**Introduction to Ethical Hacking Terminology-Five stages of hacking-**

**Ethical Hacking-**

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.

This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

**key concepts of ethical hacking**-

Hacking experts follow four key protocol concepts:

Stay legal. Obtain proper approval before accessing and performing a security assessment.

Define the scope. Determine the scope of the assessment so that the ethical hacker’s work remains legal and within the organization’s approved boundaries.

Report vulnerabilities. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.

Respect data sensitivity. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

An ethical hacker should have a wide range of computer skills. They often specialize, becoming subject matter experts (SME) on a particular area within the ethical hacking domain.

All ethical hackers should have:

* Expertise in scripting languages.
* Proficiency in operating systems.
* A thorough knowledge of networking.
* A solid foundation in the principles of information security.

limitations of ethical hacking-

* Limited scope. Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it’s not unreasonable to discuss out of scope attack potential with the organization.
* Resource constraints. Malicious hackers don’t have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.
* Restricted methods. Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).

**Five stages of hacking-**

**1. Reconnaissance**

When it comes to penetration testing, the first natural question is – What is the first hacking phase?

Before performing any penetration tests, hackers footprint the system and gather as much information as possible. Reconnaissance is a preparatory phase where the hacker documents the organization’s request, finds the system’s valuable configuration and login information and probes the networks. This information is crucial to performing the attacks and includes:

* Naming conventions
* Services on the network
* Servers handling workloads in the network
* IP Addresses
* Names and Login credentials of users connected to the network
* The physical location of the target machine

**2. Scanning**

In this stage, the ethical hacker begins testing the networks and machines to identify potential attack surfaces. This involves gathering information on all machines, users, and services within the network using automated scanning tools. Penetration testing typically undertakes three types of scans:

* Network Mapping
* This involves discovering the network topology, including host information, servers, routers, and firewalls within the host network. Once mapped, white hat hackers can visualize and strategize the next steps of the ethical hacking process.
* Port Scanning
* Ethical hackers use automated tools to identify any open ports on the network. This makes it an efficient mechanism to enumerate the services and live systems in a network and how to establish a connection with these components.
* Vulnerability Scanning
* The use of automated tools to detect weaknesses that can be exploited to orchestrate attacks.
* While there are several tools available, here are a few popular ethical hacking tools commonly used during the scanning phase:
* SNMP Sweepers
* Ping sweeps
* Network mappers
* Vulnerability scanners

**3. Gaining Access**

Once ethical hackers expose vulnerabilities through the process’s first and second hacking phases, they now attempt to exploit them for administrative access. The third phase involves attempting to send a malicious payload to the application through the network, an adjacent subnetwork, or physically using a connected computer. Hackers typically use many hacking tools and techniques to simulate attempted unauthorized access, including:

* Buffer overflows
* Phishing
* Injection attacks
* XML External Entity processing
* Using components with known vulnerabilities

If the attacks are successful, the hacker has control of the whole or part of the system and may simulate further attacks such as data breaches and Distributed Denial of Service (DDoS).

**4. Maintaining Access**

The fourth phase of the ethical hacking process involves processes to ensure the hacker can access the application for future use. A white-hat hacker continuously exploits the system for further vulnerabilities and escalates privileges to understand how much control attackers can gain once they pass security clearance. Some attackers may also try to hide their identity by removing the evidence of an attack and installing a backdoor for future access.

**5. Clearing Tracks**

To avoid any evidence that leads back to their malicious activity, hackers perform tasks that erase all traces of their actions. These include:

* Uninstalling scripts/applications used to carry out attacks
* Modifying registry values
* Clearing logs
* Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

* Tunneling
* Stenography