greatlearning
Power Ahead

Introduction to Ethical Hacking

What is Hacking?

What is Hacking?

Ethical Hacking is the protection of inter-connected systems, including hardware, software and data, from cyber attacks.

Black Hat Hacker

Grey Hat Hacker

White Hat Hacker

Computer Security Threats

- Computer Virus
- Computer Worm
- Scareware
- Key logger
- Adware
- Malware
- Backdoor
- Trojan
- Ransomware
- Spyware

Goals of ethical Hacking

- Protect the privacy of an Organization
- Transparently report all the identified bugs/weaknesses/vulnerabilities to the organization.
- Inform the vendors about the security measures and patches.

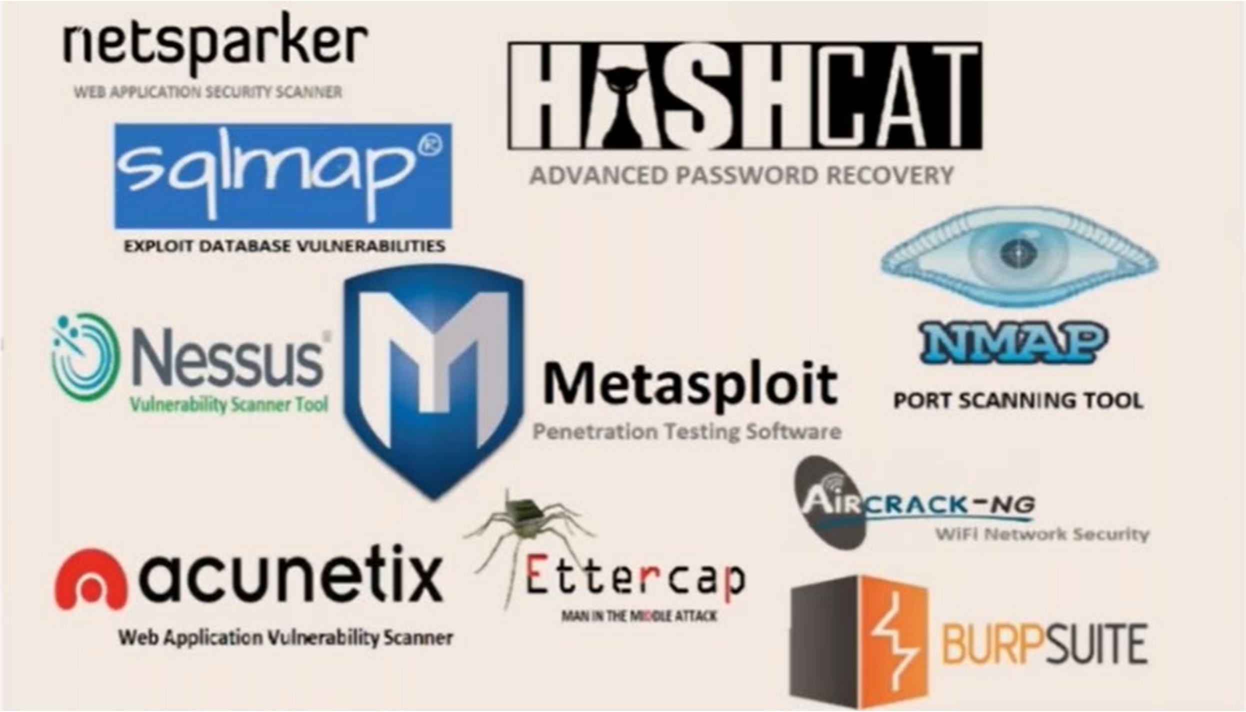
Skills Required by Ethical Hackers

Operating Systems

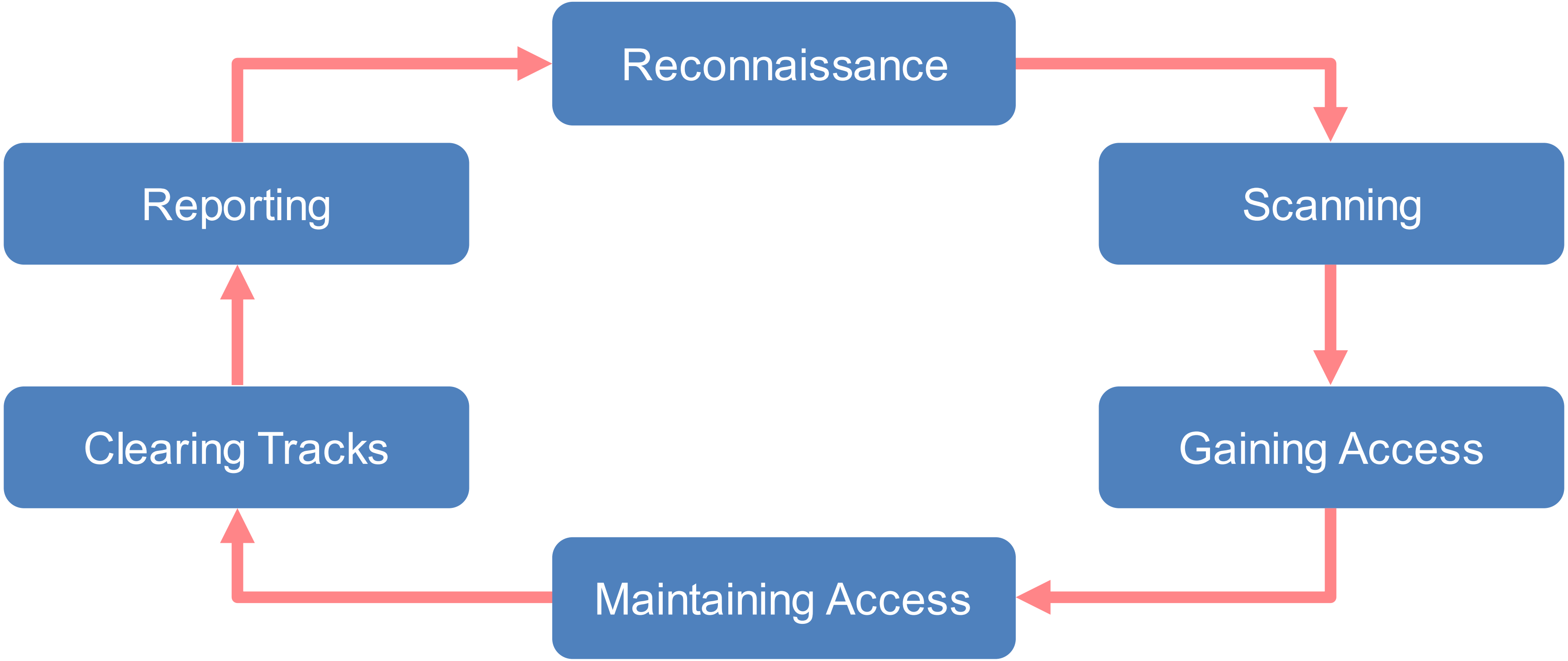
Networking

Programming Languages

Tools Used by Ethical Hackers


netsparker
WEB APPLICATION SECURITY SCANNER
HASHCAT
ADVANCED PASSWORD RECOVERY
sqlmap®
EXPLOIT DATABASE VULNERABILITIES
NMAP
PORT SCANNING TOOL
Nessus®
Vulnerability Scanner Tool
Metasploit
Penetration Testing Software
AIRCRACK-NG
WiFi Network Security
acunetix
Web Application Vulnerability Scanner
Ettercap
MAN IN THE MIDDLE ATTACK
BURPSUITE

Process of Ethical Hacking



Reconnaissance

This is the first step of hacking. It is also called as Foot printing and information gathering phase. This is the preparatory phase where we collect as much as information as possible about these the target. We usually collect information about three groups:

- Network
- Host
- People Involved

Scanning

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, live systems, various services running on the host.

Vulnerability Scanning: Checking the target for the weakness or vulnerabilities which can be exploited. Usually done with the help of automated tools.

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information. This map may serve as a valuable piece of information throughout the hacking process.

