**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: Physical Controls

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

Answer: Administrative Controls

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

Answer: Technical Controls

**Intrusion Detection and Attack indicators**

1. What's the difference between an Intrusion Detection System and an Intrusion Protection System?

Answer: IDS is a monitoring, IPS is a control system. IDS sees but does not alter network traffic. IPS sees and can prevent traffic delivery based on the contents of the packet.

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

Answer: IOA is focused on detecting the intent of an attacker and alerting/notifying before the exploit happens. IOC is forensics and analyzes computer evidence after the security has 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
2. Stage 2: Weaponization
3. Stage 3: Delivery
4. Stage 4: Exploitation
5. Stage 5: Install
6. Stage 6: Command & Control
7. Stage 7: Action on Objectives

**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: Generate an alert for tcp protocol traffic inbound from any outside network with a destination to port range 5800 thru ports 5820 throw an alert/message

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

Answer: Reconnaissance

What kind of attack is indicated?

Answer: Emerging Threat VNC scan of 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: Generate an alert for tcp inbound traffic from any outside network using port 80 to any port on the network.

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

Answer: Policies, procedures, and a

1. What kind of attack is indicated?

Answer: Emerging Threat "EXE or DLL Windows file download

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 any any any -> any 4444 (msg:"Attempt to access 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-get remove ufw

**Enable and start firewalld**

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

* Run the commands that enable and start firewalld upon boots and reboots.
* $ sudo ufw enable

$ sudo systemctl start ufw

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 ufw

**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 ufw status

* 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

$ systemctl list-unit-files --type=service

* We can see that the Home and Drop Zones are created bydefault.

**Zone Views**

* Run the command that lists all currently configured zones.

$ 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.s

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

* Run the commands that creates Web, Sales and Mail zones.
* $ sudo firewall-cmd --new-zone web --permanent
* $ sudo firewall-cmd --new-zone sales --permanent
* $ sudo firewall-cmd --new-zone mail --permanent
* **Set the zones to their designated interfaces:**
* Run the commands that sets your eth interfaces to your zones.
* $ sudo firwall-cmd --zone=web --change-interface=eth1
* $ sudo firwall-cmd --zone=sales --change-interface=eth2
* $ sudo firwall-cmd --zone=mail --change-interface=eth3

$ sudo firwall-cmd --zone=public --change-interface=eth0

**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
* $ sudo firewall-cmd --permanent --zone=public --add-service=https

$ sudo firewall-cmd --permanent --zone=public --add-service=smtp

$sudo firewall-cmd --permanent --zone=public --add-service=pop3

* Web:

$ sudo firewall-cmd --permanent --zone=public --add-service=http

* Salesfi

$ sudo firewall-cmd --permanent --zone=public --add-service=https

* Mail
* $ sudo firewall-cmd --permanent --zone=public --add-service=pop3

$ sudo firewall-cmd --permanent --zone=public --add-service=smtp

* What is the status of http, https, smtp and pop3? *Ans: success*

**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-source=135.95.103.76
* $ sudo firewall-cmd --permanent --zone=drop --add-source=76.34.169.118

$ sudo firewall-cmd --permanent --zone=drop --add-source=10.208.56.23

**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 ensures 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 --reload

**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 --list-all-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” reject’

**Block Ping/ICMP Requests**

Harden your network against ping scans by blocking icmp echo 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

**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=mail --list-all
* $ sudo firewall-cmd --zone=sales --list-all
* $ sudo firewall-cmd --zone=web --list-all
* $ sudo firewall-cmd --zone=public --list-all
* $ sudo firewall-cmd --zone=drop --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:*HIDS (Host based Intrusion Detection System) monitor the network from the NIC (Network Interface Card)*

Answer 2: *NIDS(Network Intrusion Detection System) directly monitors the network traffic*

1. Describe how an IPS connects to a network.

Answer: *Intrusion Protection System is a stand alone device that can be inserted into the network system at any point where there is network traffic and network hooks.*

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

Answer: *Signature based IDS.*

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: *Anomaly based IDS.*

**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: Host Protection

* 1. A zero-day goes undetected by antivirus software.

Answer: *OS and Application Protection*

* 1. A criminal successfully gains access to HR’s database.

Answer: *Data and Info Protection*

* 1. A criminal hacker exploits a vulnerability within an operating system.

