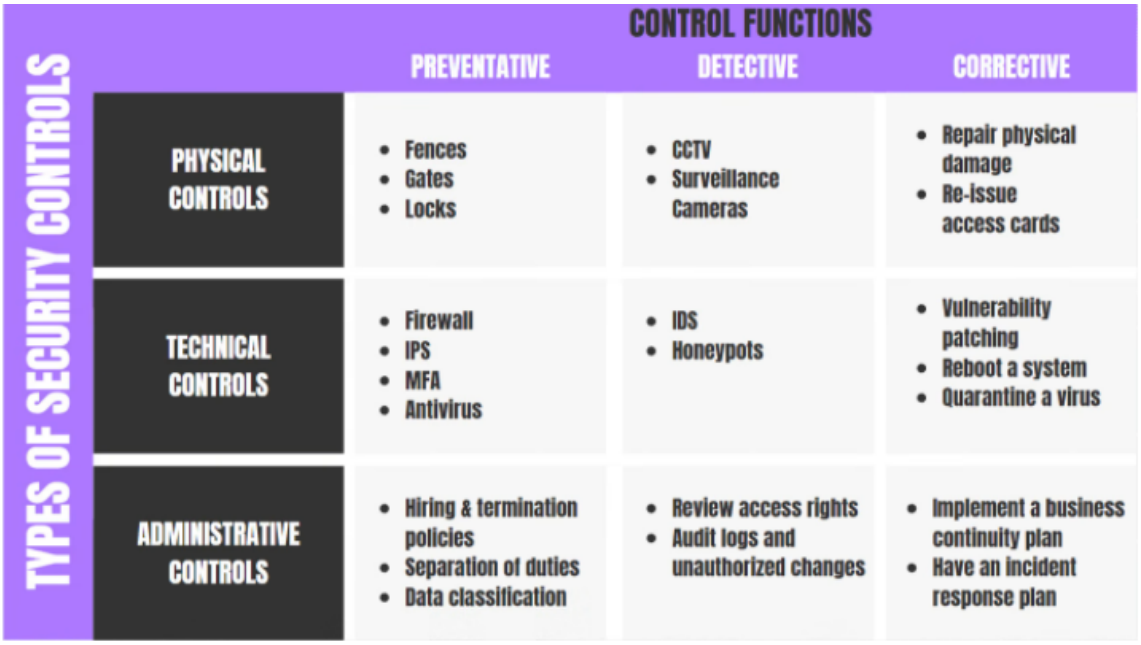
Week 11 Homework: Network Security

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: Administrative Controls
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?
   Answer: Technical Controls



Reference Materials: https://purplesec.us/security-controls/

Intrusion Detection and Attack indicators

1. What's the difference between an IDS and an IPS?
   Answer: An Intrusion Detection System (IDS) is a tool that "obviously" detects anything but fortunately most companies/vendors provide an array of signatures/methods for detecting the "stuff" they need. The stuff or what will depend based on the company along with their goals and needs which will ultimately also depend on their network. However, simply put IDS's looks through the traffic and detects what you don't want including what is written in polices along with misuse such as gaming, shopping, watching shows, listening to music or even the latest malwares. Monitoring traffic eat the ingress/egress points will show what comes and goes; however it is important to note that it is usually on internal traffic that it can monitor, it can't monitor remote stations or offices that connect to the core components. IDS's will typically on monitor traffic internally not via guest networks or what is on the public side of the firewall.

   An Intrusion Prevent System (IPS) is an IDS in most regards except for the fact that it can take action on current traffic. IPS actions include drop, reset, shun or custom scripted actions which would occur immediately upon that signature/method being noticed. But the issue is that it can't recognize the difference between legitimate and illegitimate traffic which could have a negative impact on the company such is loss in revenue. It is a great tool but it has to be leveraged with the key components that differentiate the IPS. It is important that if are utilizing an IPS that you make sure device is capable of a "failing open" which means if any part of the application fails or even the chassis fails (power loss) the unit continues to pass traffic; we don't want the IPS to impede the flow of data. The signatures and methods need to be well defined so as to avoid false positives.

