

Will Bearss

Part 1.

Security Control Types

1. Physical
2. Administrative
3. Technical

Intrusion Detection and Attack indicators

- IDS is passive, and IPS is reactive. IPS can do everything an IDS can but can also respond to attacks.
- IOA's is an attack happening in real-time, indicating that an attack is in progress but a full breach of data has not been determined. IOC indicates previous malicious activity. It indicates that an attack has previously occurred.

The Cyber Killchain

Reconnaissance - Information gathering against a target.

Ex: An attacker breaches a network and installs a remote access trojan, providing the attacker remote control over the computer.

Weaponization - Establishing attack vectors and technical profiles of targets.

Ex: An attacker successfully enumerates company employee profiles and crafts convincing phishing emails that contain malware.

Delivery - Delivering weaponized payload via email, website, USB, etc.

Ex: An employee finds a USB thumb drive in the office parking lot and plugs it into their company's workstation to see what's on it.

Exploitation - Actively compromising adversary's applications and servers while adverting security controls

Ex: An attacker telnets into a Windows server using Remote Desktop Protocol (RDP) with a default password.

Installation

Ex: An attacker breaches a network and installs a remote access trojan, providing the attacker remote control over the computer.

Command And Control (C2)

Ex: An attacker sends commands to infected hosts (zombies), which generate pings to a remote victim's IP address.

Action on Objectives

Ex: An attacker breaches a network, logs into the company's server, copies files to a folder, compress it, encrypts it, and exfiltrates the files to their local hard drive.

Snort Rule Analysis

Snort Rule #1

1. A. Alert = Action snort will take when triggered

B. Tcp = applies to all tcp packets

C. \$EXTERNAL_NET any = from any external Network Ip Address

D. -> All traffic inbound from outside the network to inside the network

E. \$HOME_NET = TO home network

F. 5800:5820 = to destination port 5800 from source port 5820

**(msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12;
threshold: type both, track by_src, count 5, seconds 60;
reference:url,doc.emergingthreats.net/2002910;
classtype:attempted-recon; sid:2002910; rev:5;
metadata:created_at 2010_07_30, updated_at 2010_07_30;)
=The message printed with the alert when the rule is matched**

2. What stage of the Cyber Kill Chain does this alert violate?

1. Scan - Reconnaissance.

3. What kind of attack is indicated?

1. "Potential VNC Scan 5800-5820"

2. Attacker scanning network on port range 5800-5820 (VNC virtual network computing ports) to try and remote control

into the host network/gain remote access.

Snort Rule #2

_____Alert = Action snort will take when triggered

Tcp = applies to all tcp packets

\$EXTERNAL_NET \$HTTP_PORTS= from Http Port of External Network

_____ -> All traffic inbound from outside the network to inside the network

\$HOME_NET = to Home Network

Any = to any port from any source

```
(msg:"ET POLICY PE EXE or DLL Windows file download HTTP";  
flow:established,to_client; flowbits:isnotset,ET.http.binary;  
flowbits:isnotset,ET.INFO.WindowsUpdate; file_data;  
content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|  
00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary;  
metadata: former_category POLICY;  
reference:url,doc.emergingthreats.net/bin/view/Main/2018959;  
classtype:policy-violation; sid:2018959; rev:4; metadata:created_at  
2014_08_19, updated_at 2017_02_01;)
```

2. What layer of the Defense in Depth model does this alert violate?

1. Classtype: policy-violation

3. What kind of attack is indicated?

1. Msg: "ET POLICY PE EXE or DLL Windows file download HTTP"

2. Preventing a DLL windows file download by blocking all HTTP ports from entering the home network.

Snort Rule #3

alert tcp any 4444 -> \$HOME_NET any \ (msg:"Possible exploit, common attacker connect-back port"; sid: 1000001; rev:1;)

Lab 1: Drop Zone

```
sysadmin@firewalld-host: ~  
File Edit View Search Terminal Help  
Mail (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: ETH3  
  sources: 201.45.105.12  
  services: smtp pop3  
  ports: 110/tcp 25/tcp  
  protocols:  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
  
Sales (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: ETH2  
  sources: 201.45.15.48  
  services: https  
  ports: 443/tcp  
  protocols:  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
  
Web (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: ETH1  
  sources: 201.45.34.126  
  services: http  
  ports: 80/tcp  
  protocols:  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
  
drop  
  target: DROP  
  icmp-block-inversion: no  
  interfaces:  
  sources:  
  services:  
  ports:  
  protocols:  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
    rule family="ipv4" source address="10.208.56.23" reject  
    rule family="ipv4" source address="135.95.103.76" reject  
    rule family="ipv4" source address="76.34.169.118" reject
```

Part 2.

IDS vs. IPS Systems

1. Mirroring and Network Tap
2. Physically connected in line with flow traffic.
3. Signature-based IDS
4. Anomaly based IDS

Defense in Depth

1. Layer 7 - Policies, Procedures, and Awareness
 2. Layer 2 - Data
 3. Layer 3/4/5 - Host, Network, or Perimeter.
 4. Layer 3 - Host
 5. Layer 4 - Network
 6. Layer 1 - Data
 7. Layer 4 - Perimeter
- One method of protecting data at rest is Hard-drive encryption.
 - One method to protect data in transit is VPN.
 - GPS provides law enforcement with the ability to track a stolen laptop.

- Firmware Passwords prevent attackers from booting a stolen laptop using an external hard drive

GREEN EGGS & SPAM

- Description of Adversary: Phishing attack.
- The motivation of Attack: Ransomware/info stealer resulting in exploiting money from targeted individuals/organizations.
- Administration policy and procedures: education on phishing/ company-wide email explaining the dangers of opening email attachments. Administer anti-virus software and attempt to uninstall trojan from the system.

Firewall Architectures and Methodologies

1. Circuit-level Firewalls
2. Stateful Packet-Filtering Firewalls
3. Application firewall or proxy firewall
4. Stateless Packet-filtering Firewalls
5. Mac Layer Firewall