Ethical Hacking

Lecture -1 (Theory)
Introduction

Halo Khalil Sharif
•B.Sc.- Computer Science.
•M.Sc.- Computer Science.

Email: halo.sharif@univsul.edu.iq

Ethical Hacking

What is Hacking

Hacking: It means to attack systems, networks, and applications by exploiting their weaknesses, in order to gain an unauthorized access to data and systems, using some techniques of hacking.

Example

login into an email account that is not supposed to have access, gaining access to a remote computer or reading information that you are not supposed to have access.

Goals of Hacking

The goals of hacking are: data theft, destruction or alteration, unauthorized access, or any other unauthorized action or purpose.

1. Gaining Unauthorized Access

To gain entry to systems, networks, or accounts without authorization.

2. Data Theft or Extraction

To obtain sensitive information like personal data, financial records, intellectual property, or trade secrets.

3. Financial Gain

To make money through illegal activities such as credit card theft, or selling compromised data.

4. Causing Disruption or Denial of Service

To disrupt or disable services, networks, or websites, often through attacks like Distributed Denial of Service (DDoS).

5. Destruction of Data or Systems

To destroy or corrupt data, delete files, or make systems unusable.

6. Espionage and Intelligence Gathering

To gather sensitive information about an organization, government, or individual.

What is Ethical Hacking?

Is the use of hacking knowledge, skills, tools, and techniques to demonstrate the true exploitable vulnerabilities of a system for the purposes of better securing it.

Ethical hackers, also known as "**white hat hackers**," are typically employed or authorized by organizations to conduct these tests, following a structured and legally compliant process to ensure their work is both safe and lawful.

Why Ethical Hacking is Important

- To prevent hackers from gaining access to information breaches.
- To fight against terrorism and national security breaches.
- To build a system that avoids hackers from penetrating.
- To test if organization's security settings are in fact secure.

Hackers

A hacker is an individual or group skilled in computer programming, networking, and systems who uses their knowledge to gain unauthorized access to computers, networks, and data.

Motivations

- Money.
- Revenge.
- Fun. ♣
- Espionage.
- Damage to people or organization.
- Hacker reputation.
- Access to Restricted Information
- Learning and Improvement

Hacker Vs. Ethical Hacker

❖ **Hacker**

- Breaks the law.
- Access computer system or network without authorization to achieve a goal outside of the creator's original purpose.

❖ **Ethical Hacker**

- Performs most of the same activities but with owner's permission.
- Employed by companies to perform Penetration Tests.

History of Hacking

- The first hacker was appeared in 1960's at the Massachusette Institute of Technology (MIT).

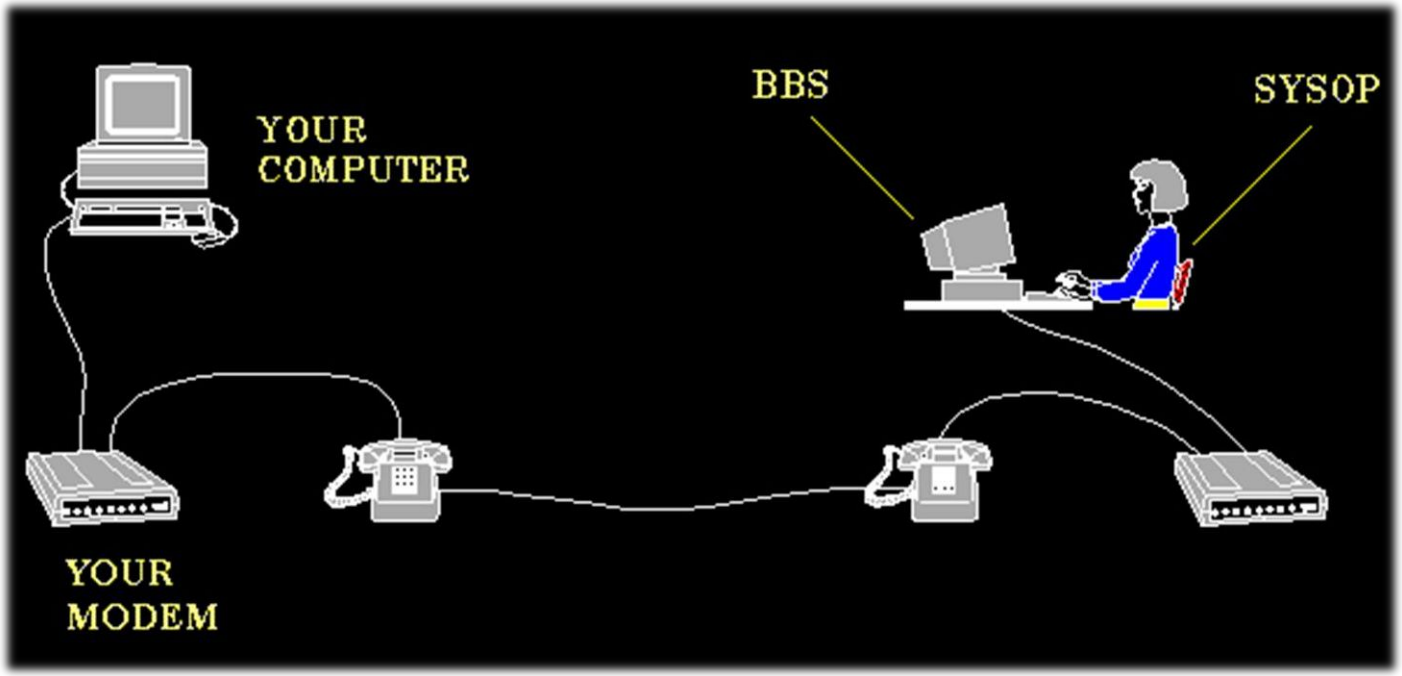
- During the 1970's, a different kind of hacker appeared:

  Phone

  Phreaker (PP) or Phone Hacker (PH).

History of Hacking

- In the 1980's, phreaks started to migrate to computers, and the first Bulletin Board System (BBS) appeared.



History of Hacking

During the 1990's, when the use of internet widespread around the world, hackers multiplied.

Some Famous Hacker

- **Kevin Mitnick**
  - He is the most famous hacker.
  - In 1981, at the age of 17, he get into a phone exchange, which allowed him to redirect subscriber calls in any way he wanted.

Some Famous Hacker

- **Robert Morris**
  - In 1988, he intended the worm program to infect only the MIT network. But during a 12-hour period, it spread rapidly, infecting thousands of systems forcing some universities to shut down their computers.

- **Mark Abene**
  - In 1991, in response to the AT&T telephone system crash that left 60,000 customers without a phone line for nine hours

See you next week

..