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: These fall under Physical Security

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

   Answer: These fall under Administrative/Management Security

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

   Answer: This can be considered Operation Security, more specifically “access control” as well as attack or intrusion indicators

Intrusion Detection and Attack indicators

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

   Answer: Intrusion Detection Systems (IDA) effectively *analyze* and *monitor* network traffic for signs that an attack, a threat, or some entity is compromising the network in some capacity. It is usually paired with a database and system baseline to use as a comparison for any changes should an attack occur/have occured. As the name implies it can only *detect*, and notify of said detection.

An Intrusion Prevention System (IPS) serves as a system that proactively denies network traffic based on a set of parameters, known as security profiles. An IPS will deny incoming packets if it meets those parameters, especially if they are previously known security threats. Essentially, the IPS has to know what it’s looking for.

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

   Answer: An Indicator of Attack (IOA) focuses on detecting the intent of an attacker regardless of the employed method. Indicator of Compromise is typically used after an attack has occured to gather corroborative evidence that a system has indeed been breached.

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 - During this stage the attacker(s) probe for weaknesses in a target's defense. Information is gathered to help plan for an attack.

2. Stage 2: Weaponization - This is where the attack is developed usually in the form of some deliverable payload or exploitation based on gathered info. The preparations are then executed to allow for the subsequent steps in the chain to occur.

3. Stage 3: Delivery - This is the delivery of the payload to the target. Once sent, this will allow the attacker to gain access to the target's systems and compromise the user's machine. Examples of this are infected emails or messages to the target.

4. Stage 4: Exploit - Once received, the payload can grant access to the attacker and the payload can then be executed.

5. Stage 5: Installation - The payload's primary intended purpose begins here as malicious code is installed, granting the attacker further access even down to root.

6. Stage 6: Command and Control - In this step a channel is created for the attacker to remotely control the target's system through another computer.
7. Stage 7:Actions - With everything established and deployed, the attacker can now achieve lateral and vertical movement within the target's systems to obtain or perform the intended action of the attacker.

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 the user of **ANY** inbound TCP traffic from “External_Net” from **ANY port** that arrives at “Home_Net” from Ports 5800 to 5820

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

   Answer: This falls under the Reconnaissance portion of the Cyber Kill Chain as we are being probed for weaknesses.

3. What kind of attack is indicated?

   Answer: Our msg alert tells us of a “Potential VNC Scan 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.

   Answer: Alert the user of **ANY** inbound TCP traffic from “External_Net” from **HTTP_Ports** that arrives at “Home_Net” from **ANY** ports. It appears that an EXE file is attempting to be delivered through any port on the local machine.

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

   Answer: This is an instance of Delivery where the weaponized payload is attempting to breach the defences of our system.

3. What kind of attack is indicated?

   Answer: This appears to be some type of injection, possibly Cross Site Scripting, as an EXE file is attempting to be sent and executed within the system.

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_NET any -> $HOME_NET 4444 (msg: “ET POSSIBLE TROJAN”)

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.

```
sysadmin@UbuntuDesktop:~$ sudo apt remove ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'ufw' is not installed, so not removed
```

- No 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.

```
sysadmin@UbuntuDesktop:~$ sudo systemctl enable firewalld.service
Synchronizing state of firewalld.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable firewalld
```

-
```
sysadmin@UbuntuDesktop:~$ sudo /etc/init.d/firewalld start
[ ok ] Starting firewalld (via systemctl): firewalld.service.
```

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.

```
sysadmin@UbuntuDesktop:~$ sudo systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
```

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:

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Take note of what Zones and settings are configured. You may 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

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin b
itcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-col
lector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox-l
ansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trus
t ftp ganglia-client ganglia-master git high-availability http https imap imaps
ipp ipp-client ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpasswd
 kprop kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mosh moun
td ms-wbt mssql murmur mysql nfs nfs3 nrpe ntp openvpn ovirt-imageio ovirt-stora
geconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql
privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh
 rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptra
p 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-cli
ent xmpp-local xmpp-server zabbix-agent zabbix-server
```

- We can see that the Home and Drop Zones are created by default.

Zone Views

- Run the command that lists all currently configured zones.

