|  |
| --- |
| Cybersecurity |
| Module 11 Challenge Submission File |

## Network Security Homework

Make a copy of this document to work in, and then fill out the solution for each prompt below. Save and submit this completed file as your Challenge deliverable.

### 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 Access Controls/Physical security control**: Walls, bollards, fences, and guard dogs  **Surveillance Controls**: Cameras and lighting |

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

|  |
| --- |
| Security Awareness Programs: Security awareness programs are a type of administrative or organizational control.  BYOD Policies: BYOD policies are also administrative controls.  Ethical Hiring Practices: Ethical hiring practices are a form of personnel security control. |

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

|  |
| --- |
| Encryption: Encryption is a technical control used to protect data confidentiality.  Biometric Fingerprint Readers: Biometric fingerprint readers are a type of access control mechanism and fall under the category of physical controls (technical control)  Firewalls: Firewalls are a network security control that fall under the category of technical controls.  Endpoint security is a category of security controls that focuses on protecting endpoints, such as computers, laptops, and mobile devices, from potential threats. It typically involves a combination of technical controls, including antivirus software, anti-malware protection, host-based firewalls, and device encryption |

Intrusion Detection Systems (IDS): are type of technical controls and are designed to monitor network traffic, identify suspicious activities or potential security breaches, and generate alerts.

#### Intrusion Detection and Attack Indicators

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

|  |
| --- |
| Intrusion Detection System (IDS):   * IDS is a passive security system that monitors network traffic and analyzes it for signs of unauthorized activity, policy violations, or known attack patterns. * It detects potential intrusions by comparing network traffic against a database of known attack signatures or using behavior-based analysis techniques. * IDS generates alerts or notifications when suspicious activity is detected, but it does not take direct action to stop or prevent the attack.   Intrusion Prevention System (IPS):   * IPS is an active security system that not only detects but also takes immediate action to prevent or mitigate attacks in real time. * It actively monitors network traffic and can automatically respond to detected threats by blocking or dropping malicious traffic, reconfiguring network settings, or taking other pre-defined protective measures. * IPS incorporates the capabilities of an IDS by detecting attack signatures or using behavior-based analysis, but it goes a step further by actively intervening to prevent attacks from being successful. |

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

|  |
| --- |
| Indicator of attack (IOA)   * IOA focuses on identifying and detecting malicious activities that are indicative of an ongoing attack or an attempt to compromise a system. * IOAs are proactive in nature and are often derived from patterns, behaviors, or techniques commonly associated with specific types of attacks . * They are based on the understanding of attacker TTPs (Tactics, Techniques, and Procedures) and are typically designed to identify the early stages of an attack before any compromise or damage occurs. * Examples of IOAs include suspicious network traffic patterns, unauthorized system modifications, privilege escalation attempts, or abnormal user behavior.   Indicator of Compromise (IOC)  IOC, on the other hand, revolves around identifying specific artifacts or traces left behind by an attacker or a compromised system. IOCs are retrospective in nature and are usually derived from known malicious indicators, such as file hashes, IP addresses, domain names, or specific patterns within network traffic.   * IOCs are often obtained through threat intelligence feeds, security research, or incident response activities. * They serve as reference points to detect, or block known malicious entities and can help identify systems that have already been compromised. * Examples of IOCs include malware signatures, known malicious IP addresses, file names associated with specific attacks, or patterns within log files. |

#### The Cyber Kill Chain

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

1. Stage 1:

|  |
| --- |
| Reconnaissance: Attackers gather information about the target system or organization. For example, an attacker may scan the target's publicly available websites, search for email addresses, or perform WHOIS lookups to identify potential entry points. |

1. Stage 2:

|  |
| --- |
| Weaponization: Attackers craft a malicious payload or select an existing exploit to deliver to the target. For instance, an attacker may embed a malicious payload in a seemingly innocent-looking email attachment or create a weaponized document containing a macro virus |

1. Stage 3:

|  |
| --- |
| Delivery: Attackers deliver the weaponized payload to the target, typically through methods like email attachments, malicious links, or infected websites. An example is a phishing email that entices the recipient to click on a link, leading to a website hosting malware. |

1. Stage 4:

|  |
| --- |
| Exploitation: The weaponized payload or exploit code is executed on the target system to gain unauthorized access or control. For example, an attacker may exploit a vulnerability in a software application to install a backdoor or gain remote access to the target system. |

1. Stage 5:

|  |
| --- |
| Installation: Attackers install malware or establish a foothold within the compromised system. This stage involves activities such as dropping and executing malicious files, creating persistence mechanisms, or establishing command and control channels. |

1. Stage 6:

|  |
| --- |
| Command and Control (C2): Attackers establish a communication channel between the compromised system and their infrastructure. This enables them to remotely control the compromised system and exfiltrate data or issue further instructions. An example could be a compromised system connecting to a remote server controlled by the attacker to receive commands. |

1. Stage 7:

|  |
| --- |
| Actions on Objectives: Once inside the target network, attackers pursue their primary objectives, which may vary depending on their motivations. It could involve data theft, unauthorized access, privilege escalation, lateral movement, or sabotage of systems. For instance, an attacker might exfiltrate sensitive data from compromised systems or disrupt critical services. |

