WEB APPLICATION VULNERABILITIES ASSESSMENT

TEJAS MHASKE

CYBER SECURITY TRAINER

VULNERABILITY ASSESSMENT CONCEPTS

1. **What is a Vulnerability?**

✓ A **vulnerability** is a flaw or weakness in a system, application, network, or process that can be exploited by a threat actor (such as a hacker) to gain unauthorized access to data, disrupt operations, or cause other harmful effects**.**

2. **What is Assessment?**

✓ An **assessment** is a systematic evaluation or analysis of a system, process, or organization to measure its performance, compliance, or security

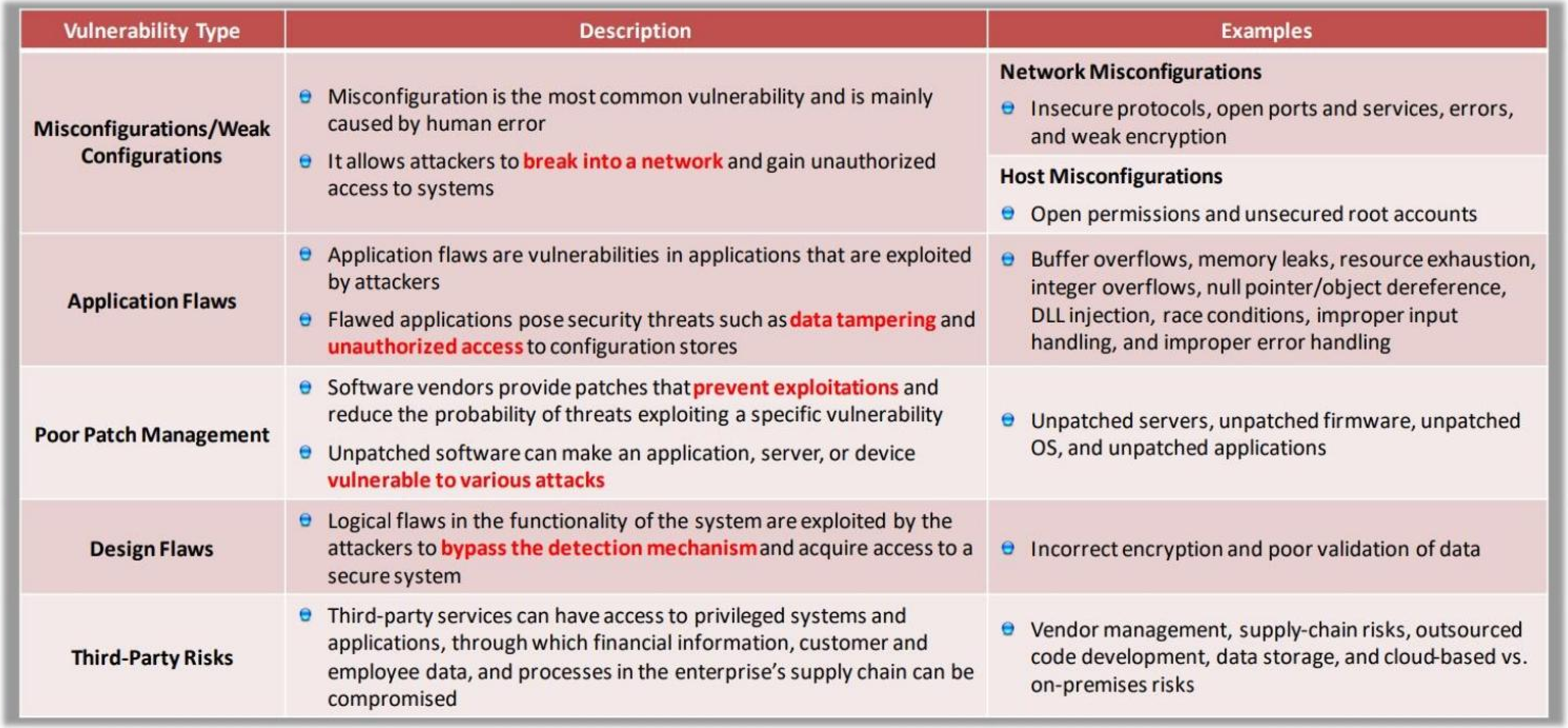
WHAT IS A VULNERABILITY ASSESSMENT?

- A **vulnerability assessment** is a systematic process used to identify, classify, and prioritize vulnerabilities in a system, application, or network.
- The goal of a vulnerability assessment is to uncover potential security weaknesses before they can be exploited by attackers.
- This involves scanning for known vulnerabilities, analyzing system configurations, and assessing the potential impact of identified issues.

