

Introducción al Hacking Ético

Lic. Bruno Zappellini Emiliano De Marco Andrada
Germán Bianchini Lucas Krmpotic Maximiliano Aguila

2019



Conceptos y Terminología

Unidad 1: Conceptos de Seguridad Informática

- Terminología:



Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información



Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad
 - Confidencialidad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad
 - Confidencialidad
 - Integridad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad
 - Confidencialidad
 - Integridad
 - Disponibilidad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad
 - Confidencialidad
 - Integridad
 - Disponibilidad
 - Autenticidad

Unidad 1: Conceptos de Seguridad Informática

- Terminología:
 - Información
 - Seguridad
 - Privacidad
 - Confidencialidad
 - Integridad
 - Disponibilidad
 - Autenticidad
 - No repudio

Definiciones

¿Qué se debe asegurar?

- Los activos de la organización.

Definiciones

¿Qué se debe asegurar?

- Los activos de la organización.

¿Qué lugar ocupa la información?

- La información constituye un activo muy importante en la organización ya que tiene un rol fundamental a la hora de cumplir sus objetivos.

Seguridad de la Información

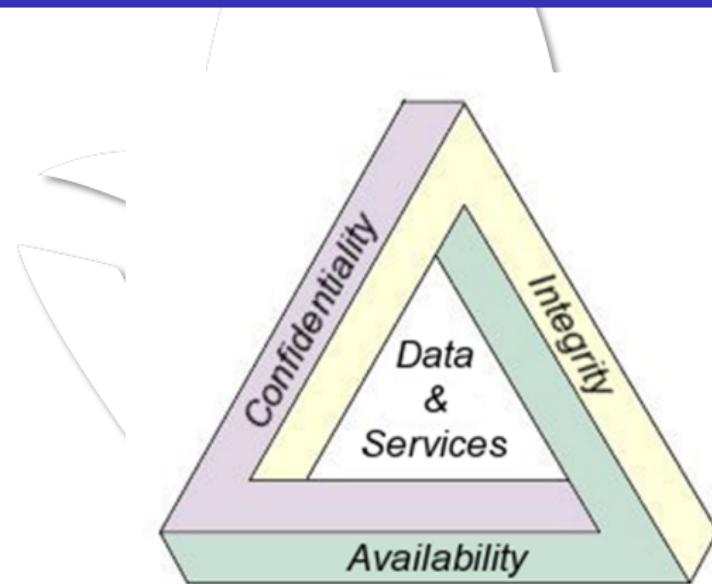


Figura 1: Triangulo de la seguridad

Seguridad de la Información

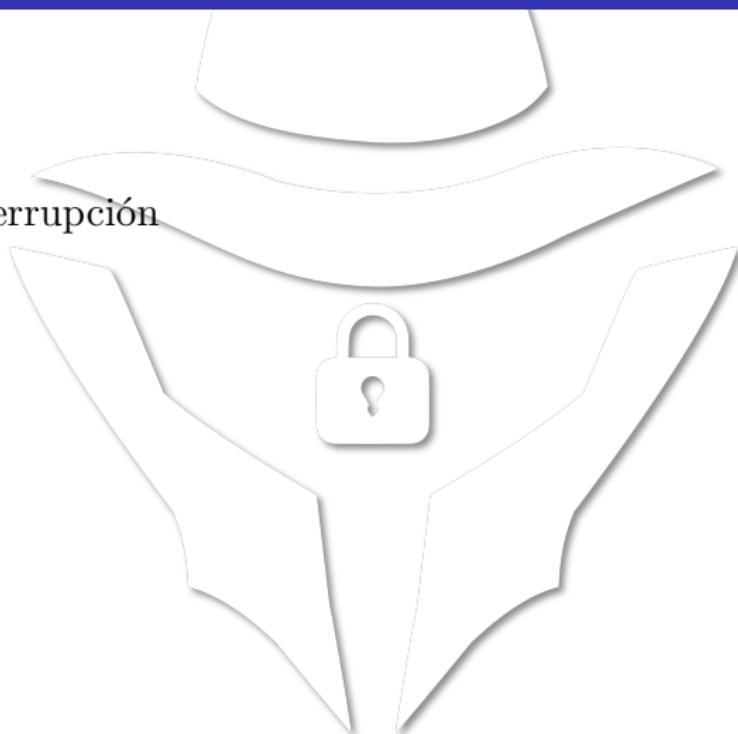
- ¿Qué significa garantizar la seguridad de la información?
 - Significa proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizadas.
- ¿Qué es garantizar la privacidad de la información?
 - Significa no revelar la información o revelarla selectivamente de manera de protegerla de cualquier intromisión.

Privacidad - Desafío

- ¿Tenés un smartphone con Android?
- ¿Te acordás donde estuviste hace un mes?
- Verifícalo en <https://maps.google.com/locationhistory>
- Otro ejemplo: ¿Por qué me vigilan, si no soy nadie? |
Marta Peirano | TEDxMadrid

