What is Hacking

Hacking :

Hacker is the one who is smart enough to steal the information such as business data, personal data, financial information, credit card information, username and password from the system he is unauthorized to get this information by taking unauthorized control over that system using different tools and techniques.

These vulnerability or weakness can be used by the hacker to commit crime or to take advantages of remote machine.

Source from EC-Council

What is Information Security

- Information Security is that the practice of protecting information from unauthorized access, usage, disclosure, disruption, modification, inspection, copying or destruction
- Information can be defined as the "Processed Data" which contains some meaningful message
- Information does not depend on language; it can be a chain of symbols, mental stimuli of living beings
- The meaning of information depends on time, place and situation. As per the time and situation information may vary
- Information security techniques can be defined as the ways and means used to secure our personal or private information from being hacked or misused

Is Hacking Legal or Illegal ?

- Hackers are the professionals who work on the technology, explore it and take it to the next level

- Its legal or not - depends upon the work mentality and the motive of the individual who works on that technology

- (NOTE: Technology is never illegal, the person who works on that technology decides whether the work is legal or not)

Is Hacking Legal or Illegal ?

- Hackers are the professionals who work on the technology, explore it and take it to the next level

- Its legal or not - depends upon the work mentality and the motive of the individual who works on that technology

- (NOTE: Technology is never illegal, the person who works on that technology decides whether the work is legal or not)

Types of Hackers

White Hat Hacker

- Those hackers are Good guys
- They Don't use their skills for illegal purpose
- Computer security experts and help to protect from Black Hats.

Black Hat Hacker

- Bad guys
- Use their skill maliciously for personal gain
- Hack banks, steal credit cards and deface websites

Grey Hat Hacker

- Those hackers are have skills of white hat and black hat hackers

Source from EC-Council

Hacker Classes

Suicide Hackers

- Hackers who aim to bring down critical infrastructure of a network for a cause and they are not worried about facing jail and any other kind of punishment also

Script Kiddies

- An hacker who compromises system by running scripts, tools, andsoftwares which are developed by real hackers.

Cyber Terrorists

- Individual with wide range of skills, Motivated by religious or political beliefs to create fear by large scale disruption

State Sponsored Hackers

- hackers working under govt. agencies to penetrate and gain top secret information.

Hacktivist

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

Source from EC-Council

Introduction of Ethical Hacking

Ethical Hacking :

Ethical Hacking involves in use of hacking tools, tricks and techniques to identify vulnerabilities to ensure system security. It is also called as penetration testing

Ethical Hacker :

An ethical hacker is a expert in cybersecurity and who attacks a security system on behalf of its owners and seeking vulnerabilities that a malicious hacker could exploit.

