Network Security Homework

Part 1

Before we get started on the lab exercise, complete the following review questions:

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?

   Physical

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

   Administrative

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

   Technical

Intrusion Detection and Attack indicators

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

IDS is passive and IPS is reactive. IDS detects and alerts of possible compromises and attacks, while IPS detects, alerts, and ALSO responds to attacks.

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

IOA is an attack in real-time, indicating that an attack is in progress but a full-breach of data is undetermined, while an IOC indicates previous malicious activity, such as a breach or previous attack.

The Cyber Kill Chain

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

1. **Reconnaissance**

   Ex: An attacker compiles employee information from LinkedIn and gets the names and phone numbers of company personnel from publicly available resources.

2. **Weaponization**

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

3. **Delivery**

   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.

4. **Exploitation**

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

5. **Installation**

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

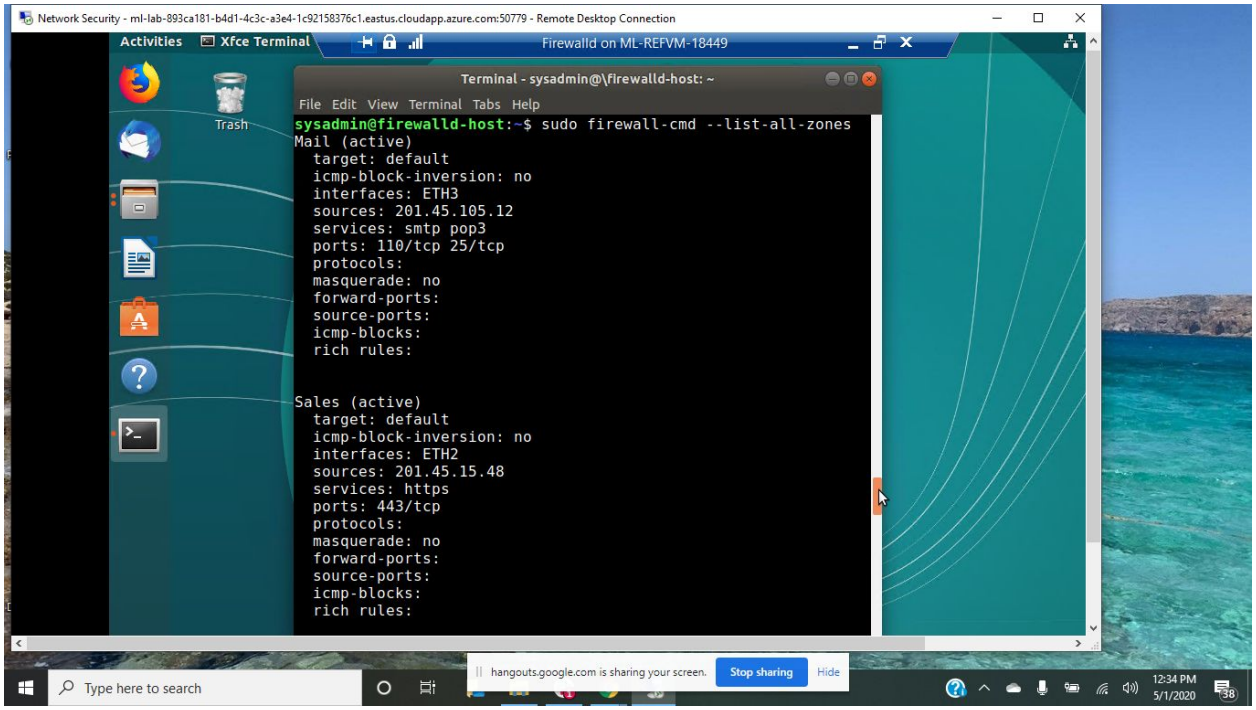
6. **Command and Control (C2)**

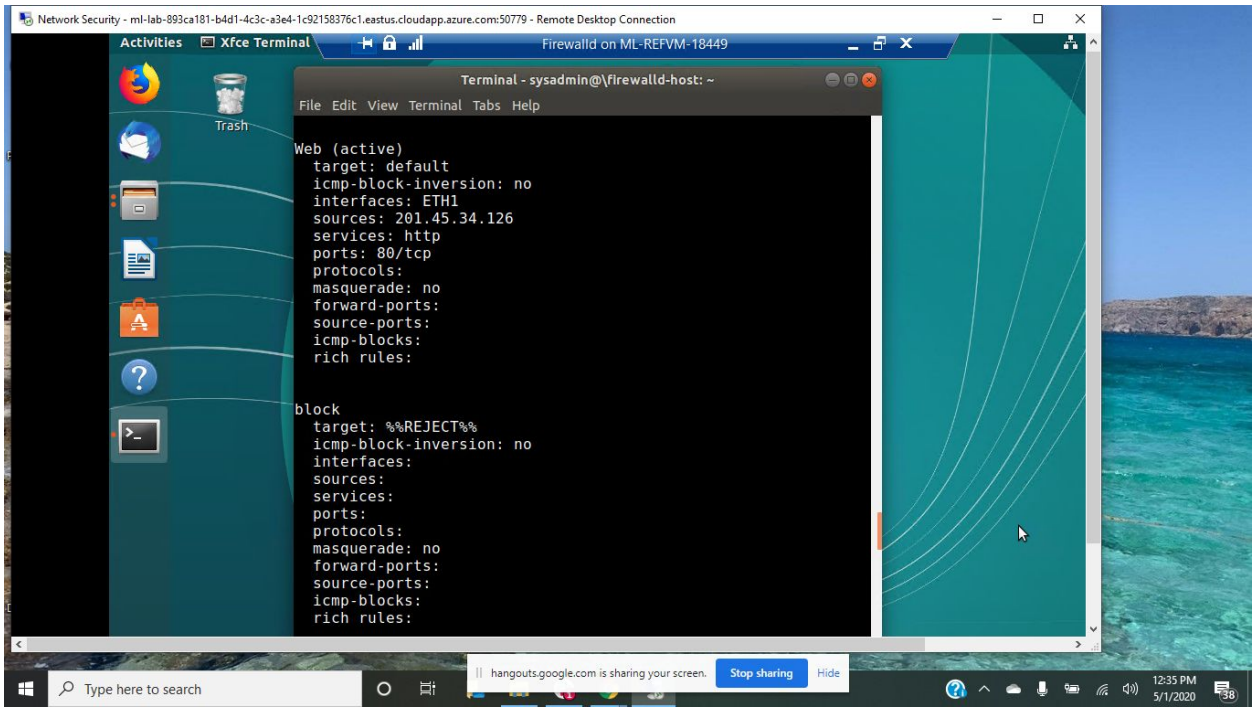
   Ex: An attacker sends commands to infected hosts (zombies), which generate pings to a remote victim's IP address.

