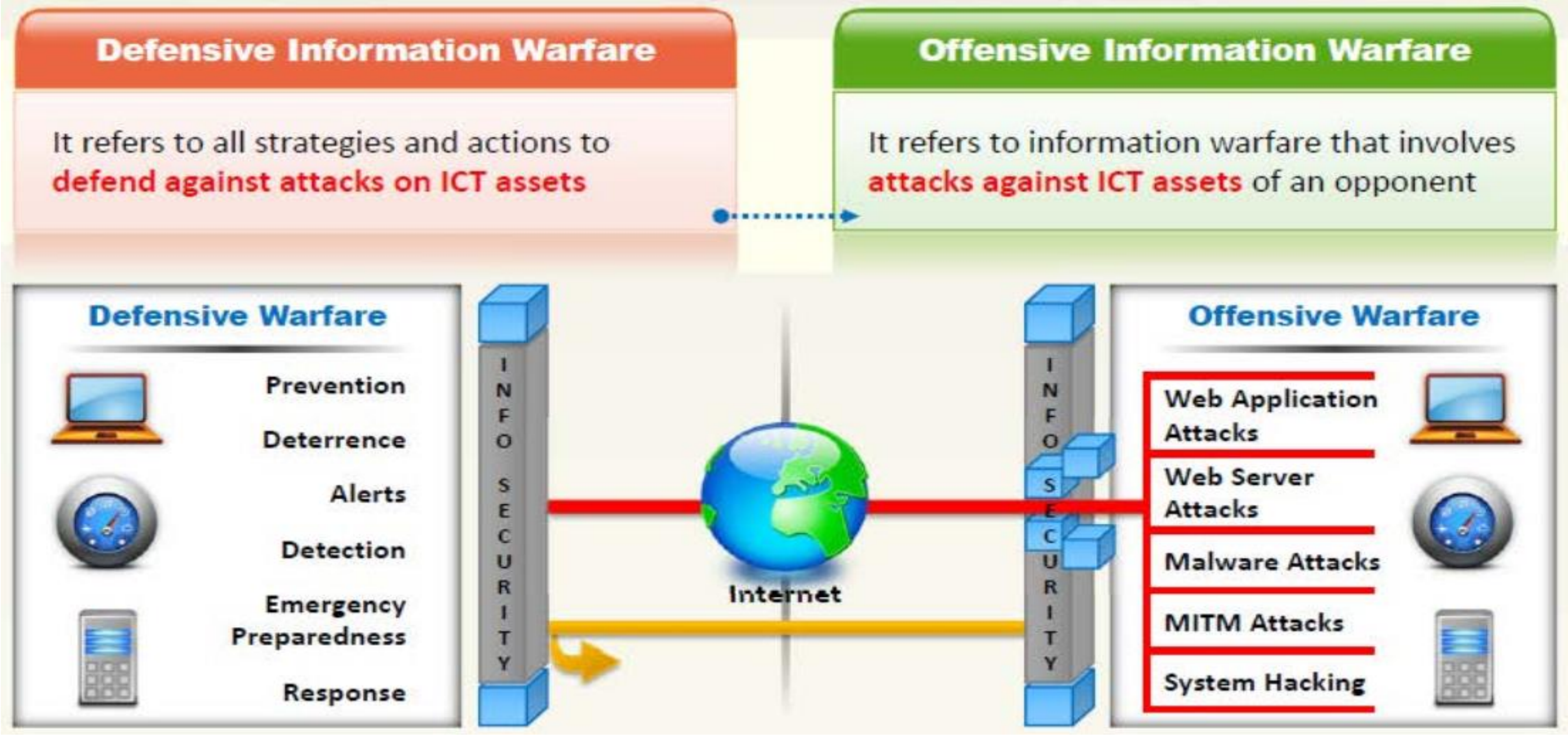
University of Babylon College of information Technology
Department of Information Security

Ethical Hacking
Lecture 2: Introduction to Ethical Hacking II

Asst.Lect. Rasha Hussein

Information Warfare



Defensive Information Warfare

It refers to all strategies and actions to **defend against attacks on ICT assets**

Offensive Information Warfare

It refers to information warfare that involves **attacks against ICT assets** of an opponent