FOOTPRINTING CONCEPTS

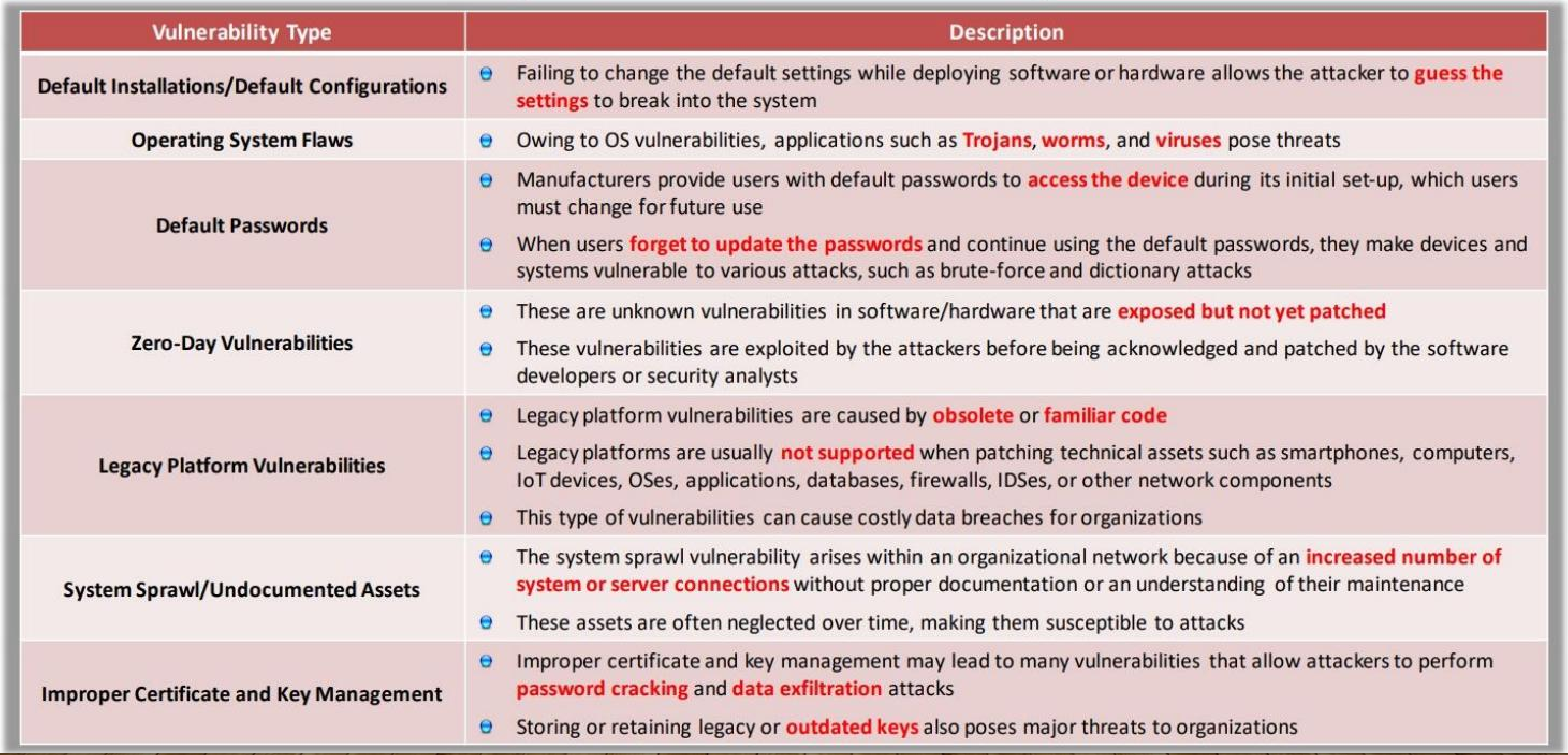
This step acts as a preparatory phase for the attacker, Who needs to gather as much information as possible to easily find ways to intrude into the target network.

Vulnerability Classification



Vulnerability Type	Description	Examples
Misconfigurations/Weak Configurations	- Misconfiguration is the most common vulnerability and is mainly caused by human error - It allows attackers to **break into a network** and gain unauthorized access to systems	**Network Misconfigurations** - Insecure protocols, open ports and services, errors, and weak encryption **Host Misconfigurations** - Open permissions and unsecured root accounts
Application Flaws	- Application flaws are vulnerabilities in applications that are exploited by attackers - Flawed applications pose security threats such as **data tampering** and **unauthorized access** to configuration stores	- Buffer overflows, memory leaks, resource exhaustion, integer overflows, null pointer/object dereference, DLL injection, race conditions, improper input handling, and improper error handling
Poor Patch Management	- Software vendors provide patches that **prevent exploitations** and reduce the probability of threats exploiting a specific vulnerability - Unpatched software can make an application, server, or device **vulnerable to various attacks**	- Unpatched servers, unpatched firmware, unpatched OS, and unpatched applications
Design Flaws	- Logical flaws in the functionality of the system are exploited by the attackers to **bypass the detection mechanism** and acquire access to a secure system	- Incorrect encryption and poor validation of data
Third-Party Risks	- Third-party services can have access to privileged systems and applications, through which financial information, customer and employee data, and processes in the enterprise's supply chain can be compromised	- Vendor management, supply-chain risks, outsourced code development, data storage, and cloud-based vs. on-premises risks

Vulnerability Classification (Cont'd)



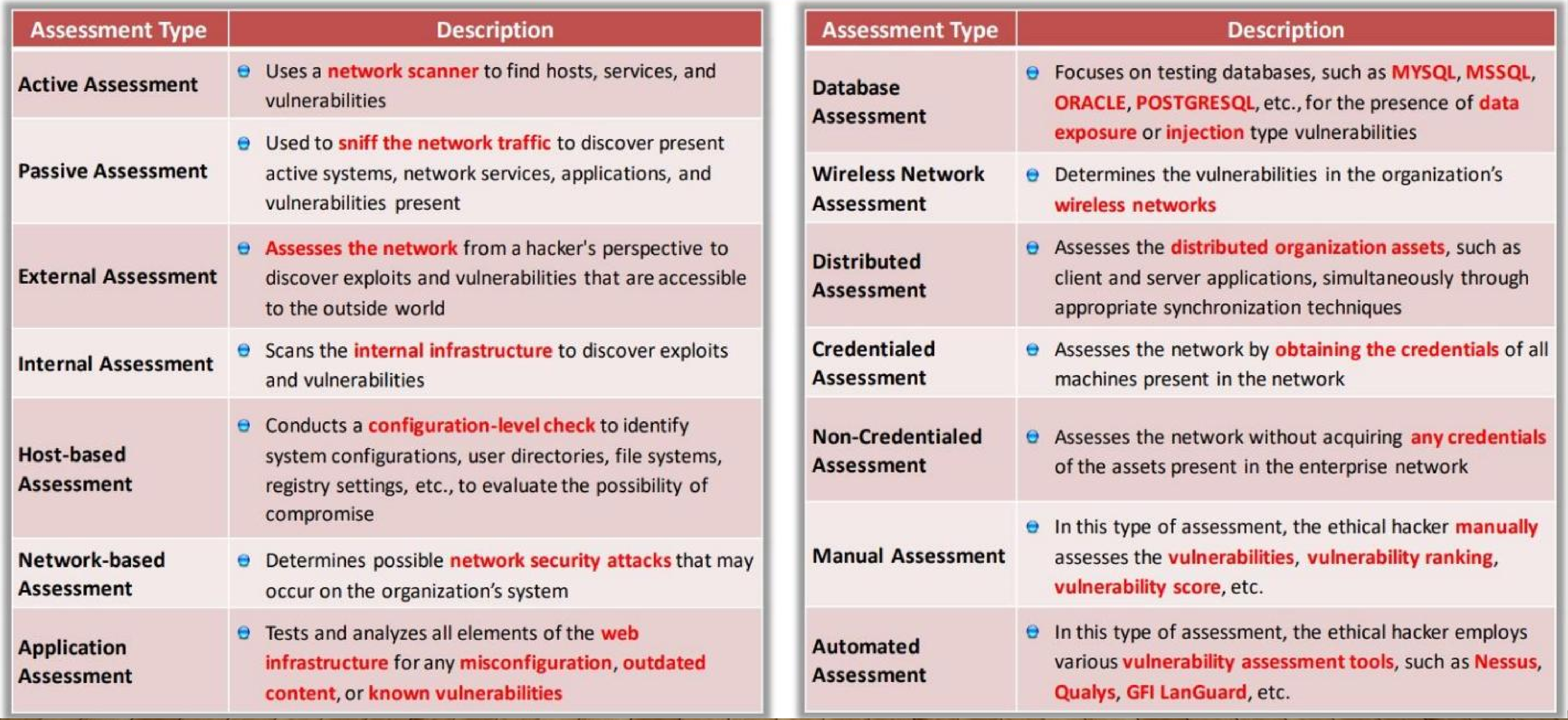
Vulnerability Type	Description
Default Installations/Default Configurations	Failing to change the default settings while deploying software or hardware allows the attacker to **guess the settings** to break into the system
Operating System Flaws	Owing to OS vulnerabilities, applications such as **Trojans**, **worms**, and **viruses** pose threats
Default Passwords	Manufacturers provide users with default passwords to **access the device** during its initial set-up, which users must change for future use When users **forget to update the passwords** and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute-force and dictionary attacks
Zero-Day Vulnerabilities	These are unknown vulnerabilities in software/hardware that are **exposed but not yet patched** These vulnerabilities are exploited by the attackers before being acknowledged and patched by the software developers or security analysts
Legacy Platform Vulnerabilities	Legacy platform vulnerabilities are caused by **obsolete** or **familiar code** Legacy platforms are usually **not supported** when patching technical assets such as smartphones, computers, IoT devices, OSes, applications, databases, firewalls, IDSes, or other network components This type of vulnerabilities can cause costly data breaches for organizations
System Sprawl/Undocumented Assets	The system sprawl vulnerability arises within an organizational network because of an **increased number of system or server connections** without proper documentation or an understanding of their maintenance These assets are often neglected over time, making them susceptible to attacks
Improper Certificate and Key Management	Improper certificate and key management may lead to many vulnerabilities that allow attackers to perform **password cracking** and **data exfiltration** attacks Storing or retaining legacy or **outdated keys** also poses major threats to organizations

