

# Máquina Access HackThebox Easy

Máquina de hoy

The screenshot shows the HackThebox interface for the 'Access' machine. At the top, there's a header with the machine name 'Access', its category 'Windows · Easy', and statistics: 0 Points, 4.83411 Reviews (5 stars), and a User Rated Difficulty bar. Below the header is a navigation bar with tabs: 'Play Machine' (active), 'Machine Info', 'Walkthroughs', 'Reviews', 'Activity', and 'Changelog'. To the right of the tabs are a heart icon and a three-dot menu. Below the navigation bar, there are two radio buttons for 'Adventure Mode' (selected) and 'Guided Mode'. To the right of these are two buttons: 'Official Writeup' and 'Video Walkthrough'. Below this is a section for the current session, showing 'EU VIP 15' and '1 player'. The 'Target IP Address' is '10.10.10.98', which has been copied. To the right of the IP address are a stop button, a refresh button, and a timer showing '23:56:53'. Below this are two sections for submitting flags: 'Submit User Flag' and 'Submit Root Flag'. Each section has a text input field with a placeholder '32 hex characters' and a 'Submit' button.

Ping inicial de reconocimiento:

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ ping 10.10.10.98
PING 10.10.10.98 (10.10.10.98) 56(84) bytes of data.
64 bytes from 10.10.10.98: icmp_seq=1 ttl=127 time=40.0 ms
64 bytes from 10.10.10.98: icmp_seq=2 ttl=127 time=45.6 ms
^C
--- 10.10.10.98 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 40.029/42.801/45.573/2.772 ms

(jouker@joukerm)-[~/Escritorio/temporal]
$ █
```

Nmap identificativo de puertos, que raro se sale de lo habitual un telnet aparte de un FTP y una página web:

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.10.98 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 21:44 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating SYN Stealth Scan at 21:44
Scanning 10.10.10.98 [65535 ports]
Discovered open port 80/tcp on 10.10.10.98
Discovered open port 23/tcp on 10.10.10.98
Discovered open port 21/tcp on 10.10.10.98
```

```
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_ SYST: Windows_NT
23/tcp    open  telnet?  syn-ack ttl 127
80/tcp    open  http     syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
| http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Anonymous permitido para acceder a la máquina, seguidamente de un protocolo telnet.

```
Archivo Acciones Editar Vista Ayuda
(jouker@joukerm)-[~]
$ whatweb 10.10.10.98
http://10.10.10.98 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.98], Microsoft-IIS[7.5], Title[MegaCorp], X-Powered-By[ASP.NET]
(jouker@joukerm)-[~]
$
```

Esto es lo que hay en la página web: posible nombre de usuario friki, lo tendré en cuenta.

10.10.10.98

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#) [HackTricks - HackTricks](#)

## LON-MC6



Con la imagen encontrada no localizo nada que hacer con exiftool:

```
FW FW 1 jouker jouker 00 00 27 17 55 user$ cat  
  
(jouker@joukerm)-[~/Escritorio/temporal]  
$ exiftool Untitled.jpeg  
ExifTool Version Number      : 13.10  
File Name                    : Untitled.jpeg  
Directory                    : .  
File Size                    : 89 kB  
File Modification Date/Time   : 2025:04:27 21:46:29+02:00  
File Access Date/Time        : 2025:04:27 21:46:29+02:00  
File Inode Change Date/Time   : 2025:04:27 21:46:29+02:00  
File Permissions              : -rw-rw-r--  
File Type                    : JPEG  
File Type Extension          : jpg  
MIME Type                    : image/jpeg  
JFIF Version                 : 1.01  
Resolution Unit              : inches  
X Resolution                  : 96  
Y Resolution                  : 96  
Image Width                  : 640  
Image Height                 : 480  
Encoding Process              : Baseline DCT, Huffman coding  
Bits Per Sample              : 8  
Color Components              : 3  
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)  
Image Size                   : 640x480  
Megapixels                   : 0.307
```

Dejando un poco la web de lado busco en el FTP compartido y con anonymous saco estos 2 archivos:

