ESERCITAZIONE S6 L4

Prima di cominciare l'esercizio si è preferito installare i due pacchetti necessari. Modificando la rete di Kali, da interna a Bridge e modificando il file di configurazione presente in */etc/network/interfaces*.

Una volta installati i pacchetti attraverso i due comandi:

sudo apt install seclists

sudo apt install vsftpd

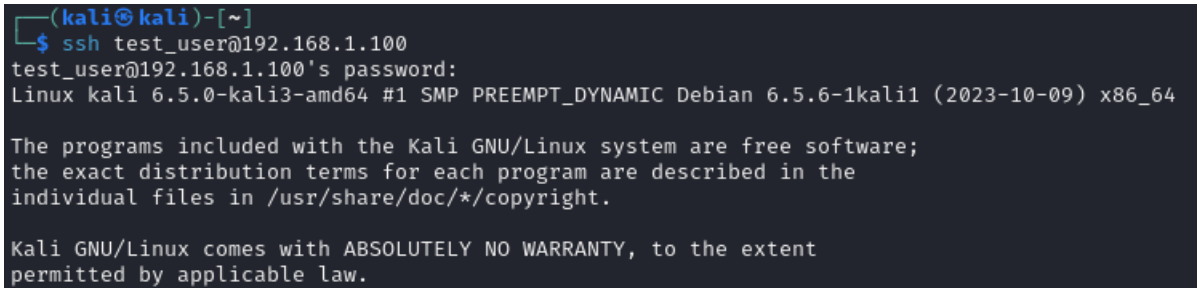
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev libtexluajit2 lua-lpeg nss
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 524 not upgraded.
Need to get 464 MB of archives.
After this operation, 1,868 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 1min 42s (4,533 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 410566 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㉿kali)-[~]
└─$ sudo apt 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 libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev libtexluajit2 lua-lpeg nss
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 524 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 1s (233 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 416194 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) ...
```

Possiamo ritornare alla configurazione precedente della macchina.

1. **SSH DA KALI A KALI**

Viene richiesto di creare un nuovo utente con il comando *sudo adduser test_user* configurato con una password che sarà *testpass*.

Una volta creato il nuovo utente andiamo ad avviare il servizio ssh con il comando *sudo service ssh start* e proviamo la connessione ssh con il comando *ssh test_user@192.168.1.100*. Se il comando è corretto otterremo come risposta:

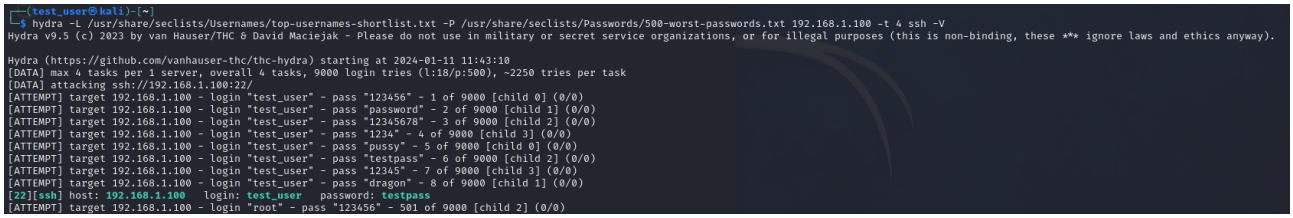


Ora proviamo ad avviare una sessione di cracking con Hydra.

Nelle liste scaricate precedentemente non sono presenti nei file l'username e la password impostati per l'accesso del nuovo utente, quindi li andiamo a inserire, rendendoli prima modificabili con *sudo chmod 777 top-usernames-shortlist.txt* e sudo chmod 777 *500-worst-passwords.txt,* e poi inserendo test_user nel file usernames che andremo ad utilizzare e testpass nel file password.

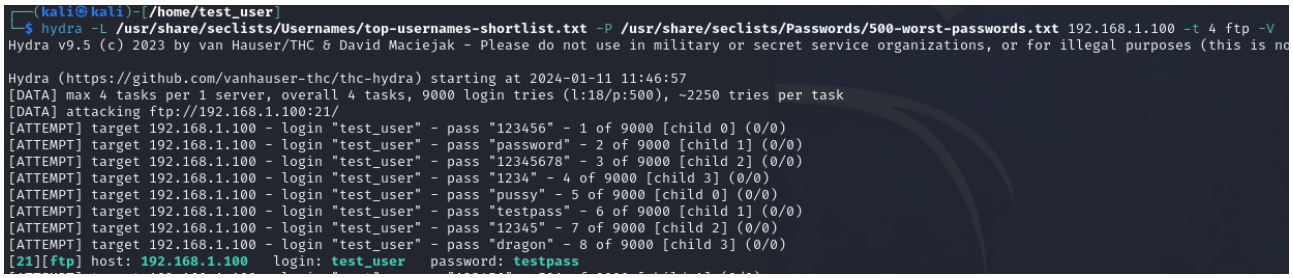
Fatto questo abbiamo tutto pronto per lanciare il comando di cracking:

Dopo l'attesa necessaria per effettuare tutti i tentativi di accesso, otterremo l'username e la password corretti.



2. FTP DA KALI A KALI

Lo stesso tipo di attacco lo possiamo effettuare anche con altri servizi, in questo caso procederemo con *FTP*, utilizzando lo stesso comando precedente, apportando solo una piccola modifica

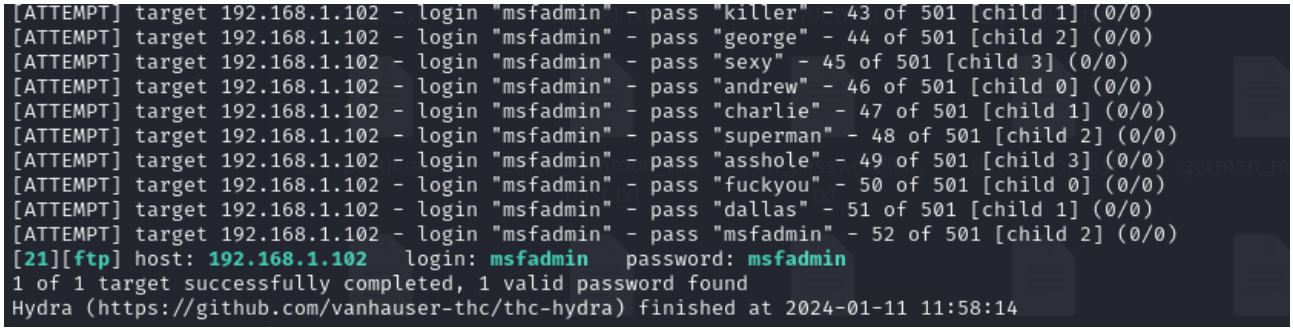


Anche in questo caso l'attacco ha avuto un esito positivo, in quanto siamo riusciti ad ottenere l'username e la password necessari ad accedere.

3. BONUS

In questo caso si procede ad un attacco su Meta (192.168.1.102) utilizzando sempre il comando di Hydra, ma questa volta sapendo che l'username per accedere è *msfadmin*.

In questo modo si provvederà ad un attacco addizionale con username fisso e le password presenti nella lista.



Anche questa volta siamo riusciti ad ottenere la password di accesso all'username msfadmin.