Ataques: Categorías

1 Interrupción

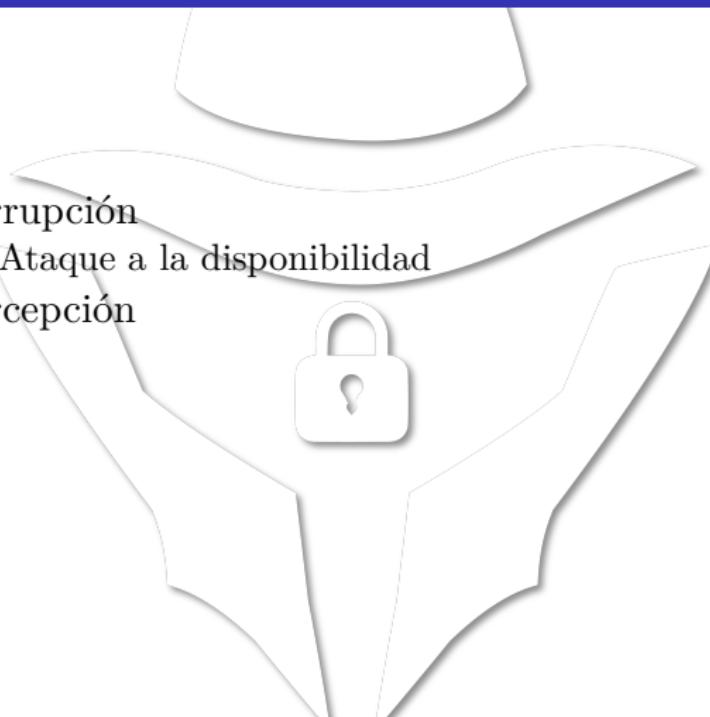


Ataques: Categorías

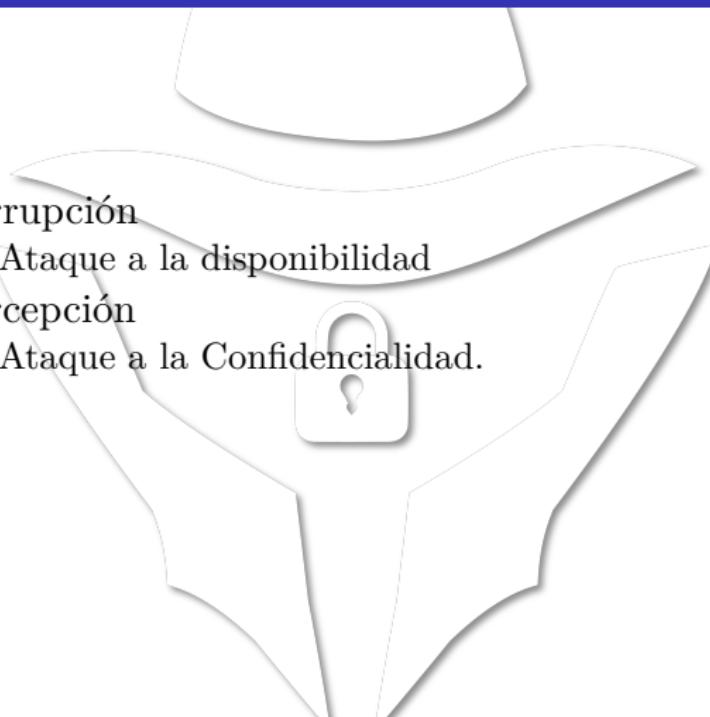
- 1 Interrupción
 - Ataque a la disponibilidad



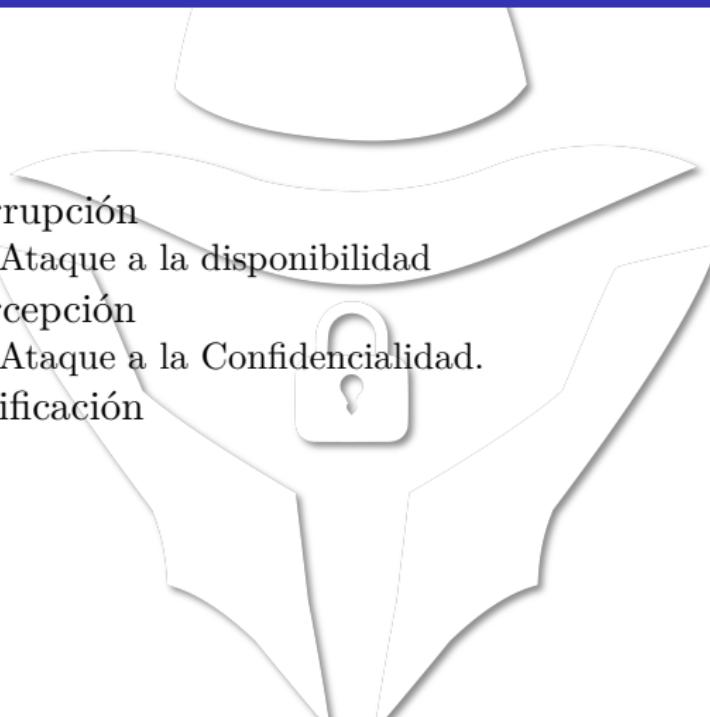
Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción

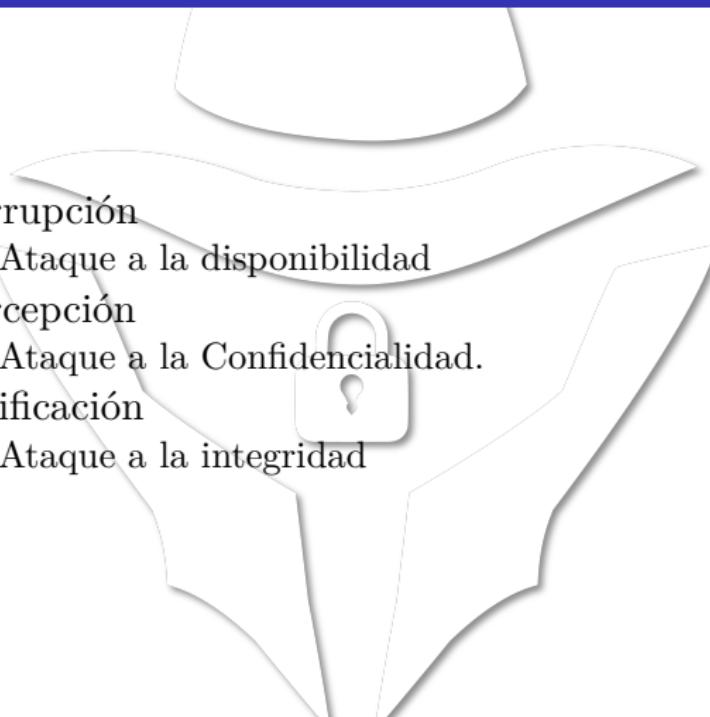
Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción
 - Ataque a la Confidencialidad.

