Security Principles

SNORT - IDS

Intrusion detection

- **What is intrusion detection ?**
  - Technically, any method that allows you to discover if someone has penetrated or is attempting intrusion into your network, host, services.
- **What is intrusion ?**
  - Unlawfully gaining access to systems, resources
  - The access itself, or the methods used, may be unlawful
  - There may not be a “breakin”
  - The result is the same
    - Someone is accessing something they are not allowed to…
- **Just because the door was open doesn’t mean I am allowed to walk in**
  - You still have an intruder!

What is an IDS ?

- An IDS is a device, or group of devices, which look for specific patterns in network traffic, for the purpose of detecting malicious intent

Snort ?

- Snort is an open source IDS, and one of the oldest ones
- Hundreds of thousands of users
- Active development of rules by the community make Snort up to date, and often more so than commercial alternatives
- Snort is fast! It can run at Gbit/s rates with the right hardware and proper tuning

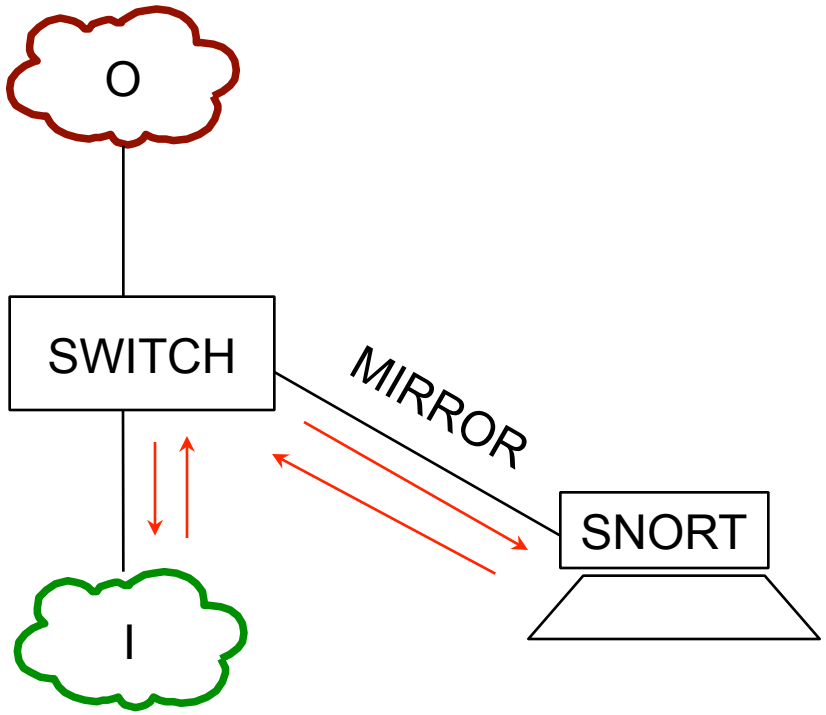
Where to place Snort ?

- Snort will need to be close to the “choke point” (the point where all traffic flows through on the way in or out of your network)
  - Inside of the border router or firewall, for example

Getting Snort to see the network

- You could run Snort in multiple ways
  - As a device “in line” behind or after the firewall /router
    - But this adds one more element that can fail in your connectivity
  - Or you could use a span/mirror port to send traffic to Snort
  - Or you can use an “optical splitter” to “mirror” or “tap into” traffic from a fiber optic link
    - This method and the previous are the most recommended

Getting Snort to see the network



Getting Snort to see the network

- Be careful not to overload your switch port
  – If you mirror a gigabit port to another gigabit port, the monitoring port (the receiving port) can drop packets if the total traffic exceeds 1 Gbit/s
- We'll illustrate this…

Monitoring Port…

- On Cisco Catalyst, this is a “SPAN” port
- You can SPAN one port to another, a group of ports to one port, or an entire VLAN to a port
- Sample config:

  interface FastEthernet 0/1

  # port monitor FastEthernet 0/2
- This would copy any packet received on F0/2 to F0/1

Monitoring Port…

- Other equipment vendors have different syntax
- HP calls it a “mirror port”

Snort configuration file

- By default, /etc/snort/snort.conf
- It's a long file – 900+ lines
- If you browse it, you will notice many "preprocessor" entries
- Snort has a number of "preprocessors" which will analyze the network traffic and possibly clean it up before passing it to the rules

Snort rules

- Snort rules are plain text files
- Adding new rules to snort is as simple as dropping the files into /etc/snort/rules/
- Groups of rules can be loaded from snort.conf using the “include” statement
- Rules can match anything
  - Technical – web attacks, buffer overflow, portscan, etc…
  - Policy/user oriented – URL filtering, keyword, forbidden applications, etc…

Tailoring the rules

- Not all rules will make sense in your network
- You will want to customize which rules you want to run
- Otherwise you will get many false positives, which will lead you to ignore Snort, or simply turn it of…
  - It doesn't help to have logs full of junk alerts you don't want
  - To avoid this, rules can be suppressed (disabled)

Updating Snort rules

- The commercially maintained snort rules are available for free with a 30 day delay from http://www.snort.org/start/rules
- The updating of rules can be automated with a tool called “Pulled Pork”, which is located at http://code.google.com/p/pulledpork/

Sample rules

- # These signatures are not enabled by default as they may generate false
- # positive alarms on networks that do mysql development.

- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL root login attempt"; flow:to_server,established; content:"|0A 00 00 01 85 04 00 00 80|root|00|"; classtype:protocol-command-decode; sid:1775; rev:2;)

- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL show databases attempt"; flow:to_server,established; content:"|0F 00 00 00 03|show databases"; classtype:protocol-command-decode; sid:1776; rev:2;)

- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL 4.0 root login attempt"; flow:to_server,established; content:"|01|"; within:1; distance:3; content:"root |00|"; within:5; distance:5; nocase; classtype:protocol-command-decode; sid:3456; rev :2;)

Reporting and logging

- Snort can be made to log alerts to an SQL database, for easier searching
- A web front-end for Snort, BASE, allows one to browse security alerts graphically

References and documentation

- Snort preprocessors:

http://www.informit.com/articles/article.aspx?p=101148&seqNum=2

- Snort documentation

http://www.snort.org/docs

- An install guide for Ubuntu 10.04:

http://www.snort.org/assets/158/014-snortinstallguide292.pdf