CYBER SECURITY AND ETHICAL HACKING

Overview

Chapter1

Bilal.H.Ali

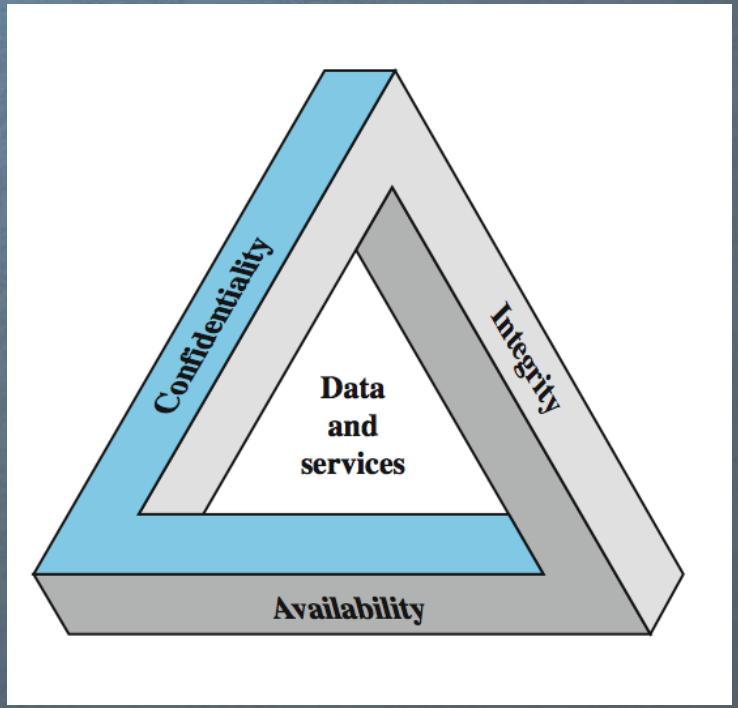
2022-2023

SECURITY

- **Computer security:**

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

- Confidentiality
- Integrity
- availability



SECURITY

Computer security:

- **Confidentiality:** Confidentiality measures protect information from unauthorized access and misuse.
- **Integrity:** Integrity measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of data.
- **Availability**: In order for an information system to be useful it must be available to authorized users. Availability measures protect timely and uninterrupted access to the system.

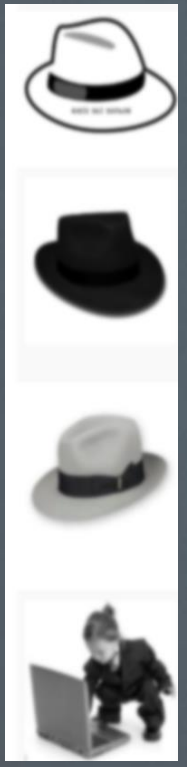
ETHICAL HACKING

introduction

- **Hack:** Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data.
- **Hacker**: A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.
- **Type of Hacker**
    - White Hat hacker
    - Black Hat hacker
    - Gray Hat hacker
    - Hacktivist
    - Hack terrorist
    - Script kiddies

ETHICAL HACKING

Type of Hacker



- **White Hat hacker(Ethical Hacker):** A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
- **Black Hat hacker(Cracker):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- **Gray Hat hacker:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
- **Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- **Hack terrorist and suicidal and ……**

ETHICAL HACKING

What is Ethical Hacking?

