**The following is my responses to Homework 10. Some of the responses got out of order due to how the question was asked (like the remove ping option). Please consider that when grading. I did not type out all the commands that have a snapshot of them. If that is something that needs to be done on this assignment please let me know.**

**Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.**

**Stage 1: Reconnaissance** This is the observational or from a distance phase where the inter gathering begins. From harvesting email addresses, conference information, contacts, and layouts of locations and systems.

**Stage 2: Weaponization** This is where the hackers would create something to infiltrate the system and deliver a payload. This could be something like creating documents and deliverables that have hidden embedded malware, worms, and viruses that were crafted specifically for this incident.

**Stage 3: Delivery** This is the delivery of the payload. Often occurring in an attachment, website (baited attack), or even the ole’ leave-the-USB-in-the-parking-lot trick.

**Stage 4: Exploitation** This is simply finding and exploiting the vulnerability of the victim’s system. This is often the specific target of the attack since a known-vulnerability is often the most fruitful reward for attackers.

**Stage 5: Installation** This is often the delivery of the payload such as a Trojan that will allow the attackers to gain access to the victim’s system.

**Stage 6: Command & Control (C2)** This is when the attackers are able to get an outside server to enter and take control of the victim’s workspace. This is the “Hands-on- keyboards” part of an attack. This would be where the attackers gained physical (or virtual) access to control devices such as data centers, servers and protected information.

**Stage 7: Actions on Objects** This is when the attacker achieves their goals and does things such as data destruction, ransomware, theft, etc.

#### 

#### 

#### **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;)**

**Break down the Sort Rule header. What is this rule doing?**

This alert is set to apply to all TCP packets. There are four protocols that Snort currently analyzes for suspicious behavior and TCP is a common one to set an alert for. The EXTERNAL\_NET lets us know any external IP location, on any port. The scan is to look at any home network, on ports 5800-5820.

**What stage of the Cyber Kill Chain does the alerted activity violate?**

The number one rule or the Reconnaissance phase.

**What kind of attack is this rule monitoring?**

This is monitoring threats or activities on ports 5800-5820 which are commonly used for virtual remote login on computers.

**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;)**

**Break down the Sort Rule header. What is this rule doing?**

This alert is for all TCP packets, from external IP address and HTTP (80, 443 secured) ports, from all traffic inbound from outside the network to Home networks on any port.

**What stage of the Cyber Kill Chain does the alerted activity violate?**

Exploitation (and kind of Reconnaissance as well)

**What kind of attack is this rule monitoring?**

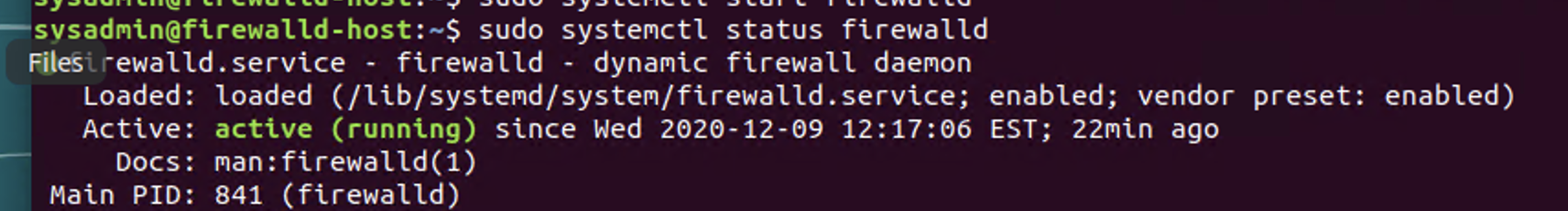
A DoS or denial of service as well as other unknown attacks to the applications. Emerging threats

