Rayshaun McIntosh

Homework Assignment 10

Part 1

Security Control Types

1. Walls, bollards, fences, guard dogs, and cameras are all examples of a Physical security control type.
2. Security awareness programs, BYOD policies, and ethical hiring practices are all examples of an Administrative security control type.
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are all examples of a Technical security control type.

Intrusion Detection and Attack Indicators

1. IDS are passive, meaning it does not respond to attacks, it just logs and document information. IPS can do everything that IDS can do except IPS will respond to malicious traffic by blocking packets when detected.
2. IOA indicates attacks happening in real time while IOC indicates previous malicious activity.

The Cyber Kill Chain (Martin, 2022) (Limited, 2017)

1. Reconnaissance – A threat actor gains as much information about the network before launching more attacks. You have two types of reconnaissance attacks, Passive and Active. Passive is the hacker looking for information not related to the victim's domain to get more information about the target. Active would be a hacker using system information to gain unauthorized access to protected digital or electronic materials.
2. Weaponization – Hackers using tools that gain then access to restricted information. Weapons like Botnet, DDoS, and Malware. All these are examples of cyber weapons created to exploit vulnerabilities.
3. Delivery - This is how attackers send malicious payloads to the victims. Could use emails, text messages, USBs, and many more ways to name a few. Either way delivery is exactly how it sounds.
4. Exploitation – When an attacker identifies a vulnerability in the victim's system, and they exploit that weakness to carry out the intended attack.
5. Installation – This simply means installing any unwanted application unto the victim's system.
6. Command and Control (C2) – When an attacker has remote continued access to a victim's environment.
7. Actions on Objectives – Basically put, the attacker was successful in their attack on the system. Meaning the attacker met their final goal.

Snort Rule Analysis

Snort Rule 1

1. What is this rule doing? TCP alert on incoming packets on ports 5800:5820
2. What stage of the Cyber Kill Chain does the alerted activity violate? Reconnaissance
3. What kind of attack is this ruling monitoring? Potential VNC Scan

Snort Rule 2

1. What is this rule doing? TCP alert on incoming packets on port 80, HTTP
2. What stage of the Cyber Kill Chain does the alerted activity violate? Installation
3. What kind of attack is this ruling monitoring? ET Policy PE EXE or DLL windows file download HTTP

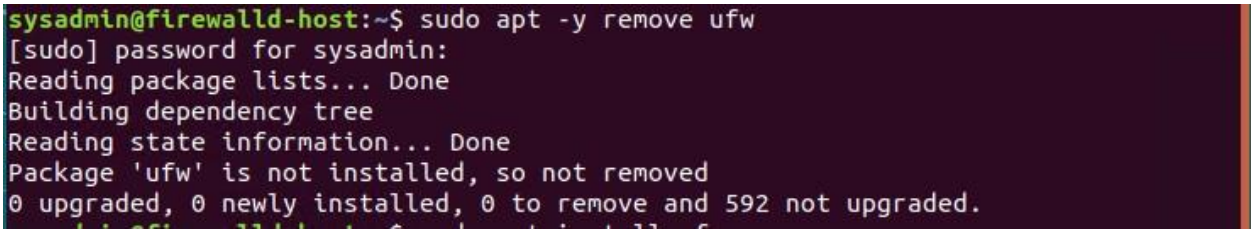
Snort Rule 3

Alert TCP $EXTERNAL_NET 4444 -> $HOME_NET any {msg: “TCP Packet Detected”;}

Part 2

- Uninstall ufw

To uninstall the program, you need to use the syntax [sudo apt -y remove ufw]. The reason we are using the -y flag is to answer yes when prompted to make sure you want to remove the program from the system. The program was successfully removed from the computer as seen below.



- Enable and start firewalld

To enable firewalld, you need to use the following syntax [sudo systemctl enable firewalld]. Once you have enabled the firewalld, you must start the program to make sure it is running on your system. To start the program, you must type [sudo systemctl start firewalld]. Nothing will prompt to tell you that the program has started so we need to check it to make sure.

