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 (Perimeter) Security, "measures [that] are designed to protect buildings, and safeguard the equipment inside. In short, they keep unwanted people out, and give access to authorized individuals.`

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

   Answer: `Administrative or Procedural Security, "the management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data."`

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

   Answer: `Operational Security (OPSEC)/ Technical Controls, "a risk management process that encourages managers to view operations from the perspective of an adversary to protect sensitive information from falling into the wrong hands."`

Intrusion Detection and Attack indicators

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

   Answer: `An IDS is an Intrusion Detection System that only observes network traffic and alerts to network attacks whereas an IPS is an Intrusion Protection System that prevents such attacks by inspecting network traffic and stops malicious traffic from attacking. IDS is financially more beneficial vs IPS.`

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

   Answer: `An IOA is one that indicates things happening in real time and focuses on revealing the intent and end goal of an attacker, whereas an IOC indicate previous malicious activity used to establish adversary's techniques, tactics, and procedures, exposing all vulnerabilities used in an attack.`

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:** Attackers scope targets out online, harvest public information, conduct in-depth research, and search for weak points in a company's network.
2. Stage 2: **Weaponization:** Once a vulnerability is identified, hackers create their attack to target the weak points.
3. Stage 3: **Delivery:** Cybercriminals execute their attacks to intended victims. Common techniques are through phishing email attacks, compromised user accounts, infected USB devices, and more.
4. Stage 4: **Exploitation:** Vulnerable software or system architecture is taken advantage of.
5. Stage 5: **Installation:** Malware is installed on the target asset.
6. Stage 6: **Command & Control:** Attackers gain control of the device, and the supply chain network is established.
7. Stage 7: **Actions on Objectives:** Now that the hacker has access to the organization, they execute actions to achieve their 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 Potentia
l VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, co
unt 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classty
pe:attempted-recon; sid:2002910; rev:5; metadata:created_at 2010_07_30, u
pdated_at 2010_07_30;)
```

1. Break down the Sort Rule header and explain what is happening.

   Answer: Snort "alert" that the "tcp" packets from any "EXTERNAL_NET"works at any ports going to the "HOME_NET"work at these ports ranging from 5800:5820

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

   Answer: Stage 1: Reconnaissance - The attack type is an "attempted-recon"

3. What kind of attack is indicated?

   Answer: A potential Virtual Network Computer/ Computing Scan for ports 5800-5820

Snort Rule #2

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE E
XE or DLL Windows file download HTTP"; flow:established,to_client; flowbi
ts:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file
_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"P
E|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata:
 former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Mai
```

1. Break down the Sort Rule header and explain what is happening.

   Answer: Snort “alert” that the “tcp” packets from any “EXTERNAL_NET”work’s HTTP ports (80, 8080, 443) going to the “HOME_NET”work on any ports with a file_data

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

   Defense in Depth: Host/ Application Security - Software bypassing rules set in the Application via HTTP

   Answer:

   Cyber Kill Chain: Stage 3: Delivery - The attack is uploading a EXE or DLL Windows file via HTTP

3. What kind of attack is indicated?

   Answer: Downloading/ stealing an executable file via HTTP when it is not supposed to.

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 4444 -> $HOME_NET any (msg:“ET Possible Rootkit, Backdoor, or Trojan Detected/ ET POLICY TROJAN Possible W32.Blaster.Worm”)

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 ufw disable    disables ufw          sudo apt remove ufw  uninstalls 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 start firewalld          (starts service)
$ sudo systemctl enable firewalld         (starts when boots)
```

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           sudo firewall-cmd --state
```

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.

```
$ 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
$ sudo firewall-cmd --permanent --new-zone=Sales
$ sudo firewall-cmd --permanent --new-zone=Mail
```

Set the zones to their designated interfaces:

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

```
$ sudo firewall-cmd --zone=Public --permanent --change-interface=eth0
$ sudo firewall-cmd --zone=Web --permanent --change-interface=eth1
$ sudo firewall-cmd --zone=Sales --permanent --change-interface=eth2
$ sudo firewall-cmd --zone=Mail --permanent --change-interface=eth3
```

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 --zone=Public --permanent --add-service=http
$ sudo firewall-cmd --zone=Public --permanent --add-service=https
$ sudo firewall-cmd --zone=Public --permanent --add-service=smtp
$ sudo firewall-cmd --zone=Public --permanent --add-service=pop3
```

- Web:

```
$ sudo firewall-cmd --zone=Web --add-service=http
```

- Sales

```
$ sudo firewall-cmd --zone=Sales --permanent --add-service=https
```

- Mail

```
$ sudo firewall-cmd --zone=Mail --permanent --add-service=smtp
$ sudo firewall-cmd --zone=Mail --permanent --add-service=pop3
```

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

  `sudo firewall-cmd --reload` `sudo firewall-cmd --list-all`

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 --zone=Drop --permanent --add-source=10.208.56.23
$ sudo firewall-cmd --zone=Drop --permanent --add-source=135.95.103.76
$ sudo firewall-cmd --zone=Drop --permanent --add-source=76.34.169.118
```
~~~

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 --reload  - or -  sudo firewall-cmd --complete-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 --get-active-zones
```

Block an IP address

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

```
$ sudo firewall-cmd --pernament --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 ehco` replies.

- Run the command that blocks `pings` and `icmp` requests in your `public` zone.