**Snort Rule #3**

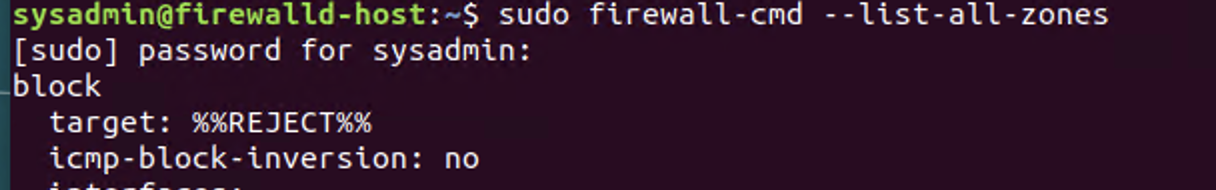
**Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the Rule Option.**

<alert tcp $EXTERNAL\_NET any 4444 → $HOME\_NET any any {msg: ALERT TCP Trojan detected}>

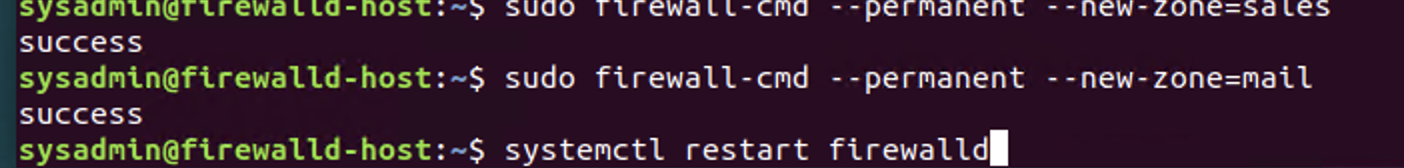
**PART 2**

****

**In order to ensure that ufw was not running and that firewalld was; I used the following commands: <sudo systmctl status ufw>, and <sudo systemctl status firewalld>. I then used <sudo systemctl start firewalld>. I verified it running with the above.**

****

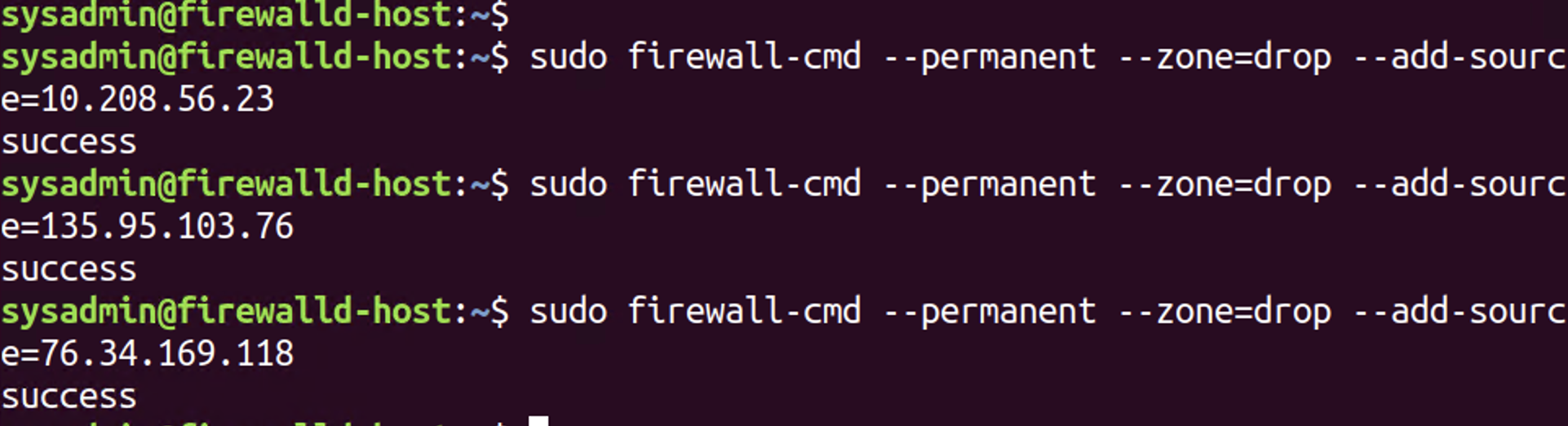
**The above command was used to list all the rules in place and running in the current configuration.**

