Final Exam

- **Due** Dec 13 at 11:59pm
- **Points** 94
- **Questions** 11
- **Available** Dec 9 at 12am - Dec 14 at 11:59pm
- **Time Limit** 360 Minutes

Instructions

The full mark for final exam is 94.

For any diagrams or figures it is highly recommended you use a computer-based drawing program (e.g., Google Drawings, Diagrams.net, Visio, etc.).

All answers require a minimum of a short paragraph. A short paragraph should be at least three sentences and no more that ten.

Grammar, punctuality, spelling, and general academic professionalism count. You must proofread your work and it is highly recommended that you use a separate program (e.g. Google Docs, Grammarly) to double check your answer before pasting into the answer box.

This quiz was locked Dec 14 at 11:59pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	268 minutes	94 out of 94

Correct answers are hidden.

Score for this quiz: **94** out of 94
Submitted Dec 13 at 9:56pm

This attempt took 268 minutes.

Question 1

4 / 4 pts

If a malicious node knows the IP addresses and port numbers of the communication parties, and range of the sequence numbers in the receiver’s window in a TCP connection, it can conduct blind reset attack. Please answer: what is a blind reset attack on TCP and how can an attacker conduct it? Optionally you may attach a diagram to support your answer.

Your Answer:

An attacker can break up an active TCP connection via a blind reset attack by delivering a faked TCP reset (RST) packet to any or both of the communication participants. As long as the attacker is aware of the communication parties' IP addresses, port numbers, and the range of sequence numbers displayed in the receiver's window, they may carry out this action from any location on the internet. The attacker first gathers this information by keeping an eye on network traffic, then utilizes it to create a fake reset packet and transmit it to the communication parties to carry out the attack. As a result, services that depend on the connection and continuing communication may be affected. Network security and safe TCP implementations are crucial for preventing this kind of attack. By using encryption and other security measures, this is possible. By encrypting the communication and making it harder for attackers to access the information required to carry out the attack, employing secure protocols, such as HTTPS or SSL, can, for instance, assist guard against blind reset assaults. Installing firewalls and other security measures can also aid in preventing attackers from being able to observe network traffic and get the required data.

The security and resistance to similar assaults of TCP implementations must also be ensured. This may be achieved by periodically testing and auditing TCP implementations to find and fix any potential vulnerabilities, as well as by keeping TCP implementations up to date with the most recent security patches and upgrades.

Organizations may assist defend against blind reset attacks and guarantee the security of their networks and communications by adopting following actions. The security of networks and communications is overall seriously threatened by a blind reset attack on TCP. Organizations may defend against these attacks and retain the integrity of their communications by protecting the network and making sure that TCP implementations are secure.

Question 2

4 / 4 pts

IP fragmentation, if implemented poorly, can be used to conduct resource exhaustion attacks (a type of DoS attack). The software will look at the offset and packet length of the fragment and allocate enough memory to hold the whole packet. Please describe how such attack is conducted. For example, the attacker will send out a 120-Byte packet that will consume 64K byte of memory at the victim.

Your Answer:

The attacker creates several IP fragments with erroneous offset and packet length values in a resource exhaustion attack employing IP fragmentation. The victim's software tries to put these pieces back together into a single packet when it receives them. The program allots more memory than is required to retain the packet due to the erroneous offset and packet length parameters. As a result, a denial of service (DoS) attack may occur when the victim's machine suddenly exhausts its memory and stops functioning. An attacker initially creates a large number of IP fragments with erroneous offset and packet length parameters before launching the assault. The attacker can then use a network of compromised devices or directly give the victim these fragments. The victim will get the pieces, and their program will attempt to put them back together into a single packet by allocating more memory than is required. This can quickly exhaust the

victim's memory, rendering the system unavailable and essentially depriving genuine users of service.

Implementing IP fragmentation safely is crucial to preventing this kind of assault. This might involve checking the offset and packet length values of incoming fragments to make sure they are accurate and setting a RAM allocation limit for packet reassembly. In order to avoid and lessen DoS assaults, it is also crucial to put other security measures in place. Examples include rate limitation and intrusion detection and prevention systems.

Question 3

12 / 12 pts

To improve end user experience and reduce core network overhead, the concept of Content Distribution Network (CDN) was proposed. The basic idea is to set up many content buffers that are close to end users. Akamai is one of the major players in the CDN market.

