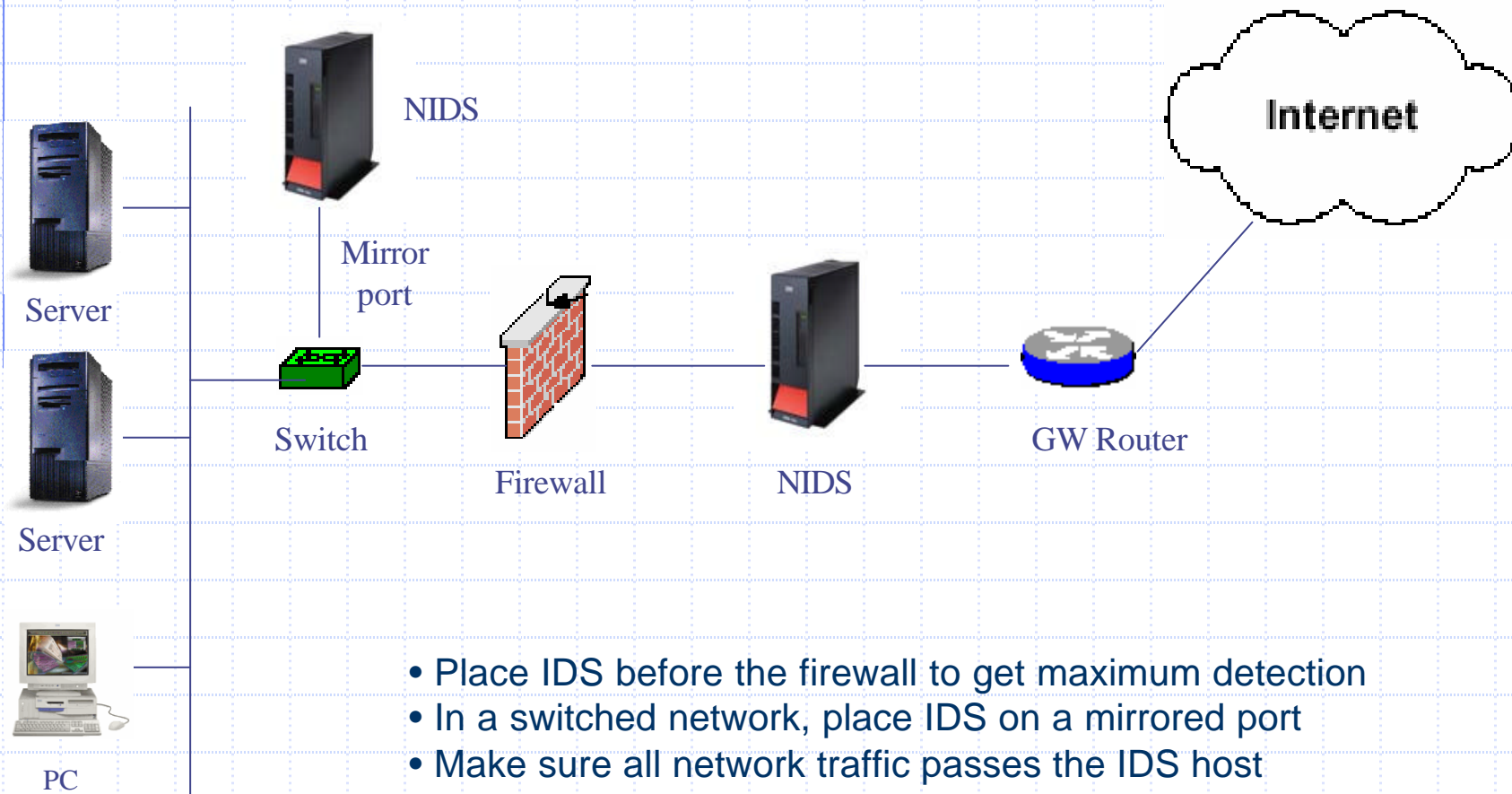
Network Management Workshop – APRICOT 2004, Kuala Lumpur

◆ How does Snort work?

