## Unit 11 Submission File: Network Security Homework

### Part 1: Review Questions

#### Security Control Types

The concept of defense in depth can be broken down into three different security control types. Identify the security control type of each set of defense tactics.

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

* Answer: This is **physical** control. This prevents physical access to hardware

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

* Answer: These are **administrative** controls. this is more focused on people and training than actual software

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

* Answer: These are **technical** controls. This is focused on software that protects the systems and resources

#### Intrusion Detection and Attack indicators

1. What’s the difference between an IDS and an IPS?

* Answer:
  + An IDS main function is to monitor traffic via network mirroring and send alerts but requires administrative action to stop any threats. IDS are not normally in line with the direct flow of data  
    An IPS main function is also to monitor network traffic but can also take action against malicious threats without direct administrative action. IPS are normaly inline with the flow of data

1. What’s the difference between an Indicator of Attack and an Indicator of Compromise?

* Answer:
  + An indicator of attack shows possible malicious activity happening in real time, such as network tampering, but not a compromise of full systems or data. An indicator of compromise means that sensitive data or systems have been compromised. When this happens it is best to use the attack to develop new defensive tactics to prevent future.

#### The Cyber Kill Chain

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

1. Stage 1: **Reconnaissance** - This involves collecting data on target systems to gain acces such as email addresses, usernames, passwords, Ip addresses, MAC addresses, and software. This could be done through social media sites or company websites
2. Stage 2: **Weaponization** - The reconnaissance information is used to develop an attack. This could be making, or finding a piece of malware designed specifically for the target system, or using known exploits to gain access
3. Stage 3: **Delivery** - This is when the attacker delivers their malware to the system, this could be done by sending it through an email to an employee, or insecure websites
4. Stage 4: **Exploitation** - This is the piece of software that executes the attack. This could be something that changes registry keys to maintain persistance on the infected system
5. Stage 5: **Installation** - This is how the software got installed on the system, normally by clicking on an email attachment with the embeded exploitation software
6. Stage 6: **Command and Control (C2)** - This is a server used to maintain communication between the compromised systems on target systems. This could easly be done through IRC
7. Stage 7: **Actions on Objectives** - this is when the attacker obtains the information they wanted such as user account information

#### 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.

* Answer:
  + alert (snort action when triggered)
  + tcp (applies rule to tcp packets)
  + $EXTERNAL\_NET (applies to packets coming from external IPs)
  + any (applies to packets from any port)
  + -> (going from $EXTERNAL\_NET to $HOME\_NET)
  + $HOME\_NET (local IPs)
  + 5800:5820 (on these ports)

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

* Answer: According to the rest of the report this is an attempt at **Stage 1: Reconnaissance**

1. What kind of attack is indicated?

* Answer: This could be a VNC scan to find a way to RDP into a system on the network

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.

* Answer:
  + alert (snort action when triggered)
  + tcp (applies rule to tcp packets)
  + $EXTERNAL\_NET (applies to packets coming from external IPs)
  + $HTTP\_PORTS (applies to packets from standard HTTP ports, likely port 80)
  + -> (going from $EXTERNAL\_NET to $HOME\_NET)
  + $HOME\_NET (going to local IPs)
  + any (on any port)

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

* Answer: This is an attack at **Stage 3: Delivery** because an EXE or DLL has be downloaded over HTTP

1. What kind of attack is indicated?

* Answer: This is likely a LotL attack because a windows update binary was downoaded

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.
* Answer:
* alert tcp $EXTERNAL\_IP 4444 -> $HOME\_IP any (msg: "External connection made to port 4444)

### Part 2: “Drop Zone” Lab

#### Log into the Azure firewalld machine

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

#### Uninstall ufw

Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of ufw.
* sudo apt remove ufw

#### Enable and start firewalld

By default, these service should be running. If not, then run the following commands:

* Run the commands that enable and start firewalld upon boots and reboots.
* sudo systemctl enable firewalld  
  sudo systemctl start firewalld
* Note: This will ensure that firewalld remains active after each reboot.

#### Confirm that the service is running.

* Run the command that checks whether or not the firewalld service is up and running.
* sudo systemctl status firewalld

#### List all firewall rules currently configured.

Next, lists all currently configured firewall rules. This will give you a good idea of what’s currently configured and save you time in the long run by not doing double work.

* Run the command that lists all currently configured firewall rules:
* sudo firewall-cmd --list-all
* Take note of what Zones and settings are configured. You many need to remove unneeded services and settings.

#### List all supported service types that can be enabled.

* Run the command that lists all currently supported services to see if the service you need is available
* sudo firewall-cmd --get-services
* We can see that the Home and Drop Zones are created by default.

#### Zone Views

* Run the command that lists all currently configured zones.
* # Note: I made a temporary alias sfcmd='sudo firewall-cmd' in my VM  
  # I'll try to remember to expand the command for the answers  
    
  sudo firewall-cmd --list-all-zones
* We can see that the Public and Drop Zones are created by default. Therefore, we will need to create Zones for Web, Sales, and Mail.

