Cybersecurity

Part 1: Review Questions

Security Control Types

The concept of defense in depth can be broken down into three 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?

```
Physical control
```

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

```
Administrative control
```

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

```
Technical control
```

Intrusion Detection and Attack Indicators

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

```
IDS: Intrusion Detection System vs IPS: Intrusion Prevention System. They both monitor and analyze packets, however, the main difference is that an IDS requires human intervention to stop an attack while an IPS can do that by itself. An IDS will only send alerts.
```

2. What's the difference between an indicator of attack (IOA) and an indicator of compromise (IOC)?

```
An indicator of attack (IOA) focuses on the intent of the attacker, and what they're trying to accomplish. This is an alert before a network is compromised. An indicator of compromise (IOC) is a post mortem, forensic activity that finds the evidence on the network after the breach has occurred.
```

The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each. Used https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/ for examples

1. Stage 1:

```
Reconnaissance: A general information gathering activity. An attacker will be looking to obtain the most amount of information as possible in this step. The information they'll be looking for includes: email addresses, user ids, os details and login credentials if possible.
```

2. Stage 2:

```
Weaponization: The main focus of this step is creating a way to infect the target. This can be in the form of ransomware, malware, or a virus to exploit a vulnerability.
```

3. Stage 3:

```
Delivery: This is the start of the attack. It can be in the form of phishing emails, or malicious links. This step can be combined with social engineering techniques for increased effectiveness.
```

4. Stage 4:

```
Exploitation: This is when the attack vector in step 2 is activated. An example would be activating the ransomware that was created for the victim's system.
```

5. Stage 5:

```
Installation: This is where the malware would be installed on the system and now the attack has entered the system.
```

6. Stage 6:

```
Command and Control: Now that control has been established, the goal is to propagate and spread laterally throughout the victim's system. The victim's system is now firmly under control of the attacker.
```

7. Stage 7:

```
Actions on Objective: Now that the attacker has spread throughout the system,  the attacker will look to carry out their goals. In the ransomware example, once the victim pays the ransom, the data being held hostage will be returned (or deleted).
```

Snort Rule Analysis

Use the provided Snort rules 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 this rule does.

```
This is an alert intended to notify the user of ANY inbound TCP traffic on
ports 5800-5820 on the external network.
```

2. What stage of the cyber kill chain does the alerted activity violate?

```
An attacker is looking for a weakness on these ports so this violates
reconnaissance.
```

3. What kind of attack is indicated?

```
The alert says “Potential VNC Scan 5800-5820”. This is a port mapping
attack.
```

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 this rule does.

```
A remote host, on http port (80) connected to our machine (client) and tried
to deliver a payload on an open port.
```

2. What layer of the defense in depth model does the alerted activity violate?

```
This is delivery, as the attacker was trying to get a payload into our
system.
```

3. What kind of attack is indicated?

```
Cross site scripting. From Emerging Threat for Policy Violation “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.

```
Alert tcp $EXTERNAL_NET -> $HOME_NET 4444 (msg: “Possible rootkit,backdoor
or trojan horse.”)
https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-sec
ure-them/
```

Part 2: “Drop Zone” Lab

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.

```
*Log into firewalld machine
Open cmd prompt
From within the terminal :sudo apt remove ufw
```

Enable and start firewalld.

By default, the firewalld service should be running. If not, then run the commands that enable and start firewalld upon boots and reboots.

```
$ <sudo systemctl enable firewalld.service>
$ <sudo /etc/init.d/firewalld start>
```

Note: This will ensure that firewalld remains active after each reboot.

Confirm that the service is running.

Run the command that checks whether the `firewalld` service is up and running.

```
sysadmin@firewalld-host:~$ sudo systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset
   Active: active (running) since Sun 2022-11-27 15:05:45 EST; 14min ago
     Docs: man:firewalld(1)
 Main PID: 956 (firewalld)
    Tasks: 2 (limit: 4647)
   CGroup: /system.slice/firewalld.service
           └─956 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid
```

List all firewall rules currently configured.

Next, list 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 ensuring that you don't duplicate work that's already done.

- Run the command that lists all currently configured firewall rules:

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all
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:
```

- 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 find out whether the service you need is available.

```
$ <sudo firewall-cmd -get-services> **There is two dashes in front of get, google docs changes this to one long dash by default
```

- Notice that the `home` and `drop` zones are created by default.

Zone views.

- Run the command that lists all currently configured zones.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
```

- Notice that the `public` and `drop` zones are created by default. Therefore, you will need to create zones for `web`, `sales`, and `mail`.

Create zones for `web`, `sales`, and `mail`.

- Run the commands that create `web`, `sales`, and `mail` zones.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=web
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=sales
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --new-zone=mail
success
```

Set the zones to their designated interfaces.