Defensive Warfare

- Prevention
- Deterrence
- Alerts
- Detection
- Emergency Preparedness
- Response

Offensive Warfare

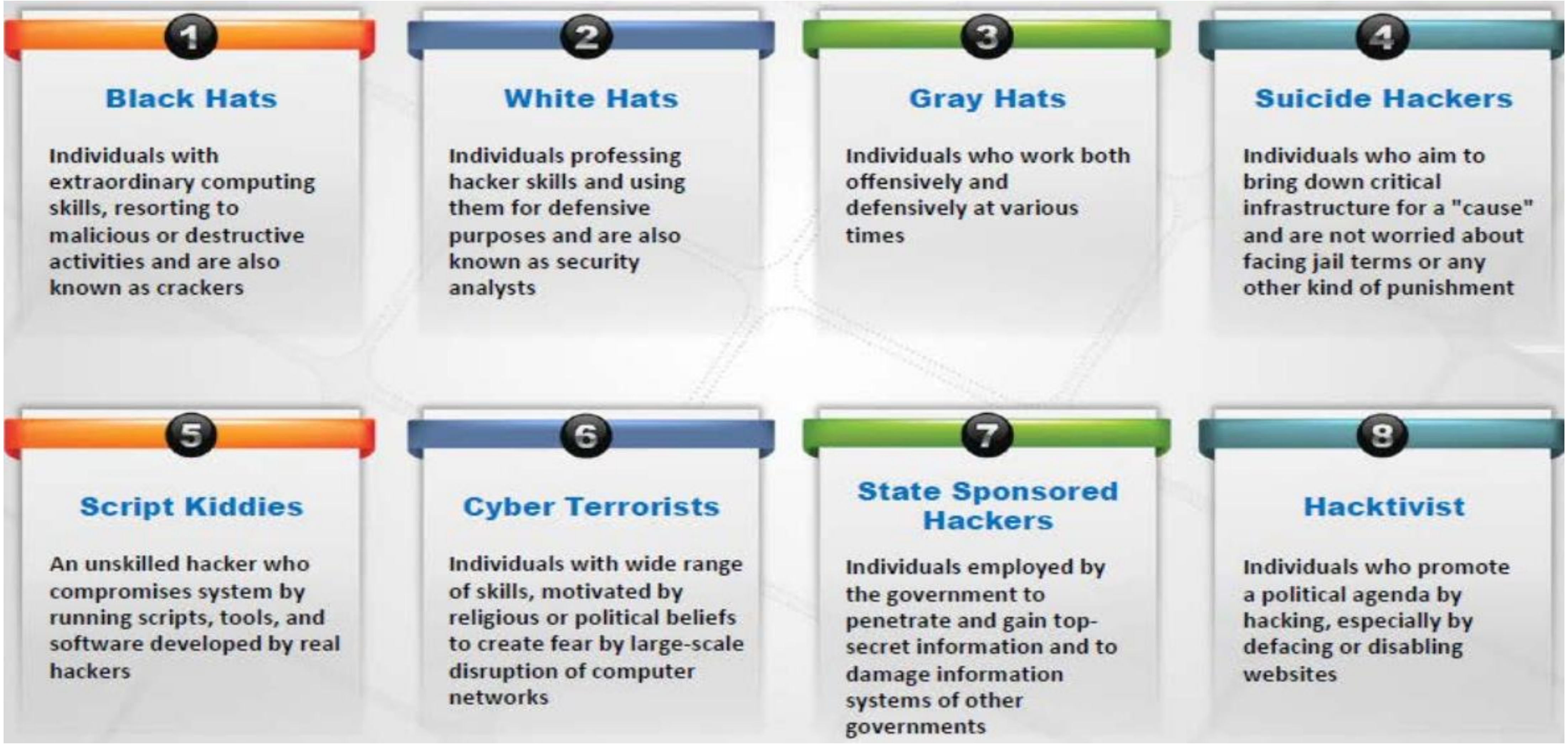
- Web Application Attacks
- Web Server Attacks
- Malware Attacks
- MITM Attacks
- System Hacking

Hacking Concepts , Types , and Phases

A hacker is a person who illegally breaks into a system or network without any authorization to destroy, steal sensitive data, or perform malicious attacks. Hackers may be motivated by a multitude of reasons:

- Intelligent individuals with excellent computer skills, with the ability to create and explore the computer's software and hardware
- For some hackers, hacking is a hobby to see how many computers or networks they can compromise
- Their intention can either be to gain knowledge or to poke around doing illegal things
- Some hack with malicious intent, such as stealing business data, credit card information, social security numbers, email passwords, etc.

