Ethical Hacking

Lecture -2 (Theory)
Terms and Testing of Ethical Hacking

M.Sc. Halo Khalil Sharif

2025 - 2026

Outlines

- Important Hacking Terms
- About Hackers
- Hacker Classes\Types
- Types of Tests in Eth. Hacking
- Hacking Phases

Important Hacking Terms

- ***Target:***
  The system or organization which will be attacked by the hacker.

- ***Vulnerability:***
  A weakness in a system, organization, software, etc. that could lead to data disclosure or alteration, unauthorized access, or denial of service.

- ***Exploit:***
  A method or technique used to exercise a vulnerability, to help improve its security, rather than for malicious purposes.

Important Hacking Terms

- ***<u>“Zero-day” Vulnerablility:</u>***

Refers to a software flaw that is unknown to the software vendor or the general public. This vulnerability can be exploited by attackers before it is discovered or patched by the vendor, meaning there are "zero days" of warning or preparation. Once it’s found and disclosed, the software company typically has to rush to create a security patch, which might take time depending on the complexity of the issue.

<u>Example:</u> August 27, 2001, Internet Explorer 6 is released.

November 3, 2010, a Zero day announced (after 9 years).

December 14, 2010, “MS10-090 patch is released.

Important Hacking Terms

❖ Authentication

Authentication refers to the process of verifying the identity of a user, device, or system attempting to access a network, application, or service. Authentication is usually based on a username and password. The username and password are used to validate the true identity of an individual.

Types of Authentication Methods:

- **Single-factor authentication (SFA)**: Uses only one form of identification, such as a password. SFA is generally less secure.
- **Two-factor authentication (2FA)**: Adds a second layer of security, such as a one-time code sent to a phone or generated by an app.
- **Multi-factor authentication (MFA)**: Requires multiple factors, such as a password, biometric verification, and a one-time code . MFA is generally the most secure.

Important Hacking Terms

- **Authorization:** After authentication, authorization determines the permissions and access levels that are granted to the authenticated user.

- **Blacklisting**

Blacklisting is one of the basic tools in cyber security. Organizations should constantly blacklist IP addresses that have developed malicious activities like phishing or spam.

- **Bot**

A bot is a software robot that uses the internet or within a system to do automated operations (scripts).

Important Hacking Terms

❖ **Ransomware**

Ransomware is a type of malicious software, or malware, used by cybercriminals to infect and control a victim’s data, computer or network. It encrypts the files or locks the system, rendering the data or services inaccessible to the user. The attacker then demands a ransom, often in cryptocurrency (typically in bitcoin), in exchange for a decryption key or other means to restore access.

Types of Ransomware:

- **Crypto Ransomware**: Encrypts files, requiring a decryption key.
- **Locker Ransomware**: Locks the user out of their system entirely.
- **Double Extortion Ransomware**: Encrypts data and threatens to release it publicly if the ransom is unpaid.

About Hackers

Hackers can be categorized several different ways, based upon: Motivation, goals, which side (good or bad) they are on, skills, etc.

Ethi

Hacker Classes\Types

❖ <u>White Hat Hacker</u>

- Good guys.
- Don’t use their skills for illegal purpose.
- Computer security experts and help to protect from Black Hat.

[illegible]

❖ <u>Black Hat Hacker</u>

- Bad guys.
- Use their skills for personal gain, such as money, revenge, etc.
- Hack banks, steal credit cards, and deface websites.

❖ <u>Gray Hat Hacker</u>

- Can be good or bad.
- It is combination of White and Black Hat Hackers.
- Use their skills to provide national security.

Types of Tests

Types of tests depend upon what your goal is:

- Vulnerability testing.
- Full penetration testing.
- Targeted testing.
- Black box testing.
- Grey box testing.
- White box testing.

Vulnerability testing

Vulnerability Scanning

- **Purpose**: Identifies known vulnerabilities in a system, application, or network.
- **Method**: Uses automated tools to scan for vulnerabilities like outdated software, misconfigurations, and missing patches.
- **Example Tools**: Nessus, OpenVAS.

Vulnerability Testing

- Testing for vulnerabilities only – no exploits

Full penetration testing

Penetration Testing (Pen Testing)

- **Purpose**: Simulates a real-world cyberattack to find and exploit vulnerabilities.
- **Method**: Ethical hackers (penetration testers) try to exploit vulnerabilities in systems, applications, or networks.
- **Types**:
  - *Black Box Testing*: No prior knowledge of the system is provided to the tester.
  - *White Box Testing*: Full knowledge of the system is provided.
  - *Gray Box Testing*: Partial knowledge is given to the tester.
- **Example Tools**: Metasploit, Burp Suite, Nmap.

ull Penetration Testing

- Full-on testing for all targets and all possible attack vectors

Targeted testing

Targeted testing in ethical hacking is a collaborative approach where both the tester (ethical hacker) and the organization's IT team work closely together to test specific systems, applications, or areas of the network for vulnerabilities. It’s sometimes referred to as **"collaborative testing"** or **"cooperative testing."**