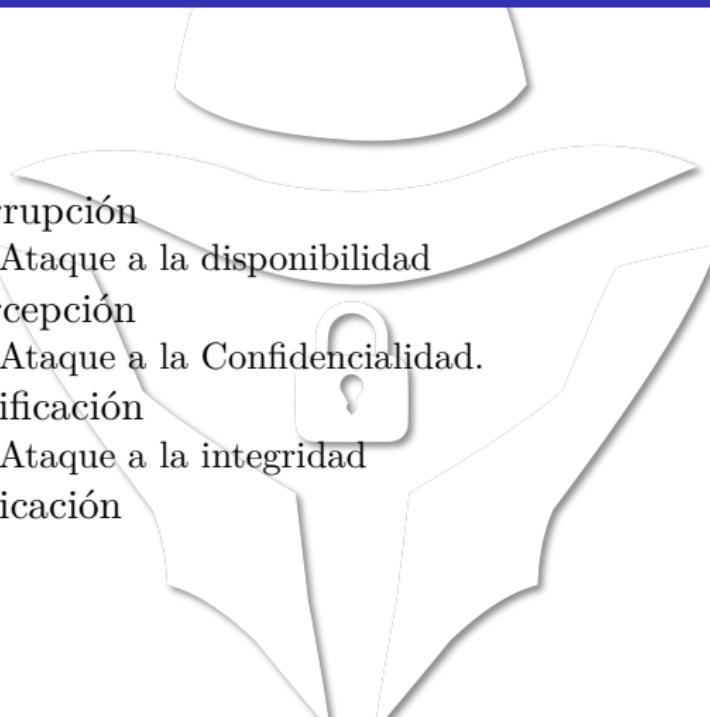
Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción
 - Ataque a la Confidencialidad.
 - 3 Modificación

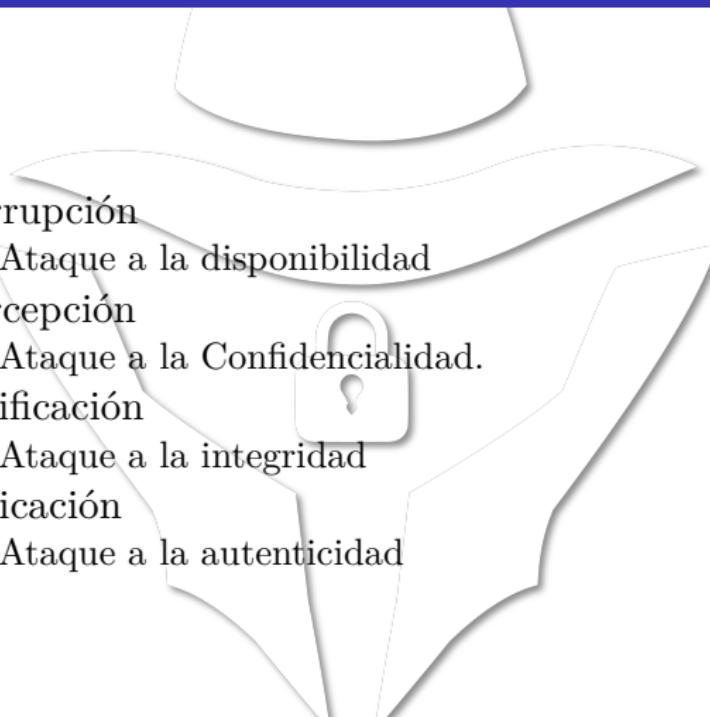
Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción
 - Ataque a la Confidencialidad.
 - 3 Modificación
 - Ataque a la integridad

Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción
 - Ataque a la Confidencialidad.
 - 3 Modificación
 - Ataque a la integridad
 - 4 Fabricación

Ataques: Categorías

- 
- 1 Interrupción
 - Ataque a la disponibilidad
 - 2 Intercepción
 - Ataque a la Confidencialidad.
 - 3 Modificación
 - Ataque a la integridad
 - 4 Fabricación
 - Ataque a la autenticidad

Flujo Normal de la Información



Vulnerabilidades y Amenazas

- Una vulnerabilidad es una debilidad de un activo.
- Una amenaza es la violación potencial de una activo.

Amenazas

Tipos de amenazas

- Naturales
 - Incendios
 - Terremotos
 - Inundaciones
- Humanas
 - Maliciosas
 - Internas
 - Externas
 - No maliciosas
 - Impericia

Amenazas - Conceptos Generales

Las amenazas atentan contra:

- La confidencialidad de la información
- La integridad de la información
- La disponibilidad de la información

Están son causadas por:

- Fallas humanas
- Ataques mal intencionados
- Catástrofes naturales

Amenazas - Conceptos Generales

La materialización de una amenaza puede causar:

- el acceso, robo, modificación o eliminación de información no autorizada
- la interrupción de un servicio o el procesamiento de un sistema
- daños físicos o robo del equipamiento y medios de almacenamiento de información

Amenazas sobre las personas

Ingeniería Social

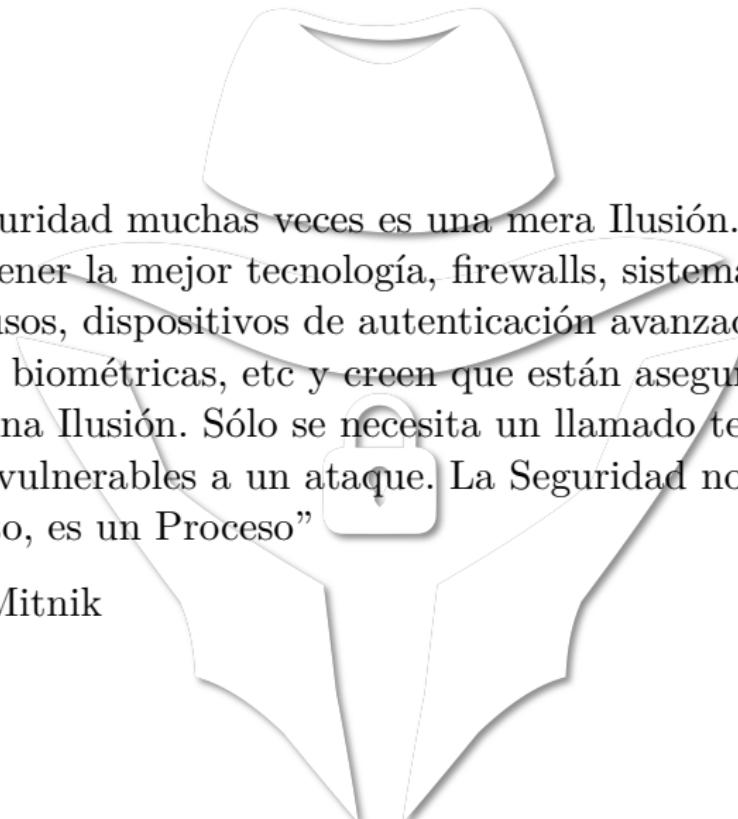
La ingeniería social es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial.

La principal defensa contra la ingeniería social es concientizarnos en el uso de políticas de seguridad

¿Por que funciona?

Según Kevin Mitnick, uno de los ingenieros sociales mas famosos de los últimos tiempos, la ingeniería social se basa en estos cuatro principios:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir “No”.
- A todos nos gusta que nos alaben.