Examples of Vulnerabilities

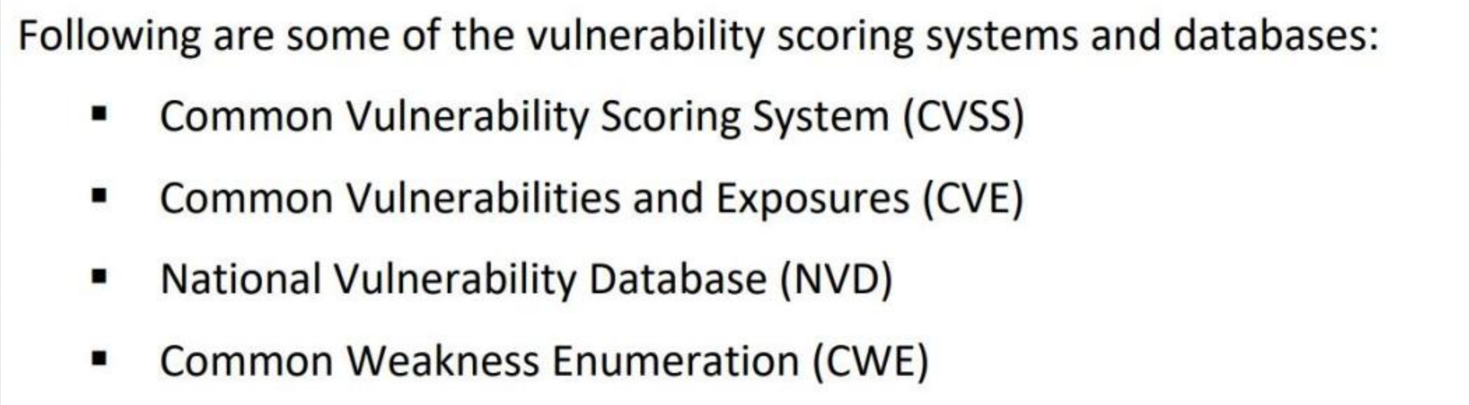
Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	An OS can be vulnerable because: • It is inherently insecure • It is not patched with the latest updates
Network Device Vulnerabilities	Various network devices such as routers, firewall, and switches can be vulnerable due to: • Lack of password protection • Lack of authentication • Insecure routing protocols • Firewall vulnerabilities

Configuration Vulnerabilities	Description
User account vulnerabilities	Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	Originating from setting of weak passwords for system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device

