INTRODUCTION TO ETHICAL HACKING QUESTION BANK

UNIT – 1

1. Write a note on Ethical Hacking. Why is it necessary?

ANS.

1. Ethical hacking means the act of locating weaknesses and vulnerabilities of computer or any information system by duplicating the intention and actions of malicious hackers.
2. The primary goal of ethical hacking is to identify and solve vulnerabilities in a system before they can be exploited by malicious hackers

Why is it necessary:

- Ethical hacking offers an objective analysis of an organisations' information security posture.
- Hackers must scan for weaknesses, test entry points, prioritize targets, and develop a plan that best suits their organization

2. What are scopes and limitations of Ethical Hacking?

Ans. 1. Ethical hackers must know the penalties for unauthorized system hacking.

2. Gain authorisation from the client and have a signed contract giving the ethical hacker permission to perform the test.

3. Maintain and follow a Non-Disclosure Agreement (NDA) with the client in the case of confidential information disclosed during the test

4. The depth and breadth of testing are determined by the client's needs and concerns.

3. What are the Skills required to be an Ethical Hacker?

ANS.

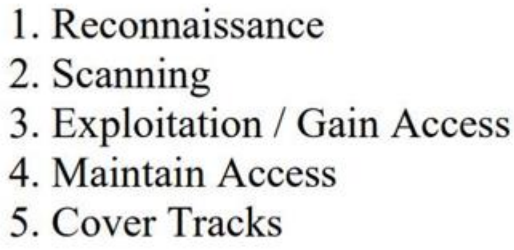
1.Basic Computer Skills:

- Understanding the fundamentals of how computers function.
- Proficiency in using the command line in Windows and configuring networking parameters

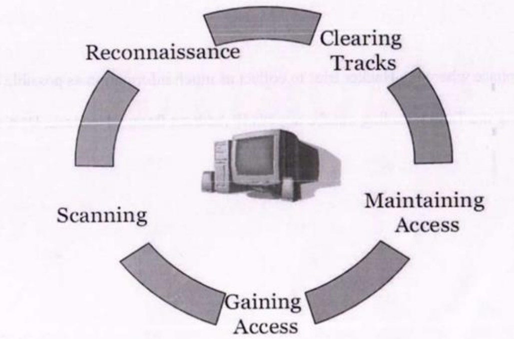
2. Networking Skills:
   - Knowledge of computer networks and how devices (hosts) communicate.
3. Linux Skills:
   • Familiarity with the Linux operating system, which is commonly used by hackers.
4. Wireshark: Wireshark is a tool that helps you inspect and analyze the traffic on a computer network. It's like a detective tool for computer networks. • Imagine the data that travels between your computer and the internet is like a series of letters being sent and received. Wireshark lets you open and read those letters to understand what's happening on the network. (MUST BE ABLE TO READ AND CAPTURE DATA PACKETS)
5. Programming Skills: Programming Skills are another most crucial skill to become an ethical hacker. Python, PHP, Java, ruby, C, C++, and JavaScript etc
6. Database : how data is preserved, how data is accessed.

7. Web Applications: you use on the Internet through your Web Browser. • web applications have also become a prime target of the hackers • You must understand the functioning of web applications and the databases backing them.
8. Cryptography: is the practice and study of techniques used to secure communication and protect information. It involves the use of mathematical algorithms to transform information (plain text) into an unreadable format (cipher text) and back again.

4. Explain the five phases of Hacking.



1. Reconnaissance
2. Scanning
3. Exploitation / Gain Access
4. Maintain Access
5. Cover Tracks



ANS.

1. **Reconnaissance:** This is the primary phase where the Hacker tries to collect as much information as possible about the target system. It includes identifying the Target, finding out the target's IP Address Range, Network.– wireshark, Maltego, Nslookup, Nikto, Burp Suite.
2. **Scanning:** It involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may use during the scanning phase can include port scanners, network mappers and vulnerability scanners.
   Nmap, or Network Mapper - It is designed to explore and map networks, identify open ports, find hosts.

   ```
   nmap [target]
   ```
3. **Exploitation/ Gaining Access:** After scanning, the hacker designs the blueprint of the network of the target with the help of data collection during Phase I and Phase 2. This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access
4. **Maintaining**: Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers by securing their access with rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks.
5. **Covering Tracks:** Hackers try to remove all traces of the attack. Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking or to avoid legal action.

6. **What are the three main types of Hackers. Explain Each.**

Ans. Hackers fall into three general categories: black hat hackers, white hat hackers, and gray hat hackers.

