## **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 Security**
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?  
     
   **Answer: Management or Administrative Security**
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
     
   **Answer: Operational Security - (Data protections Access control Intrusion Detection and Attack indicators)**

#### **Intrusion Detection and Attack indicators**

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

Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) also analyzes packets, but can also stop the packet from being delivered based on what kind of attacks it detects — helping stop the attack. (Peetters)

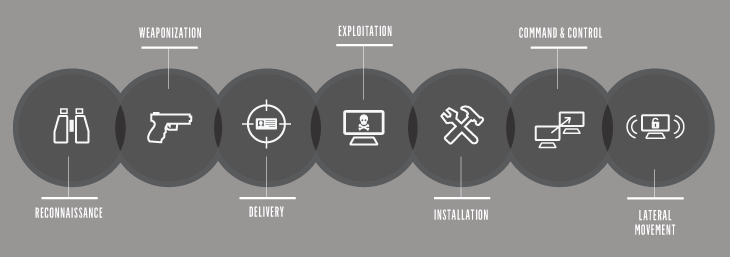
Answer: **There are several differences between the two types of systems. IDS will only issue alerts for potential attacks, while the IPS can take action against them. As IDS is not inline, so the traffic doesn’t have to flow through it. However the traffic does have to flow through the IPS. False positives for IDS will only cause alerts, while false positives for IPS could cause the loss of important data or functions.**

1. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
     
   Answer: **An Indicator of Attack (IOA) focuses on spotting the attempted attacks or reconnaissance and deducing the actor’s intent, while Indicator of Compromise (IOC) focuses on gathering conclusive evidence that a system has been breached. IOA is more reliable based on behaviours or contextual situations.**

#### **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 probe for weakness.) - Gathering info on an individual in preparation for an attack.**
2. Stage 2: **Weaponization (Build a deliverable payload using an exploit and a back-door.) - Injecting the malicious software or installing some sort of back door on said target's machine.**
3. Stage 3: **Delivery (Sending the weaponized bundle to the victim-for example, a malicious link in a legitimate-looking email.) Attackers send malicious payload by means of email or instant message.**
4. Stage 4:**Exploit (Executing code on the victim’s system.) - Gaining access & compromising the user's machine.**
5. Stage 5:**Installation (Installing malware on the target asset.) - Installing more malicious code such as granting your own user root access.**
6. Stage 6:**Command and Control (C&C) (Creating a channel where the attacker can control a system remotely.) Command channel used to control another computer.**
7. Stage 7:**Actions (Attacker remotely carries out its intended goal.) - Accomplishing the final goal on the user's machine.**



#### **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: **Alerts user of ANY inbound TCP traffic from ports 5800 to 5820 on the external network.**
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: **Reconnaissance (Attackers probe for weakness.)**
3. What kind of attack is indicated?  
     
    Answer: **Potential VNC Scan 5800-5820 (Port Mapping)**

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: **The remote host, through http ports, attempted to deliver a malicious payload to any port of the local machine.**
2. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: **Delivery (Sending the weaponized bundle to the victim-for example, a malicious link in a legitimate-looking email.)**
3. What kind of attack is indicated?  
     
    Answer: **Cross site scripting**

Snort Rule #3

* Your turn! Write a Snort rule that alerts when traffic is detected (Roesch) 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 or CrackDown") (Roesch)**

### 

### **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 remove 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 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 or not the firewalld service is up and running.  
    
   $ **sudo systemctl status firewalld.service**

#### 

#### 

#### 

#### 

#### **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.

#### 

#### 

#### 

#### 

#### 

#### 

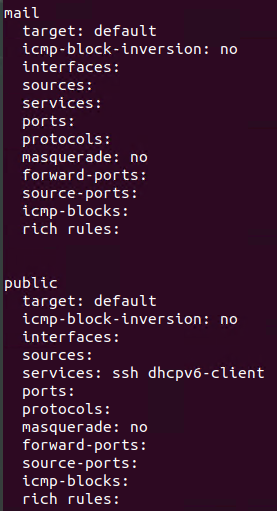
#### 

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

Run the commands that create 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**
* $ **sudo firewall-cmd --reload**
* $ **sudo firewall-cmd --permanent --list-all-zones**