Types of Hacker (Hacker Classes)



1

Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

2

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

3

Gray Hats

Individuals who work both offensively and defensively at various times

4

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

5

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

6

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

7

State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

8

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Concepts

- **Hacking**
- Hacking refers to **exploiting system vulnerabilities** and **compromising security controls** to gain unauthorized or inappropriate access to the system resources. It involves **modifying system or application features** to achieve a **goal outside of the creator's original purpose**. Hacking can be used to steal, pilfer, and redistribute intellectual property leading to business loss

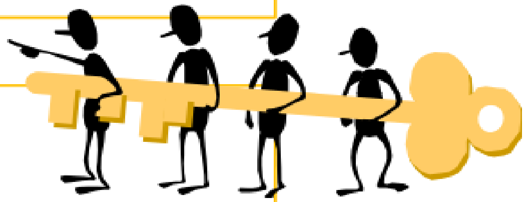
- **Ethical Hacking**

- Ethical hacking involves the use of hacking tools, tricks, and techniques **to identify vulnerabilities** so as to ensure system security. It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities in the system security.** Ethical hackers perform security assessments of their organization **with the permission of concerned authorities.**

Can Hacking be Ethical

Hacker:

- Refers to a person who enjoys learning the details of computer systems and to stretch his/her capabilities



Cracker:

- Refers to a person who uses his hacking skills for offensive purposes

Hacking:

- Describes the rapid development of new programs or the reverse engineering of the already existing software to make the code better and more efficient

Ethical hacker:

- Refers to security professionals who apply their hacking skills for defensive purposes

The Phases of Ethical Hacking(Hacking Phases)