****

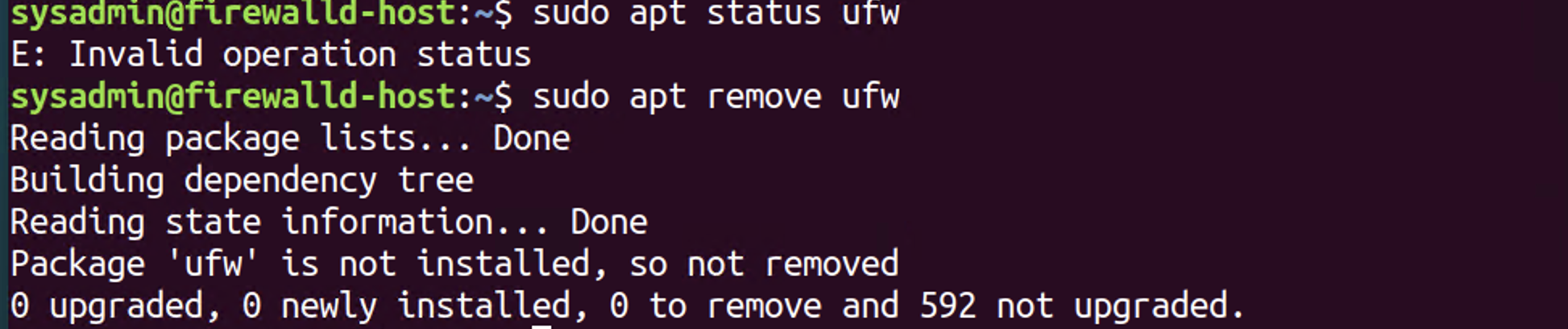
**I created new zones requested of Web, Sales, and Mail. Additionally, I restarted the firewalld to ensure that they were added.**

****

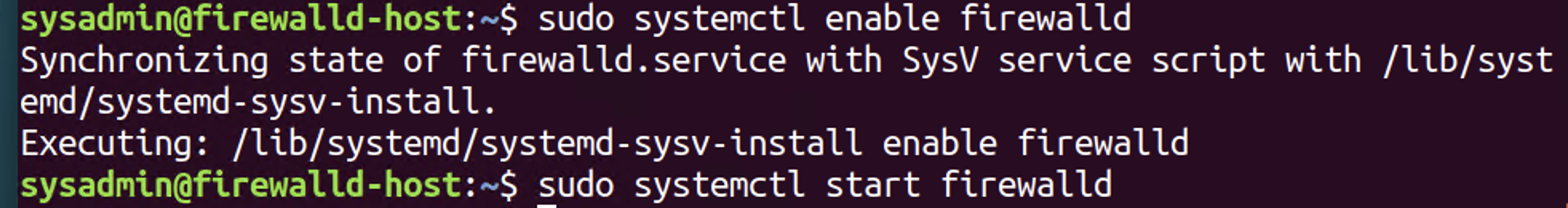
**The above screenshot was taken from when I tried to set the interface zones for the <eth> zones. I tried to do this in different ways and came back to setting each one individually.**