To prevent network eavesdroppers from getting access to data during transmission, data encryption is often used in CDN. Please describe how Akamai handles delivery of encrypted contents from the following aspects:

(1) How are the two segments of data encryption, from content source to Akamai and from Akamai to end user, achieved?

(2) How can an end user verify that the contents are delivered by the original source?

(3) Does each end user have their own data encryption key with Akamai or is it a common key shared by all users?

Your Answer:

1. Data encryption is used by Akamai, a company that offers content delivery network (CDN) services, to safeguard material while it is sent from the source to end users. This stops network eavesdroppers from getting access to the data while it's being sent. Akamai combines secure transport protocols and encryption technologies to accomplish this. Akamai commonly employs HTTPS, a secure transport protocol, to encrypt data in transit during the initial segment of data encryption, from the content source to Akamai. This guarantees that the information is secure while it is sent from the source to Akamai's servers. In the second phase, Akamai delivers the material to the end user while encrypting it using a number of encryption techniques, including AES. As the information is sent from Akamai's servers to the end user's device, it is shielded from unwanted access.
2. End users have the option of using digital signatures or other authentication procedures to confirm that the material is coming from the original source. For instance, the original source may employ a digital signature to sign the material, which the user can then validate using the source's public key. This guarantees that the material was not changed or tampered with while in transit.
3. For data encryption in CDN, Akamai combines private and public keys. Each end user may have their own particular encryption key that is used to decode the material as it is delivered for some types of content, such as streaming video. Akamai may employ a common key that all users use for other material, including static web pages. This eliminates the requirement for unique keys for every user and enables Akamai to efficiently serve the material to a large number of users.

Question 4

12 / 12 pts

In Software Defined Networks (SDN), the controller needs to collect a lot of information from the switches that it manages and issue commands to them. Therefore, it is essential to keep the control channel open and available between the controller and the switches.

In the original implementation of SDN, the control channel and data channels share the same link, which leads to the potential of jamming attacks upon the controller.

Please describe:

(1) How is the jamming attack conducted?

(2) How can an attacker identify those links shared between data channels and control channel? (You can draw a figure to help you answer the first 2 sub-questions)

(3) How can we defend against such attacks?

Your Answer:

1. The goal of a jamming attack on an SDN controller is to prevent communication between the controller and the switches it oversees. The shared connection between the controller and the switches is overloaded by sending a lot of traffic there, which achieves the desired result of preventing the controller from transmitting orders to or receiving data from the switches. Using network scanning tools, an attacker can learn the controller's and switches' IP addresses and port numbers, and then send traffic to those addresses and ports.

2. It is advised to isolate the control channel from the data channel and utilize a dedicated connection for control communication to protect against jamming attempts. As a result, there is less chance of traffic congestion and the control channel is always open, even if the data channel is backed up or otherwise affected. Secure authentication and encryption can be implemented on the control channel to prevent unwanted access and defend against many forms of assaults.
3. Jamming assaults on SDN controllers may often be disruptive and challenging to protect against. Organizations may lower their risk of such attacks and protect the availability and integrity of their network control systems by putting the suggested security measures into practice.

Question 5

8 / 8 pts

Virtual Private Networks (VPN) are ubiquitous in our modern computing environment. Answer the following questions about VPN. Optionally you may attach a diagram to support your answer.

(1) What are the most important benefits of implementing a VPN? Explain your answer.

(2) What are some potential drawback of VPNs? Explain your answer.

Your Answer:

1. Data sent between a user's device and a VPN server is encrypted when it is transferred via a virtual private network (VPN). By obscuring the user's IP address and location and safeguarding important information from interception, this increases security and privacy. VPNs are advantageous for people in nations with strong internet regulations or for enterprises that must access restricted networks since they may get around internet censorship and access forbidden websites or services.
2. The use of VPNs might have certain disadvantages, though. These include the necessity to trust the VPN provider and slower internet connections. Internet speeds may be slowed by the processing and decryption of encrypted data, especially when utilizing high-bandwidth apps. VPN providers must also earn your confidence because they have access to your data and online activities. Users may be exposed to privacy and security issues if the supplier is unreliable or has inadequate security measures. Connection problems or restrictions on access to certain resources might also result from compatibility difficulties with particular devices or programs.

Increased security and privacy, the ability to get around internet restrictions, and access to blocked information are all advantages of using a VPN. When selecting a VPN provider, consumers should be aware of any potential negatives and carefully weigh their alternatives.