“La Seguridad muchas veces es una mera Ilusión. Una compañía puede tener la mejor tecnología, firewalls, sistemas de detección de intrusos, dispositivos de autenticación avanzados como tarjetas biométricas, etc y creen que están asegurados 100%. Viven una Ilusión. Sólo se necesita un llamado telefónico y listo. Ya son vulnerables a un ataque. La Seguridad no es un producto, es un Proceso”

Kevin Mitnik

Amenazas sobre las personas

Phishing y Pharming

- El Phishing es una combinación de ingeniería social y elementos técnicos para engañar a un usuario y lograr que éste entregue involuntariamente información confidencial a usuarios malintencionados. La forma más común es mediante el envío de mails falsos, escritos como si hubieran sido enviados por la auténtica organización.
- El Pharming consiste en alterar la asociación de nombre (www.mibanco.com) a dirección real (IP) para dirigir a un usuario a una dirección que no es la verdadera. Puede ser desconcertante ya que el usuario escribe por si mismo la dirección de la página web.

Amenazas sobre las personas

SPAM

También llamado “Correo Basura”. Es uno de los principales medios para hacer llegar todo tipo de problemas a los usuarios del correo electrónico.

Se utiliza para:

- Publicidad no deseada
- Phishing (se vale de la ingeniería social)
- Transmisión de código malicioso (virus, etc)

Amenazas sobre las personas

HOAX

Son mensajes de correo electrónico engañosos que se distribuyen en cadena. Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que puede suceder si no se reenvía el mensaje o se hace lo que el mismo indica.

La motivación de un hoax es recolectar direcciones de correo y otros datos confidenciales

Amenazas en el control de acceso

Elementos del control de acceso:

- Identificación: es una secuencia de caracteres que identifica únicamente al usuario: nombre de usuario.
- Autenticación: es la verificación que realiza el sistema sobre la identificación. Se puede realizar a través de:
 - Algo que se conoce: clave de acceso
 - Algo que se posee: tokens / tarjeta
 - Algo que se es: huella digital, iris, retina, voz
- Autorización: son los permisos asociados al usuario autenticado

Ataques de contraseñas

Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente control de intentos fallidos de logueo. Este tipo de ataque puede ser realizado:

- Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el mismo.
- Por fuerza bruta: una herramienta generará combinaciones de letras, números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.

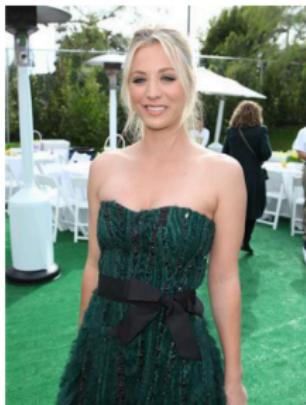


Figura 2: Famosos que sufrieron ataques de control de acceso

Más ejemplos de amenazas

Acceso no autorizado a información sensible, como puede ser:

- Información confidencial impresa.
- Información confidencial guardada en medios de almacenamiento removibles (CDs, DVDs, pendrives).
- Información confidencial almacenada en notebooks.

Más ejemplos de amenazas

- Trashing: Consiste en la búsqueda de información dentro de la basura. Esto puede representar una importante amenaza para aquellos usuarios que no destruyen información crítica o confidencial al descartarla.
- Pérdida de copias de resguardo: provocadas por daños físicos a causa de desastres naturales, por obsolescencia de los medios físicos que contienen la información, etc.

Código Malicioso (Malware)

Virus/Gusanos/Troyanos/Spyware/Keyloggers:

- Destruyen datos
- Consumen recursos del equipo
- Permiten acceso de extraños al equipo
- Roban información (números de cuentas, claves, información financiera)
- Roban nuestra identidad

Los antivirus/ antispyware nos protegen del malware, pero no nos cubren de todos los riesgos, es por ello que debemos tomar precauciones.

Malware - ¿Cómo llega a nuestro equipo?

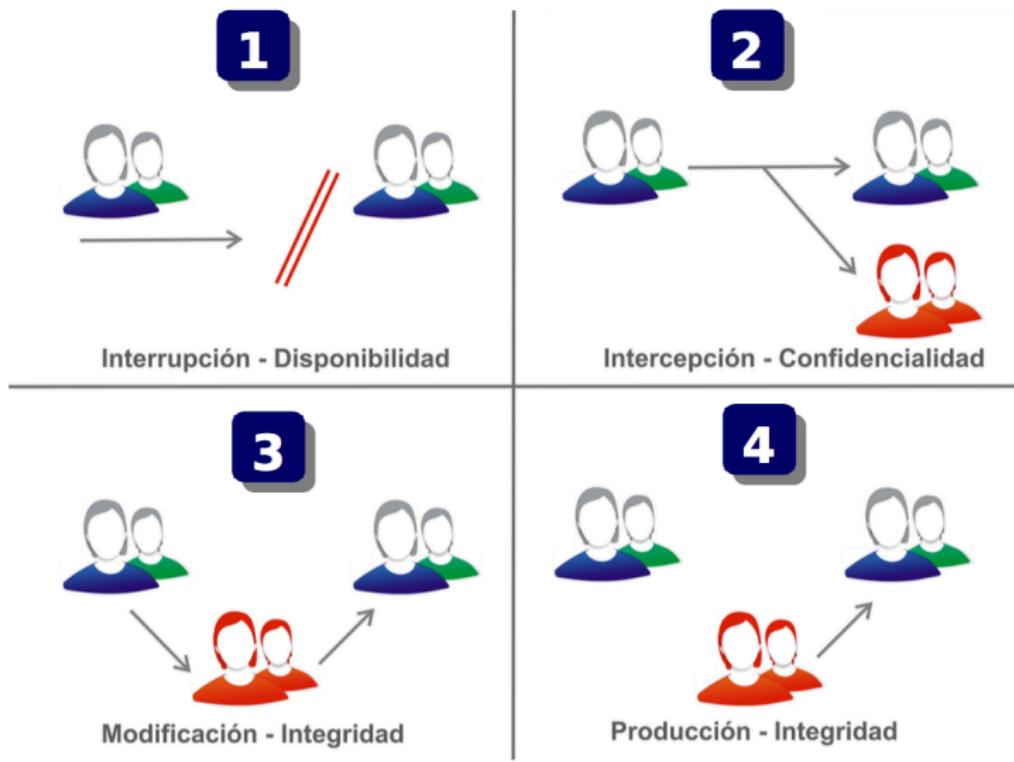
Sin nuestro consentimiento:

- Navegando por sitios de Internet que descargan su código malicioso en navegadores mal configurados y/o desactualizados.