Source from EC-Council

Introduction of Ethical Hacking

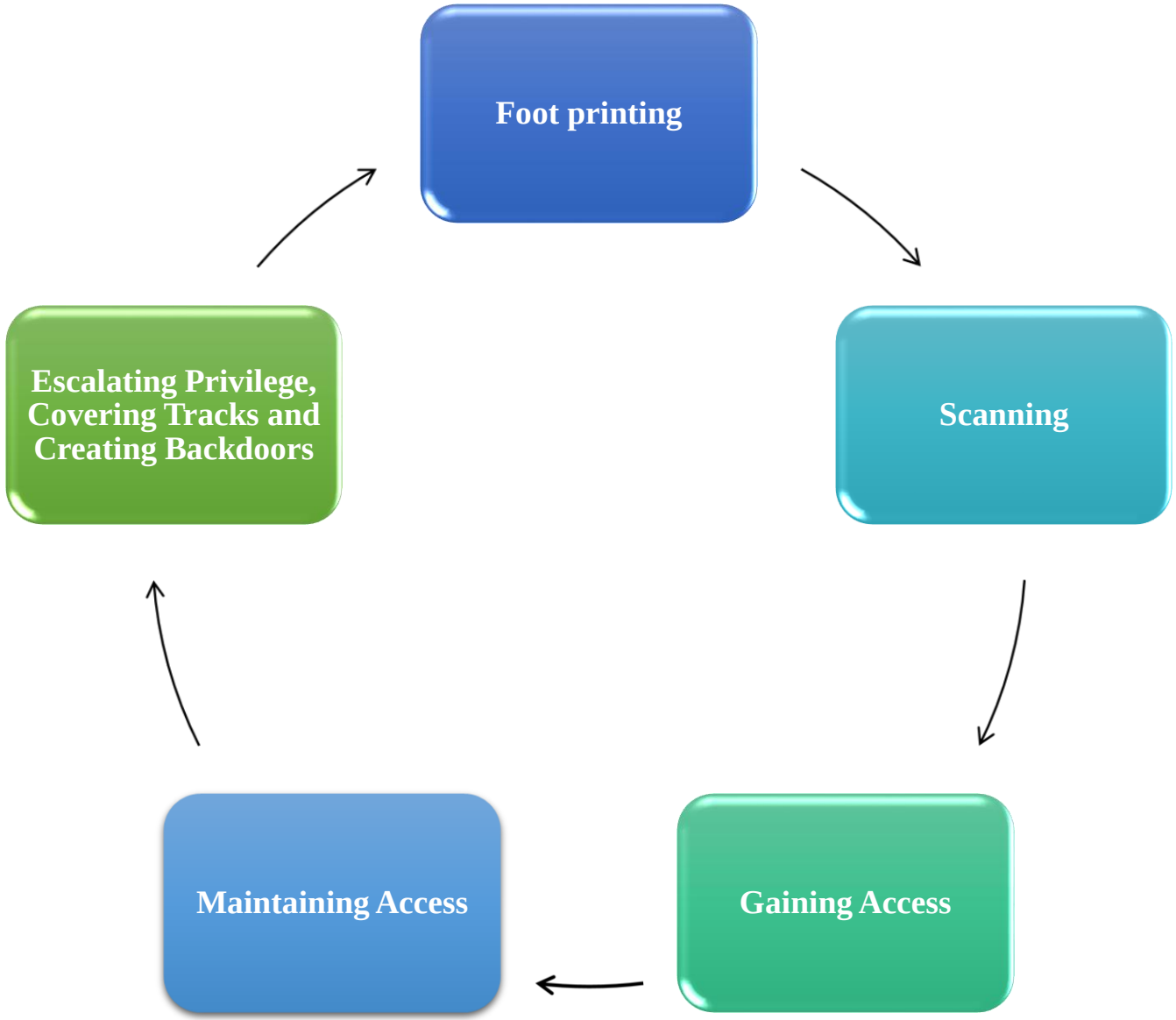
Skills required for Ethical Hacker

- Ethical Hacker has in-depth knowledge of just about all operating systems, including all popular, widely-used operating systems like Windows, Linux, Unix, and Macintosh.

- These ethical hackers are very skilled at networking and exploring capabilities of hardware and software.

- They must have detailed knowledge about older, advanced, sophisticated attacks

Phases of Hacking (Life Cycle)



Phases of Hacking (Life Cycle)

Foot printing:

Reconnaissance/Information Gathering refers to gathering Information about the Target. This was the first step of Hacking and the aim is to gather as much as information Target.

Scanning:

Scanning refers to the pre-attack phase when the Hacker scans the Network or Website using in a general manner or using specific information gathered during the first step of Reconnaissance. This is an Active State of Gathering Information.

Target Information:
OS of the Target
Open Port and Services
Vulnerable Applications

Phases of Hacking (Life Cycle)

Gaining Access:

Gaining Access refers to the Attack stage. In this Step, the Hacker will launch an Attack on the System, on the Basis of the Information Gathered during the First 2 Steps, of Reconnaissance and Scanning.

Maintaining Access:

Maintaining Access refers to a stage which is Post-Exploitation or Post-Attack. This is done once the Hacker “owns” the System. In order to Maintain Access to the Hacked system and control it remotely.

Clearing Tracks:

Covering Tracks refers to actions performed by a Hacker, Post-Exploitation, which helps is increasing the Time for which the System Compromise goes un-detected and similarly, the attacker does not get traced back

Threat Modeling

Threat Modeling is that the process or approach to spot , diagnose, the threats and vulnerabilities of a system. It is one of the way to approach for risk management which mainly focuses on analyzing the network security and application security against vulnerabilities.

1. Identify Security Objectives

2. Application overview

3. Decompose Application

4. Identify Threats

5. Identify Vulnerabilities

Introduction of Cyber Security

Cyber Security :

- Cyber Security refers to the body of technologies, Process and practices designed to protect networks, devices, programs and data from attacks, damage or unauthorized access.

