Esercizio S6L4 di Ciaschini Giorgio del 29/02/2024

Oggi la consegna prevedeva l'utilizzo del tool Hydra per craccare un servizio. In modo guidato abbiamo craccato il servizio ssh dopo averlo configurato.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Documents/username_shortlist.txt -P /home/kali/Documents/password_shortlist.txt 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 org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:39:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sess
ion found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 468 login tries (l:18/p:26), ~117 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1   login: test_user   password: testpass
[STATUS] 61.00 tries/min, 61 tries in 00:01h, 407 to do in 00:07h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Successivamente in modo autonomo siamo andati a craccare sempre su macchina virtuale il servizio ftp. L'abbiamo prima aggiornato e poi scaricato con il seguente comando.

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/vsftpd.conf
```

Poi abbiamo fatto una rapida configurazione lasciando le impostazioni di default.

```
File  Actions  Edit  View  Help
  GNU nano 7.2
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you wil
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
```

In fine siamo andati ad utilizzare il tool “Hydra” per attaccare il servizio della macchina. Come si può notare è andato a buon fine.