Question 6

10 / 10 pts

At a local coffee shop a student discovers that access on the free internet is dis-allowing access to UNCC.edu. Foolishly, this student has waited to the last minute to complete the final exam for a course and this is the only internet available at the time. How could the student *theoretically* use a virtual private network (VPN) to access UNCC.edu? Explain your answer with a short paragraph and create a diagram to show how IP tunneling is achieved with source and destination IP's.

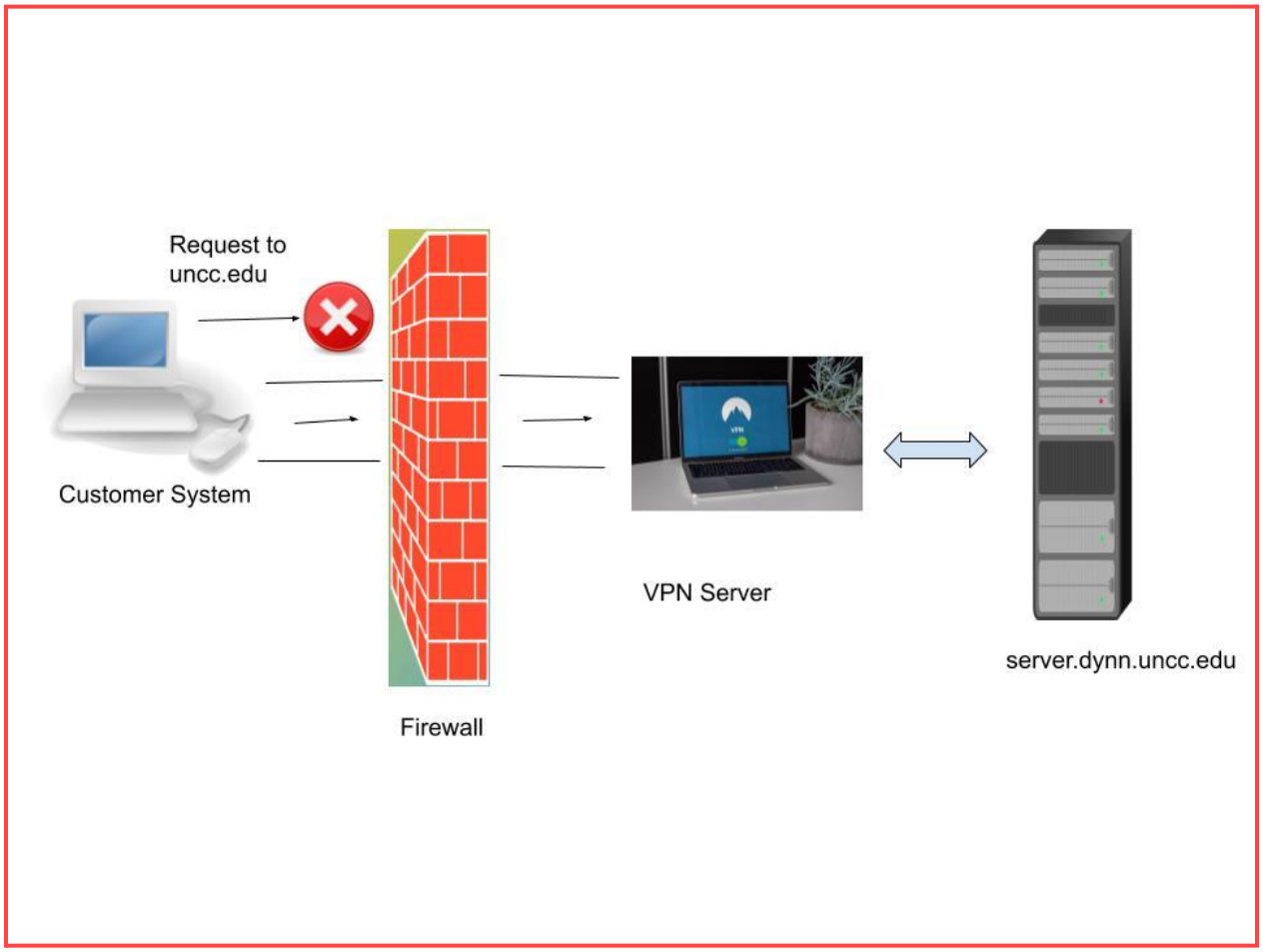
Your Answer:

Even if the local coffee shop's internet is restricting access to UNCC.edu, the student can use a virtual private network (VPN) to safely connect to the internet and access the website. The student's device initially creates a secure connection to a VPN server while utilizing a VPN. All of the student's internet traffic is then sent through the VPN server after the connection has been made. The local coffee shop's internet won't be able to prevent access to UNCC.edu because the traffic is encrypted and looks to be coming from the VPN server's IP address.