Black hat hackers

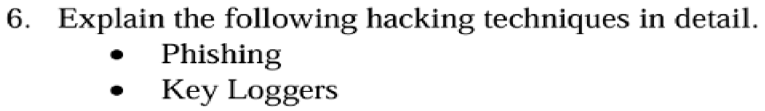
- Black hat hackers are cybercriminals that illegally crack systems with malicious intent.
- Seeking to gain unauthorized access to computer systems
- Once a black hat hacker finds security vulnerability, they try to exploit it, often by implanting a virus or other type of malware such as a trojan.
- Ransomware attacks are a common tactic used by malicious hackers to demand money

White hat hackers

- White hat hackers are ethical security hackers who identify and fix vulnerabilities.
- Hacking into systems with the permission of the organizations white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system's overall security.

Gray hat hackers

- Gray hat hackers are not necessarily bad like black hat hackers, but they still enter computer systems without permission.
- However, instead of causing harm, they find and reveal weaknesses in the system.
- When they discover new vulnerabilities, they tell the owner about it instead of exploiting it fully. However, sometimes they may ask for money to share all the details about what they found.



6. Explain the following hacking techniques in detail.
   - Phishing
   - Key Loggers

ANS:

- Phishing is a common trick used by hackers to fool you into giving away your personal information.
- It often happens through emails or text messages that look like they're from trusted sources
- How Does it Work? Imagine getting a message that seems to be from a familiar company (like Amazon or Netflix) or even a friend.
- The goal is to make you click on a link.

Keylogger:

1. A keylogger, also known as a keystroke logger or keyboard capture, is a form of surveillance technology.
2. It records every key you press on your computer or device.

Types of Keyloggers:

1. **Hardware Keyloggers:**

A tiny device connected between your keyboard and computer.

It appears as a regular part of your computer cables or connectors.

2. **Software Keyloggers:**
    1. Software that can record your keystrokes.
    2. Can be intentionally downloaded in your hard drive or sneak in with other harmful software.

7. **What is Eavesdropping? Explain**

ANS. Eavesdropping is like someone secretly listening to your private conversations. • Talking on the phone or sending messages, thinking it's private, but there is someone in middle listening to your conversation or messes with your data without you knowing.

Types of Eavesdropping:

There are two main types - Passive and Active.

Passive Eavesdropping:

- Imagine someone silently listening to your digital conversations.
    - When you're talking over the internet using VoIP (Voice over Internet Protocol).

Active Eavesdropping:

- Picture a hacker pretending to be a website where you share personal data.
- hackers imitate websites where online users can share personal data and information.
- An attacker using a sniffing program gathers the data of its target.
- MITM attack or man-in-the-middle attack is an example of an active eavesdropping attack.
- The data is captured, modified and sent to other devices

8. **What is Penetration testing? Explain the different stages of Penetration testing.**

ANS.

1. A penetration test is a simulated cyber-attack carried out by testers or ethical hackers to find vulnerabilities in a system, website, mobile application, or network
2. Basically, a penetration test is a method of hacking into a system before cybercriminals get into it and exploit it.

Different stages of Penetration testing:

1. **Planning and Reconnaissance**: The first stage involves: Defining the scope and goals of a test, including systems to be addressed and the testing methods to be used.
   Gathering INFORMATION (e.g., network and domain names) to better understand how a target works and WHAT ARE ITS vulnerabilities.
2. **Scanning**: The next step is to understand how the target application will respond to various intrusion attempts.
   This is typically done using:
   Static analysis –Testing an application's code to predict the way it behaves while running. Static analysis involves examining the code and structure of a software application without actually executing it.

   Dynamic analysis – Dynamic analysis involves observing how a software application behaves while it's running or in action. • Provides a real-time view into how the application performs during execution. It helps uncover 23 issues that might only become apparent when the application is running

3. **Gaining Access**: the main goal at this stage is to test the security of a system by trying to break into it using various techniques. Testers conduct web application attacks, such as SQL injection. These are way to get into a system without proper authorization. The aim is to understand the extent of damage that could occur if a real attacker exploits these vulnerabilities.
4. **Maintaining Access:** The idea is to see if an attacker, once inside, can remain undetected and maintain access for an extended period. The testers try to stay within the system for an extended period, imitating the actions of a persistent attacker. This could involve periodic checks to see if they can still access the system without being noticed.
5. **Analysis:** After the penetration test is complete, the results are thoroughly examined and analyzed. The analysis provides valuable insights for the organization. It helps them understand the weaknesses in their systems. and how long an attacker might go unnoticed if they exploit these vulnerabilities.