****

#### 

#### 

#### 

#### 

#### 

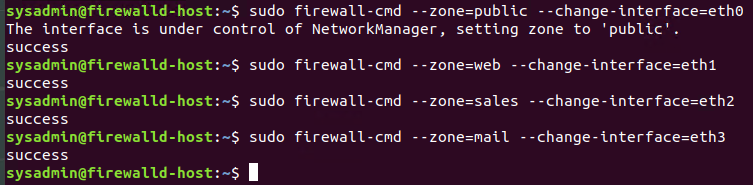
#### **Set the zones to their designated interfaces:**

Run the commands that set your eth interfaces to your zones.  
  
$ **sudo firewall-cmd --zone=public --change-interface=eth0**

$ **sudo firewall-cmd --zone=web --change-interface=eth1**

$ **sudo firewall-cmd --zone=sales --change-interface=eth2**

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

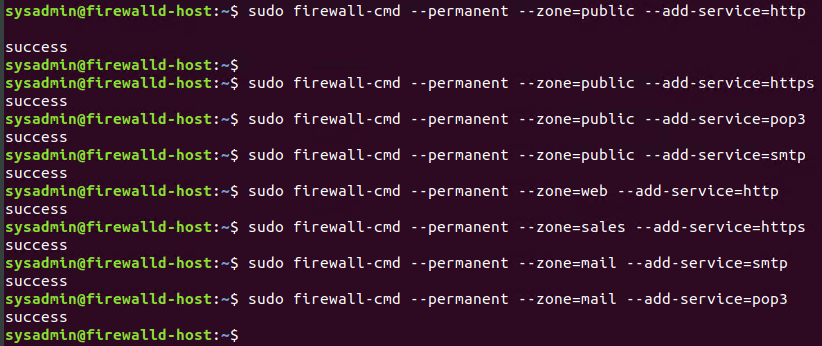
$ **sudo firewall-cmd --permanent --zone=public --add-service=https**

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

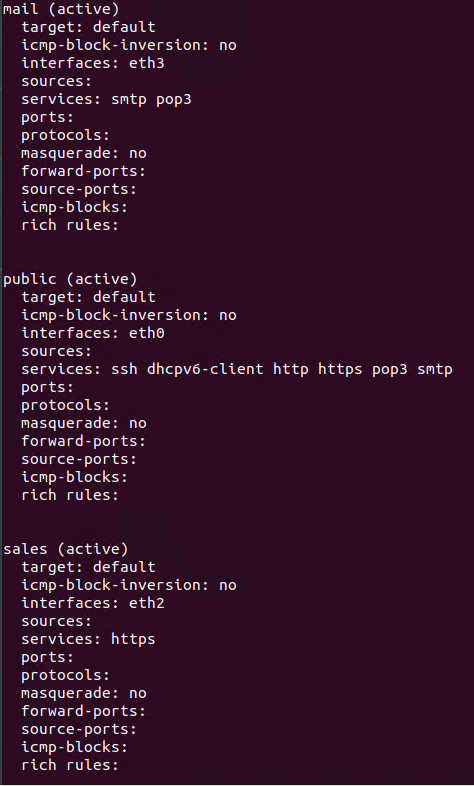
$ **sudo firewall-cmd --permanent --zone=public --add-service=smtp**

* Web:  
  $ **sudo firewall-cmd --permanent --zone=web --add-service=http**
* Sales  
  $ **sudo firewall-cmd --permanent --zone=sales --add-service=https**
* Mail  
  $ **sudo firewall-cmd --permanent --zone=mail --add-service=smtp**

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

****

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



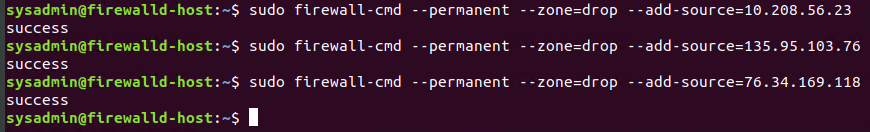
#### 

#### **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=10.208.56.23**

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

$ **sudo firewall-cmd --permanent --zone=drop --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 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**

