InSEC-Techs

Learn Ethical Hacking from “Entry to Expertise”

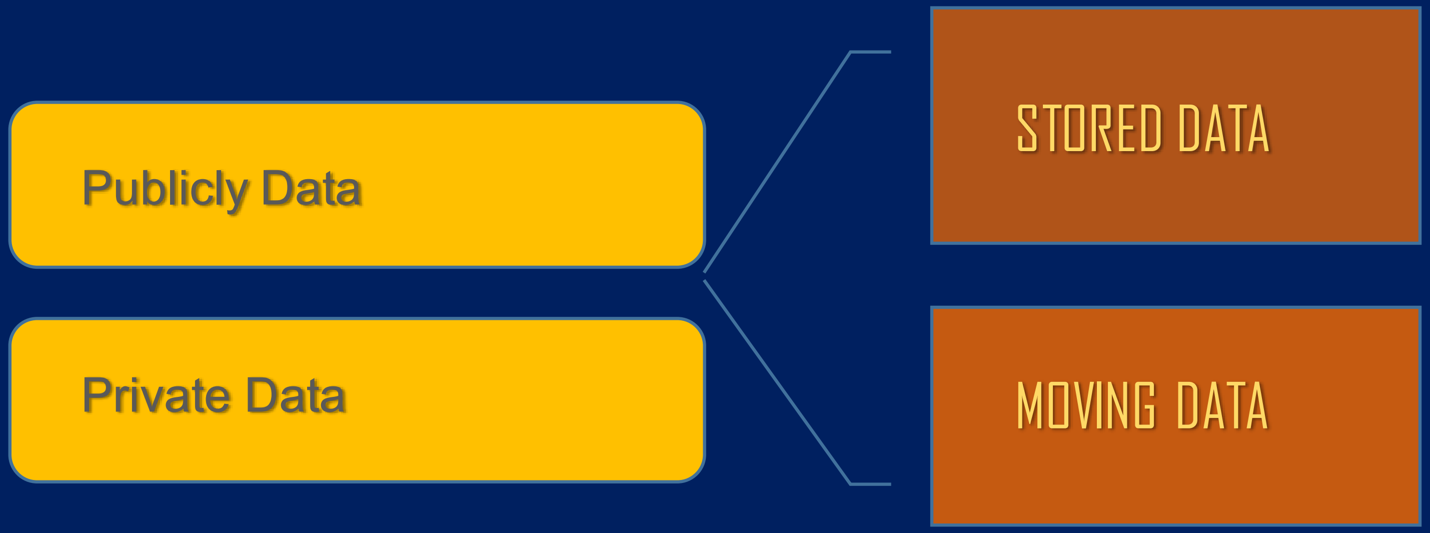
Module 2
“Introduction to Ethical Hacking”

Trainer : Kiran Thirukovela

02/1: Ethical Hacking - Course Introduction

Why Ethical Hacking is necessary ?

DATA



Publicly Data

Private Data

STORED DATA

MOVING DATA

02/2: Ethical Hacking - Course Introduction

Security_

Security in simple terms is taking a preventive measures against attacks so that impact of an attack is as low as possible.

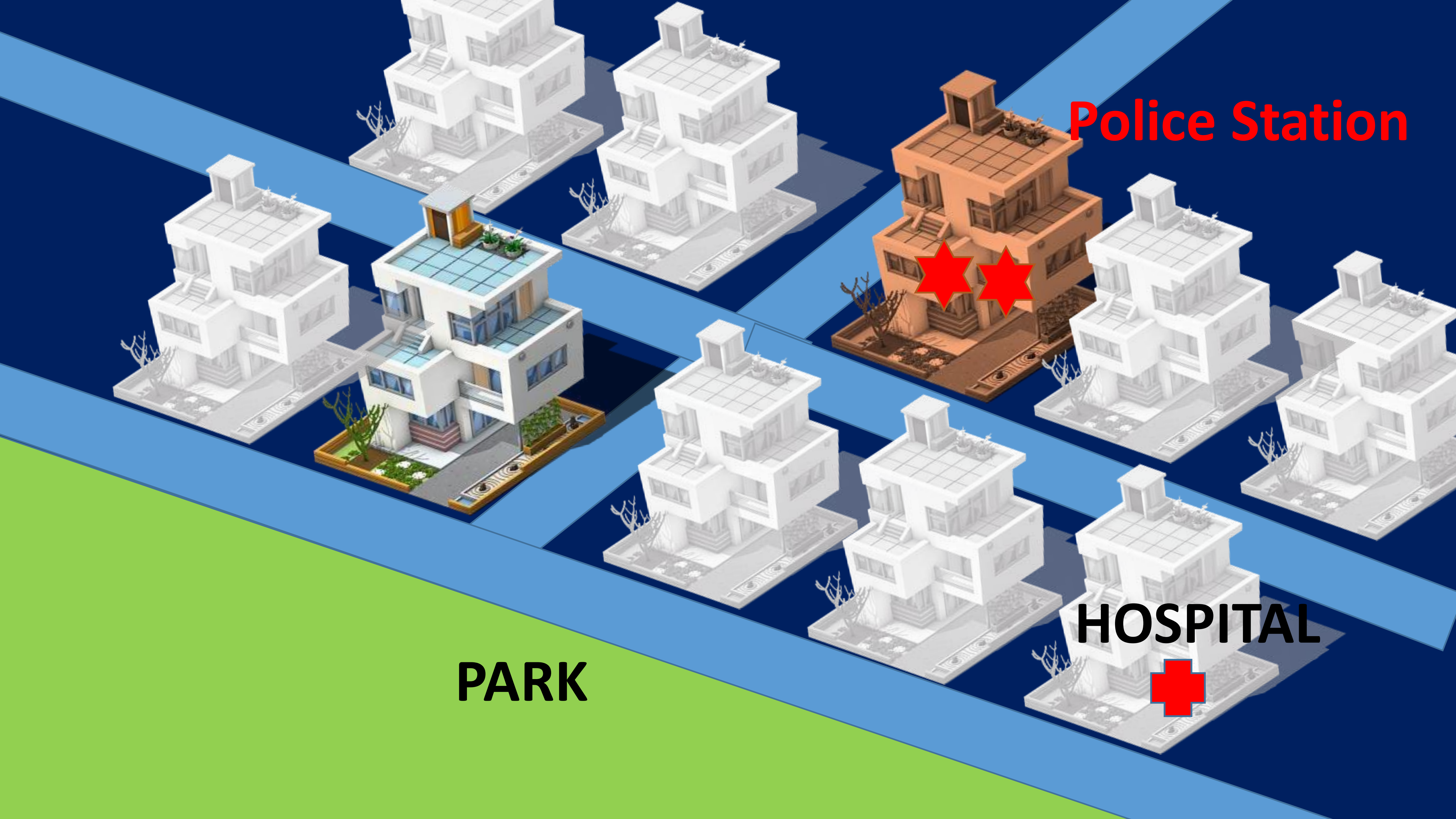
In IT domain, SECURITY is creating policies , and or implementing 'defensive or offensive' strategies and or following standardized methodologies to secure IT infrastructure from the attacks that are known or un-known and attacks that are expected or unexpected, so that the impact of attack(s) is null or as low as possible.