```
08-23-18 09:16PM 5652480 backup.mdb
226 Transfer complete.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
150 Opening ASCII mode data connection.
17% |*****
tp: Reading from network: Llamada al sistema interrumpida
0% |
550 The specified network name is no longer available.
WARNING! 470 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
ftp> cd ..
250 CWD command successful.
ftp> cd Engineer
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
08-24-18 01:16AM 10870 Access Control.zip
226 Transfer complete.
ftp> get 'Access Control.zip'
local: 'Access Control.zip' remote: 'Access Control.zip'
```

Haciendo strings al archivo backup veo un potencial password. Lo hago con strigs porque no es legible de otra forma ni de lejos.

```
9.2+
@CXR
@)AD
@]X$S
@P      u
@!j+
LVAL
administrator;
Administrator<
tte*N
45555555555555Q
NXT0
depart
(u7b
user
close
restart
file
pppermission
0QfJim
okQi
okQi
okQi
okQi
okQi
backup_admin
admin
engineer
access4u@security
admin
admin
admin
admin
tXT>
```

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ 7z x 'Access Control.zip'

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
64-bit locale=es_ES.UTF-8 Threads:3 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870

Would you like to replace the existing file:
  Path:      ./Access Control.pst
  Size:      0 bytes
  Modified:  2018-08-24 02:13:52
with the file from archive:
  Path:      Access Control.pst
  Size:      271360 bytes (265 KiB)
  Modified:  2018-08-24 02:13:52
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y

Enter password (will not be echoed): 
Everything is Ok

Size:          271360
Compressed:    10870

```

Hemos obtenido el password correcto esta vez, he tenido suerte a la primera, a ver cuanto me dura la suerte

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ ls -l
total 117468
-rw-rw-r-- 1 jouker jouker    271360 ago 24  2018 'Access Control.pst'
-rw-rw-r-- 1 jouker jouker    10870 ago 24  2018 'Access Control.zip'
-rw-rw-r-- 1 jouker jouker   970918 abr 27 21:49 backup.mdb
-rw-rw-r-- 1 jouker jouker 118489056 abr 27 18:32 firefox.exe_250427_214412.dmp
-rw-rw-r-- 1 jouker jouker      31 abr 27 17:45 hash
-rw-rw-r-- 1 jouker jouker      18 abr 27 22:08 passwords.txt
-rw-rw-r-- 1 jouker jouker   424856 nov  3  2022 procdump64.exe
-rw-r--r-- 1 root  root       1130 abr 27 21:47 scan.txt
-rw-rw-r-- 1 jouker jouker    88712 abr 27 21:46 Untitled.jpeg
-rw-rw-r-- 1 jouker jouker      86 abr 27 17:59 users.txt

(jouker@joukerm)-[~/Escritorio/temporal]
$

```

Dentro del pst intento realizar la comanda strings pero me lleva para mi casa ya que es dificil de ver

```
AYAJApA:A
ACA~A
A~AAA
AYAJA
AYApA
AJA:ASA
AxA:A,A
AYAJApA
AJAYA~A
AYAJA
AYApA
ApA:ASA
AJAYA~A
AYAJA
AYApA
AwApA:ASA
AJAYA~AVAAA
A9AYA
AJA:ASA
ASAJA:ApA
A:A9AJAxA
A9AYA
AJA:ASA
A9ASA
AxA~AYAJApA
A9ApA
A9AYA
AJA:ASA
```

Pero bueno hay literalmente una comanda para leer pst que se llama readpst, así que ejecutamos dicha comanda y se nos crea un archivo access control.mbox, al leerlo podemos ver información de un



correo.

```
(jouker@joukerm) [~/Escritorio/temporal]
$ readpst archiv.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
    "Access Control" - 2 items done, 0 items skipped.