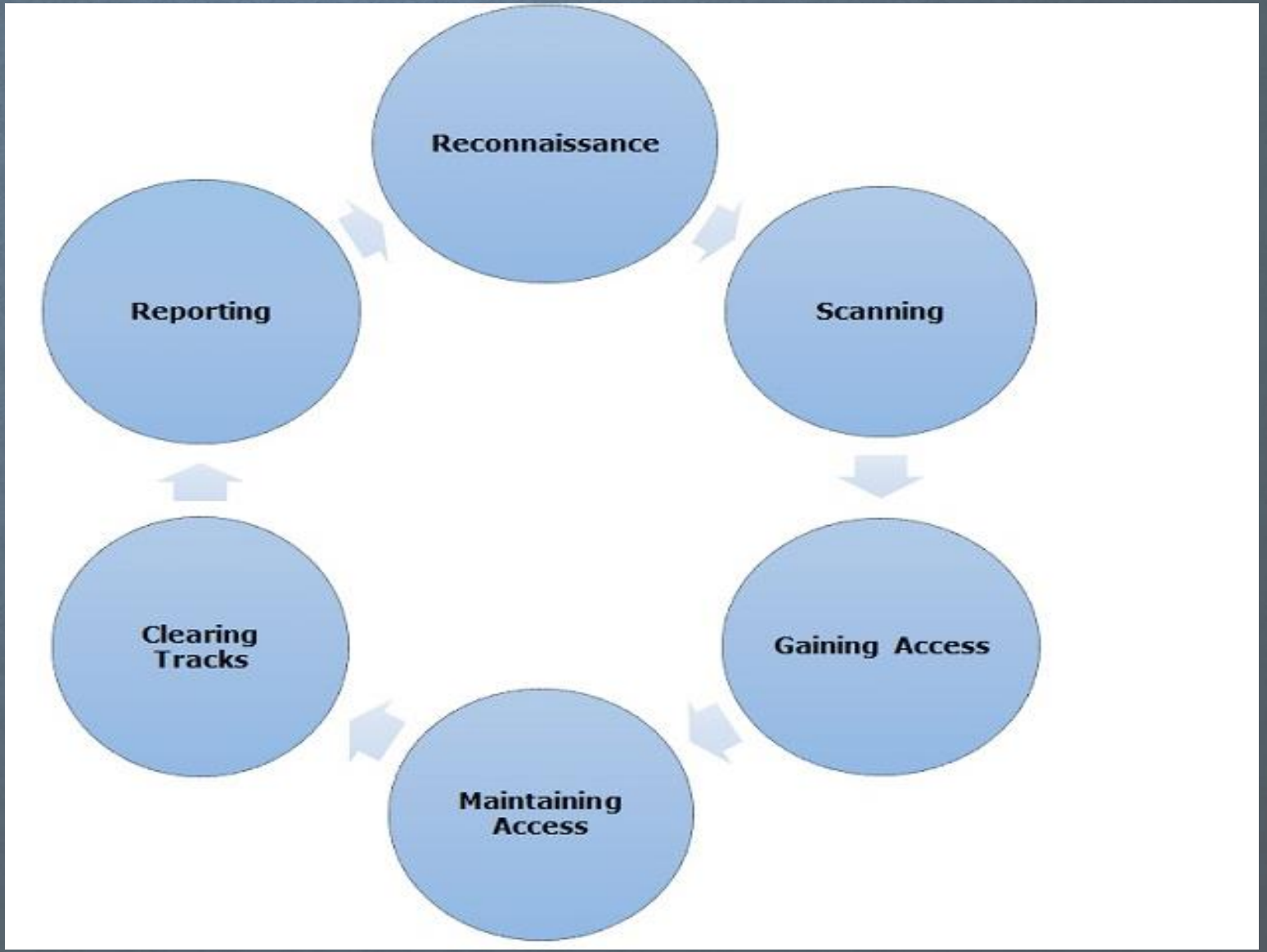
Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

Penetration Test: A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities

- Type of Pen
  - White Box Pen Test: In a white box assessment, the tester will be provided with full information about the application and its technology, and will usually be given credentials with varying degrees of access to quickly and thoroughly identify vulnerabilities in the applications, systems, or networks.
  - Black Box Pen Test: In a black box assessment, the testers are given very little or no information about the networks or systems they are testing.
  - Gray Box Pen Test: Gray box assessments are a hybrid of white and black box testing and are typically used to provide a realistic testing scenario while also giving penetration testers enough information to reduce the time needed to conduct reconnaissance and other black box testing activities.

