CYBERSECURITY E-DEGREE

NETWORK SECURITY ASSIGNMENT

PART ONE

1) **Considering what you have learned through the course, how would you describe the process of User Authentication on a website by having three different factors of authentication?**

Websites use Client and Server technology. For a website that has some form of login for the user to be authorized (process of giving permission or access rights or privileges to the user) before they can be allowed to access their resource on the page, they need to be authenticated.

The process of authentication involves:

a) The user needs to input their username and password. This process can only be known by the user and as such, it is one of the three methods of authentication known as **Something you Know – (Knowledge Factors)**.

b) If the username and password match the credentials in the database, a security token can be sent to his or her device for further verification before authorization for a resource can be granted. This security token is usually in the form of 6 digits which the user must input into the device. This is another method of authentication known as **Something that you Own** (**Ownership Factor**). It is recommended that owners of websites that require a user to be authenticated use the multi-factor authentication technology e.g., **2FA (2 Factor Authentication)** to add an extra layer of security during the user registration process and to maintain using the same during the login process.

PART TWO

2) Describe four Attack Vectors on a company that produces shoes both physical and Digital

The four attack vectors of a company that produces shoes can be:

a) **Phishing**: The threat actor can send deceptive information to an employee of the company (usually in the form of an email which could be the official employee company's email) informing him or her of a Too Good to be True deal regarding their product via a link, or an image, or an evil file link. This could lead the employee to click on the link. The malicious executable file could be automatically downloaded in a hidden folder, installed, executed and would be collecting information on the employee's computer. This is a digital attack surface through software.

b) **DDOS Attack**: The adversary can send many requests or payloads from a different computer to a single server. The server may not be able to serve these requests thereby shutting down. This is a Physical attack as the server was targeted.

c) **SQL Injection**: Assuming the shoe company has an eCommerce website with registered users, the attacker can inject malicious SQL queries into their website to steal login information. This could be used to impersonate the user or cause havoc to their accounts or other malicious activities.

d) **Man-in-the-Middle Attack (MITM)**: The hacker can create a rogue access point to which a user can connect without knowing that the network is served by the attacker. The moment the user uses the network, the hacker can intercept the information which can be used for any malicious activity. This is a Physical attack.

PART THREE

Considering the Wireless security, describe in your own words what a Krack attack is (a hard one)

Krack stands for Key reinstallation attack. This is a type of attack on the key installation of the WPA2 WIFI network. The adversary tricks the user into reinstalling an already-in-use network key. The user receives the same key twice. One from the access point, and another from the attacker.

PART FOUR

Considering what you've learned through the course, describe what machines should AntiVirus and Firewalls be installed in a network where you have 10 servers and 10 client machines, where all of them have internet and process information provided by outsiders of the company.

Firewalls filter both the inbound and the outbound data packets that flow through the company's network. Antivirus protects the systems (including the servers) from any malicious activities that can compromise the security of the system and interrupt normal operation of the system.

It is important to secure both the client and the servers as securing one without the other will allow the threat actor to attack the less secure system and penetrate the network.