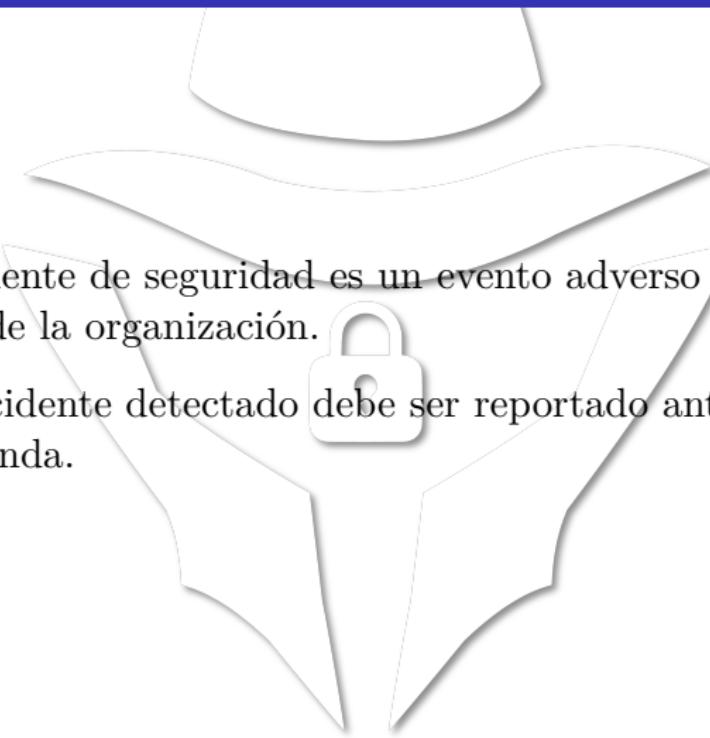
Con nuestro consentimiento:

- Instalando algún Freeware (programa gratuito). Al aceptar sus condiciones de uso (generalmente en inglés y que nunca se leen) comienzan a funcionar como espías.
- Siendo víctimas de Ingeniería social

Algunos tipos de Incidentes



Incidente de Seguridad



Un incidente de seguridad es un evento adverso que afecta los activos de la organización.

Todo incidente detectado debe ser reportado ante quien corresponda.

Buenas Prácticas

Como administradores/desarrolladores:

- Siguiendo las buenas prácticas de seguridad que indican los estándares/normas nacionales e internacionales.
- Aprobando la materia :D

Concientización

Un programa de concientización de Seguridad resulta fundamental para fortalecer los eslabones más débiles de la cadena de seguridad, las personas por:

- Desconocimiento de las amenazas.
- Desconocimiento de las medidas de seguridad
- Desconocimiento de los roles y responsabilidades de cada persona, con respecto a la seguridad

Este programa debe estar dirigido a todo el personal que trabaje con información de la organización.

El programa de concientización debe incluir:

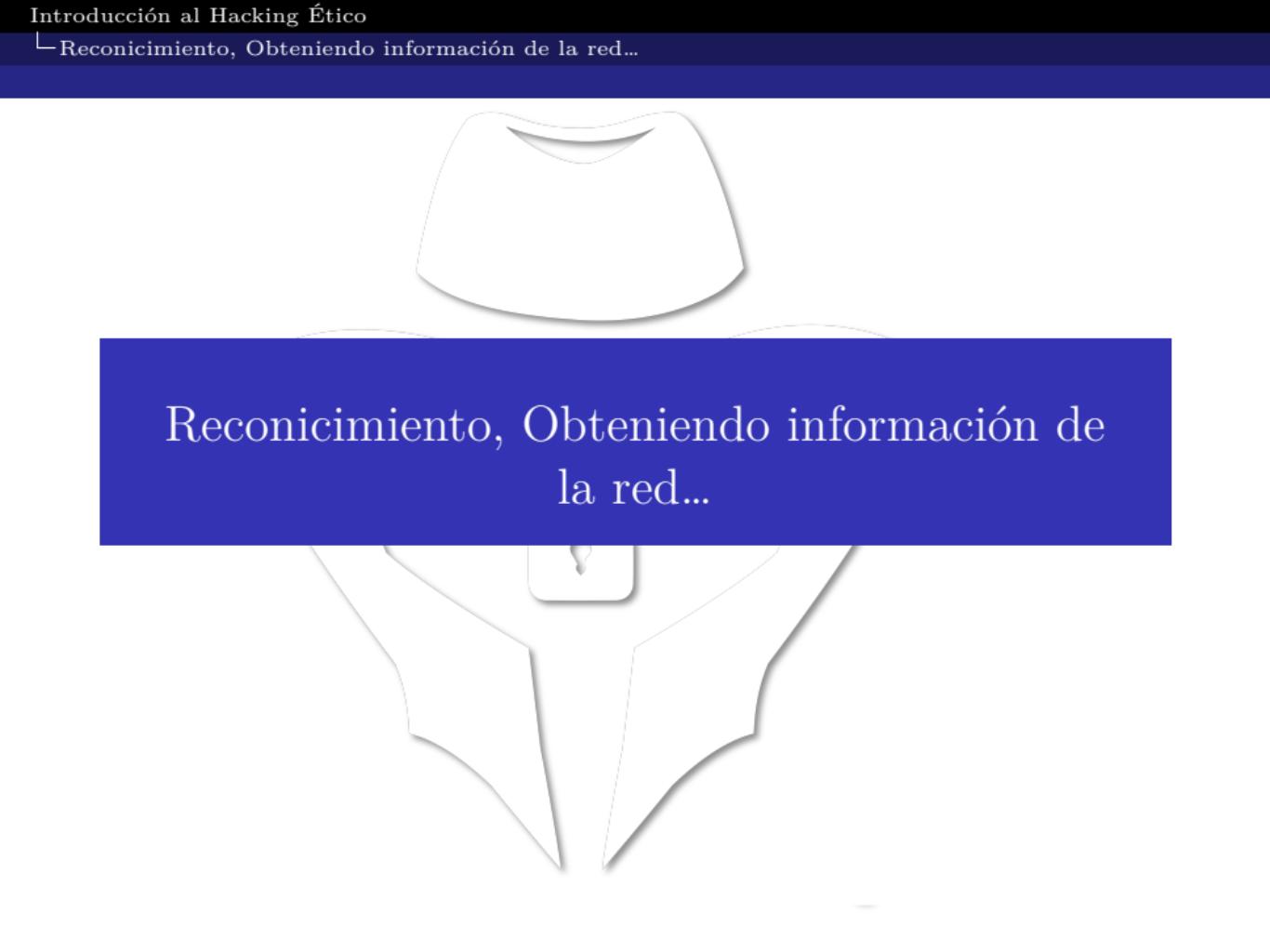
- Acciones de impacto, como ser:
 - Sesiones de concientización para los directivos
 - Sesiones de concientización para personal de TI
 - Sesiones de concientización para usuarios finales
- Acciones de seguimiento, como ser:
 - Eventos de seguridad
 - Boletines Internos
 - Posters
 - Tips para la navegación



El programa de concientización debe ser realizado a medida, teniendo en cuenta perfil de la empresa, tareas que se realizan y rasgos del personal.