Reconnaissance

- Active/passive

Scanning

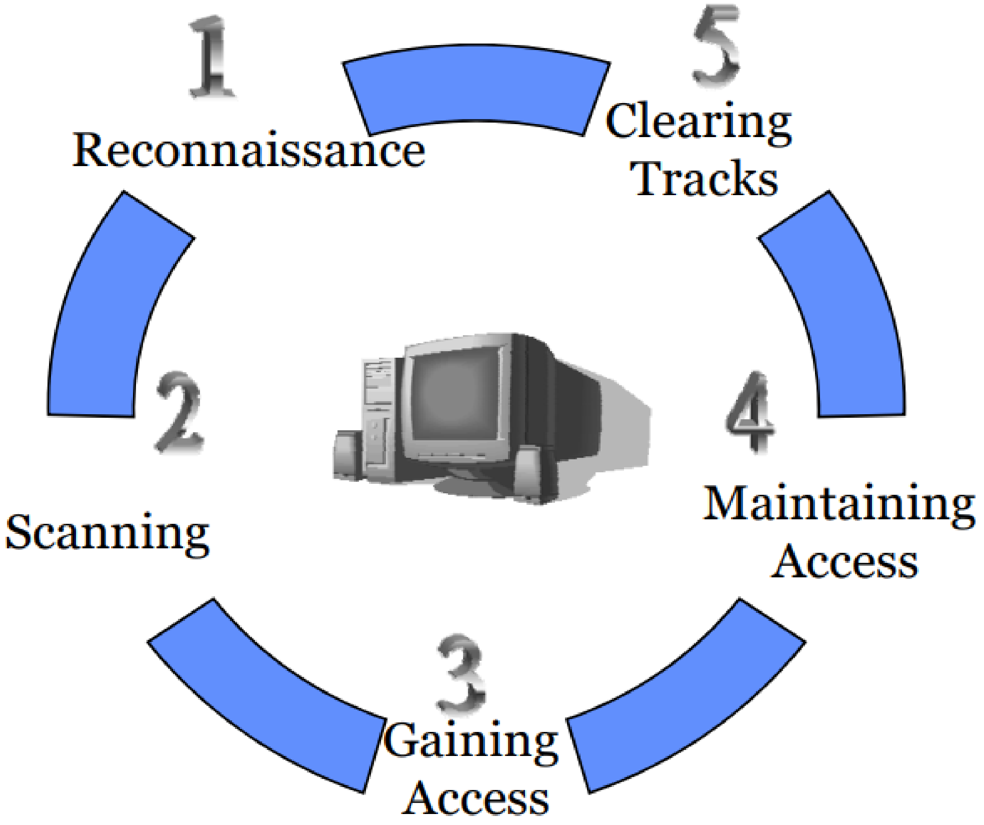
Gaining access

- Operating system level/application level
- Network level
- Denial of service

Maintaining access

- Uploading/altering/ downloading programs or data

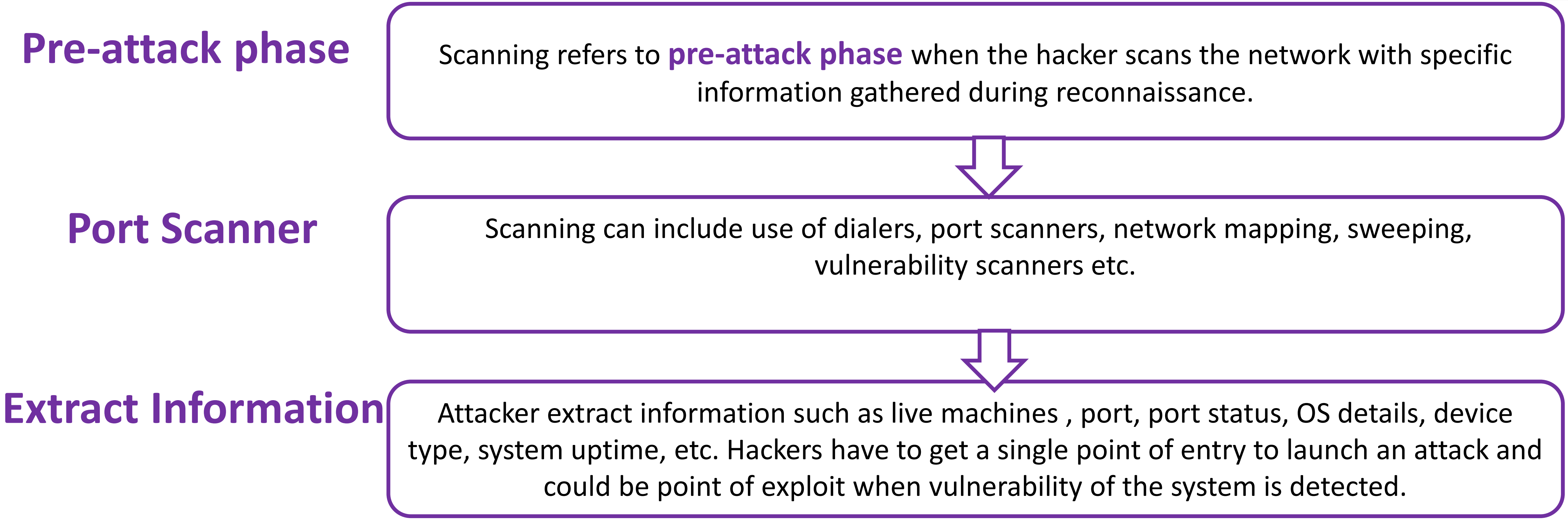
Clearing tracks



Phase 1: Reconnaissance (Active Reconnaissance vs. Passive Reconnaissance)

- **Reconnaissance** refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack. It involves network scanning either external or internal without authorization
- Business Risk – ‘Notable’ – Generally noted as a "rattling the door knobs" to see if someone is watching and responding. Could be future point of return when noted for ease of entry for an attack when more is known on a broad scale about the target.
- **Passive reconnaissance** involves monitoring network data for patterns and clues **without** directly interacting with the target. Examples include **sniffing**, information gathering etc.
- **Active reconnaissance** involves probing the network to detect and **interacting with** the target directly by any means. Example : **accessible hosts , open ports , location of routers**
- **Tools for Reconnaissance :**
- DNS :Nslookup –Whois –ARIN
- Trace route: Traceroute –Visualroutetrace
- Email : Visual route mail tracker –EmailTrackpro

Phase 2: Scanning



Pre-attack phase

Scanning refers to **pre-attack phase** when the hacker scans the network with specific information gathered during reconnaissance.