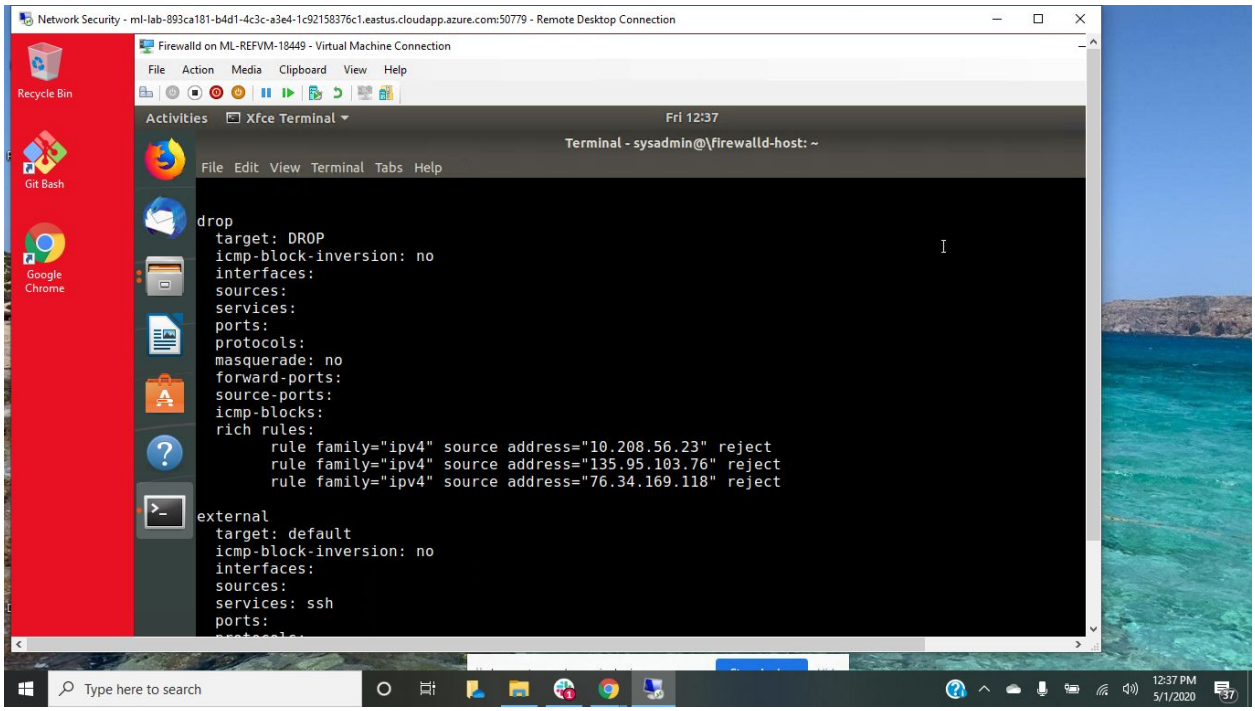
7. **Action on Objectives**

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

Lab: "Drop Zone"






Network Security - ml-lab-893ca181-b4d1-4c3c-a3e4-1c92158376c1.eastus.cloudapp.azure.com:50779 - Remote Desktop Connection
Firewalld on ML-REFVM-18449 - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Xfce Terminal
Fri 12:37
Terminal - sysadmin@\firewalld-host: ~
File Edit View Terminal Tabs Help
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
external
target: default
icmp-block-inversion: no
interfaces:
sources:
services: ssh
ports:
Recycle Bin
Git Bash
Google Chrome
Type here to search
12:37 PM
5/1/2020

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.

   alert = action Snort will take when triggered

   tcp = applies to all tcp packets

   $EXTERNAL_NET any = from any External Network IP address

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

   $HOME_NET = to Home Network

   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?

   Reconnaissance

3. What kind of attack is indicated?

   Potential VNC Scan

   Attacker trying to gain remote access on ports 5800-5820

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.

   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 destination port from any source port

(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;)

= The message printed with the alert when the rule is matched.

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

   Layer 7- Policies & Procedures

3. What kind of attack is indicated?

   (Not necessarily an attack) Preventing a DLL windows file download by blocking all http connections

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

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.

   Mirroring

   Network Tap

2. Describe how an IPS connects to a network.

   Physically connected inline with flow traffic

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

   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?

   Anomaly Based IDS

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.

        Layer 7- Policies, Procedures, and Awareness

        (If organization has a no-tailgating policy)

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

        Layer 2- Application

    3. A criminal successfully gains access to HR's database.

        Layer 1- Data

    4. A criminal hacker exploits a vulnerability within an operating system.

        Layer 3- Host

    5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.

        Layer 4- Network

    6. Data is classified at the wrong classification level.

        Layer 7- Policies, Procedures, and Awareness

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

        Layer 5- Perimeter

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

Hard drive encryption

Name one method to protect data-in-transit.

VPN

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

GPS

How could you prevent an attacker from booting a stolen laptop using an external hard drive?

Firmware Passwords

Lab: "Green Eggs & SPAM"

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 Attack

Adversarial motivation (Purpose of attack):

Ransomware/Info stealer; resulting in extorting money from targeted individuals/organizations

Recommended Mitigation Strategies:

Administration, Policies & Procedures: Education on phishing/company-wide email explaining dangers of opening email attachments

Recommendations that individuals/employees without sysadmin access not be able to download unauthorized content or visit unauthorized websites.

Administer anti-virus software and attempt to uninstall trojan from the system

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.

   Circuit-level Firewalls

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.

   Stateful Packet-Filtering Firewalls

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?

   Application/Proxy 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?

   Stateless Packet-Filtering Firewalls

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

   MAC Layer Firewall