## **Network Security**

### **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 Controls |

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

|  |
| --- |
| Management/Administrative Controls |

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

|  |
| --- |
| Operational/Technical Controls |

#### Intrusion Detection and Attack Indicators

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

|  |
| --- |
| IDS (Intrusion Protection System): designed to find threats to a system  IPS (Intrusion Prevention System): designed to protect systems from threats |

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

|  |
| --- |
| Indicator of attack (IOA): reveals that a threat is being taken place against a system  Indicator of compromise (IOC): reveals a threat, now a breach has occurred and the system is now compromised |

#### The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each.

1. Stage 1:

|  |
| --- |
| Reconnaissance: gather information. Let’s pretend someone is trying to hack into Netflix. Hackers may be trying to figure out who works there, what is their info, where is headquarters |

1. Stage 2:

|  |
| --- |
| Weaponization:the hackers develop malware to attack Netflix based on the information they gathered |

1. Stage 3:

|  |
| --- |
| Delivery: the hacker then finds a way to get their malware to people that have access to Netflix’s servers. This can be through phishing, tailgating into the building, etc. |

1. Stage 4:

|  |
| --- |
| Exploitation: the hackers get their malware into Netflix’s system |

1. Stage 5:

|  |
| --- |
| Installation: the hacker develops a backdoor so that he can access the system again without Netflix knowing. It is like leaving a window unlocked so the intruder of the house can get back inside later. |

1. Stage 6:

|  |
| --- |
| Command and Control: The hacker gains full control over the system and Netflix. This usually includes changing permissions of users to they no longer have access to the system |

1. Stage 7:

|  |
| --- |
| Actions on Objective: The hackers manipulate, gather, encrypt Netflix’s data to use for their own usually financial gain |

#### 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.

|  |
| --- |
| I highlighted the snort rule  Red:this is the action which is a notification  Orange:this is the transmission control protocol of the traffic rule  Yellow:this is the source IP or network  Green: this is the port of malicious traffic  Blue: this is the direction of traffic  Purple: this is the destination IP address  Pink:this is an optional scan rule  This is an alert that occurs whenever any information from an external network reaches our home network and send us a message “ET SCAN Potential VNC Scan 5800-5820” |

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

|  |
| --- |
| Exploitation. At this point the hackers (for instance) got an employee to open a website that tries to put malware in the system. If Netflix’s systems are strong and protected, the attack will be detected and prevented even though the employee exposed the system to malware |

1. What kind of attack is indicated?

|  |
| --- |
| This is a technical/operational attack - it looks like metadata was created |

**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.

|  |
| --- |
| This is another alert that occurs when external website information is sent to our network and it gives us the message, “ET POLICY PE EXE or DLL Windows file download HTTP” |

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

|  |
| --- |
| This is security layer 2: host protection |

1. What kind of attack is indicated?

|  |
| --- |
| Information downloaded from a http website onto your network |

**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 ip any 4444 -> $HOME\_NET any {msg: "Traffic Detected on Port 4444";} |

### **Part 2: “Drop Zone” Lab**

#### Set up.

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 |

#### 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 start firewalld  sudo systemctl enable firewalld |

|  |
| --- |
| **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.

|  |
| --- |
| sudo systemctl -state-firewalld |

#### 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:

|  |
| --- |
| sudo firewall-cmd --check-config |

* 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.

|  |
| --- |
| firewall-cmd --get-services |

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

#### Zone views.

* Run the command that lists all currently configured zones.

|  |
| --- |
| firewall-cmd --get-zones |

* 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.

|  |
| --- |
| firewall-cmd --permanent --new-zone=zone-web  firewall-cmd --permanent --new-zone=zone-sales  firewall-cmd --permanent --new-zone=zone-mail |

#### Set the zones to their designated interfaces.

* Run the commands that set your eth interfaces to your zones.