```
$ sudo firewall-cmd --pernament --zone=Public --add-rich-rule=‘rule protocol value=icmp reject’
```

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=Public --list-all
$ sudo firewall-cmd --zone=Web --list-all
$ sudo firewall-cmd --zone=Sales --list-all
$ sudo firewall-cmd --zone=Mail --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: Network TAP (Test Access Port) is a hardware device that provides access to a network. Network taps transit both inbound and outbound data streams on separate channels at the same time, so all data will arrive at the monitoring device in real time.

Answer 2: SPAN *=(Switch Port Analyzer, also known as port mirroring, 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.

   Answer: IPS connects inline with the flow of data, typically between the firewall and network switch. Requires more robust hardware due to the amount of traffic flowing through it. IPS will automatically take action by blocking and logging a threat, thus it doesnt require administrative intervention.

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

   Answer: Signature-based IDS - A signature-based IDS compares patterns of traffic to predefined signatures.

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: Anomaly-based IDS - An anomaly-based IDS compares patterns of traffic against a well-known baseline.

Defense in Depth

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:

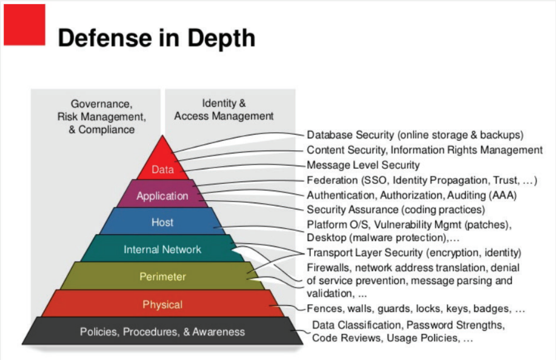
   1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

      Answer: Perimeter Physical Security

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

      Answer: Host/ Application Security

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


Defense in Depth
Governance, Risk Management, & Compliance
Identity & Access Management
Data
Application
Host
Internal Network
Perimeter
Physical
Policies, Procedures, & Awareness
Database Security (online storage & backups)
Content Security, Information Rights Management
Message Level Security
Federation (SSO, Identity Propagation, Trust, …)
Authentication, Authorization, Auditing (AAA)
Security Assurance (coding practices)
Platform O/S, Vulnerability Mgmt (patches), Desktop (malware protection),…
Transport Layer Security (encryption, identity)
Firewalls, network address translation, denial of service prevention, message parsing and validation, ...
Fences, walls, guards, locks, keys, badges, …
Data Classification, Password Strengths, Code Reviews, Usage Policies, …

Reference Defense in Depth Model

      Answer: Data Security

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

      Answer: Host - Platform O/S

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

      Answer: Internal Network Security

   6. Data is classified at the wrong classification level.

Answer: `Administrative / Procedure/ Policy / Awareness Security`

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

   Answer: `Perimeter Security - Firewalls`

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

   Answer: `Whole Disk/Drive Encryption (Bit Locker)`

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

   Answer: `End-to-End Data Encryption - like a VPN`

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

   Answer: `Find my device, or tracking application, even an airtag device hidden inside.`

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

   Answer: `Disk/ Drive Encryption and strong passwords from being cracked`

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 Firewalls/ gateways`

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: `Packet-Filtering Firewalls (Stateful)`

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: `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?

Answer: `Packet-Filtering Firewalls (Stateless)`

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

Answer: `Mac Layer Firewall`

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?
   - Hint: What do the details of the reveal?

Answer: `Downloading of the .zip file with the (2) embedded javascript files`

2. What was the adversarial motivation (purpose of attack)?

   Answer: To steal information from the victim as a later version shows it downloading “Gozi infostealer” onto the compromised computer running the scripts.

3. 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	How did they attacker locate the victim?	Emailed attachments to Italian users.
Weaponization	What was it that was downloaded?	A .zip file containing javascripts.
Delivery	How was it downloaded?	User clicked on the attachment file and saved it.
Exploitation	What does the exploit do?	Installs an executable in the background while running a script to open a decoy PDF file. Executable retrieves a Trojan Downloader called Fariet or Pony Downloader. More executables are downloaded to install Gozi info-stealer.
Installation	How is the exploit installed?	
Command & Control (C2)	How does the attacker gain control of the remote machine?	After the computer is rebooted after a few instants, Gozi starts phoning home only after the reboot.
Actions on Objectives	What does the software that the attacker sent do to complete it's tasks?	Hides itself in the users temp files directory as well as the registry keys to ensure that the scripts keep running for being able to capture data. It then records user bank login info data including security questions info without a keylogger/ screen capture. Data is then compressed and sent back out to the Command center.

Answer:

1. What are your recommended mitigation strategies?

   Answer: Implement email server anti-virus scanners, procedures to NOT download any unknown attachments in any emails from anybody unless requested or recognized.

2. List your third-party references.

   Answer: https://certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/

   https://www.secureworks.com/research/gozi

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