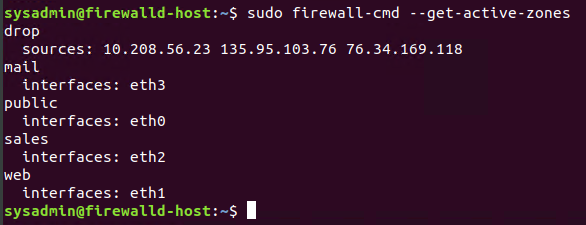
#### 

#### 

#### **View active Zones**

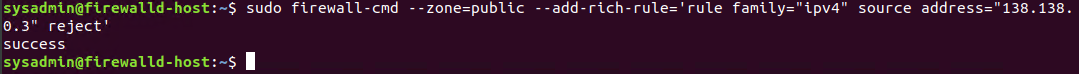
Now, we'll want to provide truncated listings of all currently **active** zones. This is a good time to verify your zone settings.

* 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 --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.

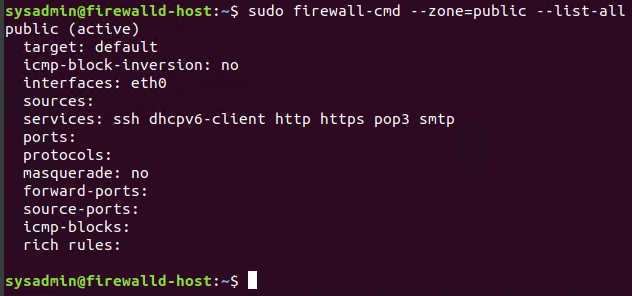
* Run the command that blocks pings and icmp requests in your public zone.  
    
   $ **sudo firewall-cmd --zone=public --add-icmp-block=echo-reply --add-icmp-block=echo-request**



#### **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.

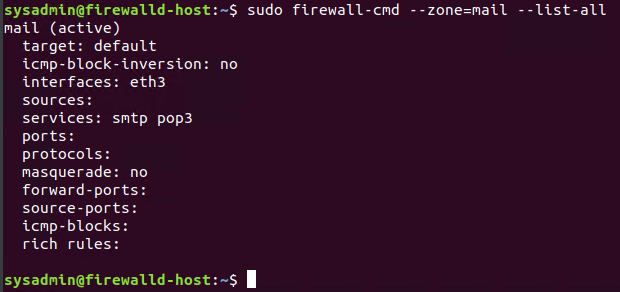
Run the command that lists all of the rule settings. Do one command at a time for each zone.  
  
$ **sudo firewall-cmd --zone=public --list-all**



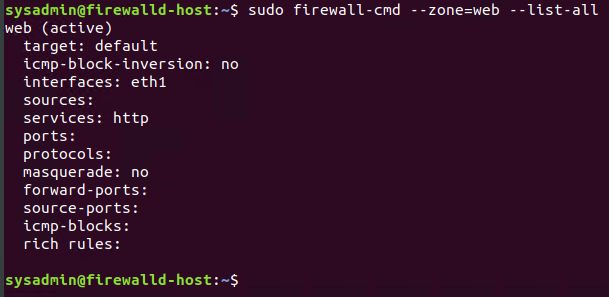
$ **sudo firewall-cmd --zone=sales --list-all**

****

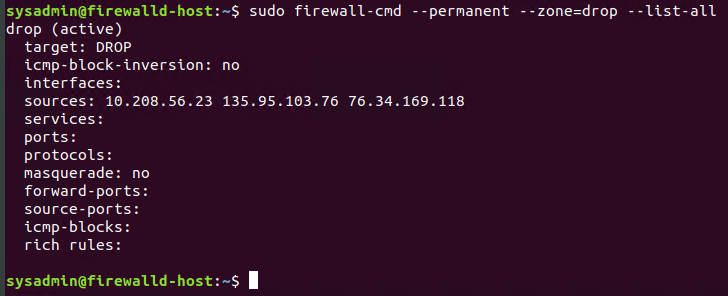
$ **sudo firewall-cmd --zone=mail --list-all**