Las actividades/ejemplos deben relacionarse con las actividades diarias del personal.





Reconicimiento, Obteniendo información de
la red...

Fases de un ataque

1 Reconocimiento



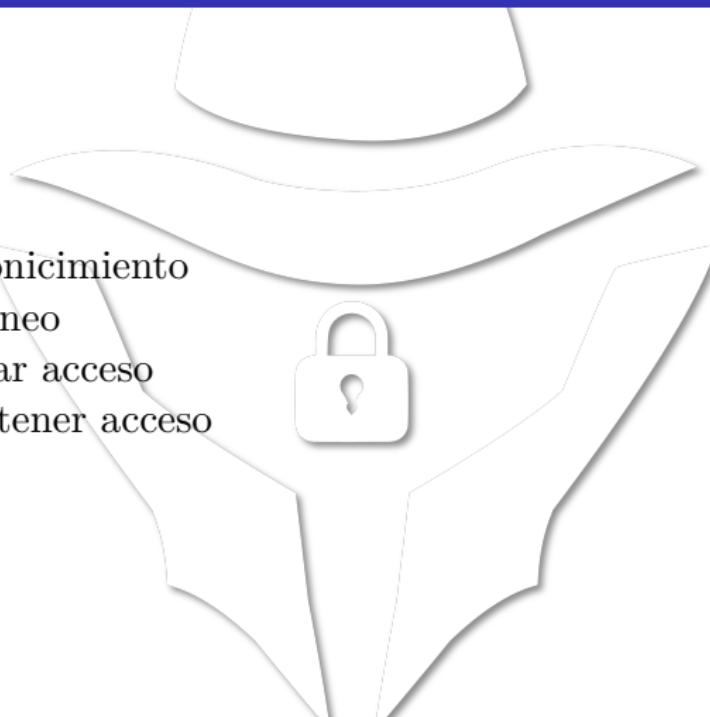
Fases de un ataque

- 
- 1 Reconocimiento
 - 2 Escaneo

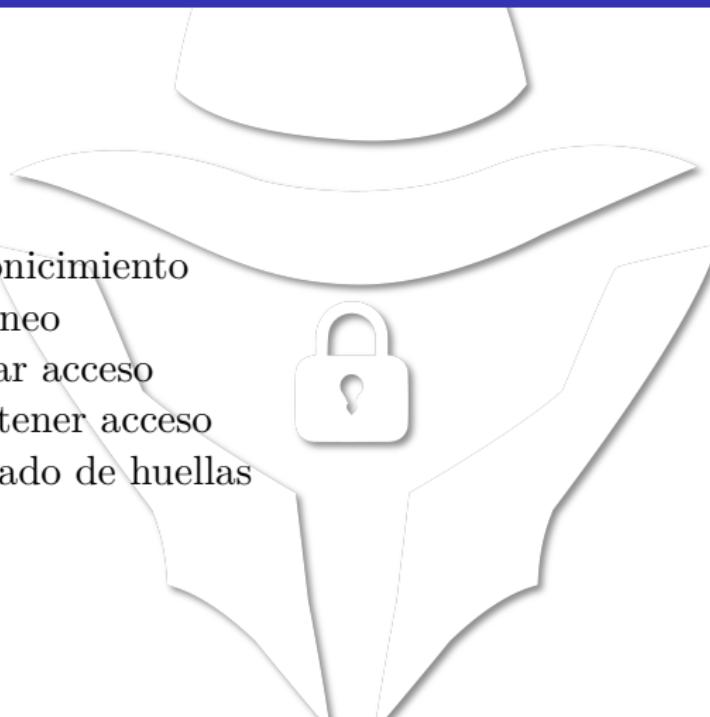
Fases de un ataque

- 
- 1 Reconocimiento
 - 2 Escaneo
 - 3 Ganar acceso

Fases de un ataque

- 
- 1 Reconocimiento
 - 2 Escaneo
 - 3 Ganar acceso
 - 4 Mantener acceso

Fases de un ataque

- 
- 1 Reconocimiento
 - 2 Escaneo
 - 3 Ganar acceso
 - 4 Mantener acceso
 - 5 Borrado de huellas

Reconocimiento: “La información es poder”

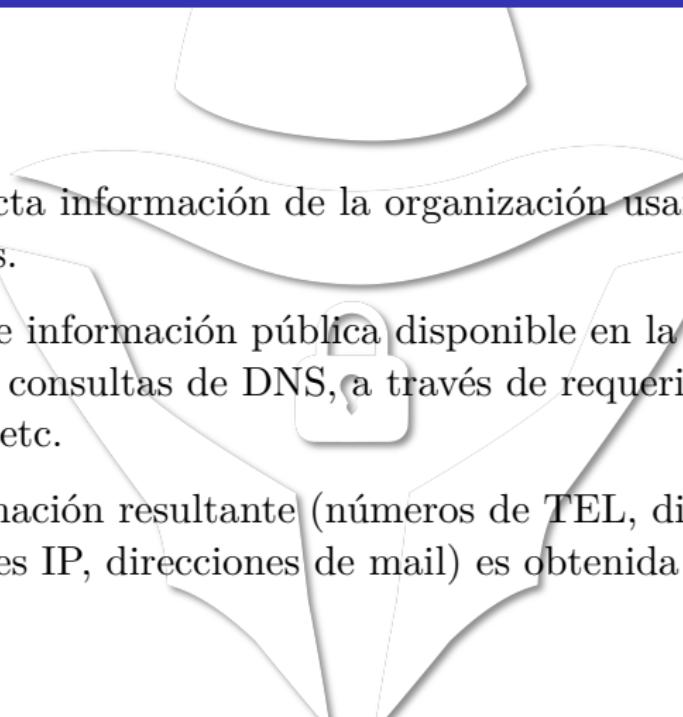
Las siguientes técnicas sirven para llevar a cabo tareas de reconocimiento. El objetivo es recolectar la mayor cantidad de información posible sobre la organización objetivo, en la fase de preparación del ataque. Cuanto mas se conozca sobre el objetivo mas posibilidades se tendrán para encontrar una vía por la que tener éxito en el ataque. Se le puede preguntar a un tercero sobre información que ellos tengan del objetivo o se puede ir directamente al objetivo para conseguir la información requerida.

