## **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 Controls
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?  
     
    Answer: Administration Controls
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
     
    Answer: Technical Controls

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

1. What's the difference between an IDS and an IPS?  
     
    Answer: as the name suggests, IDS is a detection system and IPS is a protection system. While IDS provides information about the access, whereas IPS would act as per the rule set.
2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
     
    Answer: The Indicator of Attack (IOA) is a real time evidence of an event while it is unfolding whereas the Indicator of Compromise (IOC) is a post event evidence. IOA involves contextual attributes, knowledge from IOCs of similar pattern and also the organisational risk and intelligence to build response strategies..

#### **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 - Harvesting Information from websites like Facebook or DNS registration
2. Stage 2: Weaponisation - Coupling exploit with the backdoor to deliver the payload like RAT
3. Stage 3: Delivery - Delivering the weaponised payload to the victim by means such as eMail, USB etc.
4. Stage 4: Exploitation - Exploiting the vulnerability to execute the code on the victim’s machine like using crusher.exe in a pdf file to gain persistence.
5. Stage 5: Installation - Installing malware on the victim’s machine, lick user clicking on the email attachment
6. Stage 6: Command & Control (C2) - Command channel for remote manipulation of victim by using IRC or alike to establish a connection to the attacker’s server
7. Stage 7: Actions on Objectives - With access to the victim’s machine, intruders accomplish their objectives - like harvesting the private information of the victim.

#### **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:
   1. Header is - alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820
      1. This is rule alerts with any tcp communication from $EXTERNAL\_NET on any port to $HOME\_NET on any ports between 5800 to 5820
   2. Breakdown:
      1. alert - action of the rule
      2. tcp - rule applies to all TCP traffic
      3. $EXTERNAL\_NET - applies the rule to packets coming from source IP address
      4. any - applies rule to packets coming from any source port
      5. -> - direction of traffic
      6. $HOME\_NET - applies the rule to packets with this destination IP address
      7. 5800:5820 - applies the rule to the packets with this destination port range
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: This is a VNC scan which comes to gathering information to exploit which is Stage 1 - Reconnaissance.
3. What kind of attack is indicated?  
     
    Answer: This is a passive attack which is trying to learn about the system to see if those VNC ports are open. This is a snooping attack trying to port sniff. This is an emerging threat as indicated in the message.

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:
   1. Header is - alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any
      1. This rule triggers an alert when there is tcp traffic from $EXTERNAL\_NET on $HTTP\_PORTS to any port on $HOME\_NET. As per the options set, it is looking for any exe downloads over http.
   2. Breakdown:
      1. alert - action of the rule
      2. tcp - rule applies to all TCP traffic
      3. $EXTERNAL\_NET - applies the rule to packets coming from source IP address
      4. $HTTP\_PORTS - applies rule to packets coming from these source ports
      5. -> - direction of traffic
      6. $HOME\_NET - applies the rule to packets with this destination IP address
      7. any - applies the rule to the packets to any destination port
2. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: As I guess this is an attempt to deliver the payload, it is state 3 - Delivery.
3. What kind of attack is indicated?  
     
    Answer: This is an active attack trying to modify the system resources

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.  
    
   Answer: alert any any -> $HOME\_NET 4444 (msg:”"Potentially Bad Traffic”;sid:1000001;rev=1;)

### **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 systemctl status ufw && sudo systemctl stop 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

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

#### **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:  
    
   $ firewall-cmd --list-all #This command will list the rules for the default zone

$ firewall-cmd --list-all-zones #This command will list all rules in all zones.