```
sysadmin@UbuntuDesktop:~$ 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:
```

- 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.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --new-zone-web
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --new-zone-web
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --new-zone=web
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --new-zone=sales
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --new-zone=mail
success
```

We had a little typo of “-” instead of “=” before the zone name but each zone was created successfully.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --reload
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --parmanent --list-all-zones
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --parmanent
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
```

Another typo of “a” instead of “e” in permanent. But everything checks out and the zones were successfully deployed.

Set the zones to their designated interfaces:

Run the commands that sets your eth interfaces to your zones.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=public --change-interface=eth0
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=web --change-interface=eth1
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=sales --change-interface=eth2
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=mail --change-interface=eth3
success
```

HUZZAH! Interfaces are set up to the proper 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:

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=public --add-service=http
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=public --add-service=https
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=public --add-service=pop3
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=public --add-service=smtp
success
```

- Web:

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=web --add-service=http
success
```

- Sales

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=sales --add-service=https
success
```

Mail

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=mail --add-service=smtp
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=mail --add-service=pop3
success
```

- What is the status of http, https, smtp and pop3?

```
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:


public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


sales (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth2
  sources:
```

- Looks like our services were successfully implemented

Add your adversaries to the Drop Zone.

Run the command that will add all current and any future blacklisted IPs to the Drop Zone.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=drop --add-source=135.95.103.76
success
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118
success
```

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

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

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.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --get-active-zones
drop
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
mail
  interfaces: eth3
public
  interfaces: enp0s3 eth0
sales
  interfaces: eth2
web
  interfaces: eth1
```

Block an IP address

- Use a rich-rule that blocks the IP address 138.138.0.3.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" so
urce address="138.138.0.3" reject'
success
```

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.

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

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.

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 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@UbuntuDesktop:~$ sudo firewall-cmd --zone=sales --list-all
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:
```

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=mail --list-all
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:
```

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --zone=web --list-all
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:
```

```
sysadmin@UbuntuDesktop:~$ sudo firewall-cmd --permanent --zone=drop  --list-all
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:
```

- Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.
  Looks like everything is here.

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: One method is Network-based Intrusions Detection Systems (NIDS) which monitor traffic at the level of the network from all connected devices that goes in and out. It is capable of performing analysis on traffic to observe patterns and abnormal behaviors and delivers warnings associated with those behaviors. In combination with a NIDS, a Network Test Access Port is used to provide access to a network. Network TAPs allow the transmission of data for sending and receiving data streams. This guarantees data arrival at the monitoring devices in real time.

   Answer 2: Host-based Intrusion Detection System (HIDS) runs locally on a host-based system, workstation, or server. It's primary use is to monitor the entire network for system data and look for malicious activity on an individual host. Snapshots can be taken of the local system and if any malicious change occurs, then an alert is raised. It can also monitor for changes in management in the operation of system logs, files, software, and more. SPAN ports are used in conjunction with HIDS to send a mirror image of all network data to another port where packets can then be captured and analyzed by other security applications.

2. Describe how an IPS connects to a network.

   Answer: An IPS is typically connected to a mirror port on a switch. The switch is located behind a firewall and monitors traffic for suspicious behavior

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

   Answer: IDS based signatures are unable to detect zero-days since it compares traffic from predefined lists and parameters. It cannot filter anything outside of those domains. A zero-day would not affect these parameters and thus would not be detected.

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?

Answer: An Anomaly-based network intrusion detection system works best in this situation, since as the name implies, it detects anomalies within the system.

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 (Physical)

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

        Answer: Technical Software (Application)

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

        Answer: Technical Network (Data)

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

        Answer: Technical Software (Host)

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

        Answer: Technical Network

    6. Data is classified at the wrong classification level.

        Answer: Administrative Procedures (Policy, procedures, and awareness)

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

        Answer: Administrative Network (Perimeter)

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

    Answer: Drive encryption

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

   Answer: Data encryption (VPN and Spoofers)

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

   Answer: Network cards and route tracing could help in locating stolen laptops.

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

   Answer: Disk encryption and strong passwords are your best defense. Firmware encrypted passwords are the next step up but can be more difficult to implement.

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: Circuit-Level Gateways, Stateful Inspection Firewalls, Proxy 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.

Answer: Stateful Inspection 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?

Answer: 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?

Answer: Packet-filtering firewalls

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

Answer: Next Generation Firewalls