Clearing Tracks

No thief wants to get caught. An intelligent hacker always clears all the evidence so that in later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of logs, modifying registry values and uninstalling all the applications he used and deleting all folders he created.

Demonstration

Ethical Hacking Across Domains

At it’s core, Ethical Hacking occupies a prominent role in various verticals such as:

- Web Application Environment
- Mobile Applications
- And many more…

Web Application Domain

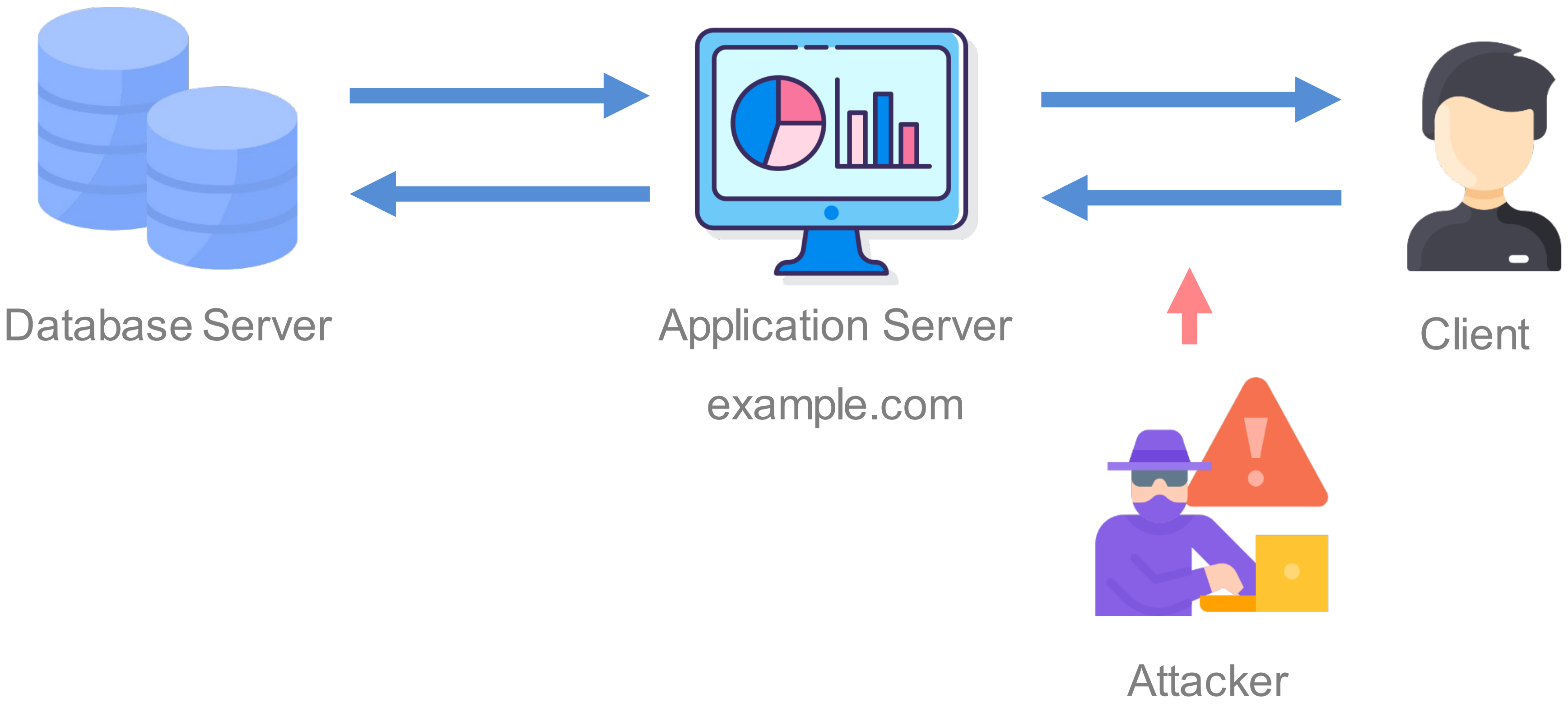
Two Major Categories:

- Client side vulnerabilities
- Server side vulnerabilities

All attacks can be categorized intro 3 major attacks:

- Parameter Tampering
- Unvalidated inputs
- Directory Traversal Attacks

Web Application Domain



Database Server

Application Server

example.com

Client

Attacker

Web Application Domain

login Name: <script>alert("You are hacked")</script> **Login Password:**

login Name: <iframe src="....org"></iframe>

Login Password:

login Name: 'Union select * from users'

Login Password:

Common Web Application attacks

- Injection Flaws eg. SQL injection, HTML injection, etc.
- Cross site Scripting eg. Reflected, Stored, etc.
- Web Services Attacks eg. DNS Cache Poising, File uploads etc.

Web Application Domain

login: <script>alert(document.cookie)</script>

password:

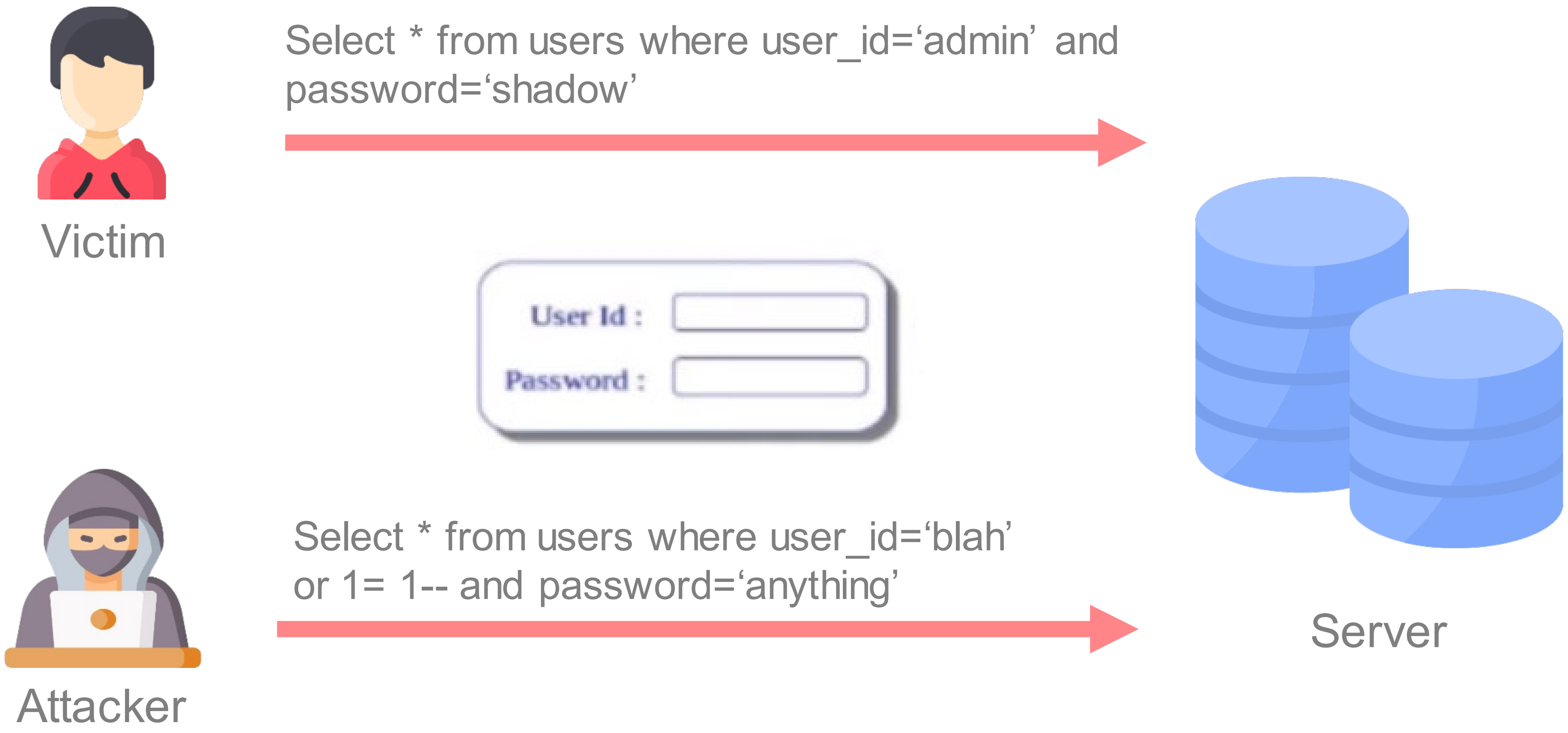
subscribe:

email: <script>code to mail him user information</script>

Hacking Methodology

- Web Footprinting – Gathering Information
- Vulnerability Scanners – w3af, Acunetix
- Identify Entry Points and Attack surface

Example : SQL injections



Select * from users where user_id=‘admin’ and password=‘shadow’

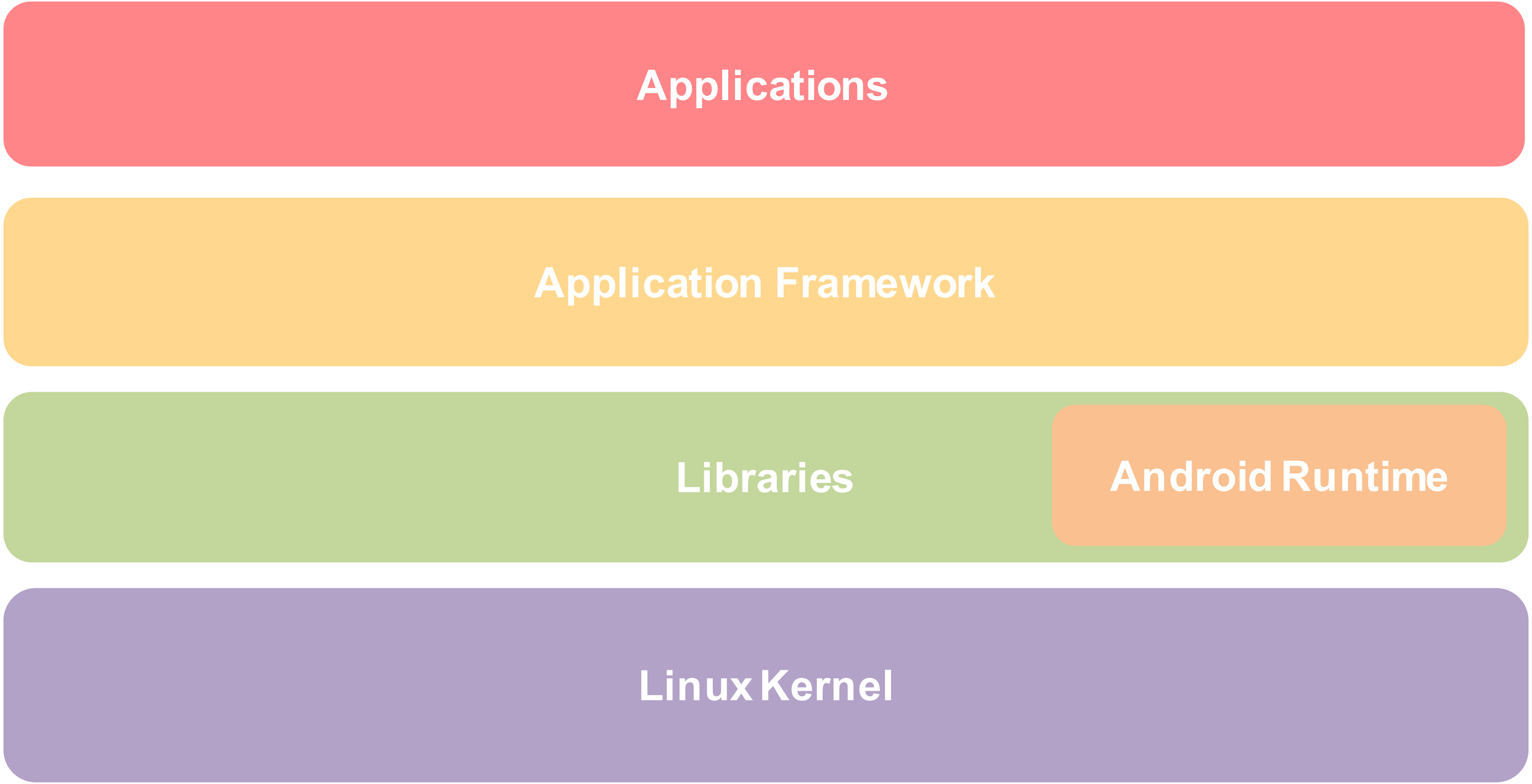
Select * from users where user_id=‘blah’ or 1= 1-- and password=‘anything’

