Intrusion Detection System

Amir Hossein Payberah
payberah@yahoo.com
Contents

- Intrusion Detection Systems
- Tripwire
- Snort
IDS (Definition)

- **Intrusion Detection** is the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problem.

- The bulk of intrusion detection research and development has occurred since 1980.
IDS (Architecture)
IDS (Information Sources)

- The first requirement for intrusion detection is a set of input data.
- Which source is the best source for intrusion detection?
Information Sources (Cont.)

- **Host-Based** Information Sources
- **Network-Based** Information Sources
Host-Based

- Operating System Audit Trails
- System Logs
- Application Information
- Target-Based Monitoring
Network-Based

- In network-based approach, information is collected form the network traffic stream as it travels on the network segment.
IDS (Analysis)

- Analysis is organizing and characterizing data about user and system to identify activity of interest.

- This process is divided into three phases:
  - Constructing the analyzer.
  - Performing analysis of live data.
  - Feedback or refinement of the process.
Analysis (Cont.)

- **Misuse Detection**
  - Engines look for something defined to be bad.

- **Anomaly Detection**
  - Engines look for something rare or unusual.
IDS (Responses)

- **Active Responses**
  - Take action against the intruder
  - Amend the environment
  - Collect more information

- **Passive Responses**
  - Alarm and notification
  - SNMP Trap
Contents

- Intrusion Detection Systems
- Tripwire
- Snort
Tripwire

- It is a **host-based** IDS.
- It is one of the most popular applications for determining when a file or directory has been **alerted**.
- It **scans** the system’s hard drive and create a database.
Tripwire Files

- `/usr/sbin/tripwirewire`
  - The tripwire binary responsible for reading, creating and updating the database.

- `/etc/tripwire/twpol.txt`
  - The tripwire policy configuration file.

- `/etc/tw.pol`
  - The signed tripwire policy file.
Tripwire Files

- **/usr/tripwire/twinstall.sh**
  - The file that signs the /etc/tripwire/twpol.txt and /etc/tripwire/twcfg.txt files.

- **/etc/tripwire/twcfg.txt**
  - Configures the environment for the /usr/sbin/tripwire binary.

- **/var/lib/tripwire/hostname.twd**
  - The default location of the Tripwire database file.
Configuring the Tripwire Policy File

- `/etc/tripwire/twpol.txt`

- `/etc/shadow -> $(IgnoreNone);`
  - Any file followed by the `IgnoreNone` argument will be checked by Tripwire’s “paranoid mode,” which means that any and all changes will be reported to you.

- `!/proc;`
  - Informs Tripwire to ignore the `/proc` directory.
Creating the Tripwire Policy File

- After you have installed Tripwire and edited the /etc/tripwire/twpol.txt, you are ready to begin the initial scan.

- Simply run the /etc/tripwire/twinstall.sh script.
  - It will then create the Tripwire configuration file.
Database Initialization Mode

- After you have created a policy file, you can then enter **database initialization** mode.
- `tripwire --init`
- `tripwire --help init`
Integrity Checking Mode

- After you have created the database, you can run Tripwire in integrity checking mode.
- `tripwire --check`
Contents

- Intrusion Detection Systems
- Tripwire
- Snort
Snort

- It is a network-based IDS.
- It places the NIC into promiscuous mode and captures all traffic on your network segment.
Snort Files and Directories

- /usr/local/snort
  - The Snort binary, when installed from an RPM package.

- /usr/local/bin/snort
  - The binary, when installed from a tarball.

- /etc/snort/
  - A directory that contains the Snort configuration file, as well as all Snort rules.
Snort Files and Directories

- `/etc/snort/snort.conf`
  - The Snort configuration file.

- `/usr/share/doc/snort-1.7`
  - The documentation directory if you install Snort using the RPM. If you install using a tarball, the documentation will be in the subdirectory where you installed all of the source files.

- `/etc/rc.d/init.d/snortd`
  - The initialization script for snortd.
Starting Snort

- Start Snort as a **simple packet sniffer**.
- This command will **log traffic only at the network level**.
- `snort -v`
Starting Snort

```
[root@keats snort]# /usr/sbin/snort -v

--- Initializing Snort ---
Initializing Network Interface eth0
Kernel filter, protocol ALL, raw packet socket
Decoding Ethernet on interface eth0

--- Initialization Complete ---

--> Snort! <--
By Martin Roesch (roesch@clark.net, www.snort.org)
04/16-16:46:17.350156 192.168.2.2:1065 -> 10.100.100.50:53
UDP TTL:64 TOS:0x0 ID:44084 IpLen:20 DgmLen:66
Len: 46

04/16-16:46:17.351600 10.100.100.50:53 -> 192.168.2.2:1065
UDP TTL:63 TOS:0x0 ID:62525 IpLen:20 DgmLen:172
Len: 152

04/16-16:46:17.352827 192.168.2.2 -> 192.168.2.5
ICMP TTL:64 TOS:0x0 ID:44085 IpLen:20 DgmLen:84
Type:8 Code:0 ID:33064 Seq:0 ECHO

04/16-16:46:17.353082 192.168.2.5 -> 192.168.2.2
ICMP TTL:128 TOS:0x0 ID:21657 IpLen:20 DgmLen:84
Type:0 Code:0 ID:33064 Seq:0 ECHO REPLY
```
Starting Snort

- If you use the -d option to have Snort capture application-layer data, you will capture additional information.

- snort -vd
Starting Snort
Logging Snort Entries

- `/usr/sbin/snort -u snort -g snort -dev -l /var/log/snort -h 192.168.2.0/24`

This command starts Snort under a user and group of Snort.

- It then logs all packets to the `/var/log/snort` directory.

- The `e` option has Snort read data link layer headers, as well.

- The `-h` command tells Snort that the 192.168.2.0/24 network is the home network and to log all packets relative to the 192.168.2.0 system.
Running Snort as a Network-Based IDS

- `snort -u snort -g snort -dev -h 192.168.2.0/24 -d -D -i eth0 -c /etc/snort/snort.conf`

- This command has snort run in **daemon mode** (-D) and specifies the eth0 interface.

- The last part of the command specifies the **snort.conf** file, which if properly configured will enable Snort to log traffic only as it violates the rules it contains.
Question?