ETHICAL HACKING

Pen Testing Phases



ETHICAL HACKING

Pen Testing Phases

- **Reconnaissance or Footprinting** : The reconnaissance or information-gathering phase is where the attacker focuses on acquiring meaningful information about their target. This is the most important phase in hacking: the more details known about the target, the easier it is to compromise a weakness and exploit it.

The following are techniques used in the reconnaissance phase:

- Using social networking platforms
- Performing Google hacking
- Performing DNS interrogation
- Social engineering

- Active: **directly** interact with the computer system to gain information. (call)
- Passive: you will not be directly connected to a computer system.(Google, news)

ETHICAL HACKING

Pen Testing Phases

- **Scanning**: The second phase of hacking is scanning. Scanning involves using a direct approach in engaging the target to obtain information that is not accessible via the reconnaissance phase. This phase involves profiling the target organization, its systems, and network Infrastructure.
  - The following are techniques used in the scanning phase:
  - Checking for any live systems
  - Checking for firewalls and their rules
  - Checking for open network ports
  - Checking for running services
  - Checking for security vulnerabilities
  - Creating a network topology of the target network

ETHICAL HACKING

Pen Testing Phases

- **Gaining access**: This phase can sometimes be the most challenging phase of them all. In this phase, the attacker uses the information obtained from the previous phases to exploit the target. Upon successful exploitation of vulnerabilities, the attacker can then remotely execute malicious code on the target and gain remote access to the compromised system.
  - The following can occur once access is gained:
  - Password cracking
  - Exploiting vulnerabilities
  - Escalating privileges
  - Hiding files
  - Lateral movement

ETHICAL HACKING

Pen Testing Phases

- **Maintaining access:** After exploiting a system, the attacker should usually ensure that they are able to gain access to the victim's system at any time as long as the system is online. This is done by creating backdoor access on the target and setting up a persistence reverse or bind connection between the attacker's machines and the victim's system.
  - The objectives of maintaining access are as follows:
  - Lateral movement
  - Exfiltration of data
  - Creating backdoor and persistent connections

ETHICAL HACKING

Pen Testing Phases

- **Covering tracks:** The last phase is to cover your tracks. This ensures that you do not leave any traces of your presence on a compromised system. As penetration testers, we would like to be as undetectable as possible on a target's network, not triggering any alerts while we remove any residual traces of the actions performed during the penetration test.
- **Reporting:** Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

ETHICAL HACKING(TERMS)

- Target:
- Vulnerability : A vulnerability is a weakness or defect that exists within technical, physical, or human systems that hackers can exploit in order to gain access to or control over systems within a network.
- Weakness: Weaknesses and vulnerabilities are both states that indicate security risks. While weakness refers to an application error or bug, it may escalate to a vulnerability in cases where it can be exploited to perform a malicious action.
- Attack:

ETHICAL HACKING(TERMS)

- Backdoor: In the world of cybersecurity, a backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.
- Zero Day: Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it.
- Risk: Risk is the potential impact that a vulnerability, threat, or asset presents to an organization calculated against all other vulnerabilities, threats, and assets.