Mobile Domain

The Mobile Device has become an inseparable part of life today. The attackers are easily able to compromise the mobile network because of various vulnerabilities, the majority of the attacks are because of the untrusted apps. The main operating systems used are:

- Android
- IOS
- Windows
- Blackberry

Example: Android



Applications

Application Framework

Libraries

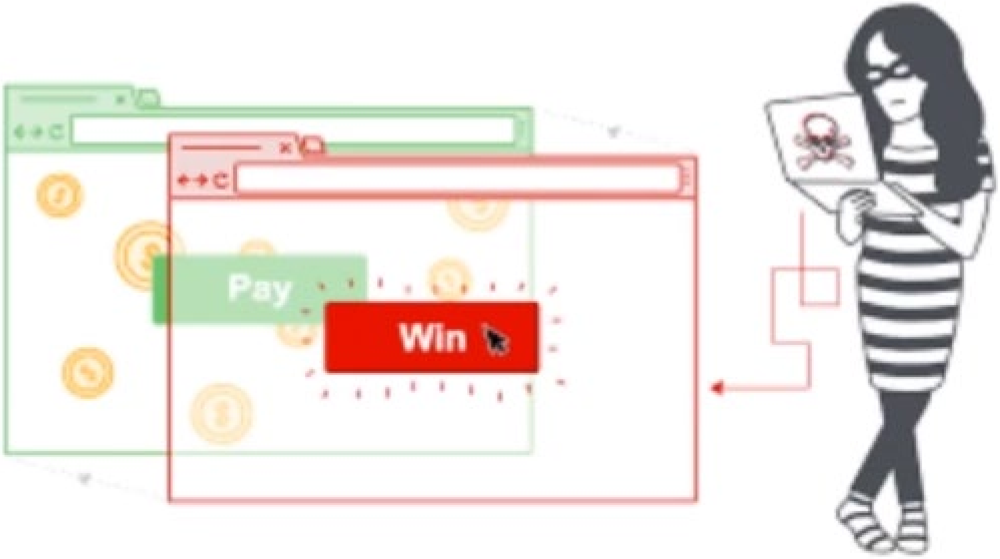
Android Runtime

Linux Kernel

Types of Android Attacks

- Untrusted APKs
- SMS
- Email
- Spying
- App sandboxing
- Rooting

Example: Tap Jacking



Network Domain

A network is an attempt to gain unauthorised access to an organisation’s network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:

- Passive: Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to data, leaving it intact.

- Active: Attackers not only gain unauthorised access but also modify data , either deleting, encrypting or otherwise harming it.

Types of Network Attacks

Endpoint attacks – gaining unauthorised access to user devices, servers or other endpoints, typically compromising them by infecting them with malware.