9. Explain Black Box, White box and Gray Box Testing?

ANS.

White Box Testing: Also known as glass box, or clear box testing. Testers have full access to the internal workings of the software. They can see the source code, architecture, and logic of the software.

Goal: Make sure the inside of the software is built correctly.

Black Box Testing: Testers have no knowledge of the internal workings of the software. They interact with the software from an external perspective, like a regular user. It's similar to using a device without knowing how it's made.

Goal: Check if the software does what it's supposed to do, without caring about how it's made inside.

Gray Box Testing: Testers have partial access to the internal structure. They can see some parts of the source code but not everything.

Goal: Mix a bit of both. Check how the software works inside a little, but also test it from the outside like a user. Aims to find defects and vulnerabilities by considering both the internal logic and the external functionality.

10. What is Reverse engineering?

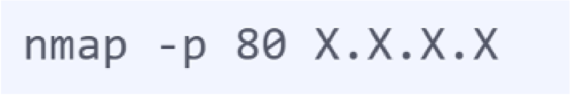
ANS.

1. Reverse engineering refers to the duplication of another producer's product following a thorough examination of its construction or how it was built.
2. It involves looking at a product made by someone else and trying to create a similar one.
3. Once you understand how the an application works, you might want to make it even better or create a similar application with some improvements.
4. People might use reverse engineering to understand how software or hardware functions, improve it, or create something similar.

11. Write note on Vulnerability assessment? Explain its types.

ANS.

1. A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures
2. Vulnerability assessments also provide an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to each threats in their organization.
3. They typically involve the use of automated testing tools, such as network security scanners.
4. Nmap can be used to discover hosts on a network, it could be used for port scanning, provide info about services running on that port.



```
nmap -p 80 X.X.X.X
```

Types of vulnerability assessments:

1. Network based scan: used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired and wireless network.
2. Host-based scans are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services
3. Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure.
4. Application scans test websites to detect known software vulnerabilities and incorrect configurations in network or web applications.
5. Database scans can identify weak points in a database to prevent malicious attacks, such as SQL injection attacks.

12. Explain the following Hacking Terminologies.

- Ransomware
- Social engineering
- Brute Force Attack
- DDoS attack

ANS.

1. **Ransomware:** Ransomware is a type of malicious software (malware) designed to encrypt files on a victim's computer or network, rendering them inaccessible, and then demand payment (typically in cryptocurrency like Bitcoin) in exchange for providing the decryption key to unlock the files.
2. **Social engineering:** Social engineering is like a trick that hackers play to get what they want. Instead of using fancy computer skills to break into systems, they use clever tactics to manipulate people into giving them access or sensitive information.
3. **Brute Force Attack:** A Brute Force Attack is a straightforward and systematic hacking method used to crack passwords or encryption keys by trying every possible combination until the correct one is found. It's like trying every key until you find the right key to unlock the door.
4. **DDoS attack:** In a DDoS attack, hackers flood a website or online service with so much traffic that it becomes overwhelmed and can't handle all the requests. Block Access: By overwhelming the website's servers or network with fake requests, the attackers effectively block legitimate users from accessing the website or service. Even though the website's servers are still running, they're so busy dealing with the fake traffic that they can't respond to genuine requests

UNIT 2

Understanding DoS and DDoS Attacks, Sniffers, and Session Hijacking in Web Application Security

1. What are DOS and DDOS Attacks? What are the symptoms of Dos Attack?

ANS.

1. A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
2. A DoS attack generally consists of efforts to temporarily interrupt or suspend services of a host connected to the Internet.
3. Distributed denial-of-service attacks are sent by two or more people, or bots.
4. Denial-of-service attacks are sent by one person or system.

Symptoms of DoS Attacks:

1. Unusually slow network performance (opening files or accessing websites
2. Unavailability of a particular website Inability to access any website
3. Dramatic increase in the number of spam emails received (email bomb)
4. Disconnection of a wireless or wired internet connection.

In the case of a wired connection, such as Ethernet, the attacker may flood the network with excessive traffic, causing switches, routers, or other network devices to become overloaded. This overload can lead to network congestion, packet loss, and ultimately the disconnection of the wired connection from the network.

2. How to protect against Dos Attack?

ANS.

1. Firewalls: Imagine a firewall as a security guard for your network. It looks at all the traffic coming in and going out and decides what's allowed and what's not.
2. By setting up strict rules, you can tell the firewall to block any suspicious or harmful traffic while letting the good stuff through.
3. Switches and routers: These are like traffic controllers for your network. You can configure them to control how much data is allowed to flow through at once.
4. Intrusion Prevention Systems (IPS): Think of an IPS as a system that's trained to recognize specific signs of a DoS attack. When it sees those signs, it jumps into action.
5. Traffic analysis tools and network monitoring: They watch the traffic in real-time, looking for anything suspicious.