Port Scanner

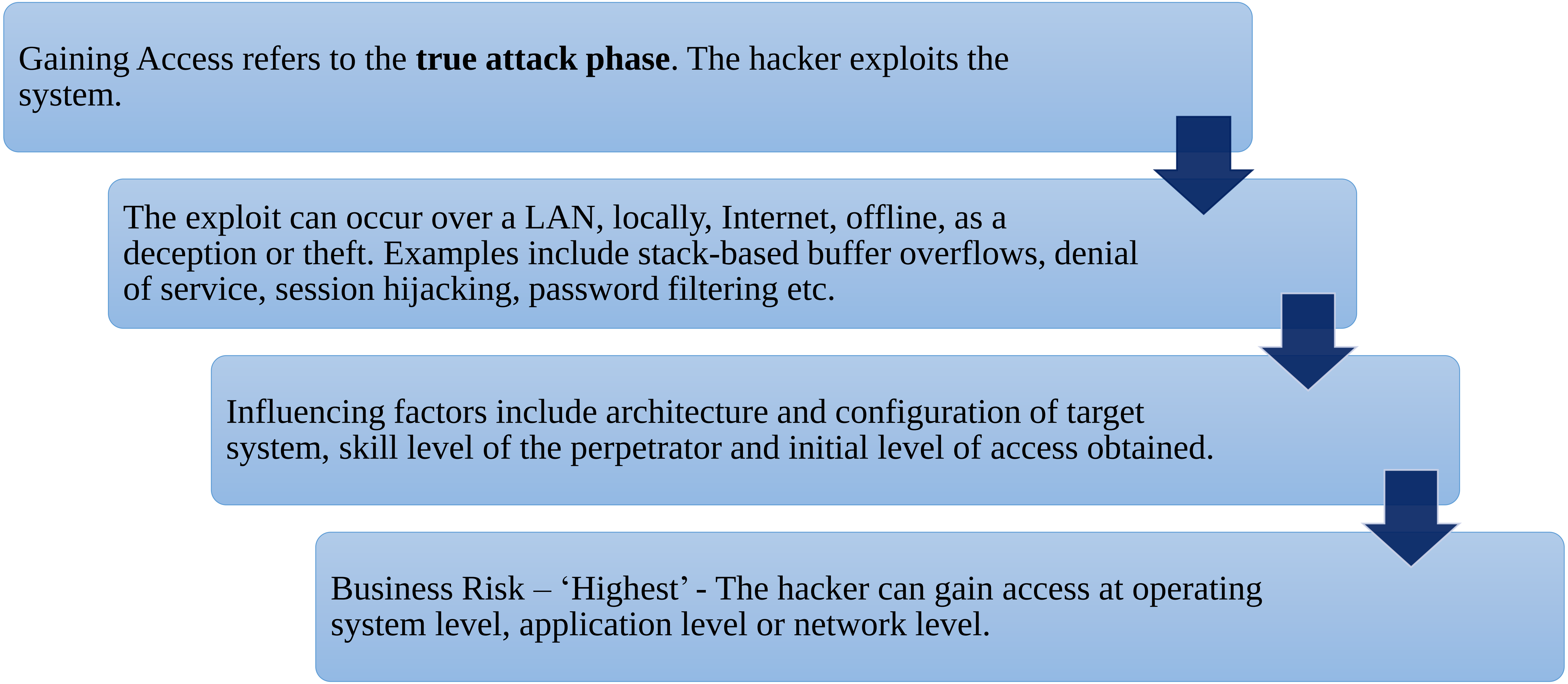
Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners etc.

Extract Information

Attacker extract information such as live machines , port, port status, OS details, device type, system uptime, etc. Hackers have to get a single point of entry to launch an attack and could be point of exploit when vulnerability of the system is detected.

- **Types of Scanning :** Network Sweeps , Network tracing, Port scans , OS fingerprinting , Version scans, Vulnerability scans
- **Tools for Scanning:** Nmap, Hping2 ,Firework ,Nessus , Nikto, Nemessis

Phase 3 - Gaining Access



Gaining Access refers to the **true attack phase**. The hacker exploits the system.

