## **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: These forms of security are all physical.
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?  
     
    Answer: This is a form of management control.
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
     
    Answer: This is a form of operational security.

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

1. What's the difference between an IDS and an IPS?  
     
    Answer: The differences between an IDS and IPS is that an IDS is a form of detecting problems and ips is a form of preventing these security risks from ever happening.
2. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
     
    Answer: The difference between the two is that an attack is an attempt to compromise and the compromise is a successful attempt of an attack.

#### **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: The first step is to perform reconnaissance on the target that is chosen to be attacked by investigating the target before an attack. This may include searching for some of the ports that may be open for incoming information on the system.
2. Stage 2: The second step is to perform weaponization, which is creating a form of attack from the vulnerabilities found from reconnaissance. This step would include creating a type of malware that would fit this person's vulnerabilities on their system.
3. Stage 3: The third step is to perform some type of way to deliver the weaponization of the attack. This step would include a way to deliver the malware such as email or personal message.
4. Stage 4: The fourth stage would be to exploit the vulnerabilities after delivering the attack. This step would include the attack actually going into effect when the target has clicked on the malware attack and begins performing the attack through those actions.
5. Stage 5: This fifth step is when the malware has successfully installed an entrance for the attacker through the vulnerabilities and delivery method for the attacker. This would be an example if the attacker successfully installed a backdoor for attack.
6. Stage 6: The sixth step is that the attacker has successfully made their way into the network through the backdoor and now has open access. This means that the backdoor has worked and the attacker can now target the data being targeted.
7. Stage 7: The last and final step is actually taking action on the objective. This would include the target actually taking the attack on the target to possibly stealing data of etc.

#### **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: The header of the snort rule is stating that it would like to look at the tcp protocols on the ip of EXTERNAL\_NET at any port with the destination port of HOME\_NET with the response port of 58000-5820 with the message of an ET Scan Potential VNC.
2. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: This would be a form of reconnaissance of the destination IP of HOME\_NET.
3. What kind of attack is indicated?  
     
    Answer: This form of attack on (Virtual Network Computing) which looks at the memory of network monitoring using the VNC.

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 Snort Rule header and explain what is happening.  
     
    Answer: The snort rule is looking for tcp protocols on EXTERNAL\_NET ip looking for TCP on HTTP\_Ports with the destination of HOME\_NET ip on any port with the message of ET policy PE exe or DLL windows files downloaded via http.

1. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: This is a form of delivery.
2. What kind of attack is indicated?  
     
    Answer: This indicates a form of cross site scripting.

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: The alert would be: alert tcp $EXTERNAL\_NET any -> $HOME\_NET 4444 (msg:"gg no re")

### **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.  
    
   $ <ADD COMMAND HERE> udo ufw disable && sudo killall ufw ; sudo systemctl disable 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.  
  
 $ Command: 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.  
    
   $Command: 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:  
    
   $ Command; 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  
    
   Command: 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.  
    
   Command; sudo firewall-cmd --get-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 creates Web, Sales and Mail zones.  
  
Command1;sudo firewall-cmd --permanent --new-zone=web

Command2: sudo firewall-cmd --permanent --new-zone=sales

* Command3:sudo firewall-cmd --permanent --new-zone=mail

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

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

2.sudo firewall-cmd --zone=web --change-interface=eth0

3.sudo firewall-cmd --zone=sales --change-interface=eth0

* sudo firewall-cmd --zone=mail --change-interface=eth0

#### **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:  
1.sudo firewall-cmd --zone=public --add-service=http

2.sudo firewall-cmd --zone=public --add-service=https

3.sudo firewall-cmd --zone=public --add-service=pop3

4.sudo firewall-cmd --zone=public --add-service=smtp

* Web:  
    
  1.sudo firewall-cmd --zone=web --add-service=http
* Sales  
  1.sudo firewall-cmd --zone=sales --add-service=https

Mail  
  
1.sudo firewall-cmd --zone=mail --add-service=smtp

* sudo firewall-cmd --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.  
  
1.sudo firewall-cmd --zone=drop --add-source=10.208.56.23

2.sudo firewall-cmd --zone=drop --add-source=135.95.103.76

3.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 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  
    
  1.sudo firewall-cmd --reload> - if 'permanent' flags not used

2.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.  
    
  1.sudo firewall-cmd -list-all-zones

#### **Block an IP address**

* Use a rich-rule that blocks the IP address 138.138.0.3.  
    
  1. sudo firewall-cmd --permanent --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.  
    
  1. sudo firewall-cmd --zone=public --add-icmp-block=echo-reply

#### **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.  
  
1.sudo firewall-cmd --zone=public --list-all>

2.sudo firewall-cmd --zone=web --list-all>

3.sudo firewall-cmd --zone=sales --list-all>

4.sudo firewall-cmd --zone=mail --list-all>

* sudo firewall-cmd --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 in 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 detection system => monitors network traffic, looking for abnormal patterns and behaviors.  
    Answer 2: Host based detection system => monitors a system, looking for malicious activity.
2. Describe how an IPS connects to a network.  
     
    Answer:An IPS is usually 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 stateless IDS is unable to detect zero-days, as it compares traffic form a set of predefined hot and cold lists, and lacks the inherent functionality to filter anything outside of those domains.
4. :Technical NetworkWhich 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: A stateful IDS is useful in detecting new exploits. While they are generally more bloated than their stateless counterparts, they offer a more robust set of tools in analyzing system traffic.

#### **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 physical
   2. A zero-day goes undetected by antivirus software.  
        
       Answer:Technical Software
   3. A criminal successfully gains access to HR’s database.  
        
       Answer:Technical Software
   4. A criminal hacker exploits a vulnerability within an operating system.  
        
       Answer: Technical Software
   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
   7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
        
       Answer:Administrative Network
2. Name one method of protecting data-at-rest from being readable on hard drive.  
     
    Answer: encryption of the hard drive
3. Name one method to protect data-in-transit.  
     
    Answer:Data Encryption
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
    Answer:A tracking software
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
     
    Answer:A Strong 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: Stateless Network 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, do these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?

Answer: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:Packet-filtering firewall

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

Answer:Data link Firewall