- Confirm service is running

To check the status of firewalld, you must type [sudo firewall-cmd --state]. You will see a status on the screen as shown below, no matter if it says running or not running, this command will show you the status of the service as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --state
running
```

- List All firewall rules currently configured

To see a list of all firewall rules you need to use the syntax [sudo firewall-cmd –list-all]. You can see all currently configured rules shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
You're performing an operation over default zone ('public'),
but your connections/interfaces are in zone 'home' (see --get-active-zones)
You most likely need to use --zone=home option.

public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- List all supported service types that can be enabled

Typing the command [firewall-cmd --get-services] will show you a list of all services as shown below.

```
sysadmin@firewalld-host:~$ firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
net-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox
-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master g
it high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpa
sswd kprop kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mosh mountd ms-wbt mssql murmur mysql nfs nf
s3 nrpe ntp openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postg
resql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh rsyncd samba samba-client sane s
ip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy syslog syslog-tls telnet tftp tftp
-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server zabb
ix-agent zabbix-server
```

- Zone Views

For you to see all the current configured zones, you need to use this command [sudo firewall-cmd --list-all-zones]. After using this command, you will see a list of all zones currently as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Create Zones for Web, Sales and Mail

To create a zone, we will need to use the following syntax [sudo firewall-cmd --permanent --new-zone=Web]. Once you type that command you will be prompted to use the password for the user that you are login as. After successfully using the password, you will see print that says [success]. Now all we need to do is us the same command again, but this time change the name to create the other two zones. [sudo firewall-cmd --permanent --new-zone=Sales and sudo firewall-cmd --permanent --new-zone=Mail]. You can see the results below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Web
[sudo] password for sysadmin:
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Sales
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=Mail
success
sysadmin@firewalld-host:~$
```

- Set the zones to their interface

For us to set the interfaces for the zones, we need to use a few different commands. The first command is [sudo firewall-cmd--permanent --zone=Web --change-interface=eth1], [sudo firewall-cmd--permanent --zone=Sales --change-interface=eth2] and [sudo firewall-cmd--permanent --zone=Mail --change-interface=eth3]. To change the public zone interface, we need to use this command [sudo firewall-cmd --zone=public --change-interface=eth0]. Once you have added all interfaces correctly to the zones, you will see [success] printed on the terminal as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Web --change-interface=eth1
success
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Sales --change-interface=eth2
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=Mail --change-interface=eth3
success
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'public'.
success
```

```
Web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
Sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
Mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Add services to active zones

Now it's time for us to add the services to the zones we created and modified. We will need to use these commands to add services [sudo firewall-cmd --zone=public --permanent --add-service=http], [sudo firewall-cmd --zone=public --permanent--add-service=https], [sudo firewall-cmd --zone=public --permanent--add-service=pop3] and [sudo firewall-cmd --zone=public --permanent--add-service=smtp]. Now that we have added all the public services, we need to finish it by adding Web, Sales, and Mail zones services. The command is the exact same except a few minor changes to the zone and service that needs to be added. Here is the command [sudo firewall-cmd --zone=Web --permanent--add-service=http], [sudo firewall-cmd --zone=Sales --permanent--add-service=https], [sudo firewall-cmd --zone=Mail --permanent--add-service=pop3] and [sudo firewall-cmd --zone=Mail --permanent--add-service=smtp]. Once services are added correctly, you will see [success] printed on the terminal as seen below.

```
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
Mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources:
  services: smtp pop3
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
Web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources:
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
Sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources:
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Add adversaries to Drop Zone

Now we want to add all blacklisted IP addresses to the drop zone. For us to be able to add the IP addresses to the drop zone, we must use the command [sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23], [sudo firewall-cmd --permanent --zone=drop --add-source=135.95.103.76] and [sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118]. Once you execute the command, you will see [success] printed on the terminal as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=135.95.103.76
success
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118
success
```

```
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Make rule permanent then reload them

Now that we have made changes to the firewalld, we need to reload to make sure all changes are permanent. To reload firewalld, we need to us the syntax [sudo firewall-cmd --reload]. After typing the command, you should see [success] printed to the terminal as you see below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --reload
success
```

