Introduction to ETHICAL HACKING

About Me

This Section is removed to avoid content abusage

Nowsher Ali Shovon

PERQUISITES

- Ethical Mind-set.
- Law Enforcement unit hires hackers.
- Unethical activities always have footprint.
- Why Hacker's get caught?
- Know how to google.
- Networking Basics.
- Coding/Scripting Basics.
- Mostly need, passion, consistency.
- Need to read more than BCS.
- Need to work more than MBBS.

Let’s Start

What is Hacking?

Attempt to break/exploit a system or network to compromise the system
In order to gain access and change.

What is Ethical Hacking?

Types of Hackers

1. Black Hat: Only bad things do.
2. White Hat: Only good intension.
3. Gray Hat: Both black and white hat.

Types of Hackers

State Sponsored Hacker

Script Kid

Spammer

Why they hack?

Money

Research

Hobby

Revenge

Show off

Steps of Hacking

Steps of Hacking?

1. Footprinting and Reconnaissance.
2. Scanning.
3. Gaining Access.
4. Maintaining Access.
5. Clearing Tracks.

1. Footprinting and Reconnaissance.

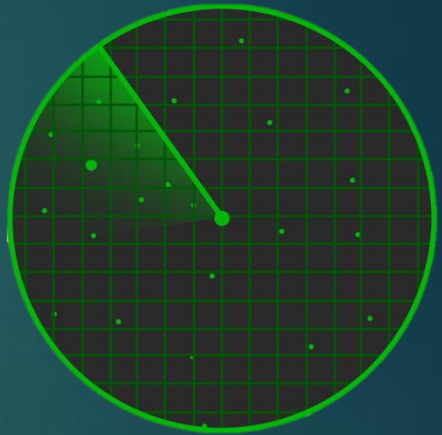
- Also called as Information Gathering.
- To gain vital information about target.
- Hackers will usually collect a large amount of information which may be useful during their attacks.
- Where an attacker seeks to gather as much information as possible about a target.

Methods :Art of Googling, Social Engineering, Dumpster Diving.

2. Scanning.

- In this phase, the hacker identifies a quick way to gain access to the network and look for information.

- There are three methods of scanning:



1. **Pre-attack:** where the hacker scans the network.

2. **Port scanning/sniffing:** port scanners, vulnerability scanners, and other data-gathering equipment.

3. **Information extraction:** attackers collect information about ports, live machines and OS details to launch an attack.

3. Gaining Access.

- Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access.
- The hacker can gain access at operating system level, application level or network level and **escalates their user privileges** to control the systems connected to it.
- The hacker has control and can use that system as they wish.

4. Maintaining Access.

- In this step, the hacker secures administrator root access to the organization's System.

- He can install **Rootkits**, Trojans or other type of **backdoor** to maintain his access.

- By doing this he can gather additional information or launch additional attacks on the network.

5. Clearing Tracks.

- Once the hacker gains access, they cover their tracks to escape the security personnel.

- They do this by clearing the cache and cookies, tampering the log files, and closing all the open ports.

- This step is important because it clears the system information making hacking a great deal harder to track.

Deleting Files...

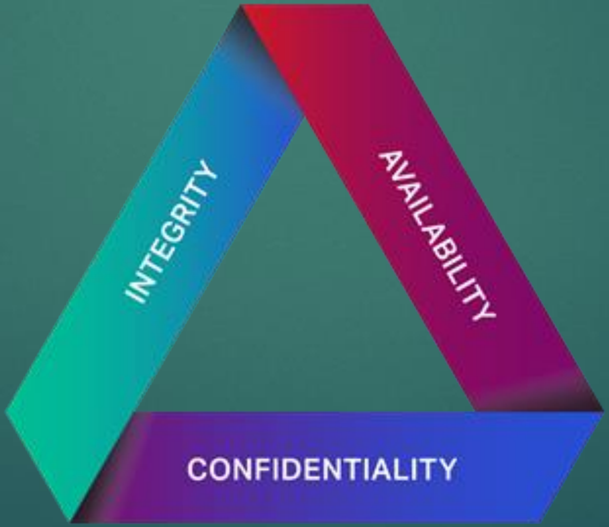
Please wait...