Types of Vulnerability Assessment

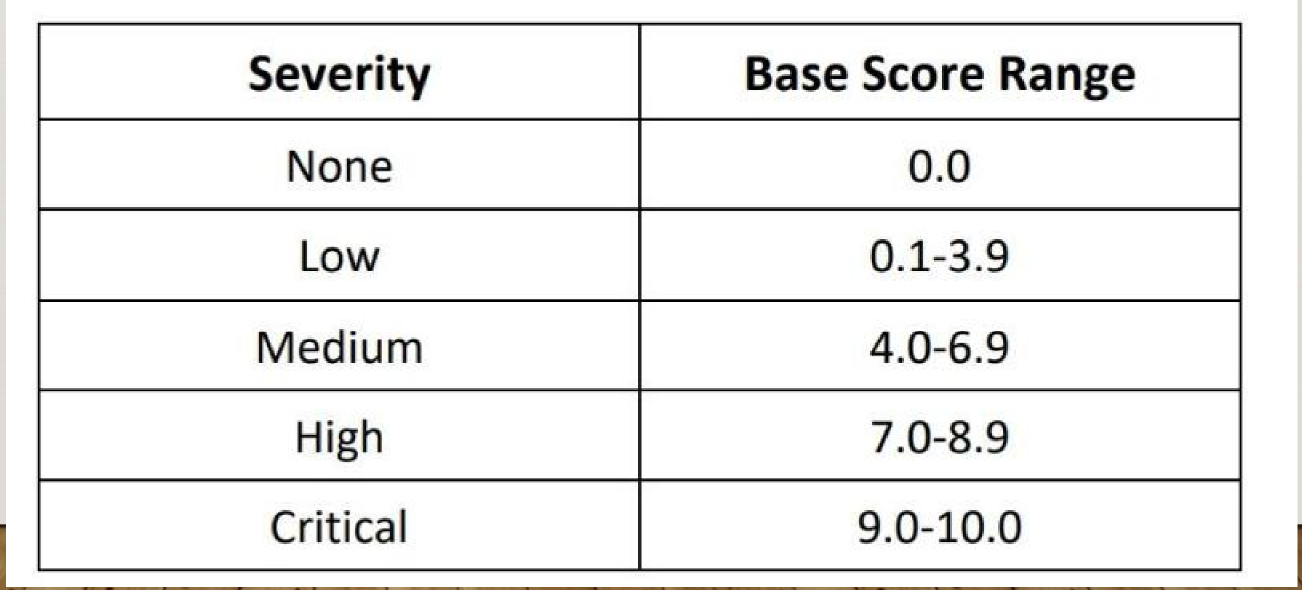


Assessment Type	Description
Active Assessment	Uses a network scanner to find hosts, services, and vulnerabilities
Passive Assessment	Used to sniff the network traffic to discover present active systems, network services, applications, and vulnerabilities present
External Assessment	Assesses the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world
Internal Assessment	Scans the internal infrastructure to discover exploits and vulnerabilities
Host-based Assessment	Conducts a configuration-level check to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise
Network-based Assessment	Determines possible network security attacks that may occur on the organization's system
Application Assessment	Tests and analyzes all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities
Database Assessment	Focuses on testing databases, such as MYSQL, MSSQL, ORACLE, POSTGRESQL, etc., for the presence of data exposure or injection type vulnerabilities
Wireless Network Assessment	Determines the vulnerabilities in the organization's wireless networks
Distributed Assessment	Assesses the distributed organization assets, such as client and server applications, simultaneously through appropriate synchronization techniques
Credentialed Assessment	Assesses the network by obtaining the credentials of all machines present in the network
Non-Credentialed Assessment	Assesses the network without acquiring any credentials of the assets present in the enterprise network
Manual Assessment	In this type of assessment, the ethical hacker manually assesses the vulnerabilities, vulnerability ranking, vulnerability score, etc.
Automated Assessment	In this type of assessment, the ethical hacker employs various vulnerability assessment tools, such as Nessus, Qualys, GFI LanGuard, etc.

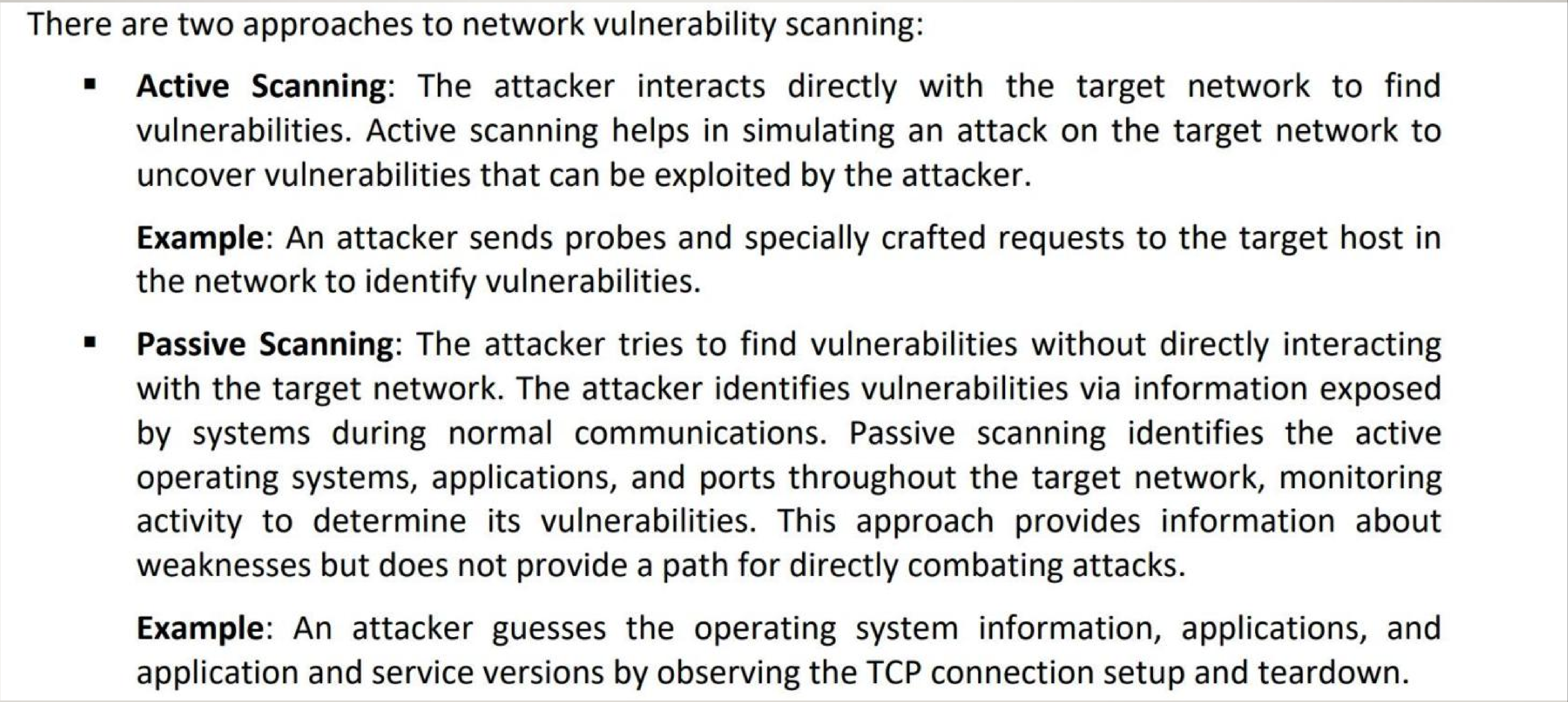


Following are some of the vulnerability scoring systems and databases:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)



Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

  Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

  Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

WHAT IS FOOTPRINTING?