The student's device initially makes a request to the VPN server to establish a connection in order to establish a VPN connection. After that, the VPN server replies to verify the connection. As soon as the connection is made, the VPN server and the student's device construct a secure encrypted tunnel through which the student's internet traffic may flow.

The student's gadget will have a source IP address that is given by the internet of the nearby coffee shop. This address can be used to prevent access to UNCC.edu as it will be displayed on the internet of the neighborhood coffee shop. The student's communication will, however, seem to originate from the VPN server's IP address after the VPN connection has been made. This IP address will serve as the student's traffic's destination and won't be blocked by the internet at the nearby coffee shop, enabling a safe connection to the UNCC.edu website.

This scenario's IP tunneling with source and destination IPs is illustrated in the following diagram:



Question 7

8 / 8 pts

A self-propagation malware works as follows. When a machine is infected, it will initiate TCP connections with other machines that it has connected with before. Then 240KB data will be transferred to the target to infect it. Assume that the traffic is NOT encrypted.

Please explain, if we are using software defined networks (SDN), how can we detect and mitigate such attacks? Please discuss from the following aspects:

(1) what type of information does the SDN controller need to collect from network traffic and analyze to detect the anomaly?

(2) After detection, what will the controller do to stop further malware propagation?

Your Answer:

Software-defined networks (SDN) require particular sorts of information from network traffic, which the SDN controller would need to gather and evaluate in order to identify and neutralize self-propagating malware.

1. The SDN controller must first gather data on the source and destination of network traffic as well as the volume and nature of the data being transported. With the use of this data, it would be possible to spot any suspicious or unusual patterns in network traffic, such as a high volume of data being transmitted between devices or a high volume of connections being made by a single machine.
2. Several steps may be taken by the SDN controller to halt the spread of malware when it has discovered an abnormality in the network flow. To stop the virus from propagating, the controller might, for instance, block the suspicious connections or isolate the infected system from the rest of the network. The controller might also send out an alert to tell network administrators of the problem and provide them the details they need to look into and fix it.

Question 8

8 / 8 pts

A key part of being able to secure a network is to understand the key components and communication points of computing devices on the network. Please describe the set-up of your home (or residence, dorm room, parents house, etc.) network and where network security controls can be placed to help secure the network. Include a simple diagram of the network with security points (e.g., firewall) highlighted.

Your Answer:

It would be great to have a little more information on the precise set-up and devices being utilized in order to describe a home network and its security points. However, a typical home network configuration includes a mix of wired and wireless devices connected to a router. The router is the central hub of the network, and it is responsible for giving internet access to all of the devices on the network. The router's integrated firewall is one of the most important security points on a home network. This firewall's purpose is to prevent incoming internet traffic that has not been specifically authorized by the user. For instance, the firewall might be set up to prevent traffic from known harmful websites or IP addresses from entering.