0%

Short Break

Question and Answer

3 Pillars of Cyber Security



CIA Triad

Pillar 1: Confidentiality

Are my systems protected from outside, unauthorized access?

Pillar 2: Integrity

Is my data corrupted, tampered with or impacted by outside threat actors?

Pillar 3: Availability

Are my systems and data readily accessible for everyday use and approved operations?

There are more 2 Pillars

Authenticity: Is my data delivered to authentic destination?

Non-Repudiation: Ensure that the sender of data is provided with proof of delivery.

Why Bangladeshi Hackers Won’t Support Us?

Ananta Jalil

Tarik Anam Khan

Terminology

Vulnerability

Vulnerability describes the **characteristics and circumstances** of a community, system or asset that make it susceptible to the damaging effects of a hazard.

Vulnerability is a weakness or some area where you are exposed or at risk.

Threat

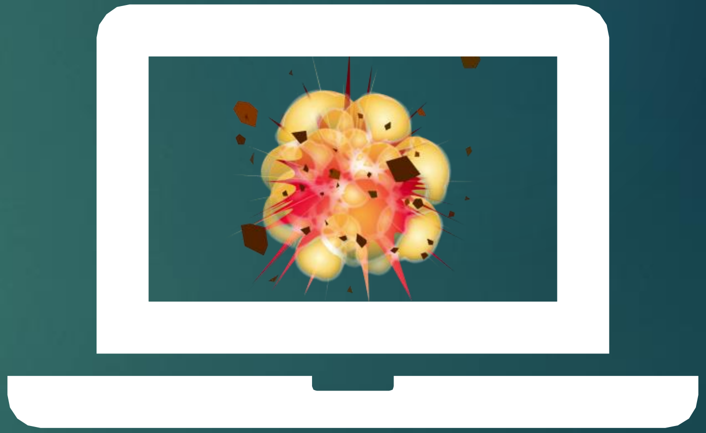
A cyber or cybersecurity threat is a **malicious act** that **seeks to** damage data, steal data, or disrupt digital life in general.

Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

Exploit

A piece of software, a chunk of data, or a sequence of commands that **takes advantage of a bug** or vulnerability which cause unintended behaviour to occur on a system.

Behaviour frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

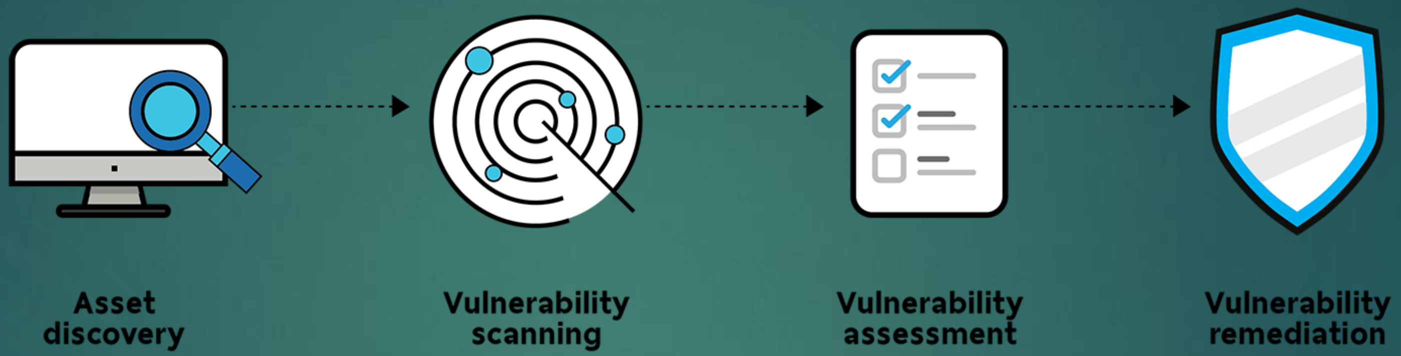


Zero day

If a hacker manages to **exploit the vulnerability before software developers can find a fix**, that exploit becomes known as a zero day attack.

It could take the form of missing data encryption, SQL injection, buffer overflows, missing authorizations, broken algorithms, URL redirects, bugs, or problems with password security.