|  |
| --- |
| firewall-cmd --zone=zone-public --change-interface=<interface-ETH0>  firewall-cmd --zone=zone-web --change-interface=<interface-ETH1>  firewall-cmd --zone=zone-sales --change-interface=<interface-ETH2>  firewall-cmd --zone=zone-mail --change-interface=<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:

|  |
| --- |
| Firewall-cmd [--permanent] [--zone=public] [--permanent] --add-service=HTTP [--timeout=timeval]  Firewall-cmd [--permanent] [--zone=public] [--permanent] --add-service=HTTPS [--timeout=timeval]  Firewall-cmd [--permanent] [--zone=public] [--permanent] --add-service=POP3 [--timeout=timeval]  Firewall-cmd [--permanent] [--zone=public] [--permanent] --add-service=SMTP [--timeout=timeval] |

* web:

|  |
| --- |
| Firewall-cmd [--permanent] [--zone=web] [--permanent] --add-service=HTTP [--timeout=timeval] |

* sales:

|  |
| --- |
| Firewall-cmd [--permanent] [--zone=sales] [--permanent] --add-service=HTTPS [--timeout=timeval] |

* mail:

|  |
| --- |
| Firewall-cmd [--permanent] [--zone=mail] [--permanent] --add-service=SMTP [--timeout=timeval]  Firewall-cmd [--permanent] [--zone=mail] [--permanent] --add-service=POP3 [--timeout=timeval] |

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

|  |
| --- |
| active |

#### Add your adversaries to the drop zone.

* Run the command that will add all current and any future blacklisted IPs to the drop zone.

|  |
| --- |
| $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE>  $ <ADD COMMAND HERE> |

#### 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:

|  |
| --- |
| firewall-cmd --reload |

#### 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.

|  |
| --- |
| irewall-cmd --get-zones |

#### Block an IP address.

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

|  |
| --- |
| $ <ADD COMMAND HERE> |

#### 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 --zone=Web --list-all Sudo firewall-cmd --zone=Mail --list-all Sudo firewall-cmd --zone=Sales --list-all Sudo firewall-cmd --zone=public --list-all Sudo firewall-cmd --zone=drop --list-all |

#### 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.

|  |
| --- |
| firewall-cmd --list-all --zone=web  firewall-cmd --list-all --zone=sales  firewall-cmd --list-all --zone=mail  firewall-cmd --list-all --zone=drop  firewall-cmd --list-all --zone=public |

* 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.

|  |
| --- |
| DS physically connects via a network tap. 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. |

|  |
| --- |
| DS physically connects via mirrored port or SPAN.SPAN (Switched 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. |

1. Describe how an IPS connects to a network.

|  |
| --- |
| IPS physically connects inline with the flow of data. An IPS is typically placed in between the firewall and network switch |

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

|  |
| --- |
| Signature-based IDS |

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

|  |
| --- |
| Physical |

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

|  |
| --- |
| Technical |

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

|  |
| --- |
| Administrative |

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

|  |
| --- |
| Technical |

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

|  |
| --- |
| Technical |

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

|  |
| --- |
| Administrative |

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

|  |
| --- |
| Technical |

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

|  |
| --- |
| Encryption |

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

|  |
| --- |
| Secure Keys |

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

|  |
| --- |
| GPS tracking |

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

|  |
| --- |
| 2-Factor Authentication |

#### 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.

|  |
| --- |
| A next-generation firewall (NGFW) |

1. 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 inspection firewall |

1. 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-level gateway |

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?

|  |
| --- |
| Packet Filtering Firewalls |

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

|  |
| --- |
| MAC Layer Firewalls |

### **“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?*)

|  |
| --- |
| An alert message was created that there was a document downloaded to our network |

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

|  |
| --- |
| Put malware onto the computer |

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** | How did the attacker locate the victim? | Passive Reconnaissance |
| **Weaponization** | What was downloaded? | Windows file (malware) |
| **Delivery** | How was it downloaded? | Email through EXE files |
| **Exploitation** | What does the exploit do? | Steals information |
| **Installation** | How is the exploit installed? | It runs in the background as attachment is opened |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | The malware connects to the hacker and sends back information |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | Compress the files |

1. What are your recommended mitigation strategies?

|  |
| --- |
| IDS system |