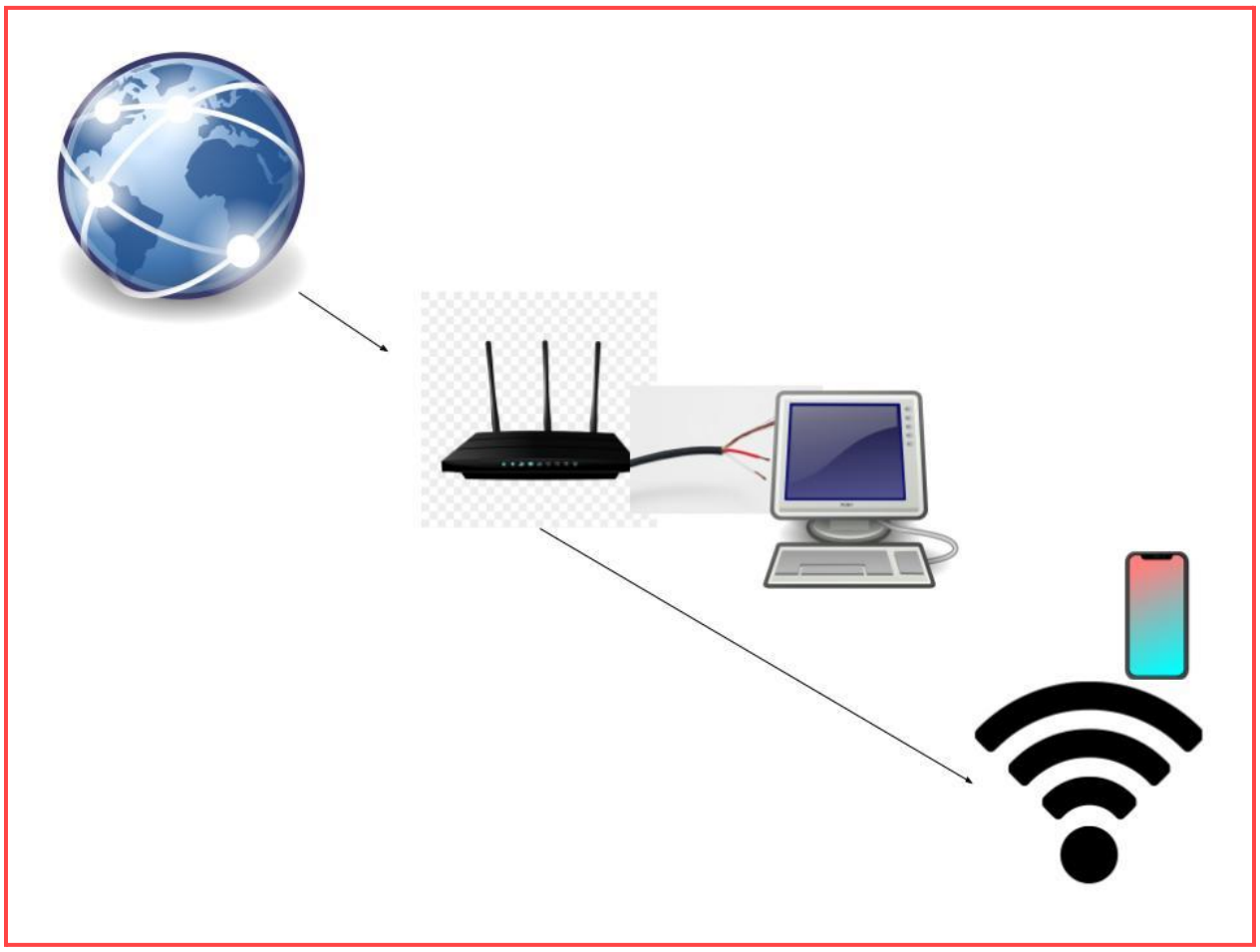
Use of strong, individual passwords for each network device is a crucial aspect of home network security. This aids in preventing unwanted access to the network and to specific networked devices. Furthermore, utilizing encryption for wireless communications can aid in thwarting eavesdropping and other kinds of assaults.

Here is a basic network design for a home with some of the most important security features highlighted. It would be great to have a little more information on the precise set-up and devices being utilized in order to describe a home network and its security points. However, a typical home network configuration includes a mix of wired and wireless devices connected to a router. The router serves as the network's core node and is in charge of connecting all connected devices to the internet.

The router's built-in firewall is one of a home network's most important security points. Incoming internet traffic that has not been specifically authorized by the user will be

blocked by this firewall. Incoming traffic from known dangerous websites or IP addresses, for instance, might be blocked by the firewall's configuration. Use of strong, individual passwords for each network device is a crucial aspect of home network security. This aids in preventing unwanted access to the network and to specific networked devices. Furthermore, utilizing encryption for wireless communications can aid in thwarting eavesdropping and other kinds of assaults.

Here is a straightforward schematic of a home network that highlights some of the most important security features.



Question 9

12 / 12 pts

Research two different examples of Distributed Denial of Service (DDoS) attacks in the real-world and identify the likely method of attack (e.g., SYN flood) to the best of your ability. Briefly describe the two attacks and then describe what defenses or methods you would use to prevent or defend against those attacks if you were charged with network security. Include links to the originating sources.

Your Answer:

Over the years, there have been several Distributed Denial of Service (DDoS) assault examples in the real world. Here are two illustrations:

The website of Krebs on Security was the subject of a significant DDoS assault in 2016 that peaked at 620 Gbps. A botnet, or network of infected devices that can be remotely managed to conduct assaults, was probably used to carry out the attack. Implementing a strong network security system with components like firewalls, intrusion detection and prevention systems, and DDoS mitigation services would be important to protect against this kind of assault.