Vulnerability Assessment



A vulnerability assessment is a **systematic review** of security weaknesses in an information system.

It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Penetration test

A penetration test, also known as a pen test, is a **simulated cyber attack** against your computer system to **check for exploitable vulnerabilities**.

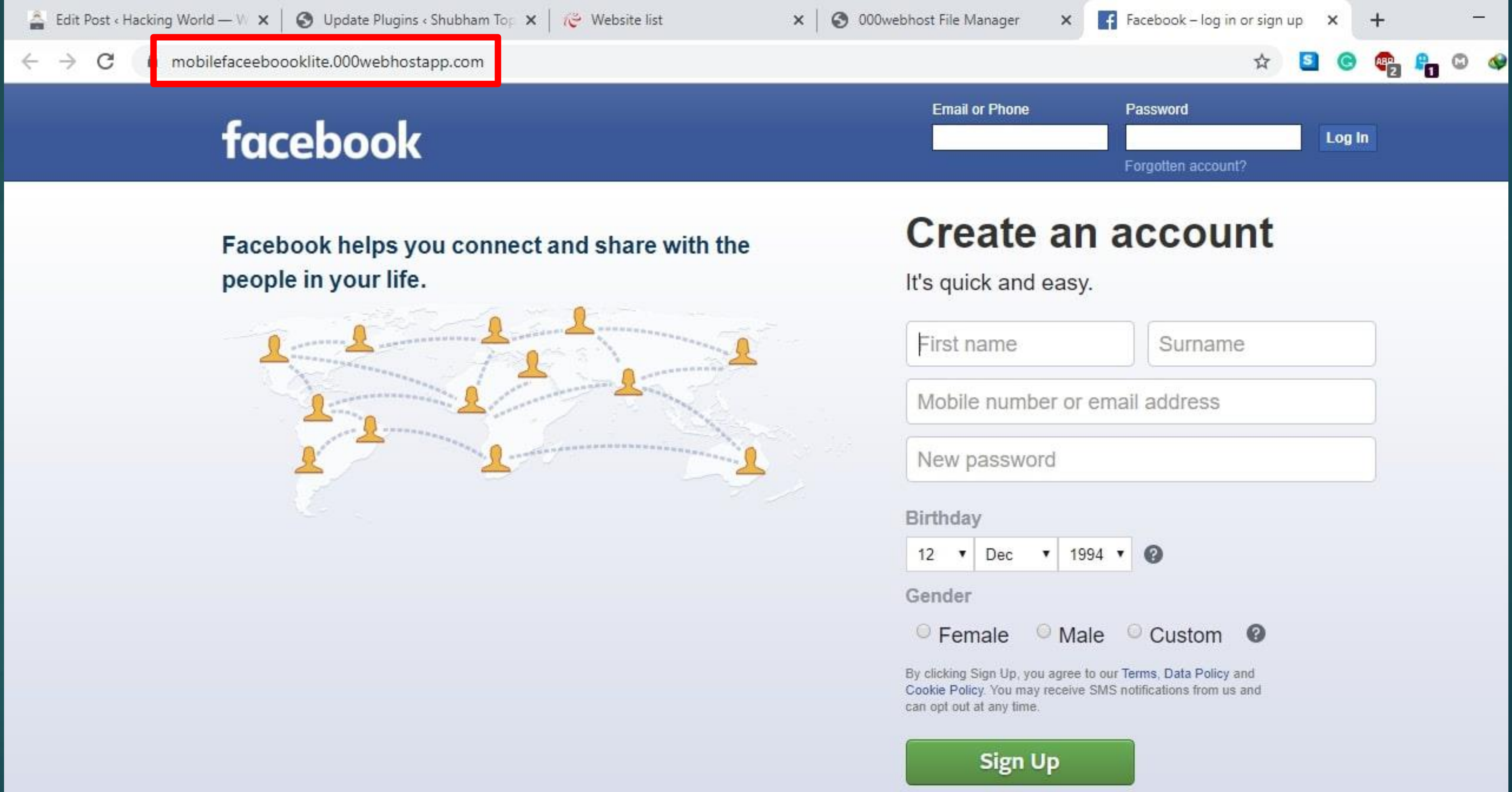
In the context of web application security, penetration testing is commonly used to augment a server, network, API and web application firewall (WAF).

