Isabella Candido

Security Control Types

With the understanding that Defense in Depth can be broken down into three different security control types, answer the following questions:

1. Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?
    a. Physical

2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?
    a. Administrative

3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?
    a. Technical

Intrusion Detection and Attack indicators

What's the difference between an IDS and an IPS?

IDS: Detects and alerts of an attack - passive & does not respond to attacks.
- Connects via network tap or mirrored SPAN.

IPS: Detects, alerts, and responds to attacks.
- Connects inline with flow of data.

What's the difference between an Indicator of Attack and an Indicator of Compromise?

IOA: attacks happening in real time
- Indicate that an attack is in progress but full breach has not been determined.

IOC: previous malicious activities
- Indicate that an attack has occurred = breach

The Cyber Kill Chain

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

Reconnaissance - gather email accounts, names, finding weaknesses.

Weaponization - creating a phishing email.

Delivery - phishing email sent to employees.

Exploitation - exploit a vulnerability, zero-day. An attacker telnets into a Windows server using Remote Desktop Protocol (RDP) with a default password.

Installation - installation of remote access trojan on target hosts.

Isabella Candido

Command and Control - remote access to control employee computers allowing continued access.
Action on objectives - attacker exchanges ransom for decryption of files.

Snort Rule Analysis

Use the Snort rule to answer the following questions:

Snort Rule #1

alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (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;)

1. Break down the Sort Rule header and explain what is happening.
    a. alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820
    b. Alert - action snort will take.
    c. Tcp - all tcp packets.
    d. $EXTERNAL_NET any - applies to packets coming from any source external net.
    e. -> - direction of packet. Outside network to inside net.
    f. $HOME_NET - to internal/ home network
    g. 5800:5820 - destination port range
2. What stage of the Cyber Kill Chain does this alert violate?
    a. Scan - reconnaissance.
3. What kind of attack is indicated?
    a. "Potential VNC Scan 5800-5820"
    b. 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 tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (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;)

1. Break down the Sort Rule header and explain what is happening.
    a. alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any

Isabella Candido

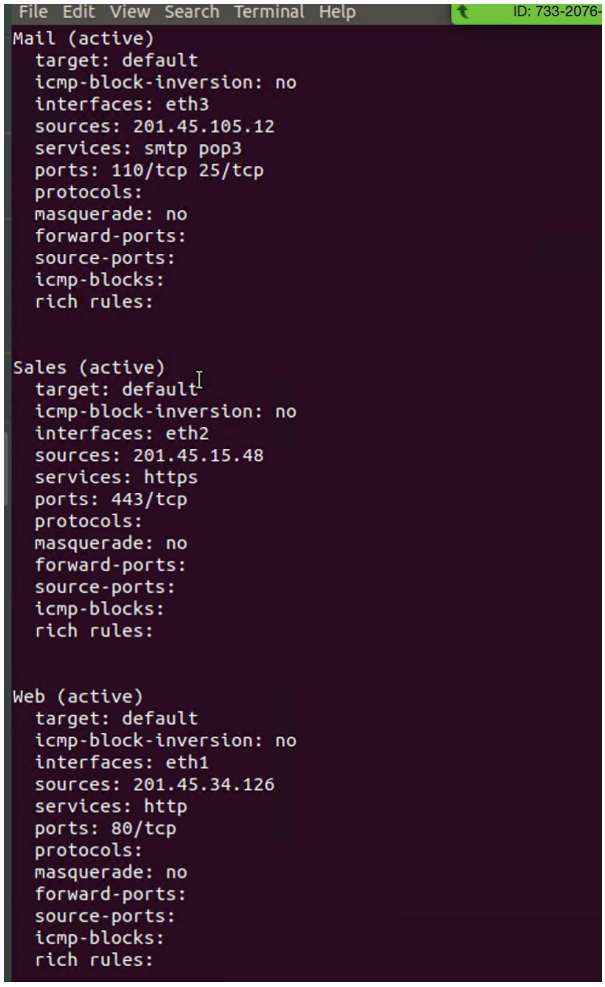
   b. Alert - action snort will take.
   c. Tcp - all tcp packets.
   d. $EXTERNAL_NET $HTTP_PORTS - http port (80) from external network.
   e. -> - direction of packet. Outside network to inside net.
   f. $HOME_NET any - to any internal/ home network port.
2. What layer of the Defense in Depth model does this alert violate?
   a. Classtype: policy-violation
3. What kind of attack is indicated?
   a. msg:"ET POLICY PE EXE or DLL Windows file download HTTP"
   b. Preventing a DLL windows file download by blocking all HTTP ports from entering home network.