   Reference material: https://cybersecurity.att.com/blogs/security-essentials/ids-ips-and-utm-whats-the-difference

2. What's the difference between an Indicator of Attack and an Indicator of Compromise?

Answer: Indicators of Compromise (IOC) can be described in the forensics world as evidence on a computer that indicates that the security of the network has been breached. Investigators usually gather this data after being informed of a suspicious incident, on a scheduled basis, or after the discovery of unusual call-outs from a network. Ideally, this information is gathered to crate "smarter" tools that can det3ect and quarantine suspicious files in the future. In the Cyber world, an IOC is an MD5 has, a C2 domain or hardcoded IP address, a registry key, filename, etc. These IOC's are constantly changing making a proactive approach to securing the enterprise impossible. Because IOC's provide a reactive method of tracking the bad guys, when you find an IOC, there is a high probability that you have already been compromised.

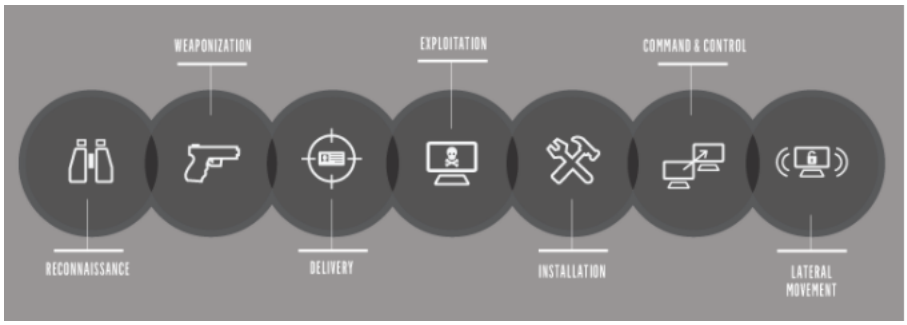
Indicators of Attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in the attack. A byproduct of the IOA approach is the ability to collect and analyze exactly what is happening on the network in real-time. The very nature of observing the behaviors as they execute is equivalent to observing a video camera and accessing a flight data recorder within your environment. So in retrospect IOA's provide content for video logs. In the cyber realm, showing you how an adversary slipped into your environment, accessed files, dumped passwords, moved laterally and eventually exfiltrated your data is the power of an IOA.

Reference Material: https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/#:~:text=Unlike%20Indicators%20of%20Compromise%20(IOCs,exploit%20used%20in%20an%20attack

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—The attacker/intruder chooses their target. Then they conduct in-depth research on the target to identify its vulnerabilities that can be eventually exploited.
2. **Stage 2**: Weaponization—The attacker/intruder creates a malware weapon (virus, worm, etc.) to exploit the vulnerabilities of the target. Depending on the target and the intent or purpose of the attacker/intruder, the malware can exploit new or undetected vulnerabilities (zero-day exploits) or it can focus on a combination of different vulnerabilities.
3. **Stage 3**: Delivery—The attacker/intruder will transmit the weapon to the target. The attacker/intruder can employ a variety of methods such as a USB, e-mail attachment or websites.
4. **Stage 4**: Exploitation—The malware starts its purpose; the program code of the malware is triggered to exploit the target's vulnerability(ies).
5. **Stage 5**: Installation—The malware installs an access point for the attacker/intruder which is it's backdoor.
6. **Stage 6**: Command and Control—The malware gives the attacker/intruder access to the target's network/system.
7. **Stage 7**: Actions on Objective/Lateral Movement—Once the attacker/intruder gains persistent access, they will take the action necessary to fulfill their purpose such as encryption for ransom, data exfiltration or even data destruction.



Reference material: https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/#:~:text=The%20Cyber%20Kill%20Chain%20consists%20of%207%20steps%3A%20Reconnaissance%2C%20weaponization,find%20detailed%20information%20on%20each

https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/#:~:text=Unlike%20Indicators%20of%20Compromise%20(IOCs,exploit%20used%20in%20an%20attack

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.

alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820

Rule Header	alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any

Answer: Traffic is coming from the internet, remote host, and coming into the internal network where it attempted to scan, on ports ranging from 5800-8520 using TCP/IP protocol with a potential ET SCAN issue.

Rule Header: The alert tells Snort what to do when it finds a packet that matches the rule criteria (usually alert); the tcp (type of traffic protocol)-there are 4 protocols that Snort currently analyzes for suspicious behavior (tcp, udp, icmp, & ip); $External_Net shows if the source address(es) are variable or literal; the $HTTP_Ports shows if the source port(s) are variable or literal; the -> shows the Direction operator which indicates the orientation of the traffic to which the rule applies; $Home_Net shows if the destination address is variable or literal; finally any shows the if the destination port(s) are variable or literal.