Terminology

Question and Answer

Some Common Attacks

1. Phishing



Edit Post ‹ Hacking World — W
Update Plugins ‹ Shubham Top
Website list
000webhost File Manager
Facebook – log in or sign up

mobilefaceeboooklite.000webhostapp.com

facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's quick and easy.

First name

Surname

Mobile number or email address

New password

Birthday

12 ▾ Dec ▾ 1994 ▾

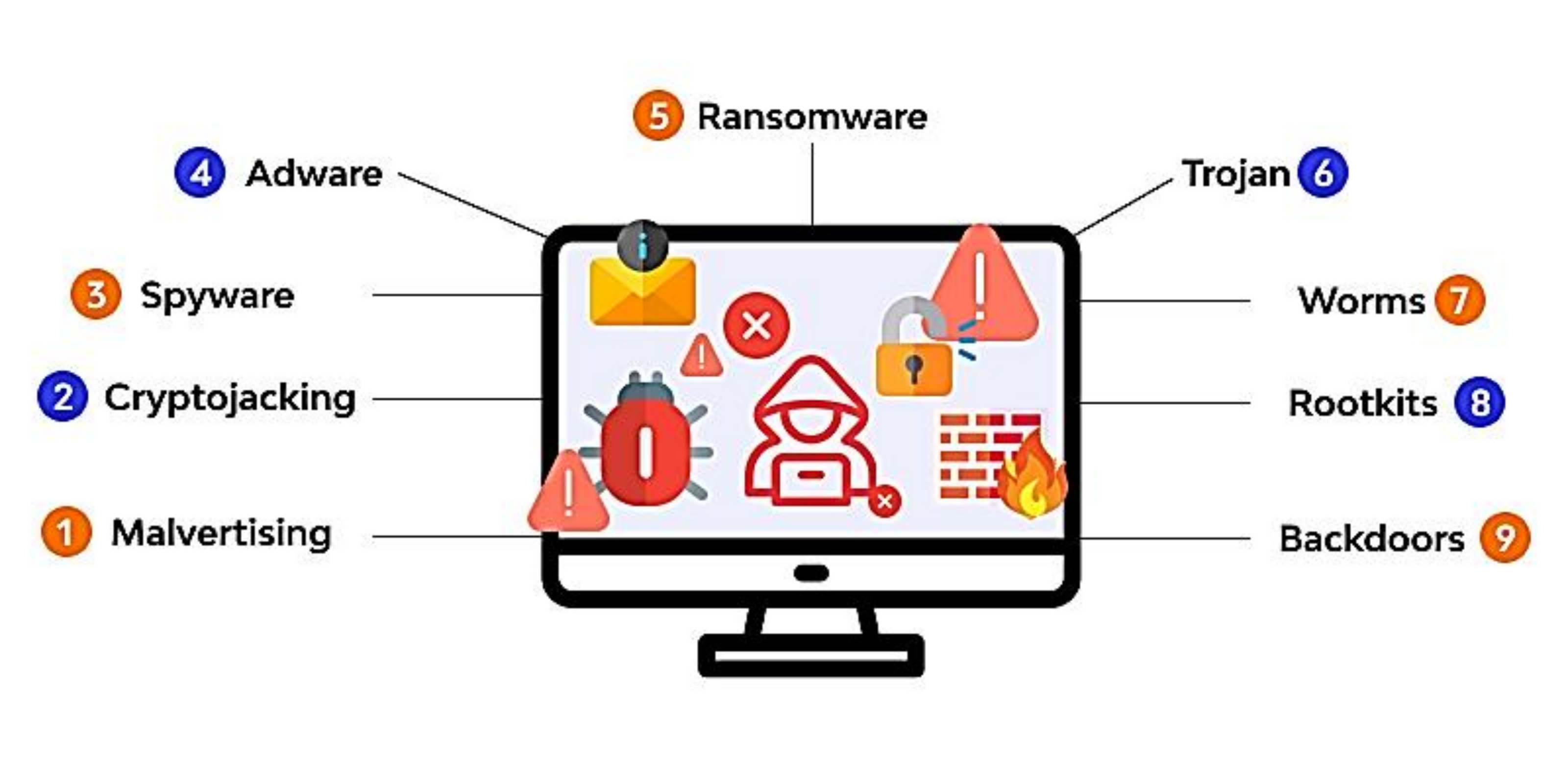
Gender

○ Female ○ Male ○ Custom