IT Security is set of strategies to prevent unauthorized access to network, services or data to maintain elements of security that are confidentiality, integrity and availability.

02/2: Ethical Hacking - Course Introduction

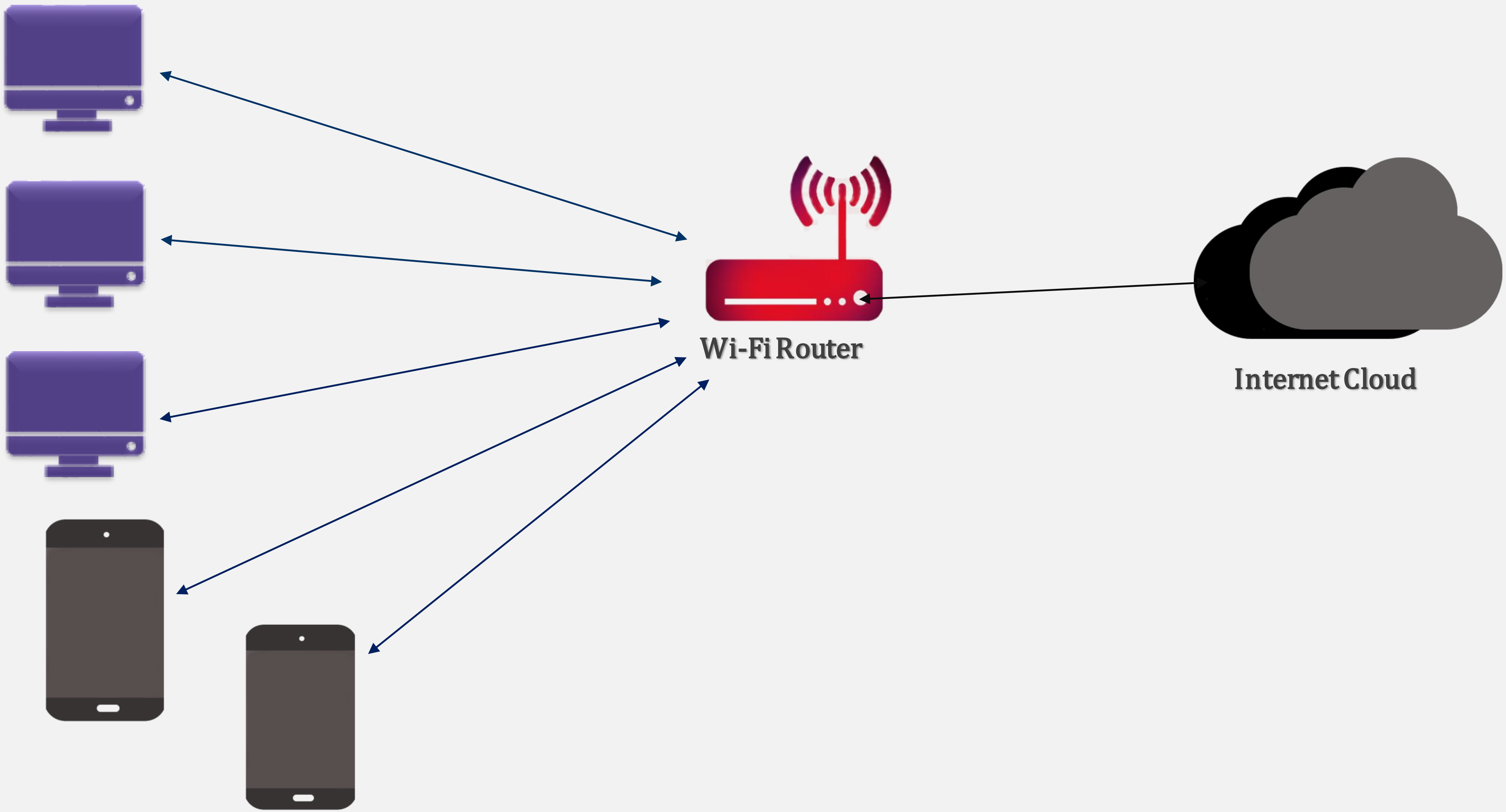
- Where is the Security implemented ?
- How strong the security ?

- Any Existing Vulnerabilities in this network (or applications ?