...

Las técnicas pueden ser ACTIVAS (intrusivas) o PASIVAS (no intrusivas):

- Footprinting
- Enumeración

Footprinting



Se recolecta información de la organización usando métodos no intrusivos.

Se vale de información pública disponible en la página WEB, a través de consultas de DNS, a través de requerimientos de WHOIS, etc.

La información resultante (números de TEL, direcciones, direcciones IP, direcciones de mail) es obtenida de forma legal.

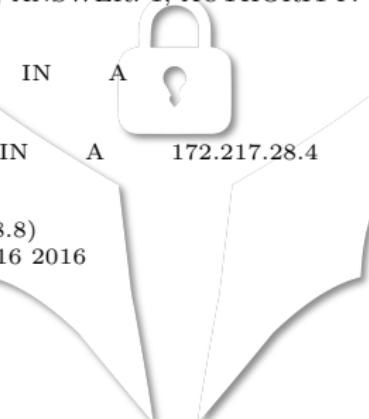
Footprinting

Se recolecta información de la organización usando métodos NO INTRUSIVOS. Se vale de información pública disponible en:

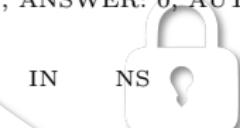
- El sitio web de la organización
- El servicio DNS
- El servicio WHOIS
- Otros servicios públicos como:
 - Netcraft
 - Webarchive
 - DomainRegisters
- Búsquedas orientadas de Google (Google Hacking)

DNS

```
$ dig www.google.com
; <<>> DiG 9.8.3-P1 <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52711
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
www.google.com.          IN      A
;; ANSWER SECTION:
www.google.com.      263    IN      A      172.217.28.4
;; Query time: 45 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 19 02:52:16 2016
;; MSG SIZE  rcvd: 48
```



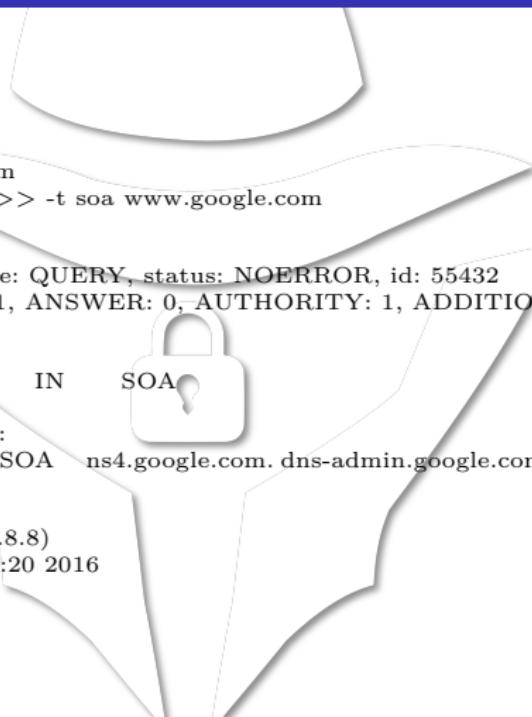
DNS



```
$ dig -t ns www.google.com

; <<>> DiG 9.8.3-P1 <<>> -t ns www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10451
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.           IN      NS
;; AUTHORITY SECTION:
google.com.      59      IN      SOA     ns4.google.com.
dns-admin.google.com. 130719806 900 900 1800 60
;; Query time: 69 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 19 03:14:58 2016
;; MSG SIZE rcvd: 82
```

DNS



```
$ dig -t soa www.google.com
; <<>> DiG 9.8.3-P1 <<>> -t soa www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55432
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.          IN      SOA
;; AUTHORITY SECTION:
google.com.      59      IN      SOA      ns4.google.com. dns-admin.google.com. 130719806 900 900 1800 60
;; Query time: 70 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 19 03:16:20 2016
;; MSG SIZE  rcvd: 82
```

DNS

```
$ dig -t mx google.com

; <<>> DiG 9.8.3-P1 <<>> -t mx google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46564
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
google.com.      IN  MX

;; ANSWER SECTION:
google.com.    599 IN  MX  40 alt3.aspmx.l.google.com.
google.com.    599 IN  MX  10 aspmx.l.google.com.
google.com.    599 IN  MX  50 alt4.aspmx.l.google.com.
google.com.    599 IN  MX  20 alt1.aspmx.l.google.com.
google.com.    599 IN  MX  30 alt2.aspmx.l.google.com.

;; Query time: 79 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 19 03:17:28 2016
;; MSG SIZE  rcvd: 136
```

WHOIS

```
$ whois 172.217.28.4
NetRange: 172.217.0.0 - 172.217.255.255
CIDR: 172.217.0.0/16
NetName: GOOGLE
NetHandle: NET-172-217-0-0-1
Parent: NET172 (NET-172-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS15169
Organization: Google Inc. (GOGL)
RegDate: 2012-04-16
Updated: 2012-04-16
Ref: https://whois.arin.net/rest/net/NET-172-217-0-0-1
```

```
OrgName: Google Inc.
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2015-11-06
```

NicAR

The screenshot shows a web browser window with the URL https://nic.ar/verificar-dominio. The page header includes the NIC Argentina logo, a lock icon, and the text "Secretaría Legal y Técnica [AR]". Below the header are navigation links for "NIC Argentina", "¿Necesitas ayuda?", and "Enterate". The main content area displays the message "Dominio no disponible" above the domain name "sancor.com.ar", which is highlighted with a red button labeled "No disponible".