Footprinting is the first step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system

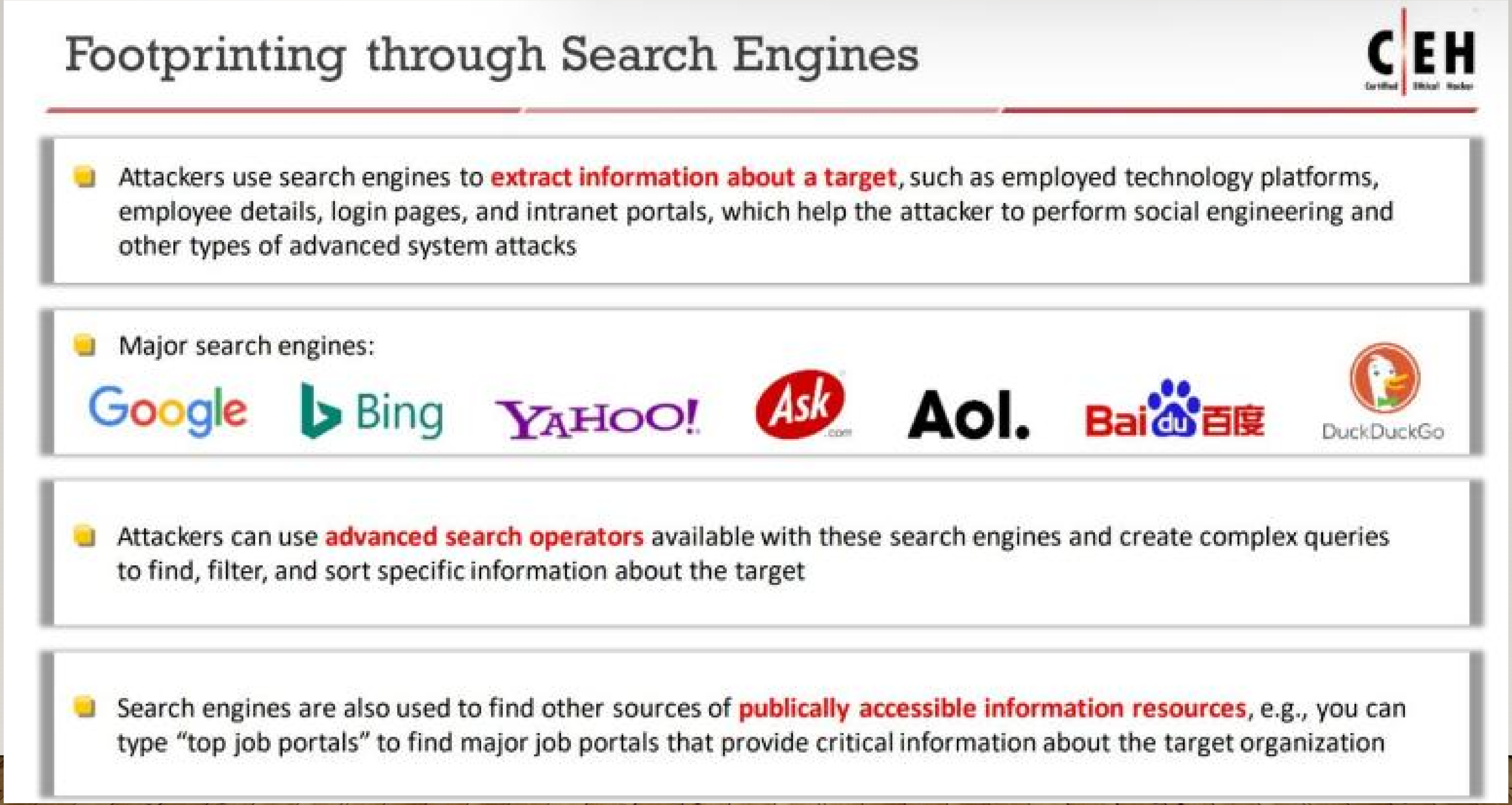
Types of Footprinting

Passive Footprinting

Gathering information about the target without

Active Footprinting

Gathering information about the target with



Footprinting through Search Engines

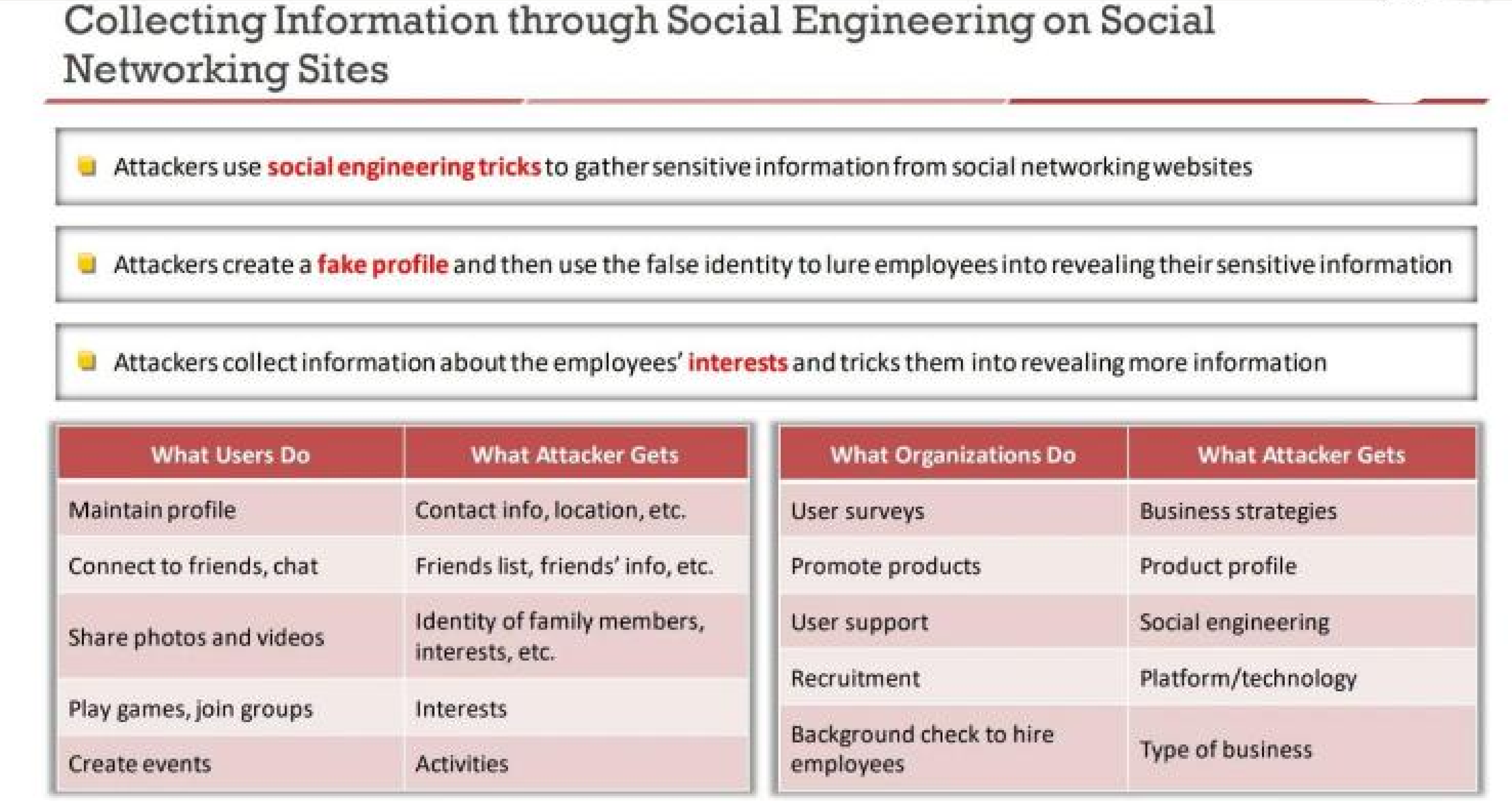
- Attackers use search engines to **extract information about a target**, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks

- Major search engines:

Google Bing YAHOO! Ask.com Aol. Bai百度 DuckDuckGo

- Attackers can use **advanced search operators** available with these search engines and create complex queries to find, filter, and sort specific information about the target

- Search engines are also used to find other sources of **publically accessible information resources**, e.g., you can type “top job portals” to find major job portals that provide critical information about the target organization



Collecting Information through Social Engineering on Social Networking Sites

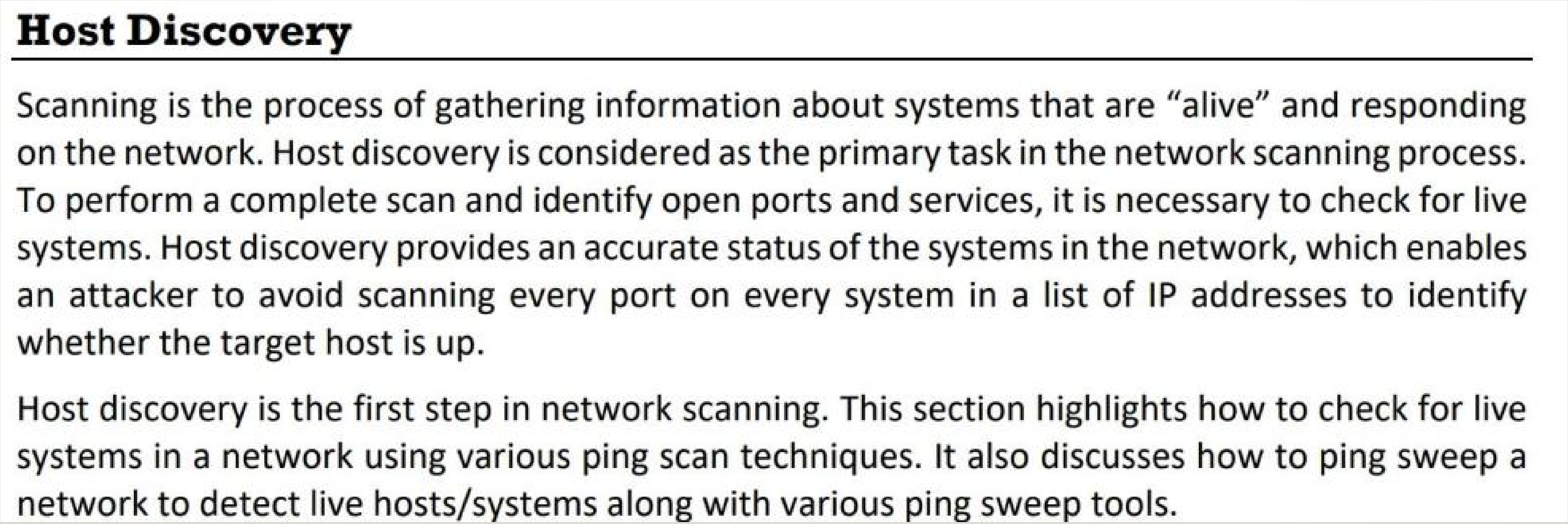
- Attackers use **social engineering tricks** to gather sensitive information from social networking websites

- Attackers create a **fake profile** and then use the false identity to lure employees into revealing their sensitive information

- Attackers collect information about the employees' **interests** and tricks them into revealing more information

What Users Do	What Attacker Gets
Maintain profile	Contact info, location, etc.
Connect to friends, chat	Friends list, friends' info, etc.
Share photos and videos	Identity of family members, interests, etc.
Play games, join groups	Interests
Create events	Activities

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology
Background check to hire employees	Type of business

