University of Babylon College of
information Technology
Department of Information Security

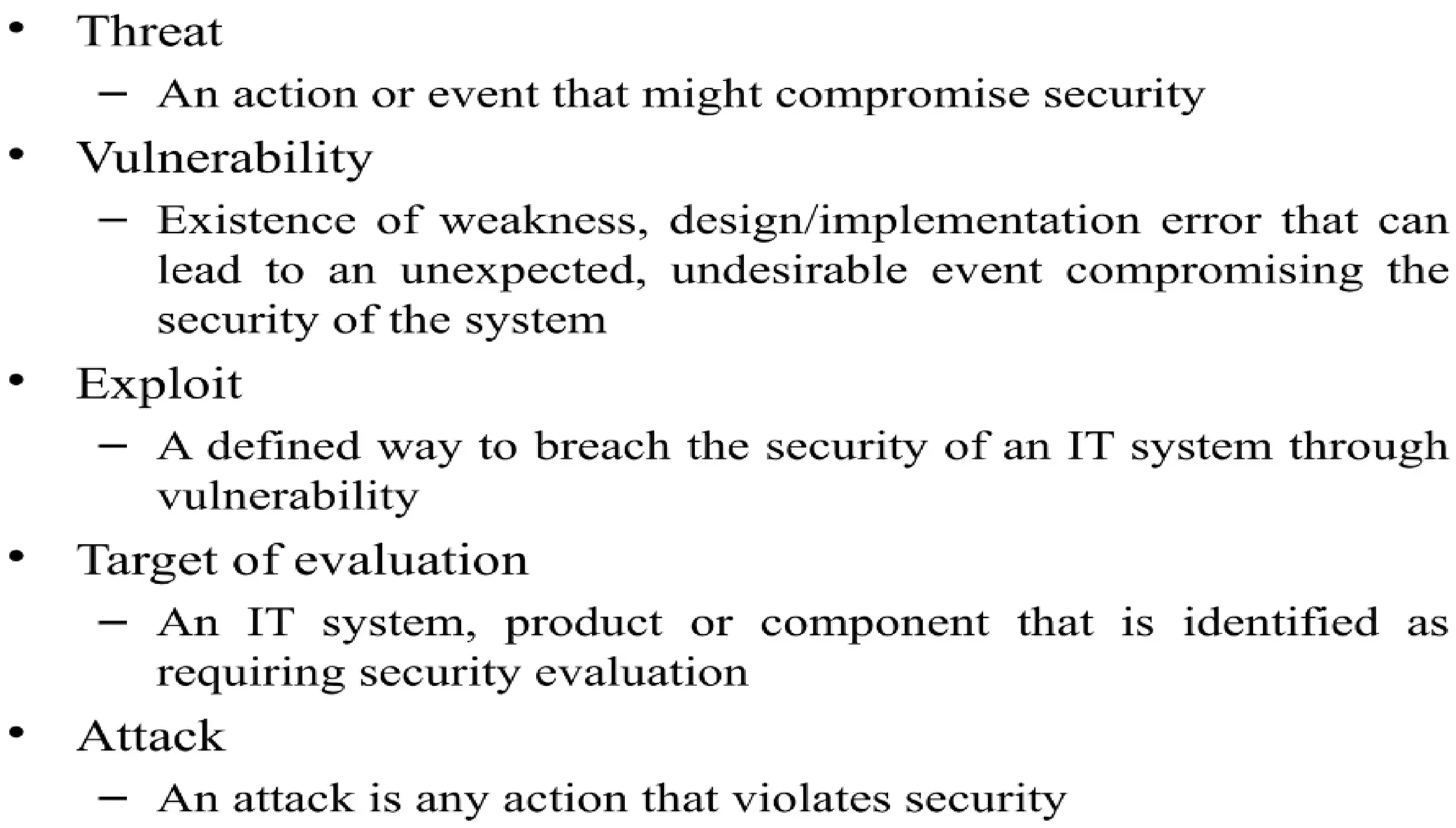
Ethical Hacking
Lecture 1: Introduction to Ethical Hacking

Asst.Lect. Rasha Hussein

What Is Ethical Hacking?

- Ethical hacking is the practice of testing a computer system, network, or application to find security vulnerabilities that could be exploited by malicious hackers. Also known as ‘white hat’ hackers, ethical hackers use the same methods and techniques as their counterparts with malicious intent, but they do so with permission from the owner of the system being tested. Ethical hacking is often mistaken for penetration testing, but pen testing is just a part of what an ethical hacker does.

Terminology

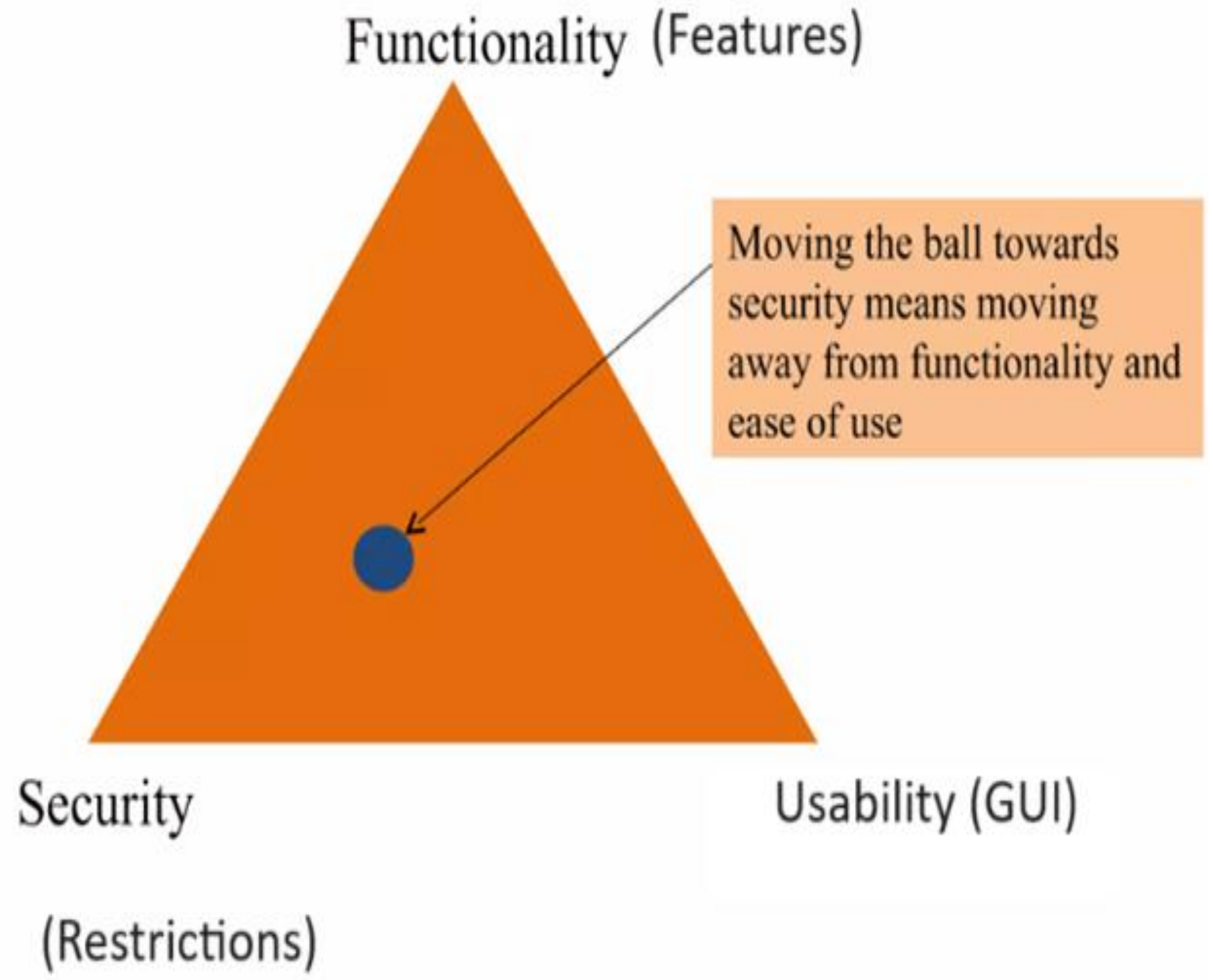


- Threat
  - An action or event that might compromise security
- Vulnerability
  - Existence of weakness, design/implementation error that can lead to an unexpected, undesirable event compromising the security of the system
- Exploit
  - A defined way to breach the security of an IT system through vulnerability
- Target of evaluation
  - An IT system, product or component that is identified as requiring security evaluation
- Attack
  - An attack is any action that violates security

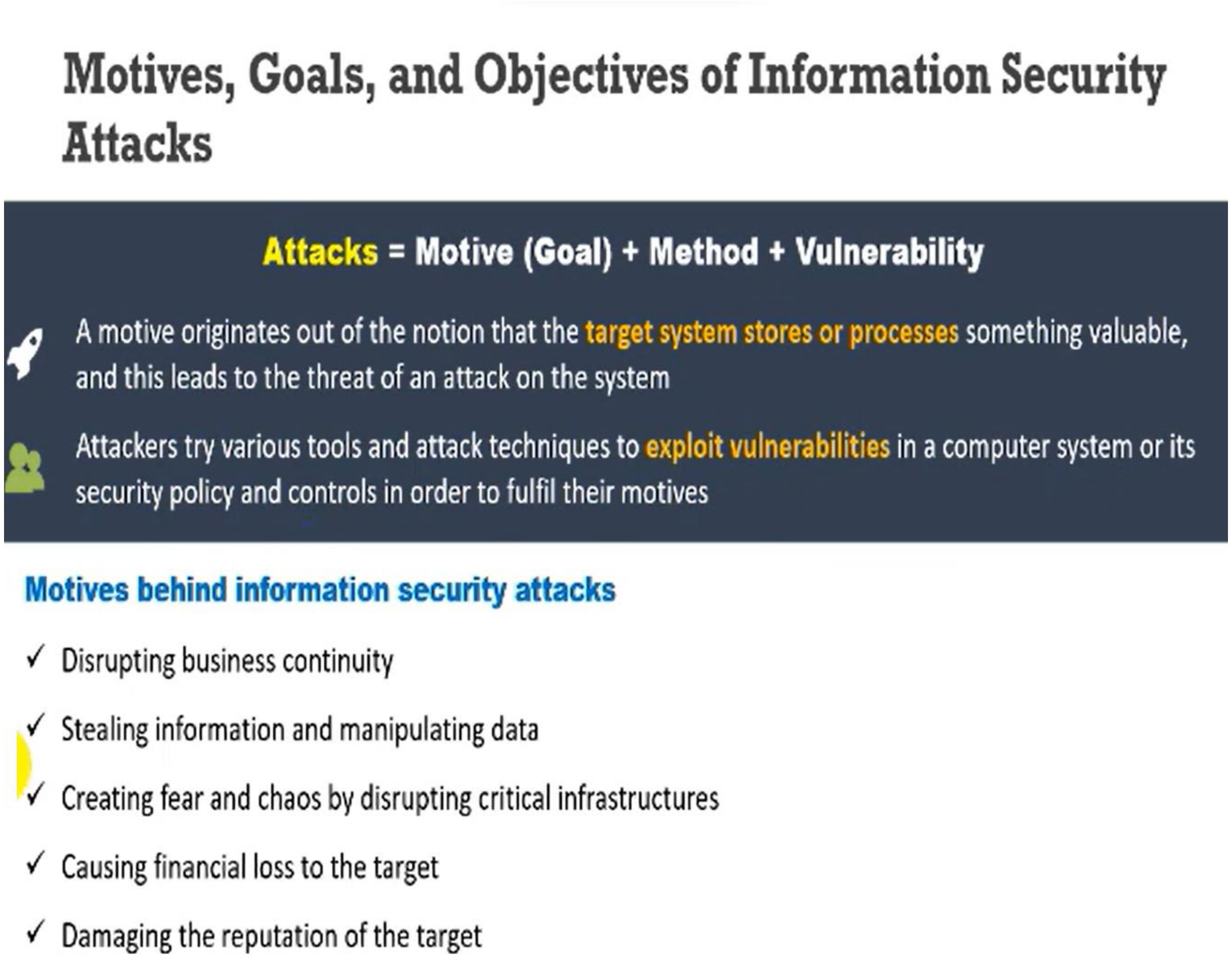
- Hack Value: is the notion among hackers that something is worth doing or is interesting. Hackers might feel that breaking down the toughest network security might give them great satisfaction, and that it is something they accomplished that not everyone could do.