3. **What is Incident Response? What are the steps involved in an incident response plan?**

ANS.

1. **Incident response is the process of managing and mitigating the effects of security incidents or attacks.**
2. **It involves a set of predefined steps and procedures to detect, contain, eradicate, and recover from security breaches in a timely and effective manner.**

The steps involved in an incident response plan:

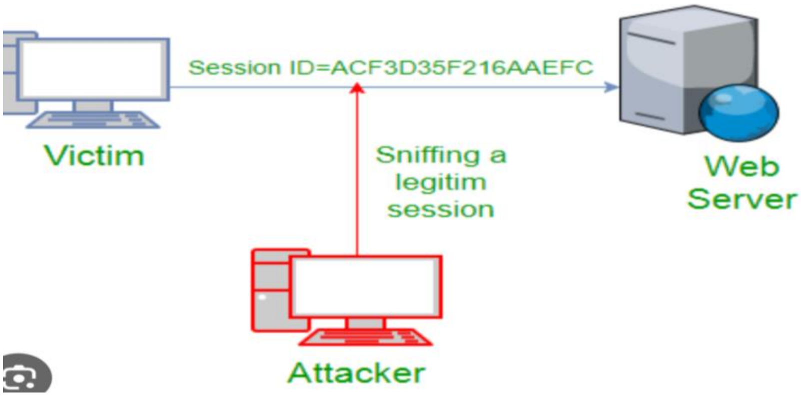
1. Preparation: This phase involves establishing an incident response team and defining their roles and responsibilities. The team should include representatives from IT, security, legal, and other relevant departments. Regular training and exercises should also be conducted to ensure that the team is prepared to respond effectively to incidents.

2. Detection and Analysis: The next step in responding to a security incident is detecting it. This may involve monitoring network traffic or using intrusion detection systems (IDS) to identify suspicious activity.

3. **Containment:** After the incident has been analysed, the next step is to contain it to prevent further damage.
   This may involve isolating affected systems from the network, blocking malicious traffic, or disabling user accounts.
   The goal is to minimize the impact of the incident and prevent it from spreading to other parts of the organization's infrastructure.
4. **Eradication:** Once the incident has been contained, the next step is to eradicate the root cause of the problem.
   This may involve removing malware from infected systems, patching vulnerabilities, or implementing additional security controls to prevent similar incidents from occurring in the future.
5. **Recovery:** After the threat has been neutralized, the organization can begin the process of restoring affected systems and services. This may involve restoring data from backups, rebuilding compromised systems, or implementing additional security measures to enhance resilience against future attacks.
6. **Post-Incident Analysis**: After everything's back in order, they take a good look at what happened. They figure out what went wrong, what they did right, and how they can do better next time.

4. **What are Sniffers? Give GOOD (ETHICAL) USES OF SNIFFERS. Also Why do hackers use packet Sniffers?**

ANS.



- **Sniffers, also known as packet analyzers or protocol analyzers.**
- **Sniffers are tools that intercept and analyze network traffic.**

GOOD (ETHICAL) USES OF SNIFFERS:

1. Network Troubleshooting: Sniffers can be used by network administrators to troubleshoot network issues.
2. By analyzing network traffic, they can identify bottlenecks, misconfigurations, or faulty devices affecting network performance.

WHY DO HACKERS USE PACKET SNIFFING:

- Hackers use packet sniffing attacks for many reasons, such as recording your online activities, reading your emails, and viewing your passwords and banking details.
- data is captured at the packet level, in its raw form, containing zeros and ones – binary digits.

5. **Explain Types of Sniffers. Mention any one tool for each type.**

ANS.

1. **Passive Sniffers:** These sniffers only capture and display packets without interacting with them. They can be used to monitor network traffic and analyze network performance.

Example – Wireshark – is a tool that allows analyst investigate the packets in depth.

It does not let to modify packets. You can only read them. Wireshark is a tool which is capable of Sniffing and investigating live traffic.

2. **Active Sniffers:** These sniffers can inject packets into the network or modify existing packets, allowing them to perform more advanced tasks such as hijacking sessions or launching attacks.

Example – Ettercap – tool for man in the middle attacks on LAN.

Allows for both Active and Passive Sniffing.

Ettercap can inject packets into the network.