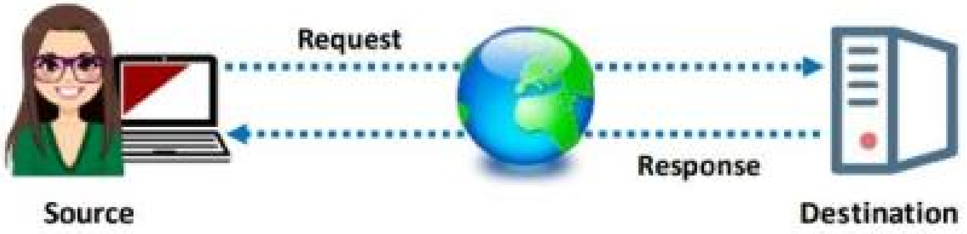


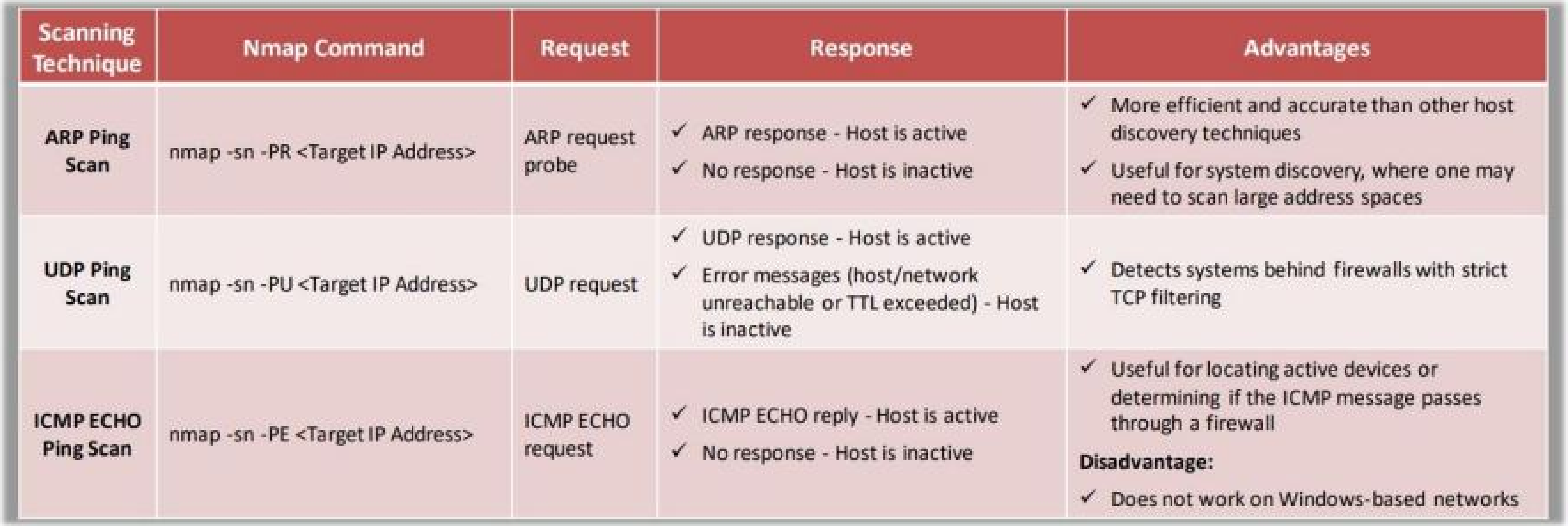
Host Discovery

Scanning is the process of gathering information about systems that are “alive” and responding on the network. Host discovery is considered as the primary task in the network scanning process. To perform a complete scan and identify open ports and services, it is necessary to check for live systems. Host discovery provides an accurate status of the systems in the network, which enables an attacker to avoid scanning every port on every system in a list of IP addresses to identify whether the target host is up.

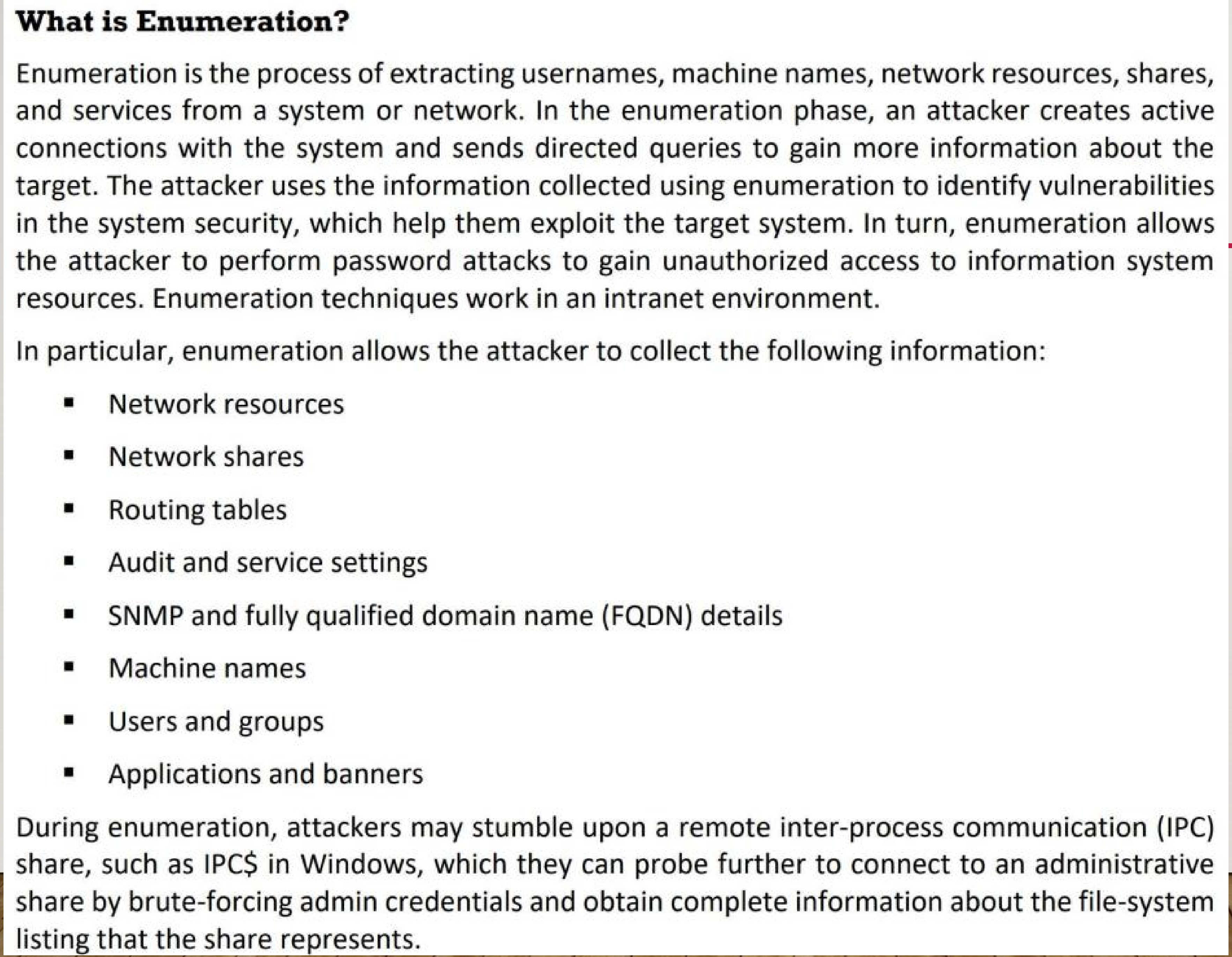
Host discovery is the first step in network scanning. This section highlights how to check for live systems in a network using various ping scan techniques. It also discusses how to ping sweep a network to detect live hosts/systems along with various ping sweep tools.