References:

1. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ Links to an external site
2. https://krebsonsecurity.com/2021/09/krebsonsecurity-hit-by-huge-new-iot-botnet-meris/Links to an external site.

I would collaborate with the network administrator to deploy the proper mitigations or remediations after the problem's root cause has been found. In order to reduce the quantity of traffic coming from particular devices or apps or to restrict suspicious traffic in order to thwart a possible cyberattack, this might involve adopting traffic shaping or rate limitation. Overall, I want to DNS service provider Dyn has been the target of a DDoS attack. Many important websites, including Netflix, PayPal, and Airbnb, were impacted by this attack. This assault makes use of the Mirai software, which turns infected IoT devices into a botnet. All of these devices have been set up to make requests of a single service. All IoT devices need to have security measures in place,

including regular updates and patches, as well as monitoring and detection systems to find and stop malware from spreading. Could be to swiftly and efficiently fix the problem and guarantee the network's performance and security.

References:

1. https://www.techtarget.com/searchsecurity/definition/distributed-denial-of-service-attack

Implementing a multi-layered security strategy that incorporates both preventative measures and real-time monitoring and reaction capabilities is often the best method to protect against DDoS assaults. Firewalls, intrusion detection and prevention systems, DDoS mitigation services, and routine security updates and patches for all networked devices should all be part of this strategy. It's also crucial to constantly check the network for indications of prospective attacks and to have a strategy in place for countering and neutralizing those that do happen.

Question 10

6 / 6 pts

As head of network security for a company you receive reports from the network administrator of excessive traffic on the network which is starting to impact the users ability to access key applications both on network and in the cloud. The network administrator is unable to determine the source of the issue but suspects a cyber attack.

As head of network security what tools and methods would you use to investigate the excessive traffic and determine its source and potential mitigations or remediations for the issue?

Hint - the excessive traffic was first detected at the core router on the network where the internet service is connected. Optionally you may attach a diagram to support your answer.

Your Answer:

The first thing I would do in my capacity as head of network security is to validate with the network administrator any allegations of excessive network traffic. This is a crucial step to confirm if the condition is real and to determine how serious it is. Once the problem is established, I would look into the cause of the traffic and identify potential fixes using a range of instruments and techniques. This would entail capturing and analyzing network traffic with tools for network traffic analysis, such as Wireshark, in order to spot any malicious behavior. To track network performance and notify me of any problems or abnormalities, I would also utilize network monitoring tools like Nagios or SolarWinds.

I would look into the problem using these tools in addition to looking through network device logs and other data. This would make it easier for me to spot any patterns or trends in the traffic and perhaps even determine where the excessive traffic is coming from.

I would collaborate with the network administrator to deploy the proper mitigations or remediations after the problem's root cause has been found. In order to reduce the quantity of traffic coming from particular devices or apps or to restrict suspicious traffic in order to thwart a possible cyberattack, this might involve adopting traffic shaping or rate limitation. My overall objective would be to ensure the network's security and performance while also swiftly and efficiently resolving the problem.

Question 11

10 / 10 pts

Review the MITRE ATT&CK Network Matrix

Links to an external site.

Choose two types of attacks categorized by MITRE in this matrix and describe in your own words those attacks. Describe potential mitigations or controls to defend against the kind of attacks you selected in your own words.

Your Answer:

Spearphishing and command injection are two types of assaults that MITRE has classified in its attack matrix and have included in the Mitre Attack Framework. A single person is targeted and personally emailed by the attacker in a social engineering assault called spearphishing in attempt to deceive them into opening a malicious link or file. The usual method for doing this is to pose as someone the victim trusts, such their employer or a coworker.

People can be taught to open emails with greater caution and to confirm the sender's identity before clicking any links or attachments in order to guard against spearphishing. To automatically recognize and prevent problematic emails, businesses can also employ email filtering and spam detection systems. Attacks called "command injection" include inserting malicious code into a system via a user input field, such a login form or search bar. This may provide the attacker access to the system without authorization and let them run arbitrary instructions, giving them the chance to steal sensitive information or cause the system to malfunction.

It is crucial to correctly verify and sanitize user input to make sure that it is free of harmful code in order to prevent command injection attacks. To achieve this, provide appropriate input filtering and use secure coding techniques to stop arbitrary code from running. Any program or application should also be updated and patched often to avoid vulnerabilities that an attacker may use against you.

Quiz Score: **94** out of 94