(jouker@joukerm) [~/Escritorio/temporal]
$ ls -l
total 117472
-rw-rw-r-- 1 jouker jouker    3112 abr 27 22:12 'Access Control.mbox'
-rw-rw-r-- 1 jouker jouker   10870 ago 24 2018 'Access Control.zip'
-rw-rw-r-- 1 jouker jouker  271360 ago 24 2018 archiv.pst
-rw-rw-r-- 1 jouker jouker   970918 abr 27 21:49 backup.mdb
-rw-rw-r-- 1 jouker jouker 118489056 abr 27 18:32 firefox.exe_250427_214412.dmp
-rw-rw-r-- 1 jouker jouker     31 abr 27 17:45 hash
-rw-rw-r-- 1 jouker jouker     18 abr 27 22:08 passwords.txt
-rw-rw-r-- 1 jouker jouker  424856 nov  3 2022 procdump64.exe
-rw-r--r-- 1 root  root      1130 abr 27 21:47 scan.txt
-rw-rw-r-- 1 jouker jouker   88712 abr 27 21:46 Untitled.jpeg
-rw-rw-r-- 1 jouker jouker     86 abr 27 17:59 users.txt

(jouker@joukerm) [~/Escritorio/temporal]
```

Un usuario posible y un password.

```
(jouker@joukerm) [~/Escritorio/temporal]
$ cat 'Access Control.mbox'
From: "john@megacorp.com" Fri Aug 24 01:44:07 2018
Status: RO
From: john@megacorp.com <john@megacorp.com>
Subject: MegaCorp Access Control System "security" account
To: 'security@accesscontrolsystems.com'
Date: Thu, 23 Aug 2018 23:44:07 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="--boundary-LibPST-iamunique-1367473067_--"

---boundary-LibPST-iamunique-1367473067_--
Content-Type: multipart/alternative;
    boundary="alt---boundary-LibPST-iamunique-1367473067_--"

--alt---boundary-LibPST-iamunique-1367473067_--
Content-Type: text/plain; charset="utf-8"

Hi there,

The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.

Regards,
John

--alt---boundary-LibPST-iamunique-1367473067_--
Content-Type: text/html; charset="us-ascii"
```

Establecemos una consola mediante telnet con el user security y el password que hemos conseguido antes, de momento hasta aquí fácil.

(jouker@joukerm)-[~/Escritorio/temporal]

\$ telnet 10.10.10.98 23

Trying 10.10.10.98...

Connected to 10.10.10.98.

Escape character is '^]'.

Welcome to Microsoft Telnet Service

login: security

password:

\*=====

Microsoft Telnet Server.

\*=====

C:\Users\security>whoami

access\security

C:\Users\security>cd Desktop

C:\Users\security\Desktop>dir

Volume in drive C has no label.

Volume Serial Number is 8164-DB5F

Directory of C:\Users\security\Desktop

08/28/2018	07:51 AM	<DIR>	.
08/28/2018	07:51 AM	<DIR>	..
04/27/2025	08:40 PM		34 user.txt
	1 File(s)		34 bytes
	2 Dir(s)	3,347,156,992 bytes free	

C:\Users\security\Desktop>type user.txt

8bfc6d2aad7ee9de21836d9fab58531f

C:\Users\security\Desktop>

Flag conseguida para el user:

Access

Windows · Easy

0 Points

★★★★★  
4,83411 Reviews

User Rated Difficulty

Play Machine

Machine Info

Walkthroughs

Reviews

Activity

Changelog

Adventure Mode

Guided Mode

Official Writeup

Video Walkthrough

EU VIP 15

1 player

Target IP Address

10.10.10.98

Submit User Flag

User flag owned

[2] Very Easy

Submit Root Flag

32 hex characters

Submit

Released on 29 Sep 2018

Created by egre55

Activar  
Ve a Con