The exploit can occur over a LAN, locally, Internet, offline, as a deception or theft. Examples include stack-based buffer overflows, denial of service, session hijacking, password filtering etc.

Influencing factors include architecture and configuration of target system, skill level of the perpetrator and initial level of access obtained.

Business Risk – ‘Highest’ - The hacker can gain access at operating system level, application level or network level.

Phase 3 - Gaining Access

- **Gaining of access can be achieved by**

  –Buffer overflows

  –Denial of services

  –Session hijacking

  –Password cracking

- **Tools for Gaining Access**
- Password Cracking
  - – Dictionary Attack, Brute-force attack : John the Ripper, sniffers
- Escalating privilege
  - – Cracking windows NT/2000 Password
- Executing Applications
  - – Host/remote key loggers
- Buffer Overflows
  - – Metasploit
- DOS attacks

- Trinvo , TFN2K

- Social Engineering

- Phishing URLs, Email, Telephone

Phase 4 - Maintaining Access

- Maintaining Access refers to the phase when the hacker tries to retain his ‘**ownership**’ of the system.
- The hacker has exploited a vulnerability and can tamper and compromise the system.
- Sometimes, hackers harden the system from other hackers as well (to own the system) by securing their exclusive access with Backdoors, RootKits, Trojans and Trojan horse Backdoors.
- Hackers can upload, download or manipulate data / applications / configurations on the ‘owned’ system.
- **Tools** : Trojans (Netcat , Loki), Rootkits (Knark, Torn etc)

Phase 5 - Covering Tracks

- Covering Tracks refers to the activities undertaken by the hacker to extend his misuse of the system without being detected.
- Reasons include need for prolonged stay, continued use of resources, removing evidence of hacking, avoiding legal action etc.
- Examples include Steganography, tunneling, altering log files etc. Hackers can remain undetected for long periods or use this phase to start a fresh reconnaissance to a related target system.
- **Tools for Covering Tracks:**
- Steganography :Camoflouge, MP3Stego
- Tunnelling : HTTPTunnel

Types of Attacks on a System

- Operating System attacks
- Application-level attacks
- Shrink Wrap code attacks
- Misconfiguration attacks

Operating system attacks

- Attackers search for vulnerabilities in an operating system's design, installation, or configuration and exploit them to gain access to a system, control, run malicious code, or crash the system.
- Applying patches and hot fixes is not easy with today's complex networks. Most patches and fixes tend to solve an immediate issue, but they cannot be considered a permanent solution.
- Some **OS Vulnerabilities**: Buffer overflow vulnerabilities, bugs in operating system, unpatched operating system, etc.
- For example, a buffer overflow attack is when an attacker sends more data than the system can handle, causing it to overwrite other parts of the memory and execute the attacker's code.

Application-level attacks

- **Application-level attacks**: Attackers **exploit the vulnerabilities in applications running** on organizations' information system to gain unauthorized access and steal or manipulate data
- Software applications come with myriad functionalities and features. There is a dearth of time to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack.
- **Application Level Attacks:**
- Buffer overflow,
- Cross-site scripting,
- SQL injection,
- Session hijacking,
- Denial-of-Service, etc.