- With an increasing amount of individuals getting connected to Internet, the safety threats that cause massive harm are increasing also.

Essential Terminology

Hack Value:

It is the notion among hackers hacker's that something is worth doing

Vulnerability:

Existence of a weakness, design, implementation errors that can lead to an unexpected event compromising the security of the system

Payload:

Payload is a part of an exploit code that performs malicious action, such as destroying, creating backdoors, and hijacking computer

Exploit:

Breaking in to IT system security through vulnerabilities

Source from EC-Council

Essential Terminology

Zero-Day Attacks:

An Attack that exploits computer applications vulnerabilities before the software developer releases patch for the vulnerability

Daisy Chaining:

It involves gaining access to one network/computer and then using same information to gain access to multiple networks and computers that contain desirable information

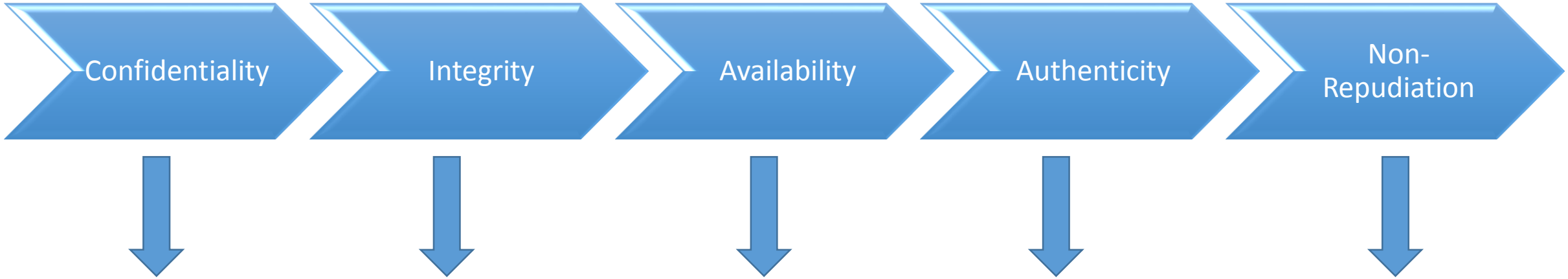
Doxing:

Publishing personally identified information about an individual collected from publicly available databases and social media

Bot:

A “Bot” is software application that can be controlled remotely to execute or automate predefined tasks

Elements of Information Security



Assurance that the knowledge is accessible only to those authorized to possess access

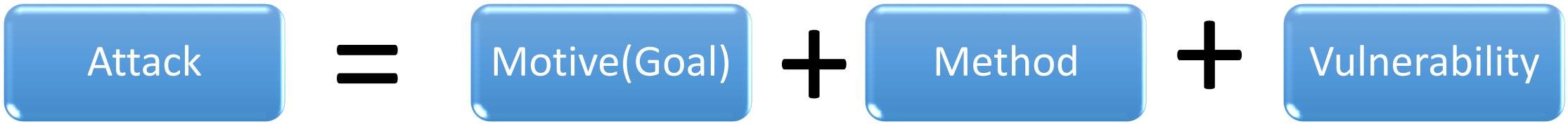
Unauthorized persons should not modify data without owner's permission.

Ability of infrastructure to function according to business expectations Data should be available 24x7

Authenticity is the process which identifies the user, or device to grant privileges, access and certain rules and policies

Guarantee that sender of message cannot later deny having sent the message and that the recipient cannot deny having received the message

Objectives of Information Security Attacks



Attacker tries various tools and attack techniques to exploit vulnerabilities in a computer system or security policy and control to achieve their motives

Motives Behind Information Security Attacks:

- Information Theft
- Manipulating Data
- Taking Revenge
- Damaging Reputation of the target
- Disrupting business continuity

Information Category Threats

Network Threats:

- Information Gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and MIMA
- DOS attacks
- Firewall and IDS attacks
- Password based attacks

Host Threats:

- Malware attacks
- Foot printing
- Password attacks
- DOS attacks
- Privilege escalation
- Backdoor attacks
- Physical Security Threats

Application Threats:

- Improper Data / Input validation
- Authentication attacks
- Security Misconfiguration
- Information Disclosure
- Broken session Management
- Cryptographic attacks
- SQL Injection attacks