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

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --change-interface=eth0
The interface is under control of NetworkManager, setting zone to 'public'.
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=web --change-interface=eth1
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=sales --change-interface=eth2
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=mail --change-interface=eth3
success
```

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@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=httpsuccess
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=http
Warning: ALREADY_ENABLED: http
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=https
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=pop3
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=public --add-service=smtp
success
```

- `web`:

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

- `sales`:

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

- `mail`:

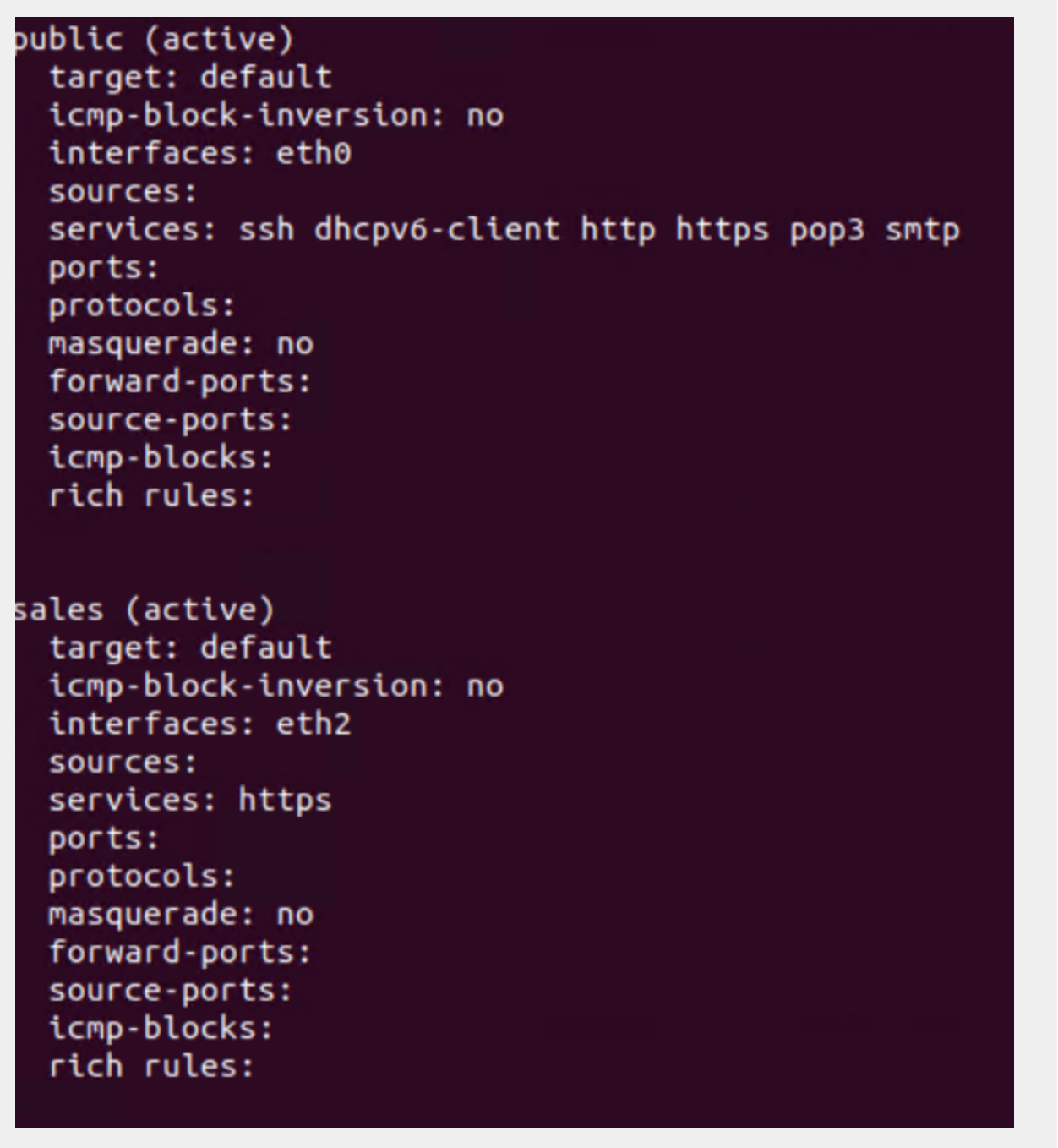
```
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=mail --add-service=smtp
success
sysadmin@firewalld-host:~$ sudo firewall-cmd --permanent --zone=mail --add-service=pop3
success
```

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

```
After running sudo firewall-cmd -reload and sudo firewall-cmd
-list-all-zones, I can see that http,https,smtp and pop3 are all services
running under the zones they were configured.
```

```
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: eth0
  sources:
  services: ssh dhcpv6-client http https pop3 smtp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```



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@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
```

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 helps ensure that the network remains secure after unplanned outages such as power failures.

- Run the command that reloads the firewalld configurations and writes it to memory:

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

View active zones.