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

Here is the list of all zones and settings configured:

* + block
  + target: %%REJECT%%
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services:
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + dmz
  + target: default
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services: ssh
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + docker (active)
  + target: ACCEPT
  + icmp-block-inversion: no
  + interfaces: docker0
  + sources:
  + services:
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + drop
  + target: DROP
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services:
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + external
  + target: default
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services: ssh
  + ports:
  + protocols:
  + masquerade: yes
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + home
  + target: default
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services: ssh mdns samba-client dhcpv6-client
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + internal
  + target: default
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services: ssh mdns samba-client dhcpv6-client
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + public (active)
  + target: default
  + icmp-block-inversion: no
  + interfaces: enp0s3
  + sources:
  + services: ssh dhcpv6-client
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + trusted
  + target: ACCEPT
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services:
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:
  + work
  + target: default
  + icmp-block-inversion: no
  + interfaces:
  + sources:
  + services: ssh dhcpv6-client
  + ports:
  + protocols:
  + masquerade: no
  + forward-ports:
  + source-ports:
  + icmp-blocks:
  + rich rules:

#### **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 --get-zones # gives the list of all configured zones

$ sudo firewall-cmd --list-all-zones #gives the list of all zones along with the rules configured within

* 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 creates 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

Firewalld service need to be reloaded with the command: sudo firewall-cmd --reload

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

Run the commands that sets 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 --zone=public --add-service=http

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

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

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

* Web:  
    
   $ sudo firewall-cmd --zone=Web --add-service=http
* Sales  
    
   $ sudo firewall-cmd --zone=Sales --add-service=https
* Mail  
    
  $ sudo firewall-cmd --zone=Mail --add-service=pop3

$ sudo firewall-cmd --zone=Mail --add-service=smtp

* What is the status of http, https, smtp and pop3? They are all enabled in the public zone.

#### **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 --zone=drop --add-rich-rule='rule family="ipv4" source address="10.208.56.23" reject'

$ sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source address="135.95.103.76" reject'

$ sudo firewall-cmd --zone=drop --add-rich-rule='rule family="ipv4" source address="76.34.169.118" reject'

OR

$ sudo firewall-cmd --zone=drop --add-source=10.208.56.23

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

$ sudo firewall-cmd --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 ensure 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 --runtime-to-permanent && sudo firewall-cmd --reload

#### **View active Zones**

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

* Run the command that displays all zone services.  
    
  $ sudo firewall-cmd --get-active-zones #This will list all the active zones

$ sudo firewall-cmd --list-services #This will list all the active services

#### **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 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=Web --list-all

$ sudo firewall-cmd --zone=Sales --list-all

$ sudo firewall-cmd --zone=Mail --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-Tap - 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  
    Answer 2: SPAN (Switch Port Analyser) in otherwards 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.  
     
    Answer: IPS connects inline with the flow of the traffic typically between firewall and the core switch.
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
     
    Answer: signature-based IDS
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:Anomoly-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.  
        
       Answer: Physical
   2. A zero-day goes undetected by antivirus software.  
        
       Answer: Technical - Endpoint Security
   3. A criminal successfully gains access to HR’s database.  
        
       Answer: Technical - Data Security
   4. A criminal hacker exploits a vulnerability within an operating system.  
        
       Answer: Technical
   5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.  
        
       Answer: Technical
   6. Data is classified at the wrong classification level.  
        
       Answer: Administrative
   7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
        
       Answer: Technical
2. Name one method of protecting data-at-rest from being readable on hard drive.  
     
    Answer: Encryption
3. Name one method to protect data-in-transit.  
     
    Answer: Hashing & Encryption
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
    Answer: GPS or systems like Find my Device if enabled
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
     
    Answer: Disk encryption like BitLocker

#### **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: Stateful Firewall & Circuit-Level Gateway Firewall

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 Firewall

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: Application or 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?

Answer: Stateless Firewall

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

Answer: MAC layer filtering 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 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:

1. What was the adversarial motivation (purpose of attack)?  
     
    Answer:
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? |  |
| **Weaponization** | What was it that 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 it's tasks? |  |

Answer:

1. What are your recommended mitigation strategies?  
     
    Answer:
2. List your third-party references.  
     
    Answer: