MALICIOUS ATTACKS, THREATS, AND VULNERABILITIES

Information Assurance and Security 1

01 Overview of Risks, Threats, and Vulnerabilities

02 Protecting Assets

03 Malicious Software

04 Malicious Attacks

05 Attack Tools

06 Security Breach

01

OVERVIEW OF RISKS, THREATS, AND VULNERABILITIES


WHAT ARE WE PROTECTING OUR INFORMATION FROM?

RISK, THREAT, ASSET, AND VULNERABILITY

Risk is the likelihood that something bad will happen to an asset. It is the level of exposure to some event that has an effect on an asset.

Asset, In the context of IT security, an asset can be a computer, a database, or a piece of information

Threat is any action that could damage an asset. Information systems face both natural and human-induced threats

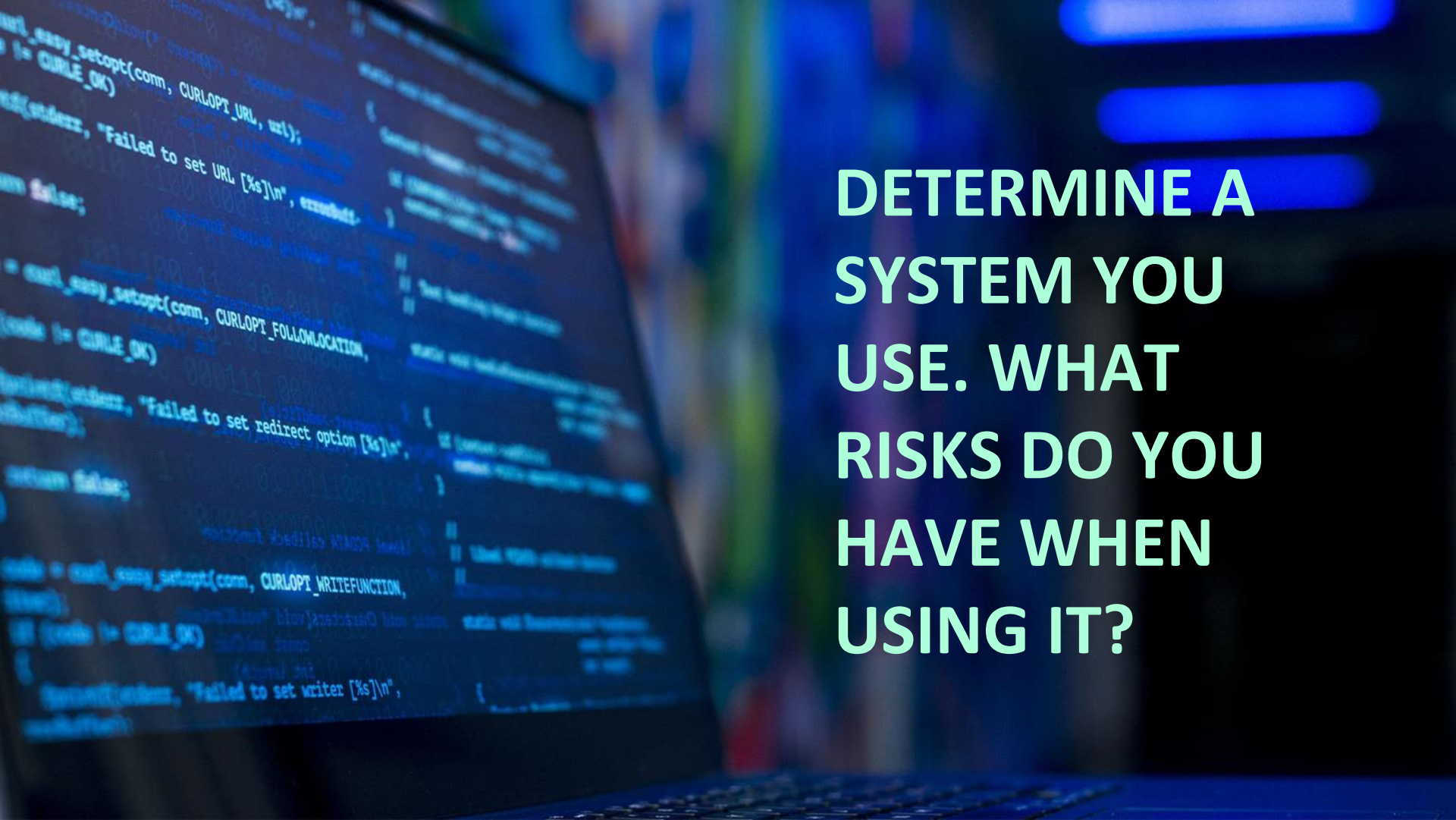
Vulnerability is a weakness that allows a threat to be realized or to have an effect on an asset.

RISK, THREAT, ASSET, AND VULNERABILITY

Risk is the probability that something bad is going to happen.

Threat is any action that can damage or compromise an asset.

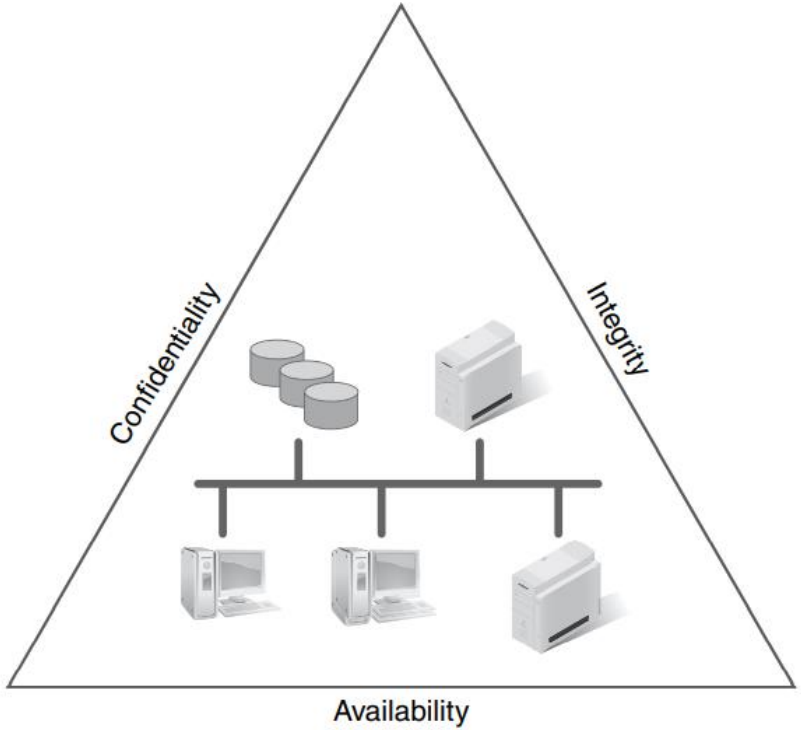
Vulnerability is a weakness in the design or software code itself. A vulnerability that can be exploited is a *threat*.


DETERMINE A SYSTEM YOU USE. WHAT RISKS DO YOU HAVE WHEN USING IT?

THREATS IN A SYSTEM

SYSTEM COMPONENT	THREAT
User	Employees' own human traits and behavior; Violations of the acceptable use policy are targeted
Workstation	Workstations, laptops, and mobile devices are the target, along with their vulnerabilities
LAN	Windows Active Directory/Domain Controllers, file servers, print servers; IP data network is a target for ID and authentication attacks
LAN-to-WAN	DMZ VLANs or dedicated remote connections; Public-facing IP devices, perimeter security with firewalls, IDS/IPS, and remote VPN terminations
WAN	IP routers, TCP/IP stacks and buffers, firewalls, gateways, switches, and WAN service providers
Remote Access	Virtual private networks (VPNs), two-factor authentication, and remote access; mobile workers and teleworkers
System/Application	Web and application servers, operating systems, and applications; Back-end database servers and database tables with sensitive data

VIOLATIONS TO THE TENETS



The three major threat types directly threaten each of the CIA tenets. They are as follows:

- **Disclosure threats** vs Confidentiality
- **Alteration threats** vs Integrity
- **Denial or destruction threats** vs Availability

02 PROTECTING ASSETS


WHAT IS THE TARGET OF PROTECTION FOR ALL ORGANIZATIONS?

ASSET

An asset is any item that has value. Although all items in an organization have some value, the term asset generally applies to those items that have substantial value. An organization's assets can include the following:

- Customer Data
- IT Assets and Network Infrastructure
- Intellectual Property
- Finances and Financial Data
- Service Availability and Productivity
- Reputation


TO WHOM ARE WE PROTECTING OUR ASSETS FROM?

HACKER

A Hacker often describes someone who breaks into a computer system without authorization. Hackers have multiple types:

- White-hat Hacker
- Black-hat Hacker
- Gray-hit Hacker

Crackers is not a hacker!

RISK, THREAT, ASSET, AND VULNERABILITIES

03 MALICIOUS SOFTWARE


WHAT IS A
MALICIOUS
SOFTWARE?

MALICIOUS SOFTWARE

Malicious software, or malware are softwares that infiltrates one or more target computers and follows an attacker's instructions. These instructions can include causing damage, escalating security privileges, divulging private data, or even modifying or deleting data. Malware exists in two main categories:

- **Infecting programs** actively attempt to copy themselves to other computers.
- **Hiding programs** hide in the computer, carrying out the attacker's instructions while avoiding detection

INFECTING PROGRAMS

Viruses - software program that attaches itself to or copies itself into another program on a computer

Worms - A self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. The worm's purpose may be simply to reduce network availability by using up bandwidth, or it may take other nefarious actions

HIDING PROGRAM

Trojan Horses - Trojan horse programs use their outward appearance to trick users into running them.

Rootkits - A malware that modifies or replaces one or more existing programs to hide traces of attacks

Spyware - A type of malware that specifically threatens the confidentiality of information

04 MALICIOUS ATTACKS


WHAT KINDS OF ATTACKS CAN A SYSTEM HAVE?

MALICIOUS ATTACKS

An attack on a computer system or network asset succeeds by exploiting a vulnerability in the system. An attack can consist of all or a combination of these four categories:

- **Fabrications** – involves the creation of some deception in order to trick unsuspecting users.
- **Interceptions** – involves eavesdropping on transmissions and redirecting them for unauthorized use.
- **Interruptions** – causes a break in a communication channel, which blocks the transmission of data.
- **Modifications** – the alteration of data contained in transmissions or files.

MALICIOUS ATTACKS

Security threats can be active or passive. Both types can have negative repercussions for an IT infrastructure

An **active attack** involves a modification of the data stream or attempts to gain unauthorized access to computer and networking systems. An active attack is a physical intrusion

In a **passive attack**, the attacker does not make changes to the system. This type of attack simply eavesdrops on and monitors transmissions.

05 ATTACK TOOLS

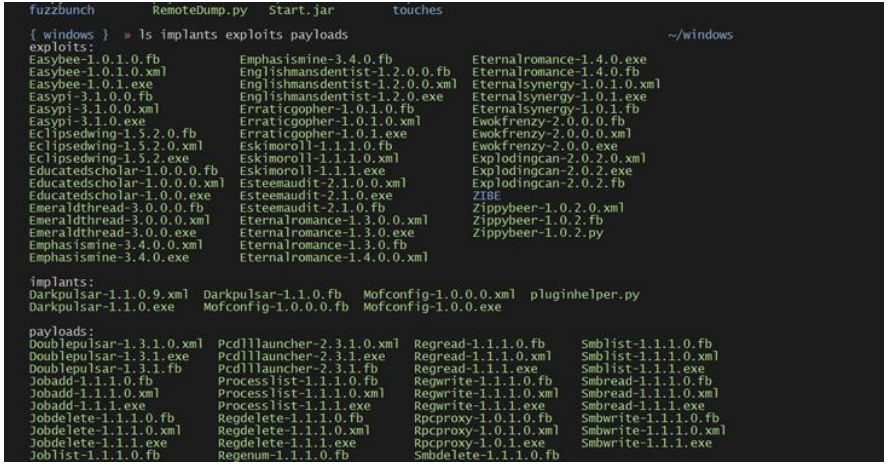

WHAT
HACKING
TOOLS DO YOU
KNOW?

ATTACK TOOLS

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Knowing how an attack is conducted and what tools are used will help you build a defense plan. In fact, many organizations use the same tools that attackers use to help identify weaknesses they need to address. It is always better to find weaknesses in your own environment before an attacker does, but it is even more important to quickly remediate that weakness.

ATTACK TOOL EXAMPLES



Protocol analyzer or packet sniffer (or just sniffer) is a software program that enables a computer to monitor and capture network traffic, whether on a LAN or a wireless network.

Port scanners are used to identify open ports or applications and services that are enabled on the IP host device

Operating system (OS) fingerprint scanner is a software program that allows an attacker to send a variety of packets to an IP host device, hoping to determine the target device's operating system (OS) from the responses.

ATTACK TOOL EXAMPLES

Vulnerability Scanners is a software program that is used to identify and, when possible, verify vulnerabilities on an IP host device.

Exploit Software is an application that incorporates known software vulnerabilities, data, and scripted commands to “exploit” a weakness in a computer system or IP host device

Wardialers is a computer program that dials telephone numbers, looking for a computer on the other end.

ATTACK TOOL EXAMPLES

Password Crackers is a software program that performs one of two functions: a brute-force password attack to gain unauthorized access to a system or recovery of passwords stored as a cryptographic hash on a computer system.

Keystroke Loggers is a type of surveillance software or hardware that can record to a log file every keystroke a user makes with a keyboard

06 SECURITY BREACH


WHAT IS A SECURITY BREACH?

SECURITY BREACH

Any event that results in a violation of any of the confidentiality, integrity, or availability (CIA) security tenets is a **security breach**.

Some security breaches disrupt system services **on purpose**.

Others are **accidental** and may result from hardware or software failures.

SECURITY BREACH EXAMPLES

Denial of Service Attack is a coordinated attempt to deny service by occupying a computer to perform large amounts of unnecessary tasks

Unacceptable Web Browsing is a violation of an organization's acceptable use policy (AUP), such as an employee's unacceptable web browsing, can itself be a security breach

Wiretapping is an attack where attackers can tap telephone lines and data communication lines.

SECURITY BREACH EXAMPLES

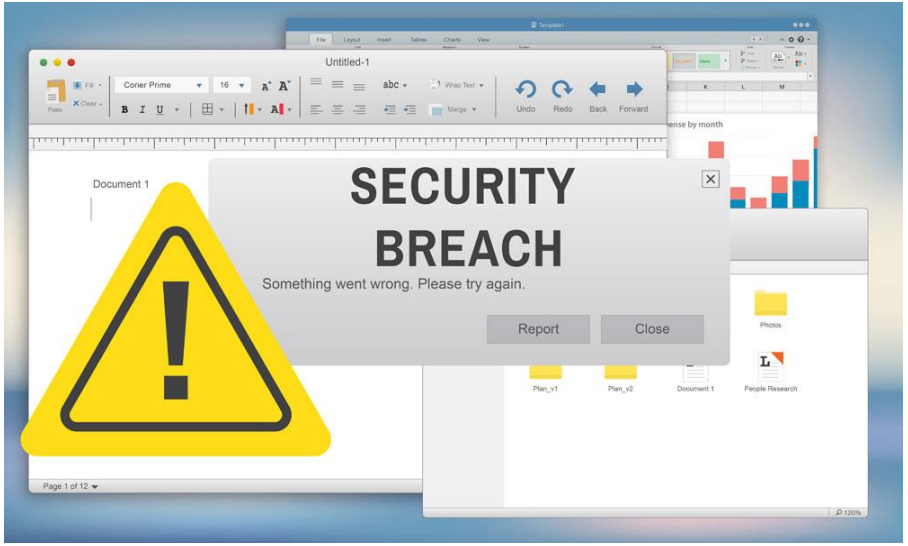
Backdoors are hidden access methods created by developers that was discovered by hackers

Data that are purposely or accidentally modified without due process impact the integrity tenet of information systems security

Spam is unwanted email

Spim is unwanted instant messages or IM chats

SECURITY BREACH EXAMPLES



Phishing email is a fake or bogus email to trick the recipient into clicking on an embedded URL link or opening an email attachment

Hoax is some act intended to deceive or trick the receiver

Cookie is simply a text file that contains details gleaned from past visits to a website

THANK YOU!