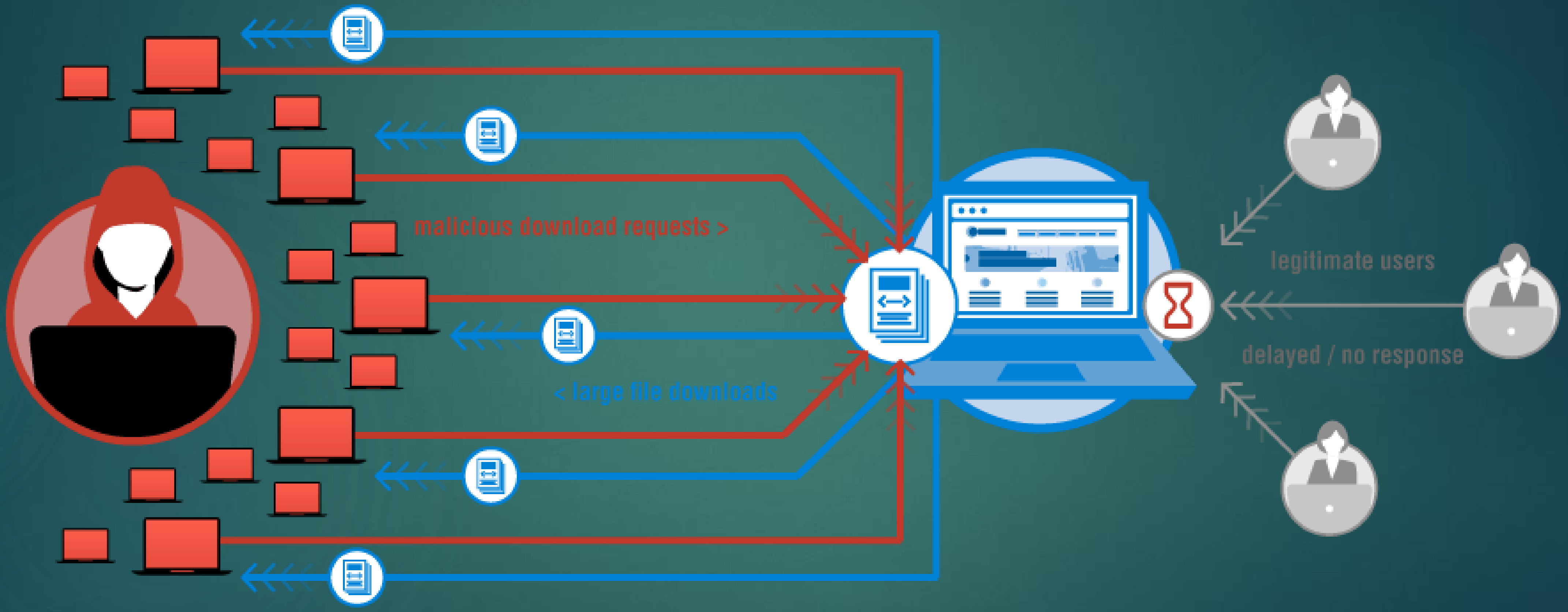
By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.

Sign Up

2. Malware


5 Ransomware
4 Adware
Trojan 6
3 Spyware
Worms 7
2 Cryptojacking
Rootkits 8
1 Malvertising
Backdoors 9

3. Denial of Service (DoS\DDoS)



4. Brute force

5. Social Engineering

Some Common Attacks

Question and Answer

Ask Your Question

Career
Where should I start
Facebook hacking
How hackers hack fb now a days?
Wifi hacking
Ransomware

Don’t ask
ভাইয়া আইডি হ্যাক করে দাও

Thank you