- View active Zones

To be able to view all active zones you must type use the command [sudo firewall-cmd --get-active-zones]. Once you use this command, all active zones will be printed to the terminal as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-active-zones
Mail
  interfaces: eth3
Sales
  interfaces: eth2
Web
  interfaces: eth1
drop
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
public
  interfaces: eth0
```

- Block an IP address

For us to block the IP address on the public zone we must use the following command [sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.0.3" reject']. After using the command, you will see success printed to the screen to show you that you command was entered correctly as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4" source addre
ss="138.138.0.3" reject'
[sudo] password for sysadmin:
success
sysadmin@firewalld-host:~$
```

Just to check, you can view the public zone by using [sudo firewall-cmd --permanent --list-all-zones] and you will be able to double check you work as shown below.

```
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv4" source address="138.138.0.3" reject
```

- Block Ping/ICMP Requests

Now we need to block Pings and ICMP request. For us to be able to execute this request we must use the following command [sudo firewall-cmd --zone=public --add-icmp=echo-reply --add-icmp-block=echo-request]. After successfully executing the command, you will see [success] printed to the terminal as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-icmp-block=echo-reply --add-icmp-block=echo-request
success
```

To check our work, we can use the following command [sudo firewall-cmd --zone=public –list-all]. Once you do this, you will be able to see the icmp blocks are in place as shown below.

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks: echo-reply echo-request
  rich rules:
        rule family="ipv4" source address="138.138.0.3" reject
```

- Rule Check

To check the rules all we need to do is use [sudo firewall-cmd --zone=public --list-all], [sudo firewall-cmd --zone=Sales --list-all], [sudo firewall-cmd --zone=Mail --list-all], [sudo firewall-cmd --zone=Web --list-all] and [sudo firewall-cmd --zone=drop --list-all]. Once you use these commands, the information to verify will be printed to the terminal as shown below.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks: echo-reply echo-request
  rich rules:
        rule family="ipv4" source address="138.138.0.3" reject
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Sales --list-all
Sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources: 201.45.15.48
  services: https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Mail --list-all
Mail (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth3
  sources: 201.45.105.12
  services: smtp pop3
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=Web --list-all
Web (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth1
  sources: 201.45.34.126
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=drop --list-all
[sudo] password for sysadmin:
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Part 3

- IDS vs IPS Systems

1. Name and define two ways an IDS connects to a network.

   Network Tap is a hardware device that provides access to a network. Network taps transmits both inbound and outbound data on different channels at the same time, so all data can arrive at the monitor in real time.

   SPAN, which means Switched Port Analyzer, sends a mirror image of all network data to another physical port, where the packets can be captured and analyzed.

2. Describe how an IPS connects to a network.

   Intrusion Prevention System connects inline with data and is typically placed between the firewall and network switch. IPS will automatically act by blocking and logging threats.

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

1.
    1. Physical Control
    2. Technical Control
    3. Technical Control
    4. Technical Control
    5. Technical Control
    6. Technical Control
    7. Technical Control
2. Encryption
3. Authentication by verifying the data source
4. GPS
5. By using Bitlocker

- Firewall Architectures and Methodologies

1. Circuit-Level Firewall
2. Packet Filter Firewall (Stateful)
3. Application (Proxy) Firewall
4. Packet Filter Firewall (Stateless)
5. Mac Layer Firewall

References

Limited, D. T. (2017). *Deloitte Touche Tohmatsu Limited*. Retrieved from Deloitte Touche Tohmatsu Limited: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

Martin, L. (2022). *Lockhead Martin*. Retrieved from Lockhead Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html