Targeted Testing

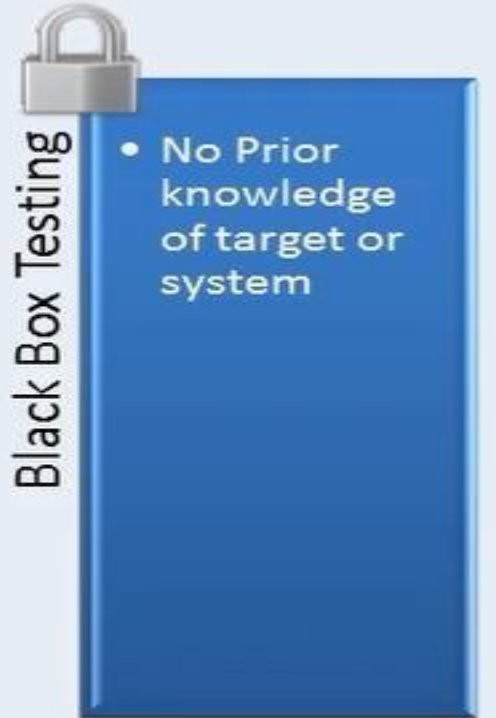
- Targets only specific pieces of the infrastructure

Black Box Testing

It refers to a security assessment methodology where the tester has **no prior knowledge** of the internal workings, architecture, or code of the target system. The approach mimics the perspective of an external attacker who tries to compromise the system without insider information.

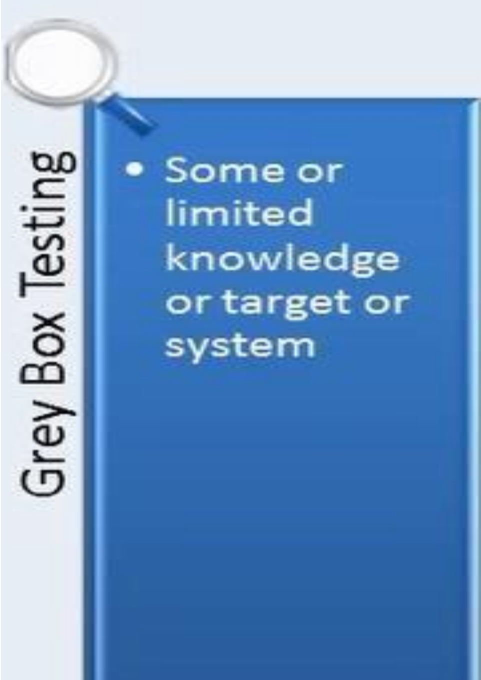
Applications in Ethical Hacking:

- **Web Applications**: Testing for vulnerabilities like SQL injection,
- cross-site scripting (XSS), or authentication bypass.
- **Networks**: Identifying open ports, misconfigured firewalls,
- or unpatched systems.
- **IoT Devices**: Exploring firmware or hardware vulnerabilities.
- **APIs**: Testing for improper access controls or data exposure.



Gray Box Testing

It refers to a security testing approach where the tester has partial knowledge of the internal structure or details of the target system, application, or network. It is a middle ground between **black box testing** (where the tester has no prior knowledge) and **white box testing** (where the tester has full knowledge).



Grey Box Testing

- Some or limited knowledge or target or system

white Box Testing

also known as **clear-box testing**, **glass-box testing**, or **transparent-box testing**, is a security assessment method where the tester has complete knowledge of the system being tested. This includes access to:

- **Source Code**: Full visibility into the software's codebase to identify vulnerabilities.
- **Architecture Documentation**: Information about the design, frameworks, and infrastructure of the system.
- **Network Configurations**: Knowledge about firewalls, routers, and internal systems.
- **Credentials**: Access to login details or authentication mechanisms.

White Box Testing

- Full system knowledge or access to architecture, etc.

Hacking Phases

1) Reconnaissance:

   Preparation phase, in which attacker gathers information about the target.

2) Scanning:

   Attacker gather infrastructure & vulnerability information

3) Gaining Access:

   Attacker actually penetrates systems.

4) Maintaining Access:

   Attacker tries to keep, extend, and escalate access to systems.

5) Clearing Tracks:

   Attacker tries to avoid detection

5 Stages of Hacking

Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Track

Reconnaissance\Footprinting

- It refers to the preparatory phase where an attacker gathers as much information as possible about the target.

- **Purpose:** this information will assist the hacker to narrow down to specific targets

, techniques, and avoid broad-scan.

- Gathering information about:

–Employees

–Organizational activities & business.

–Network infrastructure.

–Security.

Types of Information Gathered in Reconnaissance\Footprinting

- Types of systems & equipment.
- Operating systems.
- Applications & versions.
- Phone numbers.
- Products.
- Contracts.
- Financial data.
- Network infrastructure.
- Security methods & procedures.

Reconnaissance Types

❖ ***Passive reconnaissance:***

- The attacker does not interact or contact with the system directly.
- The attacker uses publicity available information such as “Google search” or “Browsing company web page”.

❖ ***Active reconnaissance:***

- The attacker tries to interact or contact with the system directly (Ex: ping).
- He may takes photos\ videos for the target or by using tools to detect router locations, network mapping, details of operation systems, and applications.

Have a nice Day!