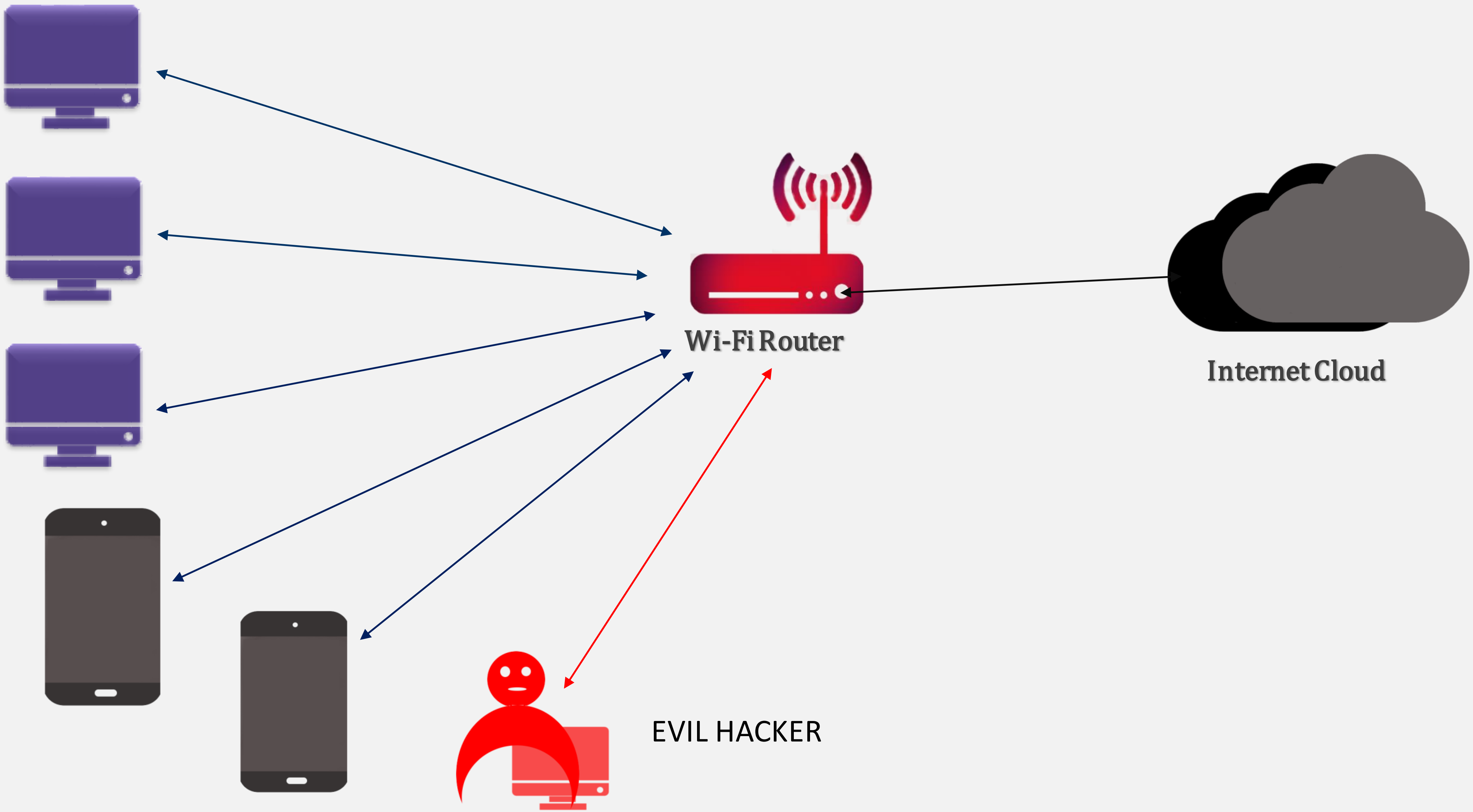

Police Station
HOSPITAL
PARK

02/2: Ethica cking - Course Introduction

02/2: Ethical Hacking - Course Introduction

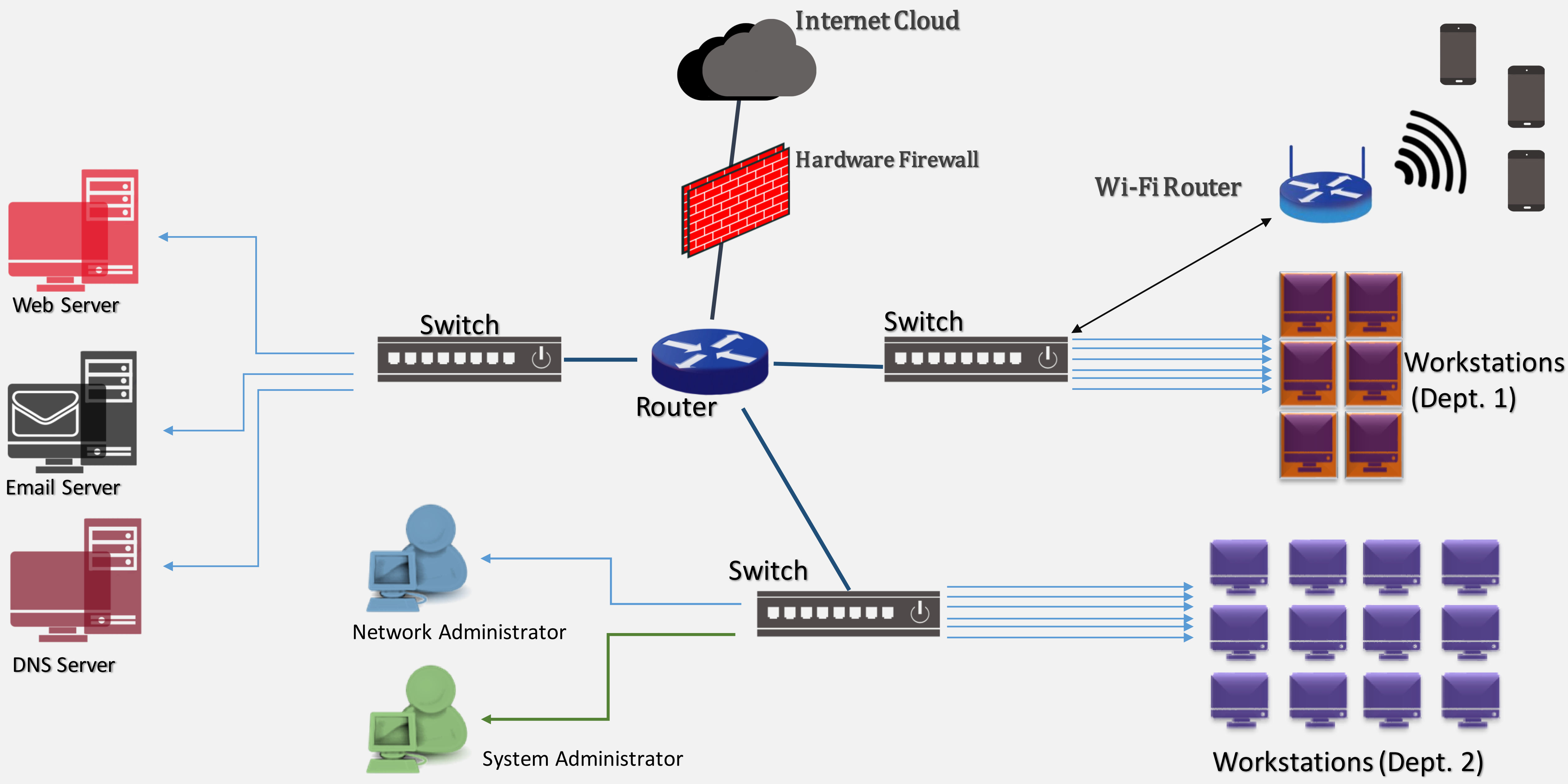


02/2: Ethical Hacking - Course Introduction



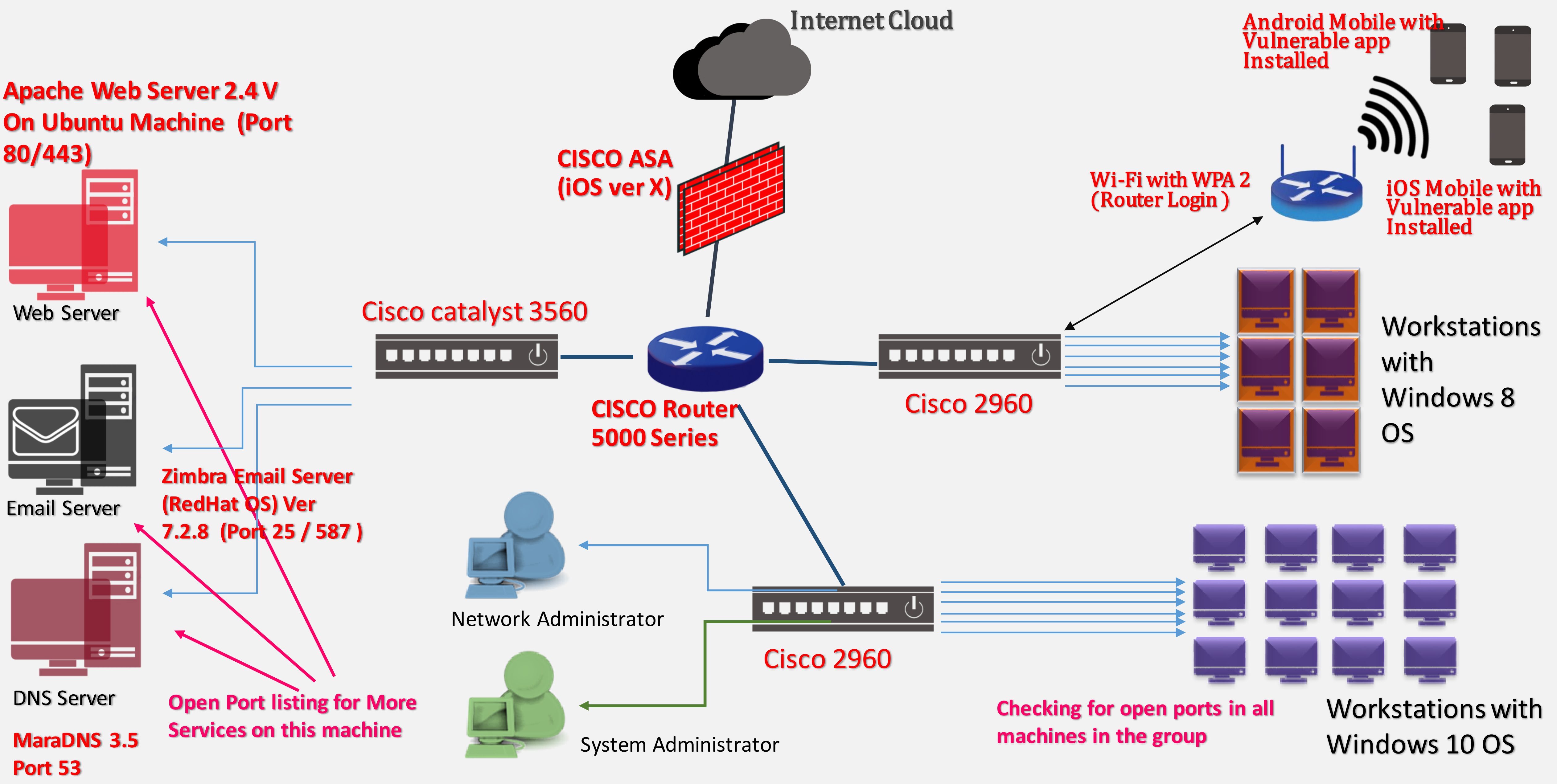
02/2: Ethical Hacking - Course Introduction

Network Design



02/2: Ethical Hacking - Course Introduction

Network Design


Internet Cloud
Android Mobile with Vulnerable app Installed
Apache Web Server 2.4 V On Ubuntu Machine (Port 80/443)
CISCO ASA (iOS ver X)
Wi-Fi with WPA 2 (Router Login)
iOS Mobile with Vulnerable app Installed
Web Server
Cisco catalyst 3560
Workstations with Windows 8 OS
Cisco 2960
CISCO Router 5000 Series
Zimbra Email Server (RedHat OS) Ver 7.2.8 (Port 25 / 587)
Email Server
Network Administrator
Cisco 2960
DNS Server
Open Port listing for More Services on this machine
Checking for open ports in all machines in the group
Workstations with Windows 10 OS
System Administrator
MaraDNS 3.5 Port 53