****

**I was able to add the blocked IP addresses to the Drop zone as demonstrated above.**

****

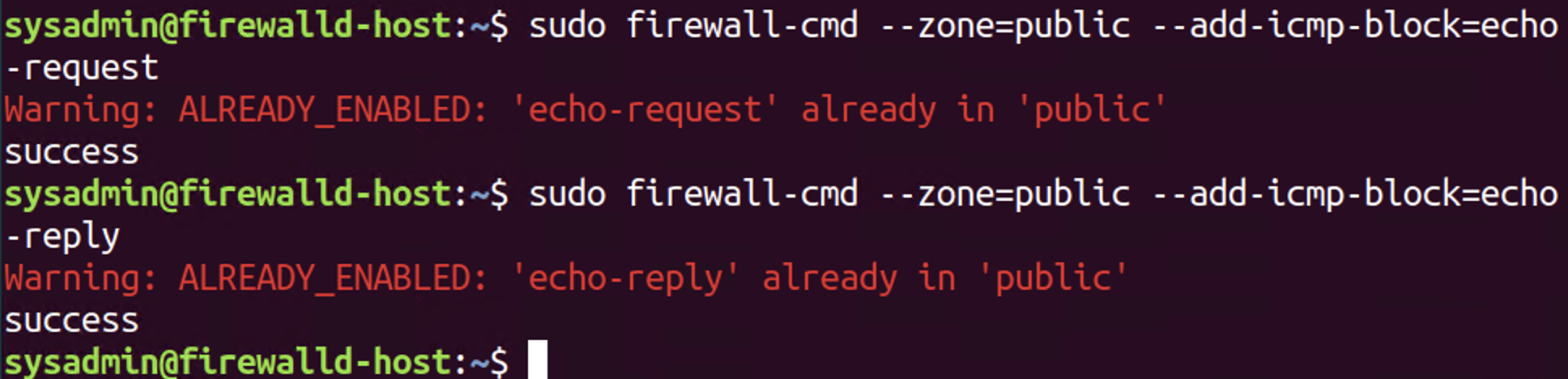
**I stopped the <ufw> from running as demonstrated above.**

****

**I enabled and started the <firewalld>**

****

**The above screenshot reflects that the firewalld was reloaded and that the active zones were listed.**

****

**Block pings and ICMP was added**

### **Part 3: IDS, IPS, DiD, and Firewalls**

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

There are two ways an IDS connects to a network. The first is a network tap. This is a physical wire that is attached to the network. The other is SPAN (Switch Port Analyzer). It is a mirror image.

**Describe how an IPS connects to a network.**

#### It is an in-line connection or physical connection.

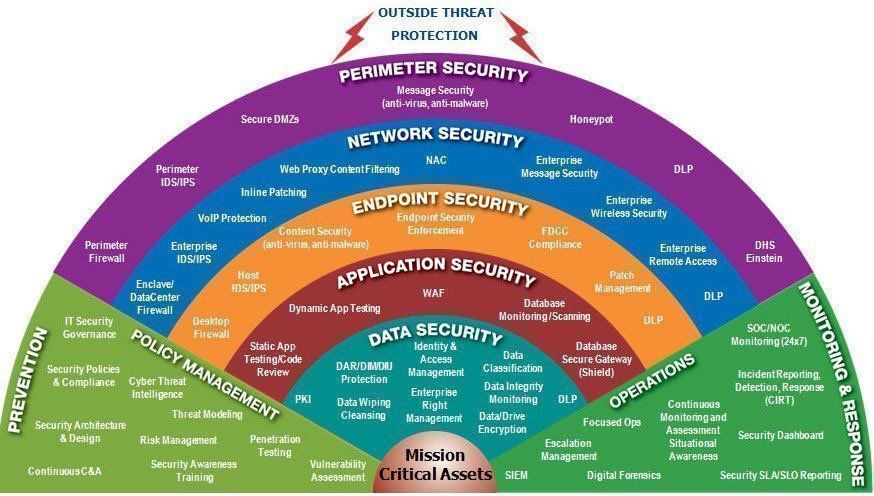
#### **What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?**

#### There are two types (anomaly and signature-based) of IDS attacks. Signature-based cannot detect Zero-Day attacks.

#### **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 attacks

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

****

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

Perimeter attack

**A zero-day goes undetected by antivirus software.**Moving from Endpoint to Application phase

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

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

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

Network Security

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

Policy Management and Prevention

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

Endpoint Security

**Name one method of protecting data-at-rest from being readable on a hard drive.  
Encryption, powering it off**

**Name one method to protect data-in-transit.**Transport Layer Security

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

GPS, geo-tracking

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

Setting an administrative password in BiOS

#### **Firewall Architectures and Methodologies**

**Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.**Stateful (Looked up in the Week 10 day 1 slide 22)

**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.**Stateful

**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?**Proxy Fire

**Which type of firewall examines data within a packet as it progresses through a network interface by examining the source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents?**

Stateless

**Which type of firewall filters based solely on the source and destination MAC address?**

MAC layer firewall

#### 