2. What stage of the Cyber Kill Chain does this alert violate?

Answer: Reconnaissance

3. What kind of attack is indicated?

Answer: 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;)

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"
```

1. Break down the Sort Rule header and explain what is happening.

   Answer: The remote host, through http ports, 80/443, coming into our internal network attempted a download to any port of the local machine which was violating a policy.

2. What layer of the Defense in Depth model does this alert violate?

   Answer: Delivery

3. What kind of attack is indicated?

   Answer: Potential malware 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.

  Answer: alter tcp $EXTERNAL_NET any -> $HOME_NET 4444 (msg: "potential malware/default Metasploit port")

Reference material: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/116/original/Snort_rule_infographic.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210217%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210217T174125Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=ff3e6b5f7428e1aaa62f508c4f6da8074819f849a207e81698e774a0bf7e0253

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.

```
sysadmin@firewalld-host:~$ sudo apt-get --purge remove ufw
[sudo] password for sysadmin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  ufw*
0 upgraded, 0 newly installed, 1 to remove and 592 not upgraded.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
(Reading database ... 221797 files and directories currently installed.)
Purging configuration files for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for systemd (237-3ubuntu10) ...
Processing triggers for rsyslog (8.32.0-1ubuntu4) ...
```

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.

```
sysadmin@firewalld-host:~$ sudo systemctl enable firewalld
Synchronizing state of firewalld.service with SysV service script with /lib/systemd/systemd-sysv-instal
l.
Executing: /lib/systemd/systemd-sysv-install enable firewalld
sysadmin@firewalld-host:~$ sudo su
root@ubuntu-desktop-base:/home/sysadmin# systemctl start firewalld.service
You have new mail in /var/mail/root
```

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.

```
root@ubuntu-desktop-base:/home/sysadmin# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset
   Active: active (running) since Wed 2021-02-17 12:42:34 EST; 58min ago
     Docs: man:firewalld(1)
 Main PID: 815 (firewalld)
    Tasks: 2 (limit: 4648)
   CGroup: /system.slice/firewalld.service
           └─815 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid
```

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:

Take note of what Zones and settings are configured; you many need to remove unneeded services & 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

```
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-test
net bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns dock
er-registry docker-swarm dropbox-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication f
reeipa-trust ftp ganglia-client ganglia-master git high-availability http https imap imaps ipp ipp-clie
nt ipsec irc ircs iscsi-target kadmin kerberos kibana klogin kpasswd kprop kshell ldap ldaps libvirt li
bvirt-tls managesieve mdns minidlna mosh mountd ms-wbt mssql murmur mysql nfs nfs3 nrpe ntp openvpn ovi
rt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql p
rivoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh rsyncd samba samba-clie
nt sane sip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy syslog sy
slog-tls telnet tftp tftp-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bos
h xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
You have new mail in /var/mail/root
```

Note: We can see that the Home and Drop Zones are created by default.

Zone Views

- Run the command that lists all currently configured zones.

```
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --list-all-zones
```

Block	**Dmz**	**Drop**
External	**Home**	**Internal**
Public	**Trusted**	**Work**

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.

```
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --permanent --new-zone=web
success
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --permanent --new-zone=sales
success
You have new mail in /var/mail/root
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --permanent --new-zone=mail
success
root@ubuntu-desktop-base:/home/sysadmin#
```

Set the zones to their designated interfaces:

- Run the commands that sets your eth interfaces to your zones.

```
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=public --change-interface
=eth0
The interface is under control of NetworkManager, setting zone to 'public'.
success
You have new mail in /var/mail/root
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=web --change-interface=et
h0
The interface is under control of NetworkManager, setting zone to 'web'.
success
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=sales --change-interface=
eth0
The interface is under control of NetworkManager, setting zone to 'sales'.
success
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=mail --change-interface=e
th0
The interface is under control of NetworkManager, setting zone to 'mail'.
success
```

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:

```
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=public --add-service=http
success
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=public --add-service=http
s
success
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=public --add-service=pop3
success
You have new mail in /var/mail/root
root@ubuntu-desktop-base:/home/sysadmin# firewall-cmd --zone=public --add-service=smtp
success
```

- Web: (would be in root so don't need sudo)
  $ firewall-cmd –zone=web –add-service=http
- Sales: (would be in root so don't need sudo)
  $ firewall-cmd --zone=sales --add-service=https
- Mail: (would be in root so don't need sudo)
  $ firewall-cmd --zone=mail --add-service=smtp
  $ firewall-cmd --zone=mail --add-service=pop3

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

Answer: Could not complete in Azure so wrote out the commands as I think they should be.

Add your adversaries to the Drop Zone (would be in root so don't need sudo)

- Run the command that will add all current and any future blacklisted IPs to the Drop Zone. **(Would be in root so don't need sudo)**
  $ firewall-cmd --zone=drop --add-source=…
  $ firewall-cmd --zone=drop --add-source=…
  $ firewall-cmd --zone=drop –add-source=…

Make rules permanent then reload them (would be in root so don't need sudo)

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
  $ firewall-cmd –reload -if 'permanent' flags not used
  $ firewall-cmd --runtime-to-permanent && firewall-cmd --reload

View active Zones (would be in root so don't need sudo)

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.
  $ firewall-cmd --list-all-zones

Block an IP address (would be in root so don't need sudo)

- Use a rich-rule that blocks the IP address 138.138.0.3.
  $ firewall-cmd --permanent --add-rich-rule="rule family="ipv4' source

Block Ping/ICMP Requests (would be in root so don't need sudo)

Harden your network against ping scans by blocking icmp ehco replies.

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

Rule Check (would be in root so don't need sudo)

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 --zone=public --list-all
  $ firewall-cmd --zone=web --list-all
  $ firewall-cmd --zone=sales --list-all
  $ firewall-cmd --zone=mail --list-all
  $ 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.

Answer: Could not complete in Azure so wrote out the commands as I think they should be.

Reference Material: https://www.thegeekdiary.com/centos-rhel-7-firewalld-command-line-reference-cheat-sheet/
https://cheatography.com/mikael-leberre/cheat-sheets/firewall-cmd/
https://stackoverflow.com/questions/42293872/ansible-firewalld-and-adding-new-zone
https://firewalld.org/documentation/howto/add-a-service.html

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: NIDS, Network-based Intrusion Detection System, is utilized to examine network traffic. Anti-theft software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected. NIDS have to include a packet sniffer to gather network traffic for further analysis. Then they analyze the flow of information between computers. They essentially "sniff" the network for suspicious behavior. You can also add your own rules and modify the analysis engine. NIDS excel in their ability to protect hundreds of computer systems from one network location. NIDS are less expensive and fairly easily to deploy. NIDS also allow administrators to protect non-computer devices, such as firewalls, print servers, routers, etc and can work with multiple operations systems and devices. Essentially "NIDS" can detect a hacker before they are able to make an unathorized intrusion.

   Answer 2: HIDS, Host intrusion detection system, you will find anti-threat applications such as firewalls, antivirus software and spyware-detection programs that are installed on every network computer that has two-way access to the outside environment i.e. the internet. They HID will monitor and analyze system configurations and applications activities; they can be installed on any device, regardless of wheather it's a desktop PC or a server. The sensors take a snapshot of existing system files and compare them with previous snapshots. They look for unexpected changes, such as overwriting, deletion and access to certain ports. Consequently, alerts are sent to administrators to investigate activities that seem "iffy". They are highly effective tool against insider threats. HIDS can identify file permission changes and unusual client-server requests, which generally tend to be a perfect concoction for internal attacks. That's why it should come as no surpirise that HIDS is often used for mission-critical machines that are not expected to change.

   Ideally, a corporate network should feature both a. HID and a NID. Both are capable of providing more security than any single firewall or anti-virus suite, but each lacks certain capabilities that the other contains. Thus, combining the two is the only way to create a truly robust defensive network.

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 will be unable to detect the Zero-Day attack because it only compares traffic from a set of predefined set of signatures/methods and does not inherently function 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: A stateful IDS is useful in detecting new exploits.

Reference Material: https://searchsecurity.techtarget.com/definition/HIDS-NIDS
https://www.techwalla.com/articles/description-of-the-difference-between-hids-nids
https://securityboulevard.com/2020/03/intrusion-detection-systems-a-deep-dive-into-nids-hids/

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 Control

   2. A zero-day goes undetected by antivirus software.

Answer: Technical Control (Software)

3. A criminal successfully gains access to HR's database.

   Answer: Technical Control (Network)

4. A criminal hacker exploits a vulnerability within an operating system.

   Answer: Technical Control (Software)

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

   Answer: Technical Control (Network)

6. Data is classified at the wrong classification level.

   Answer: Administrative Control

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

   Answer: Administrative Control

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

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

   Answer: IDK, network cards and route tracing

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

   Answer: Disk encryption and use of strong passwords (hopefully there is a strong password policy in place)

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

2. 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

3. 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 Firewall

4. 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

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

Answer: Data Link Firewall