02/2: Ethical Hacking - Course Introduction

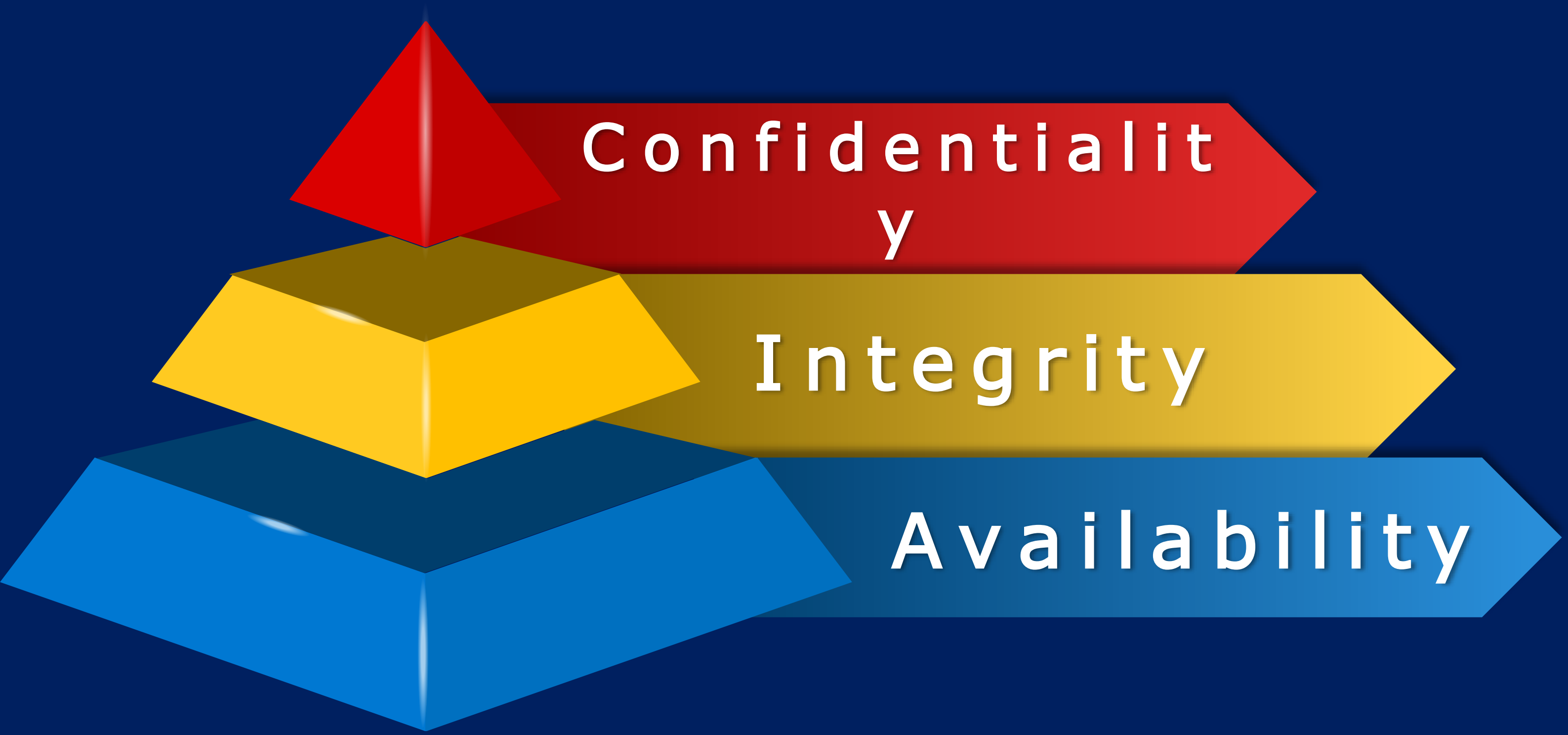
What do “Ethical Hackers” do ?

An Ethical hacker (Pen-Tester) evaluates computer infrastructure (Networks / Systems or Application) to seek answers for following..

1. What are the vulnerabilities in the target of Evolution (or) What an Intruder can see in the target system ?
2. How can intruder exploit the target system ?
3. What can intruder do with the exploited target system ?
4. How can the attacks be stopped or how can be vulnerabilities patched ?
5. Does anyone at target has ability to notice that attacks ?

02/2: Ethical Hacking - Course Introduction

CIA TRIAD



Confidentiality

Integrity

Availability

02/4: Ethical Hacking - Course Introduction

Confidentiality

No Unauthorized Access or Modification (Equals to Privacy and Secrecy)

Confidentiality can be defined as set of rules that limits access to data. Only authorized users can access data.

Example : Data Encryption

Integrity

Data is Accurate and Trustworthy

Integrity can be defined as technique that ensures Data is trustworthy and accurate.

Example: Hash values, Checksums and Data Comparsion

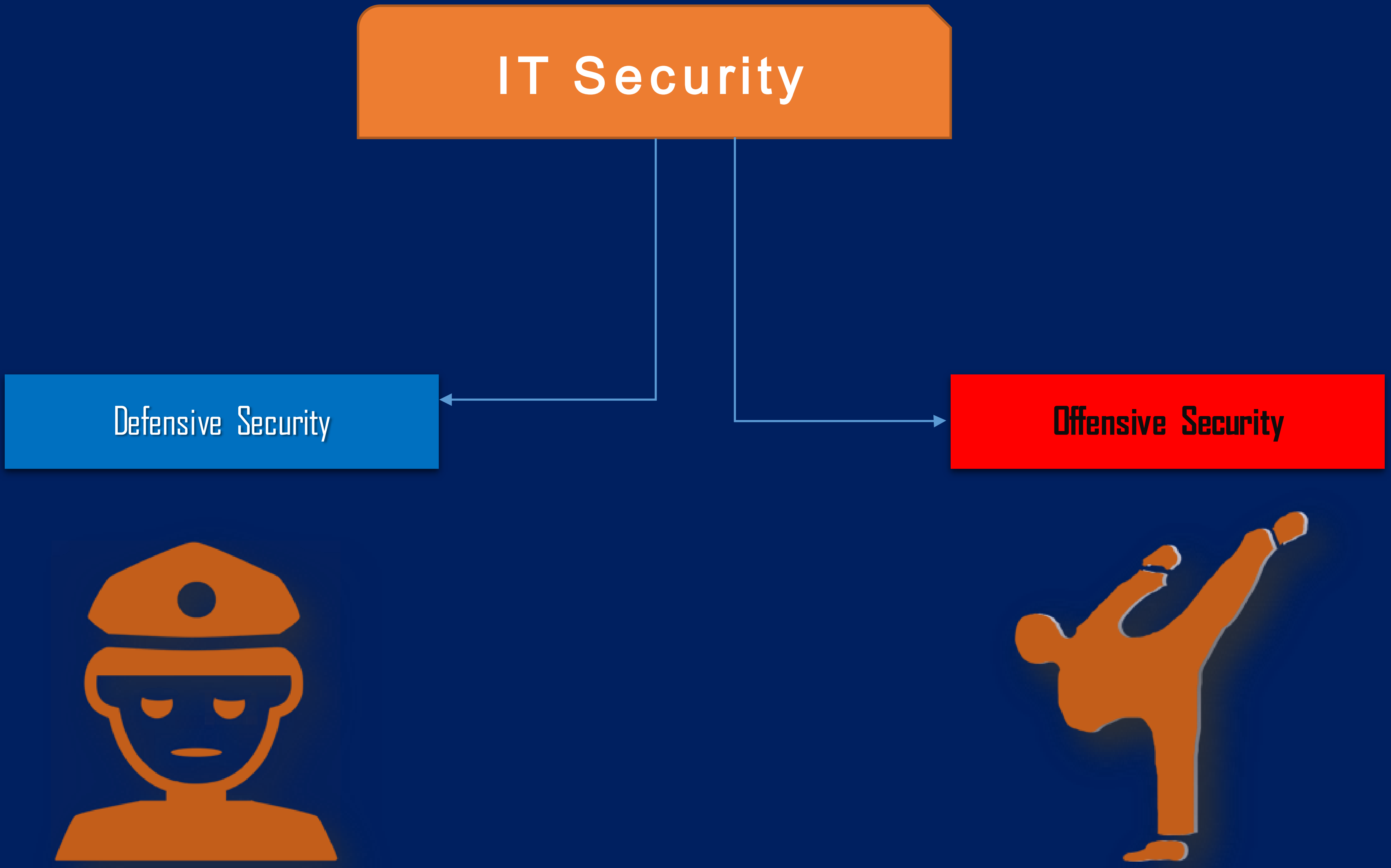
02/4: Ethical Hacking - Course Introduction