#### Create Zones for Web, Sales and Mail.

* Run the commands that creates Web, Sales and Mail zones.
* sudo firewall-cmd --permanent \  
  --new-zone=web \  
  --new-zone=sales \  
  --new-zone=mail  
    
  sudo firewall-cmd --reload  
  sudo firewall-cmd --list-all-zones

#### Set the zones to their designated interfaces:

* Run the commands that sets your eth interfaces to your zones.
* sudo firewall-cmd --permanent --zone=public --change-interface=eth0  
  sudo firewall-cmd --permanent --zone=web --change-interface=eth1  
  sudo firewall-cmd --permanent --zone=web --add-source=201.45.34.126  
  sudo firewall-cmd --permanent --zone=sales --change-interface=eth2  
  sudo firewall-cmd --permanent --zone=sales --add-source=201.45.15.48  
  sudo firewall-cmd --permanent --zone=mail --change-interface=eth3  
  sudo firewall-cmd --permanent --zone=mail --add-source=201.45.105.12  
  sudo firewall-cmd --reload  
  sudo firewall-cmd --list-all-zones

#### Add services to the active zones:

* Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.
* Public:
* sudo firewall-cmd --permanent --zone=public \  
  --add-service=http \  
  --add-service=https \  
  --add-service=pop3 \  
  --add-service=smtp \  
  --remove-service=ssh \  
  --remove-service=dhcpv6-client
* Web:
* sudo firewall-cmd --permanent --zone=mail --add-service=http
* Sales
* sudo firewall-cmd --permanent --zone=sales --add-service=https
* Mail
* sudo firewall-cmd --permanent --zone=sales \  
  --add-service=smtp \  
  --add-service=pop3  
    
  sudo firewall-cmd --reload  
  sudo firewall-cmd --list-all-zones
* What is the status of http, https, smtp and pop3?
  + the public zone has access to all listed services. Web can only communicate through http, sales can only communicate through https, and mail can communicate through smtp and pop3

#### Add your adversaries to the Drop Zone.

* Run the command that will add all current and any future blacklisted IPs to the Drop Zone.
* sudo firewall-cmd --permanent --zone=drop \  
  --add-add-source=10.208.56.23 drop\  
  --add-add-source=135.95.103.76 drop \  
  --add-add-source=76.34.169.118 drop  
    
  sudo firewall-cmd --reload

#### Make rules permanent then reload them:

It’s good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This ensure that the network remains secured after unplanned outages such as power failures.

* Run the command that reloads the firewalld configurations and writes it to memory
* sudo firewall-cmd --runtime-to-permanent

#### View active Zones

Now, we’ll want to provide truncated listings of all currently **active** zones. This a good time to verify your zone settings.

* Run the command that displays all zone services.
* sudo firewall-cmd --get-active-zones

#### Block an IP address

* Use a rich-rule that blocks the IP address 138.138.0.3.
* sudo firewall-cmd --permanent --zone=public \  
  --add-rich-rule='rule family="ipv4" source address="138.138.0.3" block'

#### Block Ping/ICMP Requests

Harden your network against ping scans by blocking icmp ehco replies.

* Run the command that blocks pings and icmp requests in your public zone.
* sudo firewall-cmd --permanent --zone=public \  
  --add-icmp-block=echo-reply\  
  --add-icmp-block=echo-request  
    
  sudo firewall-cmd --reload  
  sudo firewall-cmd --runtime-to-permanent

#### Rule Check

Now that you’ve set up your brand new firewalld installation, it’s time to verify that all of the settings have taken effect.

* Run the command that lists all of the rule settings. Do one command at a time for each zone.
* sudo firewall-cmd --zone=drop --list-all  
  sudo firewall-cmd --zone=public --list-all  
  sudo firewall-cmd --zone=web --list-all  
  sudo firewall-cmd --zone=sales --list-all  
  sudo firewall-cmd --zone=mail --list-all
* Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.

### Part 3: IDS, IPS, DiD and Firewalls

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.

* Answer 1:
  + **Network tap** (Test Access Port) is not in line with main data flow. Instead, it is a device monitors both inbound and outbound data on separate channels in real time
* Answer 2:
  + A **Switch Port Analyzer** (SPAN / port mirroring) sends all network data to a different physical port where packets are captured to be analyzed. Like a network tap it is not in the direct flow of network data

1. Describe how an IPS connects to a network.

* Answer:
  + An IPS is a machine that is directly in line with the flow of data, generally between the firewall and the switch. This requires a much more robust machine to filter all the traffic since it must be able to handle the whole network’s bandwith to maintain acceptable availability

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

* Answer: **Signature-based** IDS are good for detecting known attacks, but require more regular updates as new signatures are released

1. 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?

* Answer: **Anomally-based** IDS are best to handle zero-day attacks because they focus on unusual network traffic instead of relying predefined signatures

#### Defense in Depth

1. 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.
   * Answer: administrative Policy
   1. A zero-day goes undetected by antivirus software.
   * Answer: technical software
   1. A criminal successfully gains access to HR’s database.
   * Answer: technical network
   1. A criminal hacker exploits a vulnerability within an operating system.
   * Answer: technical software
   1. A hacktivist organization successfully performs a DDoS attack, taking down a government website.
   * Answer: technical netwrok
   1. Data is classified at the wrong classification level.
   * Answer: administrative procedures
   1. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.
   * Answer: administrative network
2. Name one method of protecting data-at-rest from being readable on hard drive.

* Answer: disk encryption

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

* Answer: data encryption using secure network protocols such as HTTPS

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

* Answer: IP or MAC address tracking could lead law enforcement to a stolen laptop

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

* Answer: Disable booting from USB and password protect access to the BIOS/UEFI

#### 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.

Answer: Circut Level Gateway

1. 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.

Answer: Stateful firewalls

1. 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?

Answer: Application / Proxy firewalls

1. 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?

Answer: Stateless firewalls

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

Answer: MAC Layer Firewalls