Snort Rule #3

Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the Rule Option.

alert tcp $EXTERNAL_NET 4444 -> $HOME_NET any (msg:"ET POLICY TROJAN potential W32.Blaster.Worm"

Lab: "Drop Zone"



```
File  Edit  View  Search  Terminal  Help                ID: 733-2076-
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:
```

Isabella Candido

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports: 80/tcp 443/tcp 110/tcp 25/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --list-all
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
sysadmin@firewalld-host:~$
```

Isabella Candido

Part 2

Now, we will work on another lab. Before you start, complete the following review questions.

IDS vs. IPS Systems

1. Name and define two ways an IDS connects to a network.
    a. Network tap: test access port
        i. Hardware tool, transits inbound and outbound data streams at the same time.
        ii. Creates a copy of the bidirectional traffic streams.
    b. Mirrored SPAN port: Switched Port Analyzer-
        i. Port mirroring - sends a copy or mirror image of all packets to another port where packets are analyzed.
        ii. A function of switch

2. Describe how an IPS connects to a network.
    a. Physically connected inline with flow of traffic.

3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?
    a. Signature-based IDS

4. Which type of IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network?
    a. Anomoly-based.

Defense in Depth

- For each of the following scenarios, provide the layer of Defense in Depth that applies:

    1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.
        - Physical layer 6 - criminal physically entering into workplace.
        - Policies layer 7 - if the company has a no tailgating policy.

    2. A zero-day goes undetected by antivirus software.
        - Application layer 2

3. A criminal successfully gains access to HR's database.
    - Data layer 1

4. A criminal hacker exploits a vulnerability within an operating system.
    - Application layer 2 or Host layer 3.

5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.
    - Network layer 4

6. Data is classified at the wrong classification level.
    - Policies and procedures.

7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.
    - Perimeter layer 5

- Name one method of protecting data-at-rest from being readable on hard drive.
    1. Hard drive encryption

- Name one method to protect data-in-transit.
    1. VPN

- What technology could provide law enforcement with the ability to track and recover a stolen laptop.
    1. GPS

- How could you prevent an attacker from booting a stolen laptop using an external hard drive?
    1. Firmware passwords.

Lab: "Green Eggs & SPAM"

Threat Intelligence Card

- **Indicator of Attack**

    - **Source IP/Port** 188.124.9.56/80
    - **Destination Address/Port** 192.168.3.35/1035
    - **Event Message** ET TROJAN JS/Nemucod.M.gen downloading EXE payload
    - **Infection Type** (ex. Trojan, Virus, Worm, etc..)

    - **Malware Type** (ex. ransomware, Zombie "DDoS", RAT, etc..)
- Description of adversary:
    - Phishing email attack - Trojan-Downloader.JS.Nemucod downloads and runs additional malicious files onto the system and gathers information.
- Adversarial motivation (Purpose of attack):
    - Ransomware - money. Stealing info.
- Recommended Mitigation Strategies:
    - Employee policies and education on suspicious emails.
    - download antivirus software to remove the trojan.

For the final part of the homework, complete a set of review questions about firewall architecture and methodologies:

Firewall Architectures and Methodologies

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.
    a. Packet filtering firewalls - Stateless.

2. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.
    a. Packet filtering firewalls - Stateful.

3. Which type of firewall intercepts all traffic prior to being forwarded to its final destination. In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?
    a. Circuit level firewalls.

4. Which type of firewall examines data within a packet as it progresses through a network interface by examining source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents?
    a. Application / proxy firewall.

5. Which type of firewall filters based solely on source and destination MAC address?
    a. MAC layer firewall.