Availability

Availability refers to, Availability of data or resources all the time.

Availability ensures that data or network resource is available to authorized users all the time.

02/3: Ethical Hacking - Course Introduction

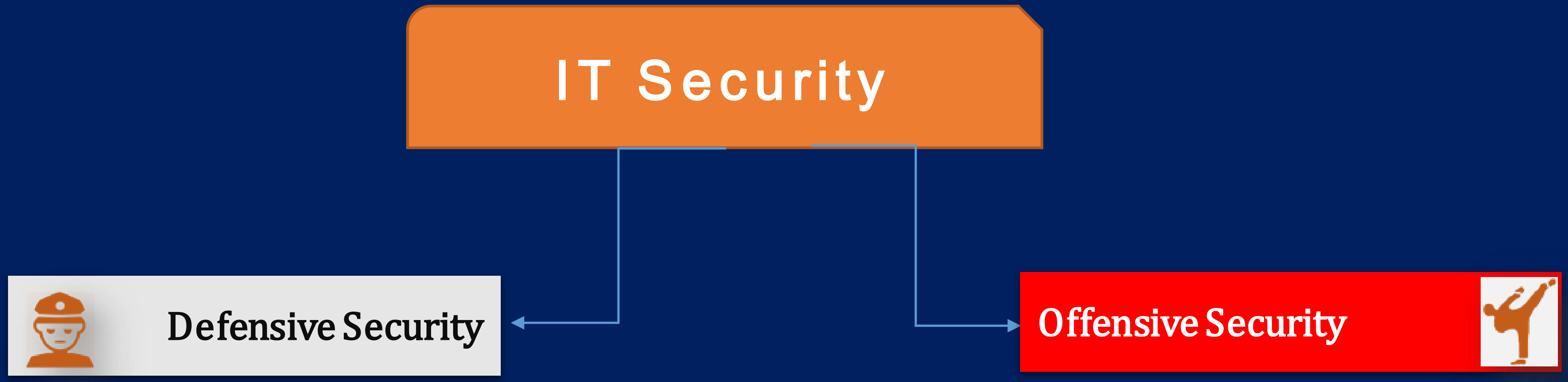


IT Security

Defensive Security

Offensive Security

02/3: Ethical Hacking - Course Introduction



IT Security

Defensive Security

Offensive Security

Firewalls (SW & HW)
Advanced Security Appliances.
IPS (Intrusion Prevention Systems)
IDS (Intrusion Detection Systems)
WIDPS - Wireless intrusion prevention and detection system
UTM – Unified Threat Management
NAC- Network Access Control
Proxy Server
Anti-Virus
DMZ – De-Militarized Zone