- Sniffs, decodes the application layer data of a packet
- Can be given rules to collect traffic that has specific data contained within its application layer
- Detect many types of hostile activity, including buffer overflows, CGI scans, etc.
- Its decoded output display is somewhat more user friendly than tcpdump's output
- Can provide administrators with enough data to make informed decisions on the proper course of action in the face of suspicious activity
- Alerts administrators in real time via various methods

Network Management Workshop – APRICOT 2004, Kuala Lumpur

◆ Snort – NIDS placement



- Place IDS before the firewall to get maximum detection
- In a switched network, place IDS on a mirrored port
- Make sure all network traffic passes the IDS host
- Best to run IDS in bridge mode for transparent network operation

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Architecture

There are three primary subsystems:

1. The packet decoder
 2. The detection engine
 3. The logging and alerting subsystem
- These subsystems ride on top of the libpcap promiscuous packet sniffing library, which provides a portable packet sniffing and filtering capability
 - Program configuration, rules parsing, and data structure generation takes place before the sniffer section is initialized
 - Keeps the amount of per packet processing to the minimum required to achieve the base program functionality

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Architecture

1. The packet decoder

- The decode engine is organized around the layers of the protocol stack present in the supported data-link and TCP/IP
- Speed is emphasized in this section
- majority of the functionality of the decoder consists of setting pointers into the packet data for later analysis by the detection engine
- provides decoding capabilities for Ethernet, SLIP, and raw (PPP) data-link protocols
- ATM support is under development

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Architecture

2. The detection engine

- Snort maintains its detection rules in a two dimensional linked list of what are termed **Chain Headers** and **Chain Options**
 - **Chain Headers** - list of common attributes
 - **Chain Options** - the detection modifier options
- To speed the detection processing, the commonalities are condensed into a single Chain Header and then individual detection signatures are kept in Chain Option structures
- All rule chains are searched recursively for each packet in both directions
- The detection engine checks only those chain options which have been set by the rules parser at run-time
- The first rule that matches a decoded packet in the detection engine triggers the action specified in the rule definition and returns

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Architecture

3. The logging/alerting subsystem

- is selected at run-time with command line switches
- three logging and five alerting options are available
- Logging options:
 - log packets in their decoded, human readable format to an IP-based directory structure or
 - OR in tcpdump binary format to a single log file
 - Decoded format logging allows fast analysis of data collected by the system
 - Tcpdump format is much faster to record to the disk and should be used in instances where high performance is required
 - Logging can also be turned off completely -- leaving alerts enabled for even greater performance improvements

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Architecture

3. The logging/alerting subsystem

– Alerting options:

- Sent to syslog
- Logged to an alert text file in two different formats – full, fast
- Sent as WinPopup messages using the Samba program

- syslog alerts are sent as security/authorization messages that are easily monitored with tools such as swatch
- WinPopup alerts allow event notifications to be sent to a user-specified list of Microsoft Windows consoles
- Full alerting writes the alert message and the packet header information
- fast alert option writes a condensed subset of the header information - allowing greater performance under load
- a fifth option to completely disable alerting, which is useful when alerting is unnecessary or inappropriate

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Writing Snort rules

- Snort rules are simple to write, yet powerful enough to detect a wide variety of hostile or merely suspicious network traffic
- There are three base action directives that Snort can use when a packet matches a specified rule pattern: **pass**, **log**, or **alert**
- **Pass** rules simply drop the packet
- **Log** rules write the full packet to the logging routine that was user selected at run-time
- **Alert** rules generate an event notification using the method specified by the user at the command line
- ... and then log the full packet using the selected logging mechanism to enable later analysis

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Using Snort

There are three main modes in which Snort can be configured:

1. Sniffer Mode

- simply reads the packets off of the network and displays them for you in a continuous stream on the console

2. Packet logger mode

- logs the packets to the disk

3. Network intrusion detection mode

- is the most complex and configurable configurations
- allows Snort to analyze network traffic for matches against a user defined rule set
- perform several actions based upon what it sees.

Network Management Workshop – APRICOT 2004, Kuala Lumpur



Snort Lab

- Installation
- Sniffer mode
- Packet Logger Mode
- Network Intrusion Detection Mode
- NIDS Mode Output Options
- High Performance Configuration
- Changing Alert Order
- Miscellaneous