Assignment: Ethical hacking

1. Explain CIA triad.

Ans: The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

1. What is a Firewall and why is it used?

Ans: A firewall is a network security device that prevents unauthorized access to a network. It inspects incoming and outgoing traffic using a set of security rules to identify and block threats.

1. What is the difference between VA(Vulnerability Assignment) and PT(Penetration Testing)?

Ans: VA : Vulnerability assessment is the technique of finding and measuring security vulnerabilities in a given environment. It is an all-embracing assessment of the information security position.

PT : Penetration testing is done for finding vulnerabilities, malicious content, flaws, and risks. It is done to build up the organization’s security system to defend the IT infrastructure.

1. What is the difference between HIDS and NIDS?
2. Explain SSL Encryption

Ans: Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server.

1. What is Data Leakage?

Ans: [Data leakage occurs when sensitive information is unintentionally exposed to unauthorized parties](https://www.bing.com/ck/a?!&&p=c4a480cd0deae339ad7828014332a06dcbef7842bbe838c0e8cabcd46bf7e66eJmltdHM9MTczMjQwNjQwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=What+is+Data+Leakage%3f+&u=a1aHR0cHM6Ly93d3cuaWJtLmNvbS90aGluay90b3BpY3MvZGF0YS1sZWFrYWdl&ntb=1).

1. What is a Brute Force Attack? How can you prevent it?

Ans: Done

1. Explain MITM attack and how to prevent it?

Ans: [A man-in-the-middle (MITM) attack is a security attack that occurs when someone intercepts traffic between two computers and steals information](https://www.bing.com/ck/a?!&&p=ea65e8a4d1bf550fb95f90dad8b652096beb78d5db770cba85f838feb37eb119JmltdHM9MTczMjQwNjQwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=Explain+MITM+attack&u=a1aHR0cHM6Ly93d3cuaG93dG9nZWVrLmNvbS82Njg5ODkvd2hhdC1pcy1hLW1hbi1pbi10aGUtbWlkZGxlLWF0dGFjay8&ntb=1).

1. Explain XSS attack and how to prevent it?

Ans: [Cross-Site Scripting (XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application](https://www.bing.com/ck/a?!&&p=89c6b245eb9c7c6eadd1dfaefb7f5adf27d1986ab1a7370e1d4c9aad463aa588JmltdHM9MTczMjQwNjQwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=Explain+XSS+attack+&u=a1aHR0cHM6Ly9vd2FzcC5vcmcvd3d3LWNvbW11bml0eS9hdHRhY2tzL3hzcy8&ntb=1).

1. What is a Botnet?

Ans: A botnet is a network of compromised computers, also known as zombies or bots, that are controlled by a third party, often referred to as a botmaster.

1. Explain SSL and TLS

Ans: SSL: done

TLS: Transport Layer Security (TLS) is a cryptographic protocol designed to provide secure communication over a computer network.

1. Define the terms Virus, Malware, and Ransomware.

Ans: Done.

1. What is Phishing? Provide an example.

Ans: [Phishing](https://www.knowbe4.com/phishing?hsLang=en) is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

1. Define the terms Encryption and Decryption.

Ans: Done.

1. What is a DDoS attack and how does it work?

Ans: DDoS attacks involve multiple compromised systems targeting a single system to cause a Denial of Service.

1. What is a zero-day vulnerability?

Ans: A zero-day vulnerability is a security loophole in software, hardware or firmware that threat actors exploit before the vendors can identify and patch it.

1. What is network sniffing

Ans: Network sniffing is a passive technique used to monitor and analyze network communication.

1. What is a Security Operations Center (SOC)?

Ans: [A Security Operations Center (SOC) is responsible for protecting an organization against cyber threats](https://www.bing.com/ck/a?!&&p=66acaaf9e8259fa01e16e77f1dd264ff30fe84d6d6a31527096c4ae8211a4283JmltdHM9MTczMjQwNjQwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=What+is+a+Security+Operations+Center&u=a1aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvU2VjdXJpdHlfb3BlcmF0aW9uc19jZW50ZXI&ntb=1)

1. What is the importance of forensics in cyber security?

Ans: [Forensics in cyber security is the process of collecting, processing, preserving, and analyzing evidence from digital devices](https://www.bing.com/ck/a?!&&p=dc2a615f776d9e959adbc5cdab27e87528888c28cded607a7b1a458660ec54b1JmltdHM9MTczMjQwNjQwMA&ptn=3&ver=2&hsh=4&fclid=1dcdf568-3d87-6e75-32ad-e1b43c1c6f7f&psq=What+is+the+importance+of+forensics+in+cyber+security&u=a1aHR0cHM6Ly93d3cubmF0aW9uYWwuZWR1LzIwMjEvMDcvMTQvZGlnaXRhbC1mb3JlbnNpY3MtY3liZXJzZWN1cml0eS8&ntb=1).

1. Discuss the future trends in cyber security. Which skills are important for cyber security professionals?

Ans: Done

1. What is the difference between IDS and IPS?

Ans: Done.