CS4238: Computer Security Practice

Lecture 7: Intrusion Detection Systems

Intrusion Detection System (IDS)

IDS: Some Definitions

- Intrusion Detection (ID):
  - The process of monitoring events occurring in a computer system or network, and analyzing them for signs of possible *incidents*
- Incidents:
  - Violations or imminent threats of violation of: computer security policies, acceptable use policies, or standard security practices [Scarfone & Mell, NIST, 2007]
- IDS:
  - A device or software that automates the intrusion detection process

IDS: More Definitions

- Intrusion Prevention System (IPS):
  - Has all the capabilities of an IDS, and can also attempt to *stop* possible incidents: “active” IDS
- Role of an IDS/IPS:
  - As a second line of defense
  - Can be thought as a “burglar alarm”
  - Complements firewall, anti-virus, etc.
- We will just use the term “IDS” to refer to both IDS and IPS

IDS Classification

- IDSs can be categorized based on their:
  - Audit (event information) source location
  - Detection method
- Based on their audit source location:
  - Host-based IDSs (HIDSs):
    deal with audit data generated on *a (single) host*
  - Network-based IDSs (NIDSs): monitor *network traffic*

IDS Classification

- Based on their detection method:
  - *Misuse (signature-based) detection IDSs*: model known attacks using attack patterns (signatures), and detect them using pattern matching
    - + High degree of detection accuracy
    - - Inability to identify new attacks
  - *Anomaly (behavioral-based) detection IDSs*: define “normal” behavior on a system, and flag any deviations from normal as potential attacks
    - + Able to detect novel attacks
    - - Hard to accurately define normal behavior, hard to keep a low positive rate

Snort NIDS

What is Snort?

- A very popular, free and open source NIDS and NIPS
- Snort development:
  - First created by Martin Roesch in 1998
  - Now developed by Sourcefire, which was founded by Roesch, and was later acquired by Cisco in 2013
- Claimed as "the most widely deployed intrusion prevention system in the world, with over 5 million downloads and over 600,000 registered users" (https://www.snort.org/, Oct 2018)
- Entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time" in 2009

Snort Capabilities

- Snort: "It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging (https://www.snort.org/)
- Four modes of operations:
  - Packet sniffer mode
  - Packet logger mode
  - NIDS mode
  - NIPS (Snort inline) mode
- Reference:
  - Snort Users Manual (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/snort_manual.html)

Packet Sniffer Mode

- Packet sniffer mode: reads the packets off of the network and displays them in a continuous stream on the console (screen)
- To print out the TCP/IP packet headers:

```
./snort -v
```

- To also print out the application data:

```
./snort -dv
```

- To additionally show the data link layer headers:

```
./snort -dev
```

Packet Logger Mode

- Packet logger mode: logs the packets to disk
- To log packets into the directory `.log` relative to the home network (e.g. 192.168.1.0/24):

```
./snort -dev -l ./log -h 192.168.1.0/24
```

- To log packets into a more compact binary (tcpdump) format for later analysis:

```
./snort -l ./log -b
```

Network Intrusion Detection System Mode

- NIDS mode: performs detection & analysis on network traffic
- Run using the configuration file `snort.conf`:

```
./snort -dev -l ./log -h 192.168.1.0/24
   -c snort.conf
```

- Default output directory: `/var/log/snort`
- Sample Snort alert message:

```
[**] [116:56:1] (snort_decoder): T/TCP Detected [**]
```

- Three shown numbers: *Generator ID* (e.g. decode/116 component), *Snort/Signature ID* (e.g. 56 as a T/TCP event), *Revision ID* (e.g. 1)

Snort Rules & Rule Components

- Sample Snort rules:

```
alert tcp any any -> any any (flags:0; msg:"Null Scan";)

alert tcp any any -> 192.169.1.0/24 111 (content:"|00 01
86 a5|"; msg:"mountd access";)
```

- Rule action:
  - Options: `alert`, `log`, `pass`, `activate`, `dynamic`
  - Other options when running as NIPS: `drop`, `reject`, `sdrop`
- Protocol: `tcp`, `udp`, `icmp`, `ip`
- Source IP address
- Source port no

Snort Rules & Rule Components

- Sample Snort rules:

```
alert tcp any any -> any any (flags:0; msg:"Null Scan";)

alert tcp any any -> 192.169.1.0/24 111 (content:"|00 01
86 a5|"; msg:"mountd access";)
```

- Direction operator: ->, <> (there is no <-)
- Destination IP address
- Destination port no
- Rule option classes: non-payload (e.g. `flags`), payload (e.g. `content`), general (e.g. `msg`), and post-detection (e.g. `replace`) classes

Snort Ruleset Distribution

- Two sets of rules distributed on the Snort.org web site:
  - *Community* Ruleset
  - *Snort Subscriber* Ruleset
- Community Ruleset: freely available to all users (including Unregistered users) under the GPLv2
- Snort Subscriber Ruleset:
  - Subscribers: will receive rulesets *in real-time* as they are released to Cisco customers
  - Registered users: will receive rulesets *30 days* after Subscribers

Network Intrusion Prevention System (Snort inline) Mode

- NIPS mode:
  - Controls packet traffic flows
  - Integrates with iptables by receiving packets from iptables rather than libpcap
- Use the command line argument `-Q` and snort config option `policy_mode`:

```
snort -Q
config policy_mode:inline
```

Network Intrusion Prevention System (Snort inline) Mode

- NIPS (Snort inline) mode allows 3 additional rule actions to trigger:
  - `drop`: block and log the packet
  - `reject`: block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP
  - `sdrop`: block the packet but *do not log* it → silent drop

Using and Extending Snort

- Various programs can be installed to work with Snort to make it easier to use
  - GUI for snort (http://blog.snort.org/2011/01/guis-for-snort.html): BASE, OSSIM, SGUIL, Snorby
  - Other popular programs: Barnyard2, PulledPork
- Alternatively, just use *Security Onion* (*SO*) distro:
  - An Ubuntu-based Linux distro for intrusion detection, network security monitoring, and log management
  - Contains: Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner
  - Has a setup wizard that "allows you to build an army of distributed sensors for your enterprise in minutes!" (https://securityonion.net/)
- Reference for SO: Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response"