****

$ **sudo firewall-cmd --zone=web --list-all**

****

$ **sudo firewall-cmd --permanent --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-based Intrusion Detection System (NIDS) → Monitors traffic at network level from all devices going in and out. It performs analysis on the traffic looking for patterns and abnormal behaviors upon which a warning is sent.**  
     
    Answer 2: **Host-based Intrusion Detection System (HIDS) → Monitors the entire network for system data and looks for malicious activity on an individual host. It can take snapshots, and if they change over time maliciously, an alert is raised. It also analyzes the changes management in the operating system logs, files, as well as the software and much more.**
2. Describe how an IPS connects to a network.  
     
    Answer: **An IPS is usually connected to a mirror port on a switch located directly behind the 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: **A Signature-based IDS is unable to detect zero-days, as it compares traffic from a set of predefined lists, and lacks the inherent functionality to filter anything outside of those domains.**
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 network intrusion detection plays a vital role in protecting networks against malicious activities.**

#### 

#### **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, & 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, spoofers.)**
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
   Answer: **Idk, network cards and route tracing (Trackers)**
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
     
   Answer: **Disk Encryption and Strong Passwords. For the mega-paranoid, a mandatory BIOS or UEFI password policy is a great idea. (Firmware encrypted password)**

#### **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: **There are few that are capable of TCP handshake → Circuit-Level Gateways, Stateful Inspection Firewalls, Proxy Firewalls (Application Level/Cloud), and Next-Generation Firewalls.**

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: **Stateful Inspection Firewalls**

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: **Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)**

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: **Packet-filtering firewalls**

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

Answer: **Next-Generation Firewalls (Data link / MAC filtering)**

### 

### **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: **Trojan Downloader of JS.Nemucod → which downloads and runs additional malicious files onto the system. These files are typically info-stealers.**

1. What was the adversarial motivation (purpose of attack)?  
     
    Answer: **Downloading malware including Teslacrypt, a variant of ransomware.**
2. 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? | **Active reconnaissance - A hacker uses system information to gain**  **unauthorized access to protected digital or electronic**  **materials, and may go around routers or even firewalls to**  **get it.** |
| **Weaponization** | What was it that was downloaded? | **Malware**  **Malicious software is injected into a system or network to do things the owner would not want done. Examples include: Logic**  **bombs, worms, viruses, packet sniffers (eavesdropping on a network).** |
| **Delivery** | How was it downloaded? | **Adversary-controlled delivery, which involves direct**  **hacking into an open port** |
| **Exploitation** | What does the exploit do? | **Install malware (a downloader) and download additional malware from the Internet, allowing attacker**  **command execution.** |
| **Installation** | How is the exploit installed? | **Possible malwares include ransomware and remote-access Trojans and other unwanted applications.** |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | **Made to look like benign traffic via falsified HTTP headers** |
| **Actions on Objectives** | What does the software that the attacker sent do to complete it's tasks? | **The attacker's final goal could be anything from extracting a**  **ransom from you in exchange for decrypting your files to**  **exfiltrating customer information out of the network.** |

Answer: **The attacker has sent a TROJAN malware via the HTTP port to gain access to the system, and install files to decrypt all the data and lock the system from providing any other access. Attackers can collect ransom to release the data and other files from the network.**

1. What are your recommended mitigation strategies?  
     
    Answer: **There are proposed five methods an organization can use to stop different stages of an attack. These are:**
   1. **Detect—determine attempts to scan or penetrate the organization**
   2. **Deny—stop attacks as they happen**
   3. **Disrupt—intercept data communications carried out by the attacker and interrupt them**
   4. **Degrade—create measures that will limit the effectiveness of an attack**
   5. **Deceive—mislead an attacker by providing false information or setting up decoy assets**
2. List your third-party references.  
     
    Answer:

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

**Submitted by: Ketan Vithal Patel**