#### 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

|  |
| --- |
| Alert: The action that snort will when triggered  Tcp : specifies protocol rule (will match TCP traffic)  $EXTERNAL\_NET any: represents external network “any” represent any port on the external network.  “->” : direction of the traffic  $Home\_Net: represents external network  5800:5820: specifies the destination port within the range of 5800 and 5820 |

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

|  |
| --- |
| Reconnaissance |

1. What kind of attack is indicated?

|  |
| --- |
| Emerging threat of Network SCAN (VNC Scan of port 5800-5820) |

**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.

|  |
| --- |
| Alert: The action that snort will when triggered  Tcp : specifies protocol rule (will match TCP traffic)  $EXTERNAL\_NET any: represents external network “any” represent any port on the external network.  “->” : direction of the traffic  $Home\_Net: represents external network |

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

|  |
| --- |
| Layer3: Delivery |

1. What kind of attack is indicated?

|  |
| --- |
| The 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 any -> $HOME\_NET 4444 (msg:"ET SCAN Potential VNC Scan 4444"; 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;) |

### Part 2: “Drop Zone” Lab

#### Set up.

Log into the Azure firewalld machine 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, 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  $ sudo systemctl start 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 firewall-cmd --state |

#### 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 –list-all |

* Take note of what zones and settings are configured. You may need to remove unneeded services and settings.

#### List all supported service type s 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 |

* Notice 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 |

* 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.

|  |
| --- |
| $ 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 –add-services=http –zone=public --permanent  $  $  $ |

* web:

|  |
| --- |
| sudo firewall-cmd –add-services=http –zone=web --permanent |

* sales:

|  |
| --- |
| $ sudo firewall-cmd –add-services=http –zone=sales --permanent |

* mail:

|  |
| --- |
| $ sudo firewall-cmd –add-services=http –zone=mail --permanent |

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

|  |
| --- |
| Sudo systemct1 status httpd  Sudo systemctl status postfix  Sudo systemctl status dovecot |

#### 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  $ <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:

|  |
| --- |
| $ sudo 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.

|  |
| --- |
| $ Sudo firewall-cmd –get-active-zones |

#### Block an IP address.

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

|  |
| --- |
| $ 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 ehco 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=sale --list-all  $ sudo firewall-cmd --zone=mail --list-all  $ sudo firewall-cmd --zone=web --list-all  $ |

* 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.

|  |
| --- |
| Inline IDS: Connect directly in line with network traffic, actively monitoring and intercepting packets in real-time |

|  |
| --- |
| Passive IDS: Connected to a copy of the network traffic, analyzing it without actively participating in the network flow. |

1. Describe how an IPS connects to a network.

|  |
| --- |
| An IPS connects to the network either through inline, bump-i-the-wire or through port mirroring/SPAN. It actively monitors and prevents threats in real-time, operates transparently and analyzes copies traffic respectively. |

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

|  |
| --- |
| Signature-based IDS: relies on a database of known attack signatures or patterns. It compares the network traffic against these signatures to identify matches indicating potential attacks or malicious activities. |

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 or Behavior-based IDS: detects suspicious traffic by comparing it to a baseline and excels at identifying network probing and sweeping activities by identifying deviations from normal behavior. |

#### 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 security |

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

|  |
| --- |
| Intrusion Detection/Prevention system(IDS/IPS) |

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

|  |
| --- |
| Access Control and authentication |

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

|  |
| --- |
| Patch Management and System Hardening |

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

|  |
| --- |
| Network Security and DDOS mitigation |

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

|  |
| --- |
| User Awareness and Data Classification |

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

|  |
| --- |
| Network Security and IDS/IPS |

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

|  |
| --- |
| Disk Encryption: is a method of protecting data-at-rest on a hard drive by converting it into an unreadable format using cryptographic algorithms. |

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

|  |
| --- |
| Transport Layer security: These protocols provide secure and encrypted communication channels over networks, ensuring that data transmitted between systems remain confidential and protected from eavesdropping or tampering. |

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

|  |
| --- |
| Geolocation Tracking: enables the determination of the precise geographic location of a device, such as a laptop, by utilizing various techniques |
|  |

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

|  |
| --- |
| **Full Disk Encryption**: Implement full disk encryption on the laptop's internal hard drive. By encrypting the entire hard drive, including the operating system and user data, we’llensure that even if an attacker manages to boot from an external device, they won't be able to access the encrypted data without the encryption key or passphrase |

#### 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 Proxy |

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 packet filtering 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.

|  |
| --- |
| Proxy firewall |

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 firewall |

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

|  |
| --- |
| MAC Layer Firewall |

### Optional Additional Challenge 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?*)

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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? |  |
| **Weaponization** | What was downloaded? |  |
| **Delivery** | How was it downloaded? |  |
| **Exploitation** | What does the exploit do? |  |
| **Installation** | How is the exploit installed? |  |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? |  |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? |  |

1. What are your recommended mitigation strategies?

|  |
| --- |
| [Enter answer here] |

1. List your third-party references.

|  |
| --- |
| [Enter answer here] |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.