Network Security Admins/Engg

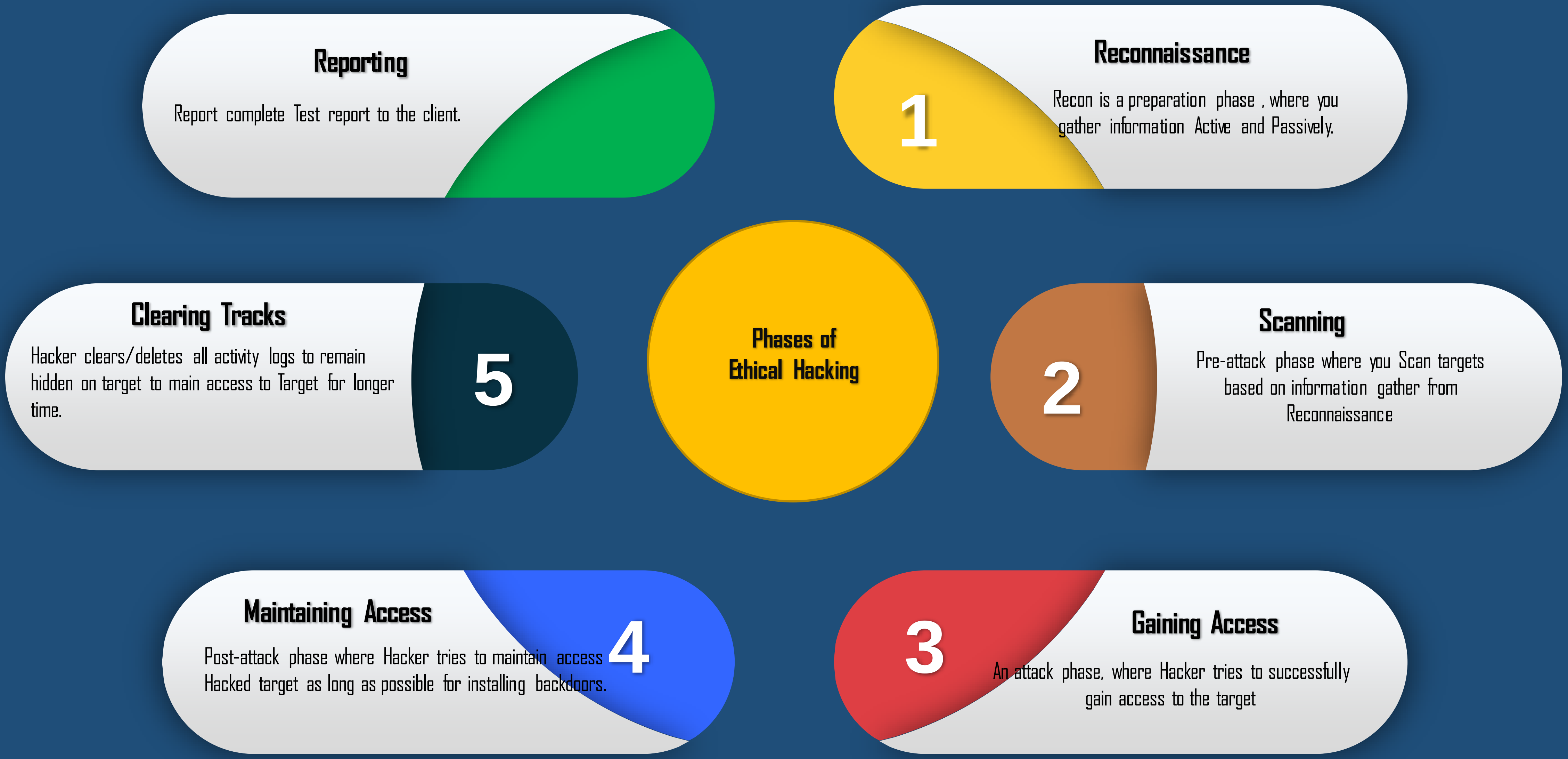
Vulnerability Assessment and

Penetration Testing

Penetration Tester / Security Analyst

02/4: Ethical Hacking - Course Introduction

Phases of Ethical Hacking



Phases of Ethical Hacking

1 Reconnaissance

Recon is a preparation phase , where you gather information Active and Passively.

2 Scanning

Pre-attack phase where you Scan targets based on information gather from Reconnaissance

3 Gaining Access

An attack phase, where Hacker tries to successfully gain access to the target

4 Maintaining Access

Post-attack phase where Hacker tries to maintain access Hacked target as long as possible for installing backdoors.

5 Clearing Tracks

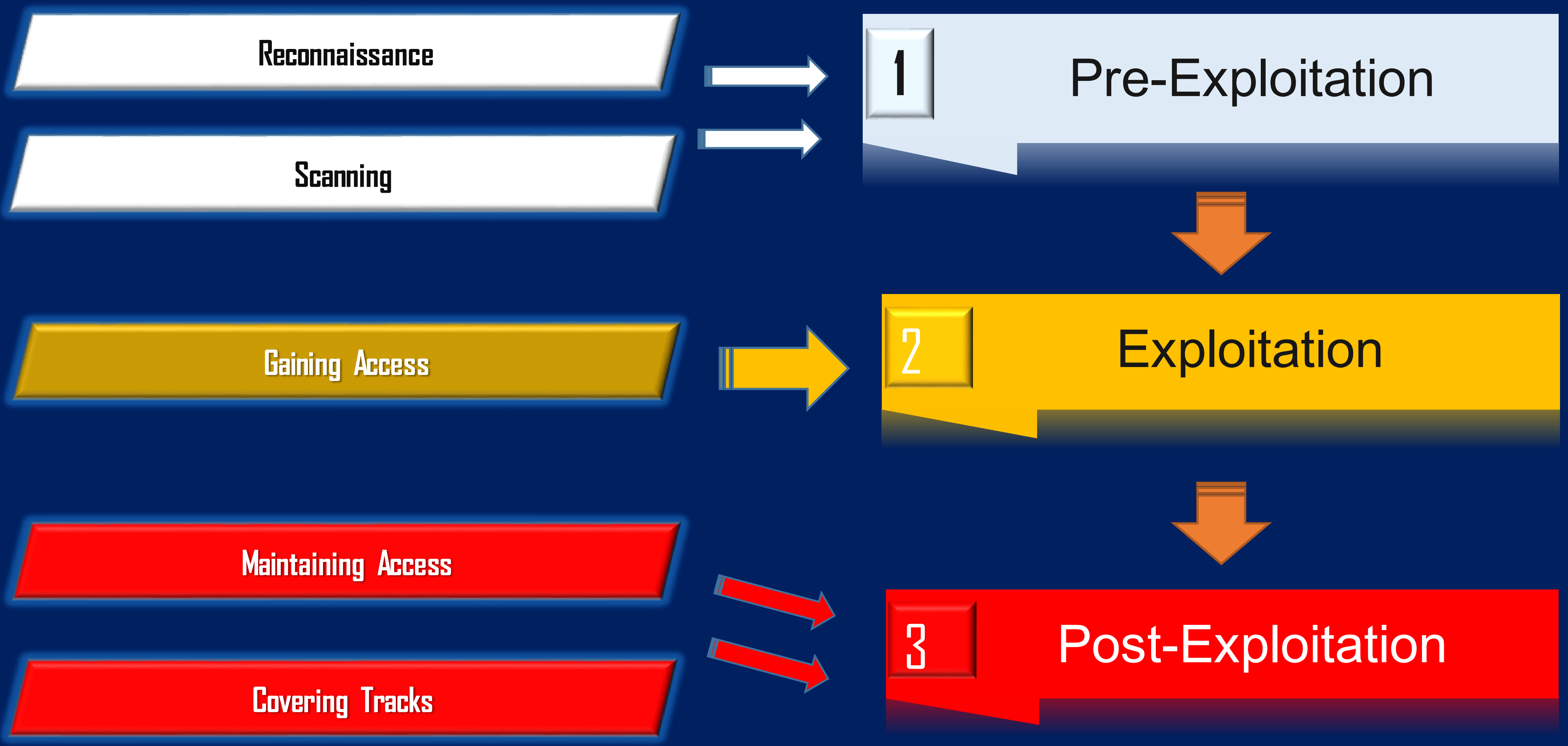
Hacker clears/deletes all activity logs to remain hidden on target to main access to Target for longer time.

Reporting

Report complete Test report to the client.