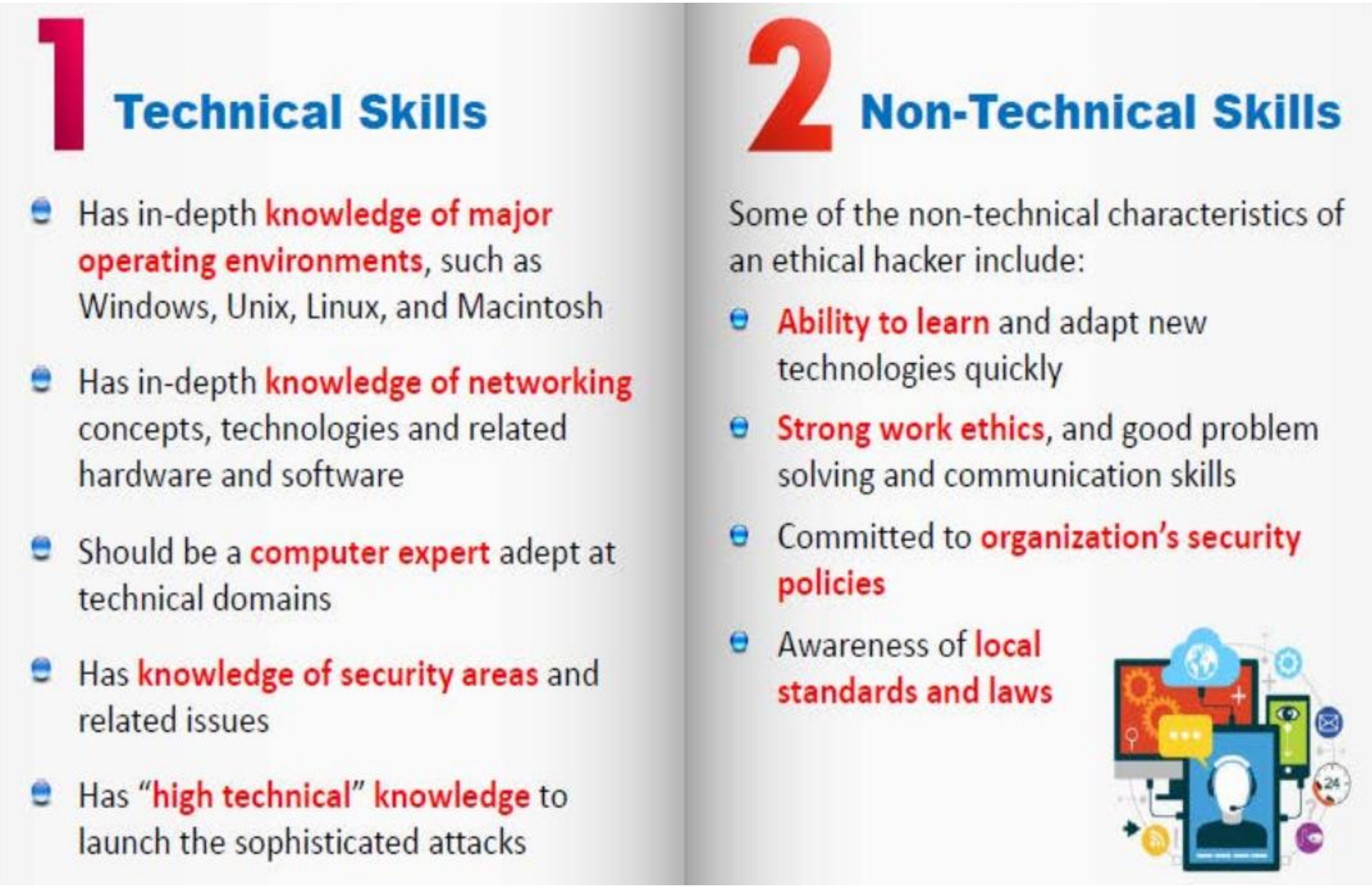
Shrink wrap code attacks

- Attackers **exploit the default configuration and settings** of the off-the-shelf libraries and code.
- Operating system applications come with numerous sample scripts to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink-wrap code attacks

Misconfiguration attacks

- **Misconfiguration attacks:** Most administrators don't have the necessary skills to maintain or fix issues, which may lead to configuration errors. Such configuration errors may become the sources for an attacker to enter into the target's network or system.
- Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in illegal access or possible owning of the system
- In a corporate network while installation of new devices, the administrator must have to change the default configurations. If devices are left upon default configuration, using default credentials, any user who does not have the privileges to access the device but has connectivity can access the device. It is not a big deal for an intruder to access such type of device because default configuration has common, weak passwords and there are no security policies are enabled on devices by default. Similarly, permitting an unauthorized person or giving resources and permission to a person more than his privileges might also lead to an attack. Additionally, Using the organization in Username & password attributes make it easier for hackers to gain access.

Skills of an Ethical Hacker



1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has "**high technical**" **knowledge** to launch the sophisticated attacks

2 Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- **Ability to learn** and adapt new technologies quickly
- **Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**

Thank You