3. **Protocol-Specific Sniffers:** Some sniffers are designed to analyze specific network protocols, such as HTTP, FTP, or SNMP, providing a more focused view of network activity.

Example – Fiddler – is a protocol specific sniffer tool designed for analyzing HTTP and HTTPs, FTP traffic.

It provides user friendly interface for capturing, inspecting and modifying HTTP requests and responses.

Commonly used by Web developers and security professionals to analyse web traffic in web applications.

6. How to protect against Sniffer Attacks?

ANS.

1. Use encryption, such as SSL/TLS, to secure data transmitted over the network.

2. Strong authentication mechanisms, such as two-factor authentication, to protect against eavesdropping and unauthorized access.

3. Regularly update network devices and software

4. Implement access control.

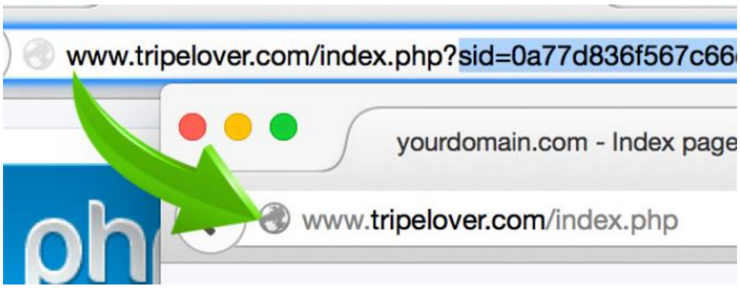
7. What is Session Hijacking. Explain Session Fixation.

Ans. Session hijacking, also known as cookie hijacking, is the exploitation of a

valid computer session to gain unauthorized access to information or services in a computer system.

- Imagine you're using a website, and you log in with your username and password. After you log in, the website gives you a special code (called a session token) to show that you're authorized to use the site. This code is like a ticket that lets you do things on the website, like posting comments or shopping.
- Now, AN ATTACKER wants to use your account without your permission. They could try to steal this special code (session token) to pretend they're you. This is called session hijacking.

Session Fixation:


www.tripelover.com/index.php?sid=0a77d836f567c66
yourdomain.com - Index page
www.tripelover.com/index.php
ph

- **1. Session fixation:** In a session fixation attack, an attacker aims to fixate or control a user's session identifier, such as a session cookie or URL parameter, to gain unauthorized access to the user's account.

1. Initial Access: The attacker begins by accessing the target website or application that uses session identifiers for authentication, such as an online banking site.
2. Session Initiation: The attacker initiates a session with the website, receiving a temporary session identifier from the server.

3. Session Fixation: The attacker creates a link containing the session identifier obtained in step 2 and sends it to the victim, TRICKING them to click on it. This link could be embedded in an email, social media message, or any other form of communication.
4. Victim Interaction: The victim clicks on the link sent by the attacker, unknowingly using the session identifier provided by the attacker to authenticate with the website.
5. Exploitation: With the victim's session now associated with the attacker's identifier, the attacker can access the victim's account, without authentication. They may then perform various malicious activities, such as transferring funds in the case of a banking website, changing account settings, or accessing sensitive information.
6. Maintaining Access: The attacker may continue to exploit the compromised session for as long as it remains VALID.

8. Explain Physical access and File storage methods of Session Hijacking.

ANS.

Physical access: When you log in to a website or application, the server generates a session token for you. This token is stored temporarily in the server's memory.

- The server keeps track of which token belongs to which user so that it can recognize you when you make more requests.
- **File Storage:** Sometimes, especially for more complex systems or when sessions need to last longer than just the current session, session tokens are stored in files on the server's hard drive. These files contain information about your session, including your session token.

Why is it Vulnerable?

- If someone gets physical access to the server where these session tokens are stored, they could potentially steal them.
- Memory Access: If an attacker gains access to the server's memory, they could find the session token associated with your session.
- File Access: Similarly, if they can access the files where session tokens are stored, they could retrieve them from there.

9. How will you mitigate the risk of session Hijacking?

ANS.

Mitigating the Risk To prevent this, developers and system administrators implement security measures:

- Encryption: (SSL/TLS) Session tokens should be encrypted when stored, making them unreadable even if someone gains access to them.
- Access Controls: Limiting physical access to the server.
- Regular Security Checks: Periodic audits and checks help identify vulnerabilities that could be exploited by attackers.
- Token Lifespan: Session tokens should have a limited lifespan, expiring after a certain period of inactivity or when the user logs out.
- Encourage users to log out of websites when they are finished using them to reduce the risk of session hijacking