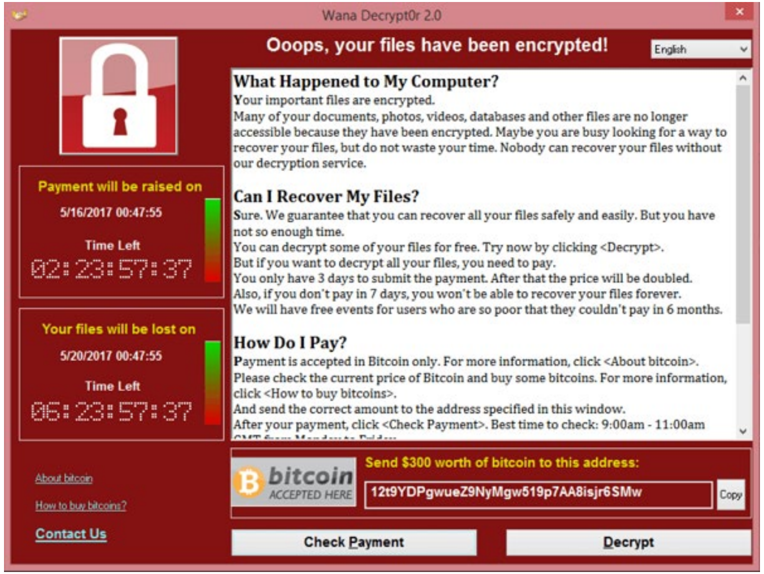
Malware attacks – infecting IT resources with malware, allowing attackers to compromise systems, steal data and do damage. These also include ransomware attacks.

Vulnerabilities, exploits and attacks – exploiting vulnerabilities in software used in the organization, to gain unauthorised access, compromise or sabotage systems.

Advanced persistent threats – These are complex multi-layered threats, which include network attacks but also other attack types.

Ransomware

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cyrptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

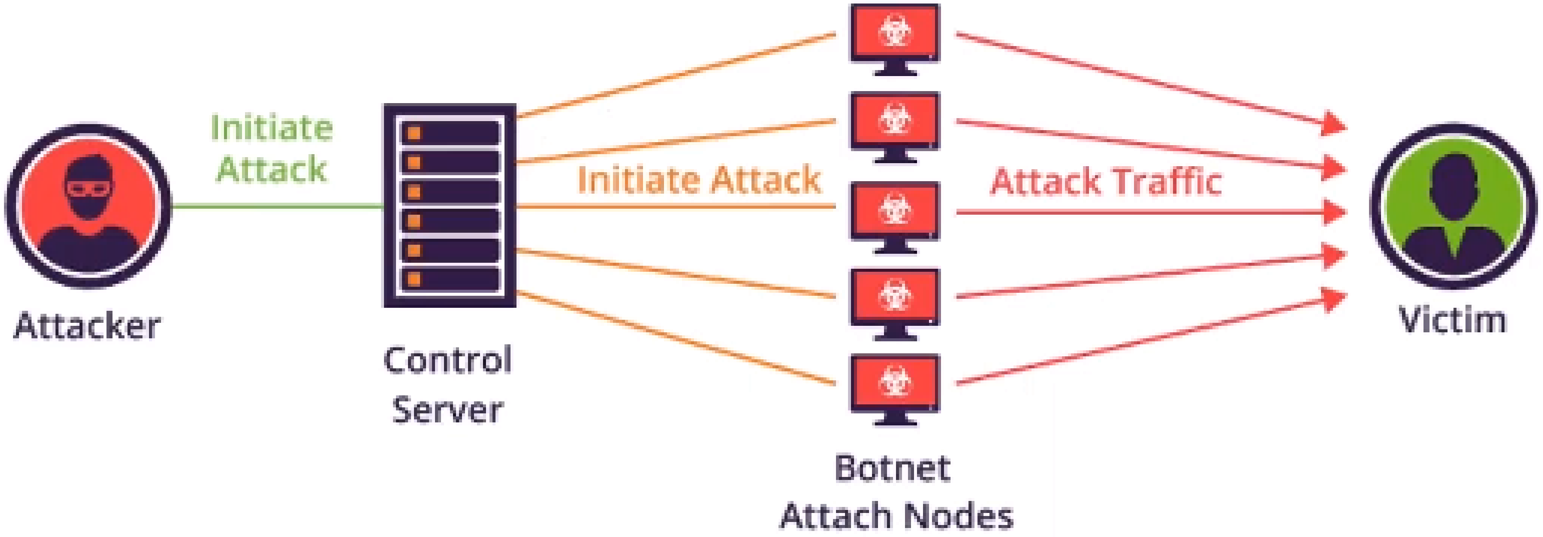
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Example : DDOS attack



Other Domains

- Cloud Computing
- IOT
- Block chain
- Edge Computing

Demonstration – SQL injection

THANK
YOU