The Security, Functionality, and Usability Triangle

- Level of security in any system can be defined by the strength of three components : The **Security, Functionality, and Usability** Triangle


Functionality (Features)
Moving the ball towards security means moving away from functionality and ease of use
Security
(Restrictions)
Usability (GUI)

Motives, Goals, and Objectives of Information Security Attacks



Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system

Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

Motives behind information security attacks

- ✓ Disrupting business continuity
- ✓ Stealing information and manipulating data
- ✓ Creating fear and chaos by disrupting critical infrastructures
- ✓ Causing financial loss to the target
- ✓ Damaging the reputation of the target

Information Security Threats

Information security threats are broadly classified into three categories, as follows:

1. Natural Threats

Natural threats include natural disasters such as earthquakes, hurricanes, floods, or any nature-created disaster that cannot be stop. Information damage or lost due to natural threats cannot be prevented as no one knows in advance that these types of threats will occur. However, you can implement a few safeguards against natural disasters by adopting disaster recovery plans and contingency plans.

2. Physical Security Threats

Physical threats may include loss or damage of system resources through fire, water, theft, and physical impact. Physical impact on resources can be due to a collision or other damage, either intentionally or unintentionally. Sometimes, power may also damage hardware used to store information.

3. Human Threats

Human threats include threats of attacks performed by both insiders and outsiders. Insider attacks refer to attacks performed by disgruntled or malicious employees. Outsider attacks refer to attacks performed by malicious people not within the organization. Insider attackers can be the biggest threat to information system as they may know the security posture of the information system, while outsider attackers apply many tricks such as social engineering to learn the security posture of the information system.

Information Security Threats

3. Human threats can be further classified into three types, as follows:

- **Network Threats**

A network is defined as the collection of computers and other hardware connected by communication channels to share resources and information. As the information travels from one computer to the other through the communication channel, a malicious person may break into the communication channel and steal the information traveling over the network.

- **Host Threats**

Host threats are directed at a particular system on which valuable information resides. Attackers try to breach the security of the information system resource.

- **Application Threats**

If the proper security measures are not considered during development of the particular application, the application might be vulnerable to different types of application attacks. Attackers take advantage of vulnerabilities present in the application to steal or damage the information

Ethical Hacking

- Ethical hackers are also known as white hats
- Ethical hacking is done to test and evaluate the security of an information system, network, etc.
- Ethical hacking is done in a similar fashion as malicious hacking
- The major difference is the intent which is to identify the intent of malicious hacking is to steal, destroy, or restrict access to digital information

Types of Ethical Hacking

1- System Hacking

- System hacking is how hacktivists access personal computers across a network. IT security professionals can utilize **packet sniffing**, **privilege escalation**, **password cracking**, and other defensive techniques to counteract these dangers.

2- Social Engineering

- Through social engineering, threat actors are influencing people to share their personal data with them. It is common for eugenics to be used together with **social engineering** because it is typically easier to target your natural difficulty trusting than it is to figure out how to spoof your device.

3- Web Server Hacking

- Real-time online content is produced by a server running application software and databases. Threat actors may be trying to intercept the server in order to steal credentials, passcodes, and corporate information from the web application. To achieve their objective, attackers may employ social engineering tactics, ping deluge assaults, **port scans**, sniffing attacks, and gluing.
- **4- Web Application hacking**
- Web hacking is the process of exploiting software over HTTP by exploiting the software's visual chrome browser, meddling with the URI, or colluding with HTTP aspects not stored in the URI.

5- Wireless Networks Hacking

- Wireless networks transfer data through radio waves, making it easy for a hacker to simply access the system. These attackers frequently employ network sniffing in order to find the Identifier and bodge a wireless network.

How are Ethical Hackers Different from Malicious Hackers?

Ethical Hacker	Malicious Hackers
In the case of ethical hackers, the intent is to help the owner identify any cracks or issues in the security system.	Malicious Hackers hack into systems with the intent to cause harm. They tend to steal sensitive information, hinder work operations, etc.
Ethical Hacking is legal as ethical hackers have the proper permissions and approvals.	Malicious hackers do not have permission to hack into the systems. They forcefully enter to cause harm. It is illegal and a punishable offence.
The organization or the owner employs white hack hackers.	Black hat hackers do so without consent.

The Benefits of Ethical Hacking

It Identifies Vulnerabilities Early

It Enhances Security Posture

It Saves Money

Goals of Ethical Hacking

- Protect the privacy of organization
- Transparently report all the identified bugs/weaknesses/vulnerabilities to the organization.
- Inform the vendors about the security measures and patches.

Thank You