Host Discovery Techniques





Scanning Technique	Nmap Command	Request	Response	Advantages
ARP Ping Scan	nmap -sn -PR <Target IP Address>	ARP request probe	✓ ARP response - Host is active ✓ No response - Host is inactive	✓ More efficient and accurate than other host discovery techniques ✓ Useful for system discovery, where one may need to scan large address spaces
UDP Ping Scan	nmap -sn -PU <Target IP Address>	UDP request	✓ UDP response - Host is active ✓ Error messages (host/network unreachable or TTL exceeded) - Host is inactive	✓ Detects systems behind firewalls with strict TCP filtering
ICMP ECHO Ping Scan	nmap -sn -PE <Target IP Address>	ICMP ECHO request	✓ ICMP ECHO reply - Host is active ✓ No response - Host is inactive	✓ Useful for locating active devices or determining if the ICMP message passes through a firewall **Disadvantage:** ✓ Does not work on Windows-based networks



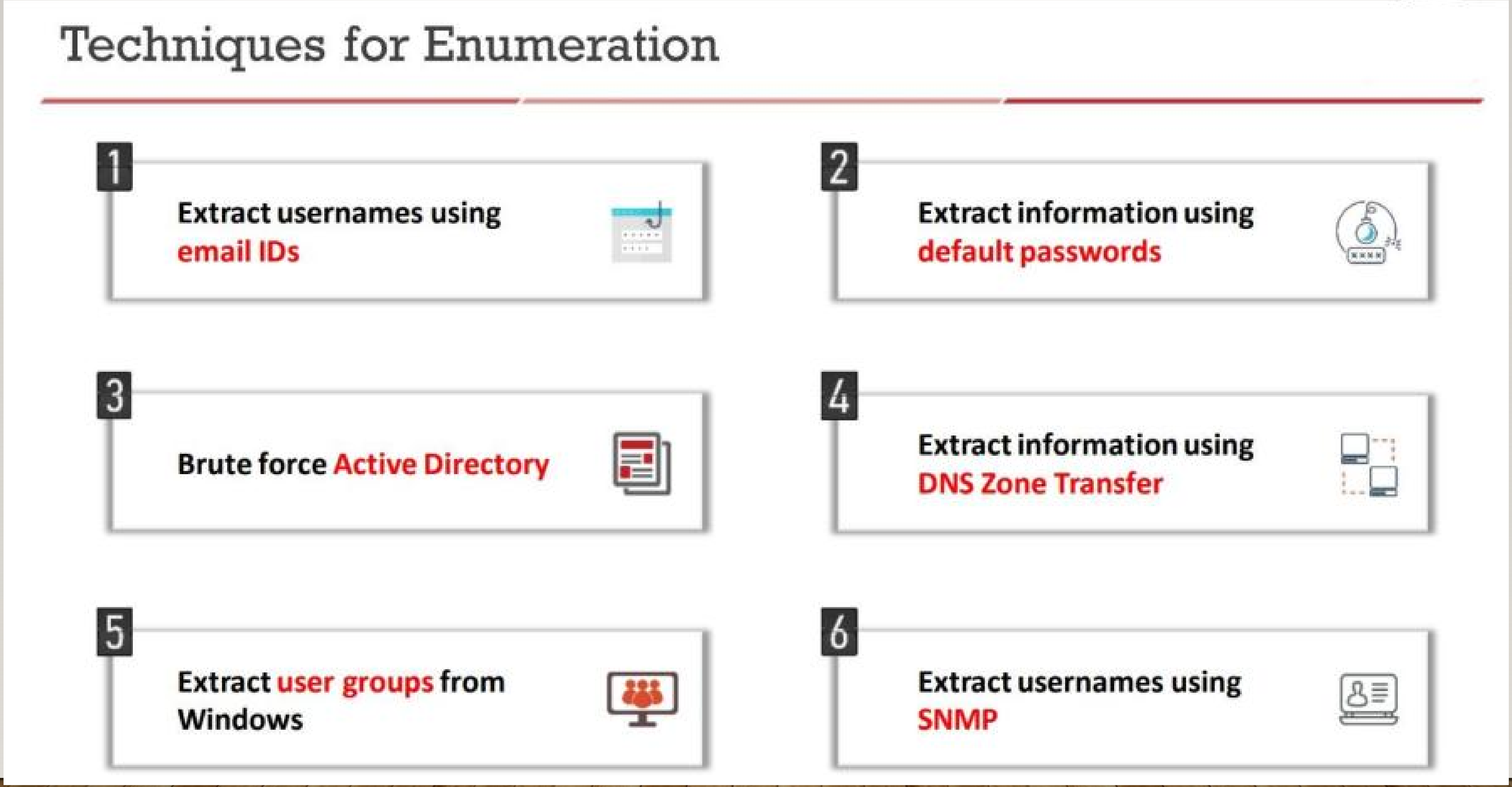
What is Enumeration?

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. The attacker uses the information collected using enumeration to identify vulnerabilities in the system security, which help them exploit the target system. In turn, enumeration allows the attacker to perform password attacks to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

In particular, enumeration allows the attacker to collect the following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and fully qualified domain name (FQDN) details
- Machine names
- Users and groups
- Applications and banners

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.



Techniques for Enumeration

1. Extract usernames using **email IDs**

2. Extract information using **default passwords**

3. Brute force **Active Directory**

4. Extract information using **DNS Zone Transfer**

5. Extract **user groups** from Windows

6. Extract usernames using **SNMP**

WEBSITE CRAWLING

Crawling in this context aims to discover all accessible parts of the website, including URLs, forms, input fields, hidden pages, and scripts. This helps build a comprehensive map of the website's attack surface.

- **Automated Scanning Tools**: Security scanners such as Burp Suite, OWASP ZAP, and Nessus use crawling as an initial step to identify what needs to be tested. These tools navigate through the site just like a regular web crawler but focus on finding security flaws.
- **Identifying Vulnerable Components**: Crawling helps in finding various components like:
- Unprotected directories
- Input forms (potential for SQL injection, XSS, etc.)
- Exposed APIs
- Old or outdated scripts
- Configuration files that may expose sensitive data

VULNERABLE PARAMETER

- A vulnerable parameter refers to any input or variable within a web application that can be manipulated by an attacker to exploit security weaknesses.
- Example:-

1- Query String Parameters: Found in the URL after the ? symbol (e.g., example.com/page?id=123). Often vulnerable to SQL Injection, XSS, and Open Redirects.

2- Cookie Parameters: Manipulating cookies (Set-Cookie) can lead to session fixation, data theft, and XSS.

धन्यवाद