# Cyber-Attacks and Defenses Task - Theoretical

# Question 1

**What is the difference between an active and a passive cyber-attack?**  
The purpose of a passive attack is to gain access to the computer system or network and to collect data without being detected. As opposed to this, active cyber-attacks are often aggressive attacks that victims immediately become aware of when they occur.

# Question 2

**Name three types of active cyber-attacks.**  
Session Hijacking Attack  
DoS  
DDoS  
Message Modification Attack  
Masquerade Attack  
Ransomware  
Brutal-force attack

# Question 3

**What is spoofing?**  
Spoofing is when a person or program successfully identifies as another by falsifying data to gain an illegitimate advantage.

# Question 4

**Give five examples of technologies that can be spoofed.**  
Caller ID  
  
GPS  
  
DNS  
  
Email address  
  
IP address  
  
MAC address  
  
Website

# Question 5

**How can you defend yourself against spoofing?**  
Remain vigilant against the most common types of spoofing, be on your guard for the signs of a spoofing attack.   
  
If you’re being asked for personal information, call to confirm using the number listed on the website, enter their URL into your browser, check the website for signs of website spoofing and don’t click links in suspicious emails.   
  
Don’t open attachments you aren’t expecting, especially if they have abnormal file extensions.   
  
If an attacker manages to obtain your login credentials, they won’t be able to do much damage if you regularly change your password.   
  
Hover over links before clicking so that you’ll know where you’re going. If you decide to click, confirm the URL after the page loads to ensure you weren’t redirected.   
  
If you’ve received a spoofed email or other communication, let the supposed sender know that they’ve been spoofed.

# Question 6

**Explain what a DoS attack is.**  
A denial-of-service (DoS) attack is designed to shut down a system or network, rendering its resources unavailable to users. DoS attacks do this by flooding the target with traffic, causing it to fail. In this scenario, the DoS attack prevents legitimate users from accessing the service or resource (staff, members, or account holders).  
  
Distributed denial-of-service (DDoS) attacks have the same objective as DoS attacks, but they are launched from a larger number of devices and have a more significant impact.

# Question 7

**There are four main types of DoS attacks; what are they?**  
Application layer attacks   
  
Distributed DoS  
  
Advanced persistent DoS   
  
DoS as a service

# Question 8

**Describe and explain one of the DoS attacks you cited in the previous question.**  
Application layer attacks – a DDoS attack where attackers target application layer processes. The attack over-exercises functions or features of a website to disable them. It is often used against financial institutions to distract IT and security personnel from security breaches.   
HTTP flood is application layer attack.  
  
Distributed DoS – a DDoS attack occurs when multiple systems flood the resources of a system, usually one or more web servers. Multiple machines can generate more traffic than one machine, they are harder to turn off than one, and the behavior of each can be stealthier, making it harder to track and shut down.   
  
Advanced persistent DoS – a DoS attack which can last for weeks.   
  
DoS as a service – some vendors provide simple web-based front-end services and accept payment over the web. They are marketed and promoted as stress-testing tools and can be used to perform unauthorized denial-of-service attacks and allow attackers access to attack tools.

# Question 9

**What is the difference between a DoS and a DDoS attack?**  
Launched by:DoS( 1 computer, 1 network),DDoS(several computers)  
  
Launched by - Explanation  
  
DoS  
One computer and one computer network are used to flood a network or server with packets - in HTTP, for instance, it can be a flood of HTTP requests.  
  
DDoS  
These attacks use computers not owned by the attacker. The attacker must first compromise other computers and use them to launch an attack on a single system.  
  
Magnitude:DoS(Medium),DDoS(High)  
  
Magnitude - Explanation  
  
A DDoS attack is much more complicated to execute, but has great advantages for attackers:  
  
-The greater capacity of several combined machines allows attack to be more disruptive.  
  
-When distribution is random and spread around the world, it is harder to identify the original offender.  
  
-Shutting down multiple machines to stop an attack is much harder than shutting down a single machine.  
  
-It's extremely difficult to identify the attackers behind a DDoS attack since they are hidden behind many (mostly compromised) systems and machines.  
  
-The consequences of such attacks are usually devastating and much harder to withstand.

# Question 10

**Name five methods for defending against DoS or DDoS attacks.**  
Application front end hardware   
Blackholing and sinkholing   
IPS based prevention   
Firewalls   
DDoS protection service   
Increase bandwidth   
Risk management   
Switches   
Routers

# Question 11

**Describe and explain one of the five methods you mentioned in the previous question.**  
Application front end hardware - Front-end hardware analyzes packets when they enter the system. The front-end hardware identifies the packets, determines whether they are normal or malicious, and prevents DoS or DDoS attacks.   
  
Blackholing and sinkholing - Blackholing - redirects malicious traffic to a nonexistent "black hole" server, thus preventing the harmful traffic from reaching the server. Sinkholing redirects the traffic to a valid IP address and distinguishes between legitimate and harmful traffic (ineffective against large-scale DDoS attacks)  
  
IPS based prevention - Intrusion-prevention systems can identify DoS attacks by analyzing the traffic and denying access to harmful traffic.   
  
