Intrusion Detection System with Snort

By Alberto Morales
Outline

▪ What is an IDS?
▪ What is Snort?
▪ Famous incidences
▪ Other tools
What is an Intrusion?

- To compromise a **computer** system by breaking the security of such a system or causing it to enter into an insecure state.
- Access without permission.
What is an IDS & IPS?

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

- IDS takes a **passive** approach

An intrusion prevention system (IPS) is the same as IDS but also tries to block malicious activity or policy violations.

- IPS take an **active** approach
Detection Method

- **Anomaly-based detection**: A two-step approach that involves training a system to establish a definition of “normal” behavior and then alerts when it detects anomalous data.

- **Misuse (or Signature)-based detection**: Activity is compared with signature database.
Data Source

- **Network-based**: are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
  - Advantage: Monitors multiple devices on a network.

- **Host-based**: run on individual hosts or devices on the network.
  - Advantage: Can analyze decrypted traffic. Capable of verifying if an attack was successful.
What is Snort?

Snort is an open source network intrusion prevention system (IPS) by Cisco. It is capable of performing real-time traffic analysis and packet logging on IP network.
Snort Rule

Rule Example:

```
log tcp 192.168.1.3 80 -> 192.168.1.2 8080 (msg: "TCP packet detected"); sid:10000001; rev:1;
```
Famous DDoS Attacks

- **Two teenagers have been charged with cyber crimes related to the 2014 holiday attacks that brought down the PlayStation Network and Xbox Live:** Those distributed denial-of-service (DDoS) attacks knocked millions of customers offline, rendering the gaming networks useless and costing Sony and Microsoft both money and goodwill with fans. [1]

- **Scientologist Church Gets Hit Hard By Anonymous:** well known and reputable hacktivist group that calls themselves Anonymous attacked the Church of Scientology in a major DDoS attack. This attack took place on January 8, 2008 and was called Project Chanology. [2]

- **The world’s largest DDoS attack took GitHub offline for fewer than 10 minutes:** 1.35 terabits per second of traffic hit the developer platform GitHub all at once. Within 10 minutes it had automatically called for help from its DDoS mitigation service, Akamai Prolexic. [3]
Real Time Threat Map

https://cybermap.kaspersky.com/
Other tools

- **Metasploit**
  - The Metasploit framework is a tool for developing and executing exploit code against a remote-target machine.

- **Monitoring Traffic**
  - Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, and communications protocol development.
References