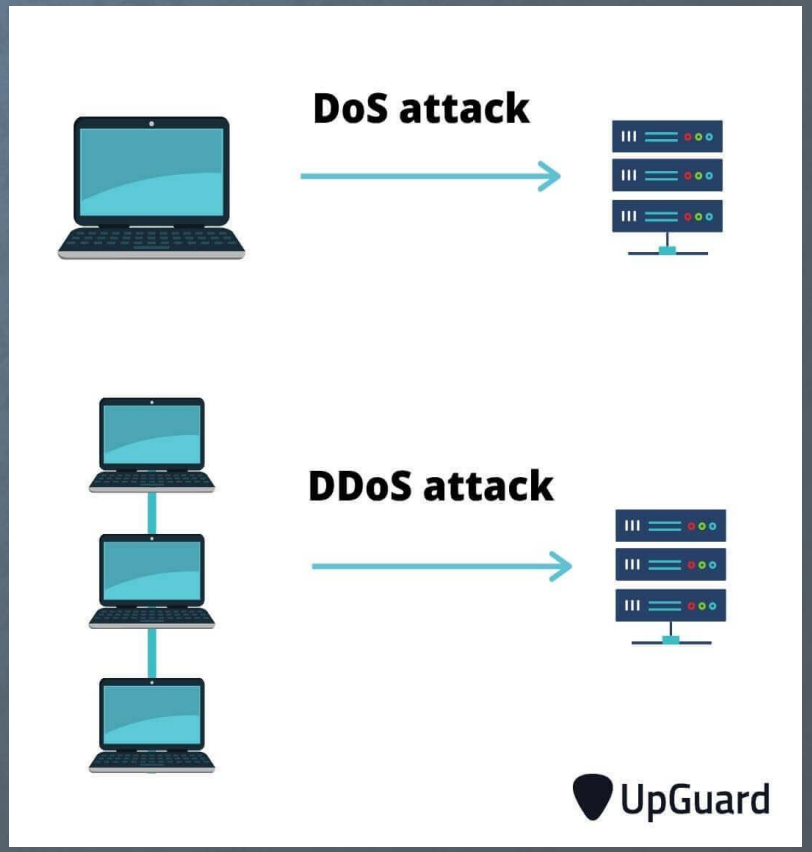
ETHICAL HACKING(TERMS)

DOS and DDOS:

A denial of service (DoS) is a type of cyber-attack that floods a computer or network

so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network.

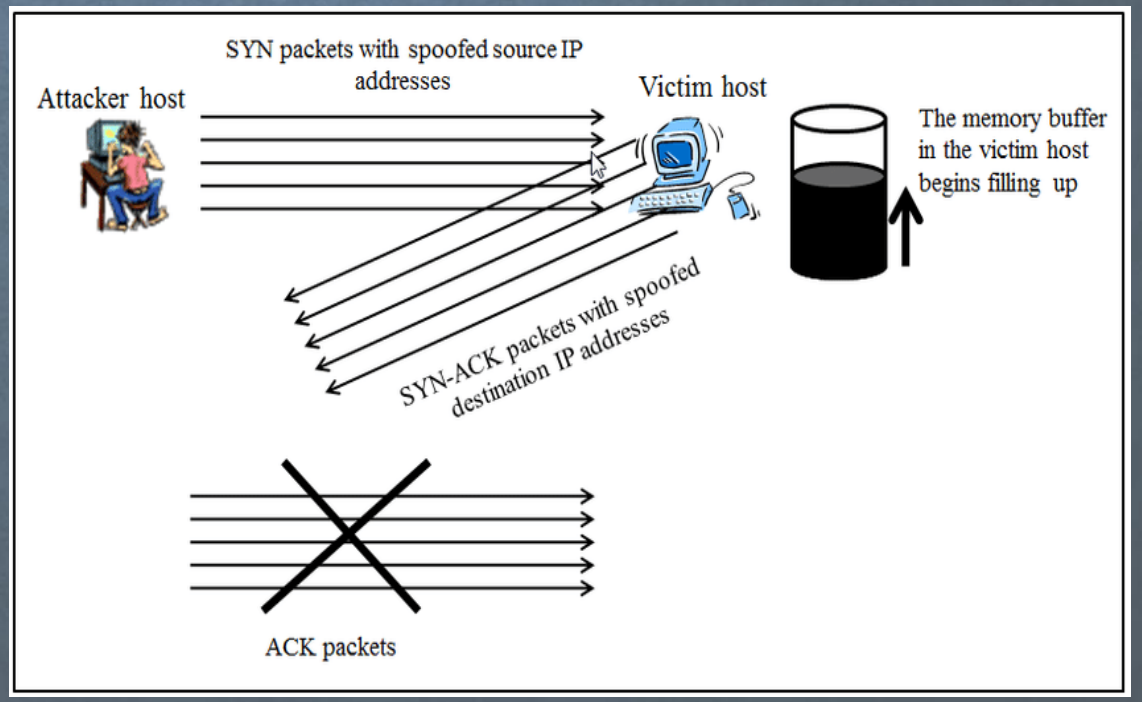
- .