Answer: *OS and Application Protection*

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

Answer: *Perimeter Defence Protection*

* 1. Data is classified at the wrong classification level.

Answer: *Data and Info* Protection

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

Answer:*Perimeter Defense*

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

Answer: *Encryption at rest*

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

Answer: *Encrypt data and connections*

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

Answer: *Tracking apps and GPS*

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

Answer:

**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: *Stateless inspection firewall*

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: *Circuit-level gateway*

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: *Next-generation firewall*

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: *Stateful inspection firewall*

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

Answer: Uncomplicated Firewall (UFW)

**Bonus Lab: "Green Eggs & SPAM"**

In this activity, you will target spam, uncover its whereabouts, and attempt to discover the intent of the attacker.

* You will assume the role of a Jr. Security administrator working for the Department of Technology for the State of California.
* As a junior administrator, your primary role is to perform the initial triage of alert data: the initial investigation and analysis followed by an escalation of high priority alerts to senior incident handlers for further review.
* You will work as part of a Computer and Incident Response Team (CIRT), responsible for compiling **Threat Intelligence** as part of your incident report.

**Threat Intelligence Card**

**Note**: Log into the Security Onion VM and use the following **Indicator of Attack** to complete this portion of the homework.

Locate the following Indicator of Attack in Sguil based off of the following:

* **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

Answer the following:

1. What was the indicator of an attack?

Answer: *Sguil list the record with a status of RT – alert was triggered “ET Trojan JS/Nemucod.M.gen downloading EXE payload”*

What was the adversarial motivation (purpose of attack)?

Answer: *Attacker was attempting to get control of a device by slaving the device to a remote command and control server*

1. Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

| **TTP** | **Example** | **Findings** |
| --- | --- | --- |
| **Reconnaissance** | *The attacker accessed ip/port 192.168.204.13:50089 from ip/port 178.62.255.107:80 and managed to gain access with a malicious SSL certificate* |  |
| **Weaponization** | *The attacker was attempting to upload a file containing executable JavaScript disguised as a .EXE file. The .EXE file would contain an attached zip file when the zip file is clicked mime would run the javascript* |  |
| **Delivery** | *Trojan* |  |
| **Exploitation** | *System eth1-1 ip192.168.204.13 was targeted and attacked* |  |
| **Installation** | *Executable file or email* |  |
| **Command & Control (C2)** | *The Trojan would need to create some code that auto checks into a remote command and control server* |  |
| **Actions on Objectives** | *The code would call an attached zip file, the zip file would cause windows to try and execute the javascript because of the file type or script syntax.* |  |

Answer:

1. What are your recommended mitigation strategies?

Answer: 1) *Scan the system. find and remove the Trojan. Reinforce the upload/download utilities*

1. List your third-party references.

Answer:

Network Security Monitoring -  Elsevier B.V.  - [Network Security Monitoring - an overview | ScienceDirect Topics](https://www.sciencedirect.com/topics/computer-science/network-security-monitoring#:~:text=NSM%20is%20the%20collection%2C%20detection%2C%20and%20analysis%20of,Defense%20%28CND%29%20per%20DoD%208500.2.%201%20These%20are%3A)

Inform IT – Pearson - [The Basic Sguil Interface | Why Sguil Is the Best Option for Network Security Monitoring Data | InformIT](https://www.informit.com/articles/article.aspx?p=350390&seqNum=3)

Firewalls – Archlinux - [Firewalls (Српски) - ArchWiki (archlinux.org)](https://wiki.archlinux.org/title/Firewalls_(%D0%A1%D1%80%D0%BF%D1%81%D0%BA%D0%B8))

Firewalls – phoenixNAP - [8 Types of Firewalls: Guide For IT Security Pros (phoenixnap.com)](https://phoenixnap.com/blog/types-of-firewalls)

[Cyberteam Security Services - Defence in Depth Security Model](https://cyberteamsecurity.com/defence-depth-security-model.html#:~:text=The%20four%20key%20layers%20of%20the%20defence%20in,and%20Application%20Protection.%204%20Layer%204%3A%20Data%2FInformation%20Protection.) - CyberTeam

[Gaining\_the\_Advantage\_Cyber\_Kill\_Chain.pdf (lockheedmartin.com)](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf#:~:text=The%20Cyber%20Kill%20Chain%C2%AE%20framework%20is%20part%20of,must%20complete%20in%20order%20to%20achieve%20their%20objective.)

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.