Firewalls - Utilizing stateful firewalls to validate and filter packets that are trying to enter the network.   
  
DDoS protection service - Filter network traffic through a protective service. All network traffic is routed through the service, and any malicious or harmful traffic is blocked from gaining access to the network.  
Increase bandwidth - The premise behind DDoS attacks is to overload the network by taking up all available bandwidth. Extending the network's available bandwidth makes it less likely for DDoS attacks to succeed.   
  
Risk management - Ensure the data centers are placed on different networks and spread out over different physical locations. This way, if a single data center is targeted, the others remain safely out of reach.   
  
Switches - Use automatic rate-filtering to identify and prevent DoS attacks.   
  
Routers - Can filter packets (similarly to switches). The filtering can be set manually according to defined criteria to identify DoS attacks.

# Question 12

**Explain what a man-in-the-middle (MITM) attack is and how it works.**  
A man-in-the-middle attack is a type of cyberattack in which an attacker eavesdrops on a conversation between two targets. The attacker may try to “listen” to a conversation between two people, two systems, or a person and a system.  
  
The goal of a MITM attack is to collect personal data, passwords or banking details, and/or to convince the victim to take an action such as changing login credentials, completing a transaction or initiating a transfer of funds.  
  
 MITM attack generally consists of two phases: interception and decryption.  
  
Phase #1: Interception  
In the interception phase, cybercriminals gain access to a network through an open or poorly secured Wi-Fi router and/or by manipulating domain name system (DNS) servers. Attackers then scan the router looking for vulnerabilities and possible points of entry. Most often this is done through a weak password, though cybercriminals may also use more advanced methods such as IP spoofing or cache poisoning.  
  
Once a target is identified, the attacker typically deploys data capture tools to access and collect the victim’s transmitted data, strategically redirect traffic or otherwise manipulate the user’s web experience.  
  
Phase #2.Decryption  
The second phase of an MITM attack is decryption. This is when stolen data is decoded and made intelligible to the cybercriminals. Decrypted data can be leveraged for any number of nefarious purposes, including identity theft, unauthorized purchases or fraudulent bank activity. In some cases, man-in-the-middle attacks are conducted for no obvious purpose other than to disrupt business operations and create chaos for victims.

# Question 13

**MITM attacks can be prevented or detected by two means: authentication and tamper detection. Explain each of these in your own words.&nbsp;  
  
  
Authentication  
Tamper detection**

Authentication – provides some degree of certainty that a given message has come from a legitimate source.   
  
Tamper Detection – shows evidence that a message may have been altered.

# Question 14

**A buffer overflow attack is a type of host-based active cyber-attack.&nbsp;  
  
  
What is a buffer overflow attack?&nbsp;  
How can it be exploited?&nbsp;  
How can you protect your network from this exploitation?**  
1)It’s an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.  
  
2)An attacker can send data designed to cause a buffer overflow, write into areas known to hold executable code and replace it with malicious code, or overwrite data regarding the program's state, causing behavior that was not intended. Buffers are common in operating system code, so the attacker can perform privilege escalation and gain unlimited access to the computer's resources.  
  
3)  
Require network users to select strong passwords and change them on a regular basis  
Enable multi-factor authentication (MFA) on all network assets and applications  
Develop and deploy strong encryption protocols  
Equip all network assets with virtual private network (VPN) capabilities  
Deploy a comprehensive threat monitoring and detection solution  
Segment the network to ensure potential breaches are contained  
Educate employees on the risks of public Wi-Fi networks

# Question 15

**As a future cybersecurity expert, what steps would you take to defend your network from the cyber-attacks mentioned in this task?**  
-Implement Network Segmentation.  
  
-Deploy Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)  
  
-Use Strong Encryption: Employ encryption protocols, such as SSL/TLS, for network communications to protect against MitM attacks.   
  
-Secure Network Infrastructure: Ensure that routers, switches, and other network devices are properly configured and regularly updated with the latest security patches. Disable unnecessary services and use strong passwords for device administration.  
  
-Implement DoS Protection Measures: Utilize DoS protection solutions, such as rate limiting, traffic filtering, or DoS mitigation services. These measures help identify and mitigate DoS attacks by filtering or diverting malicious traffic.  
  
-Conduct Regular Security Audits and Penetration Testing: Perform comprehensive security audits of your network infrastructure and conduct periodic penetration testing to identify vulnerabilities. Fix any identified weaknesses promptly.  
  
-Train Employees on Security Awareness: Educate your staff about the risks of cyber-attacks, such as phishing, and teach them best practices for maintaining strong passwords, identifying suspicious emails, and reporting potential security incidents.  
  
-Monitor Network Traffic and Log Data: Implement robust network monitoring and log management solutions to detect anomalies, such as sudden traffic spikes or unusual behavior. Analyzing network logs helps identify potential DoS or MitM attacks.  
  
-Keep Software and Systems Updated: Regularly apply security patches and updates to all software, operating systems, and network equipment.   
  
-Develop an Incident Response Plan: Create a documented incident response plan that outlines the steps to be followed in case of a cyber-attack.  
  
-Backup and Disaster Recovery: Regularly backup critical data and systems and store the backups securely.  
  
-Multi-authentication  
  
-Antivirus