02/4: Ethical Hacking - Course Introductio

Phases in Ethical Hacking



Reconnaissance

Scanning

1 Pre-Exploitation

Gaining Access

2 Exploitation

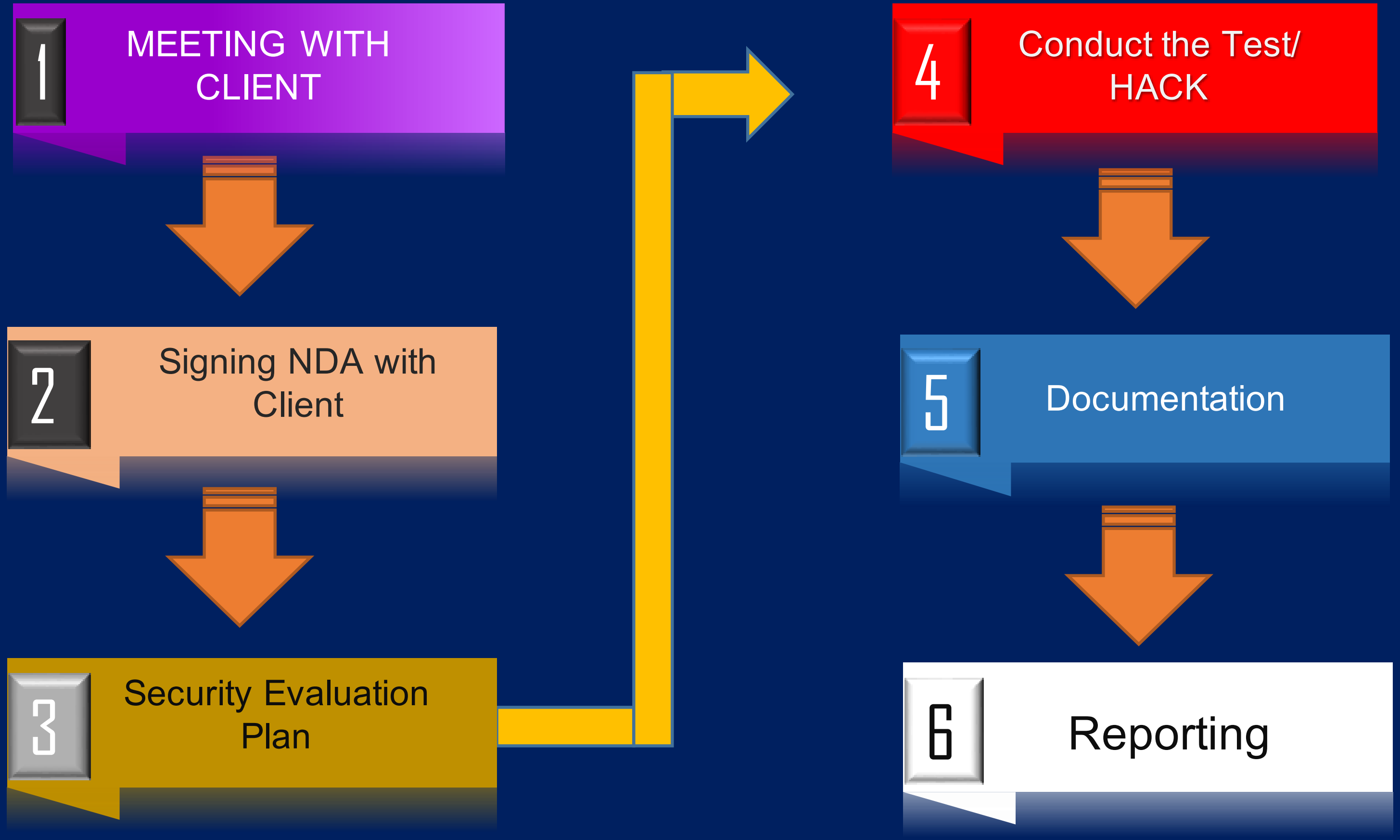
Maintaining Access

Covering Tracks

3 Post-Exploitation

02/5: Ethical Hacking - Course Introduction

Penetration Test (On Floor Approach)_



1 MEETING WITH CLIENT

2 Signing NDA with Client

3 Security Evaluation Plan

4 Conduct the Test/ HACK

5 Documentation

6 Reporting

02/5: Ethical Hacking - Course Introduction

Types of Penetration Testing

Black-Box Testing

Black box is a method of Penetration Testing, where Hacker has no knowledge of the target, except target name or IP etc. Client will not provide any information to hacker, and want Hacker to simulate real time cyber criminal attacks. These are basically External attacks.

Grey-Box Testing

Grey box is a method of Penetration Testing, where Hacker has some knowledge of the target with user level access and some knowledge shared about the target like applications information, hosted platforms, IP addresses and Range etc

White-Box Testing

White box is a method of Penetration Testing in which Hacker has complete knowledge of the target that you request using engagement tool kit and hacker will access to target machines or source code or testing application etc.

02/5: Ethical Hacking - Course Introduction

How does “Ethical Hackers” HACK ?

1. Remote Network

Hacker / Tester simulates the hack from remote location over the internet as a true Cyber criminal. The Primary defence to mitigate this kind of attacks are Border Firewalls, Filtering routers & Security policies.

2. Local Network

Hacker / Tester conducts the test from local network i.e. clients internal network as an authorised and with scope of testing, The primary defence to challenge the test/hack is intranet firewalls, strong internal security policies.

3. Stolen Devices

Cyber criminals steal devices like laptop(s) , Smartphones , Hard disks from targeted location or from a targeted person and extract valuable information from stolen devices. Physical security must be implemented to high valued devices.

02/5: Ethical Hacking - Course Introduction

How does "Ethical Hackers (Cyber Criminals)" HACK ?

4. Social Engineering

In this type of attack, attacker target individuals of target organization or just target persons like friends or relative and extract required information from them using verbal communication, like asking personal/private information as a casual act.

5. Physical Entry

Hacker's physically intrude into organizations bypassing security guards (mostly using fake ID cards) and once inside the organization, hacker can execute attacks like stealing documents, files, devices, connecting to internal network and spying (MITM) & so on. Proper physical security with biometric identification techniques like fingerprint scanning & IRIS scanning will be helpful

Dumpster Diving: This is information gather technique used by hacker , where hacker goes to target organization's premises or inside the building and look into trashcan's for documents of vital importance.