ETHICAL HACKING(TERMS)

TCP SYN flood attack:

- In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake.
- Increase the size of the connection queue and decrease the timeout on open connections.



ETHICAL HACKING

Threat: thread and types

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

- Humans
  - Nonmalicious
  - Malicious
  - Random: In a random attack the attacker wants to harm any computer or user
  - Directed: In a directed attack, the attacker intends harm to specific computers, perhaps at one organization
- Nonhuman

ETHICAL HACKING

Methods of attack

- spoofing
- Social Engineering
- Footprinting
- Password Hacking:
- **Botnets:**
- man-in-the-middle (MITM):
- **Sniffing:**
- SQL Injections,
- Cross-site Scripting,
- Rootkits,
- TCP SYN flood attack,
- **Session hijacking**

ETHICAL HACKING

Methods of attack

- Social Engineering：social engineering techniques to find vulnerabilities
  - phishing：send Email
- Footprinting

Password Hacking: With the right password, a cyber-attacker has access to a wealth of information.

Social engineering is a type of password attack.

- Botnets: Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks.
- man-in-the-middle (MITM): (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network.
- Sniffing: Collect and monitor when information is exchanged. wireshark
- SQL Injections, Cross-site Scripting, Rootkits, TCP SYN flood attack, **Session hijacking**

ETHICAL HACKING

Methods of attack

- **Spoofing**, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware.

Spoofing attacks come in many forms, including:

- Email spoofing
- Website and/or URL spoofing
- Caller ID spoofing
- Text message spoofing
- GPS spoofing
- Extension spoofing
- IP spoofing
- Facial spoofing

ETHICAL HACKING

Methods of attack:Types of spoofing

- Email spoofing: is the act of sending emails with false sender addresses, usually as part of a phishing attack designed to steal your information, infect your computer with malware or just ask for money.
- Website and/or URL spoofing: is all about making a malicious website look like a legitimate one. The spoofed site will look like the login page for a website you frequent—down to the branding, user interface, and even a spoofed domain name that looks the same at first glance. Cybercriminals use spoofed websites to capture your username and password (aka login spoofing) or drop malware onto your computer (a drive-by download).
- Caller ID spoofing: happens when scammers fool your caller ID by making the call appear to be coming from somewhere it isn't. Scammers have learned that you're more likely to answer the phone if the caller ID shows an area code the same or near your own. In some cases, scammers will even spoof the first few digits of your phone number in addition to the area code to create the impression that the call is originating from your neighborhood (aka neighbor spoofing).

ETHICAL HACKING

Methods of attack:Types of spoofing

- Text message spoofing: or SMS spoofing is sending a text message with someone else's phone number or sender ID. Companies frequently spoof their own numbers, for the purposes of marketing and convenience to the consumer, by replacing the long number with a short and easy to remember alphanumeric sender ID. Scammers do the same thing—hide their true identity behind an alphanumeric sender ID, often posing as a legitimate company or organization.

The spoofed texts will often include links to

  - SMS phishing sites (smishing)
  - malware downloads.

- GPS spoofing: occurs when you trick your device's GPS into thinking you're in one location, when you're actually in another location.
- Extension spoofing: Extension spoofing occurs when cybercriminals need to disguise executable malware files. One common extension spoofing trick criminals like to use is to name the file something along the lines of "filename.txt.exe." The criminals know file extensions are hidden by default in Windows so to the average Windows user this executable file will appear as "filename.txt."

ETHICAL HACKING

Methods of attack:Types of spoofing

- IP spoofing: is used when someone wants to hide or disguise the location from which they're sending or requesting data online. (vpn)
- Facial spoofing

Facial spoofing might be the most personal, because of the implications it carries for the future of technology and our personal lives. As it stands, facial ID technology is fairly limited. We use our faces to unlock our mobile devices and laptops, and not much else. Soon enough though, we might find ourselves making payments and signing documents with our faces. Imagine the ramifications when you can open up a line of credit with your face. Scary stuff.