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

- Run the command that displays all zone services.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --get-active-zones
[sudo] password for sysadmin:
drop
  sources: 10.208.56.23 135.95.103.76 76.34.169.118
mail
  interfaces: eth3
public
  interfaces: eth0
sales
  interfaces: eth2
web
  interfaces: eth1
```

Block an IP address.

- Use a rich-rule that blocks the IP address `138.138.0.3` on your `public` zone.

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source 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@firewalld-host:~$ sudo firewall-cmd --zone=public --add-icmp-block=echo-reply --add-icmp-block=echo-
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@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:
  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:
  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:
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
sysadmin@firewalld-host:~$ sudo firewall-cmd --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 the 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, you'll 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.

```
Network Tap: Hardware device that provides access to a network. Transits
incoming and outgoing traffic simultaneously on separate channels.
```

```
SPAN: Switched port analyzer (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.

```
Connects inline within the flow of data. Is typically placed between
firewall and network switch.
```

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

```
Signature based IDS.
```

4. What 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. For each of the following scenarios, provide the layer of defense in depth that applies:

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

```
This is a physical threat, and in the defense in depth model, would pertain to the perimeter layer.
```

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

```
This is at the application layer.
```

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

```
The data layer.
```

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

```
*Assuming endpoint user's OS, this would be at the host layer.
```

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

```
This is at the network layer.
```

f. Data is classified at the wrong classification level.

```
This violates the confidentiality of the CIA cybersecurity triad. In terms of the defense in depth model, this affects data because the wrong people may have access to data they shouldn't.
```

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

```
Firewalking gets packets from an untrusted source through a firewall. This relates to the perimeter.
```

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

```
Encrypt the drive.
```

3. Name one method of protecting data-in-transit.

```
Use data encryption.
```

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

```
I would recommend using an application such as prey. The criminal would need to connect to the internet, but it is a good free option everyone could install on their device. Otherwise, you could install hardware that has live location tracking - depends on the contents of your laptop.
```

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

```
Go into os settings: 1) disable any boot settings besides internal SSD 2)disable secure boot 3) disable usb boot. Would stop them, but you better hope your laptop never crashes.
https://www.dell.com/community/Storage-Drives-Media/External-Hard-Drive-Preventing-Boot-Windows-10-Alienware-Alpha/td-p/4754972
```

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.

```
Circuit level firewalls on the session layer. They look at the header of the packet.
```

2. Which type of firewall considers the connection as a whole? Meaning, instead of considering only individual packets, these firewalls consider whole streams of packets at one time.

```
Stateful packet filtering firewalls. They examine the connection, looking at streams of packets.
```

3. Which type of firewall intercepts all traffic prior to forwarding it 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.

```
Application firewalls. They intercept all data on the way to its final
destination incognito. The proxy firewall is actually the first stop, and
forwards traffic deemed to be safe.
```

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?

```
Stateless packet filtering firewalls.
```

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

```
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 junior 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 in to the Security Onion VM, and use the following **indicator of attack** to complete this portion of the assignment.

Locate the 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 questions:

1. What was the indicator of an attack? (*Hint: What do the details reveal?*)

```
Trojan downloader of js.nemucod. This is a trojan that downloads and
installs other programs onto your pc without your consent.
```

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

```
Purpose of the attack is to download malware and unwanted software. Software
is typically info stealers.This malware can also connect to a remote host
using port 80. Also, ransomware could be installed and could lock you out
unless you comply with demands.
```

Malware can connect to a remote host to do any of the following:

- Check for an Internet connection
- Download and run files (including updates or other malware)
- Report a new infection to its author
- Receive configuration or other data
- Receive instructions from a malicious hacker
- Search for your PC location
- Upload information taken from your PC
- Validate a digital certificate

```
From -
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-descriptio
n?Name=TrojanDownloader:JS/Nemucod
```

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 the attacker locate the victim?	Attacker most likely used active recon. They would have to locate a valuable target (you) and then decide on sending an email with a malicious zip file attachment. To increase the probability of success, a hacker worth their salt would craft the message in a way that was attractive so you would trust the email.
Weaponization	What was downloaded?	In the latest campaigns, it has been ransomware by the name TeslaCrypt or Locky.
Delivery	How was it downloaded?	By opening the attached zip file and running the javascript within.
Exploitation	What does the exploit do?	Downloads a ransomware. The goal is a network bound attack and remote access.
Installation	How is the exploit installed?	User opens the email, clicks the zip file and then the javascript runs.
Command & Control (C2)	How does the attacker gain control of the remote machine?	Connects to remote host using port 80
Actions on Objectives	What does the software that the attacker sent do to complete its tasks?	Creates a %/TEMP%/ file with self executing scripts that steals data and connects to remote host via 80.

4. What are your recommended mitigation strategies?

```
Scan your computer to verify that you have found the malware. Start in safe
mode so that if you’re infected, the malware won’t run properly with it’s
auto start functions. Quarantine the infection, and then remove using an
anti malware software.
```

5. List your third-party references.

```
https://www.f-secure.com/v-descs/trojan-downloader_js_nemucod.shtml
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:JS/Nemucod
https://www.cisecurity.org/insights/blog/malware-analysis-report-nemucod-ransomware
```