Dominio no disponible

No disponible

sancor.com.ar

Datos del dominio

Nombre y Apellido: SANCOR COOPERATIVAS UNIDAS LIMITADA

Documento: 30501677643

Fecha de Alta: 01/01/1996

Fecha de vencimiento: 01/01/2017

Delegación 0: dns1.sancor.com.ar

Delegación 1: dns2.sancor.com.ar

Netcraft

ADVERTISEMENT

NETCRAFT

Netcraft Services

- [Netcraft News](#)

Phishing & Security

- [Anti-Phishing Toolbar](#)
- [Phishing Site Feed](#)
- [Hosting Phishing Alerts](#)
- [Fraud Detection](#)
- [Phishing Site Countermeasures](#)
- [Audited by Netcraft](#)
- [Open Redirect Detection](#)
- [Web Application Security Testing](#)
- [Web Application Security Course](#)

Internet Data Mining

- [Million Biggest Websites](#)
- [Hosting Provider Switching Analysis](#)
- [Hosting Provider Server Count](#)
- [Hosting Reseller Survey](#)
- [SSL Survey](#)

Internet Exploration

- [What's that site running?](#)
- [SearchDNS](#)
- [Sites on the Move](#)

Search Web by Domain

Explore 1,318,750 web sites visited by users of the [Netcraft Toolbar](#) 19th August 2016

Search:

example: site contains .netcraft.com

Results for google.com

Found 449 sites

Site	Site Report	First seen	Netblock	OS
1. www.google.com		november 1998	google inc.	linux
2. google.com		april 2000	google inc.	linux
3. news.google.com		april 2002	google inc.	linux
4. maps.google.com		april 2005	google inc.	linux
5. mail.google.com		june 2004	google inc.	linux
6. translate.google.com		november 2001	google inc.	linux
7. feedproxy.google.com		september 2008	google inc.	linux
8. www.google.com.au		august 1999	google inc.	linux
9. www.google.com.ar		august 1999	google inc.	linux
10. www.google.com.br		march 2002	google inc.	linux
11. www.google.com.mx		july 2002	google inc.	unknown

Figura 5: netcraft

Netcraft - Consulta por un sitio en particular

NETCRAFT

Site report for www.sancor.com

Search... →

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Rank Fraud Detection

Lookup another URL:
Enter a URL here

Share:

Background

Site title	SanCor	Date first seen	August 1997
Site rank	971747	Primary language	Spanish
Description	Not Present		
Keywords	Not Present		

Network

Site	http://www.sancor.com	Netblock Owner	Sancor S.A.
Domain	sancor.com	Nameserver	dns1.sancor.com.ar
IP address	200.45.108.250	DNS admin	mdns@sancor.com
IPv6 address	Not Present	Reverse DNS	host250.200-45-108.telecom.net.ar
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	Telecom Argentina
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	AR		

Figura 6: netcraft

Webarchive

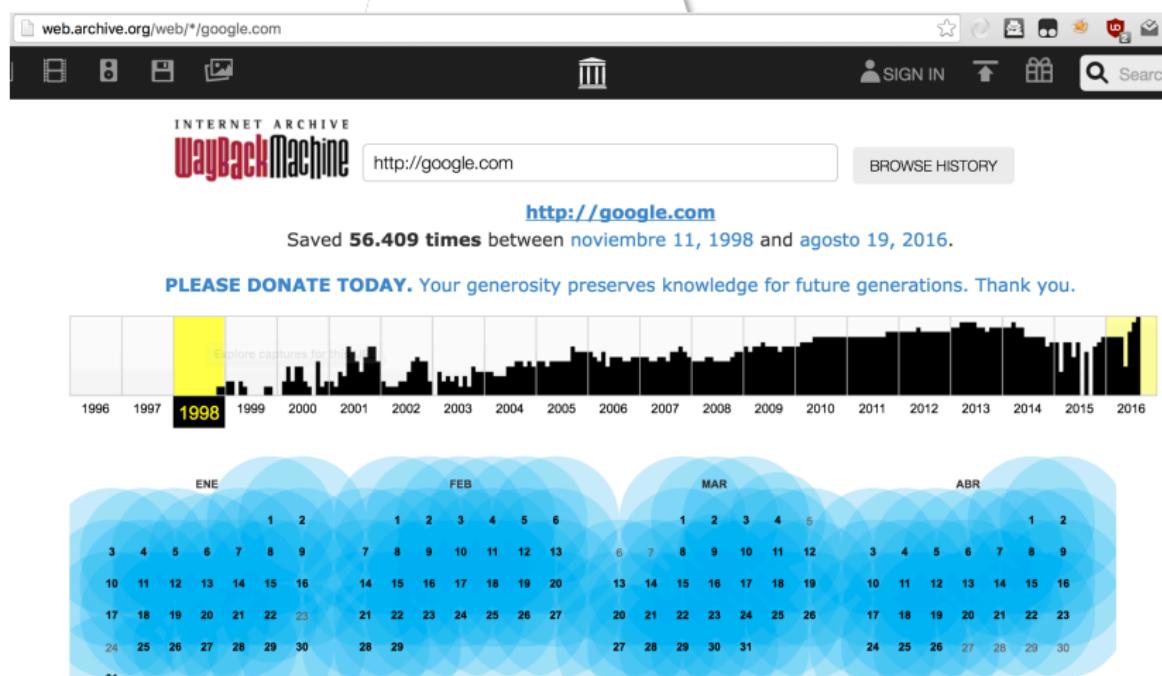


Figura 7: webarchive

Webarchive



Figura 8: webarchive

Ejemplo del portal de Google en diciembre de 1998.

Google hacking

Utilizando las busquedas avanzadas de google es posible dar rápidamente con algún tipo de información.

http://www.google.es/advanced_search



Figura 9: google hacking

Google hacking

¿Qué podemos encontrar con google hacking?

- Productos WEB vulnerables
- Sitios con algún error en particular
- Archivos con información sensible
- Portales de autenticación de usuarios
- Listado de directorios Interfaz de management de distintos dispositivos:
 - APs, Impresoras, cámaras, etc

<http://www.hackersforcharity.org/ghdb/>

<https://www.exploit-db.com/google-hacking-database>

Ejemplo Google Hacking (cont)

Archivos XLS en la UNP: site:unp.edu.ar filetype:xls

https://www.google.com.ar/search?q=insite%3A+ing.unp.edu.ar+filetype%3Apdf&oq=insite%3A+ing.

site:unp.edu.ar filetype:xls

Todos

Imágenes

Noticias

Maps

Más ▾

Herramientas de búsqueda

1 resultado (0.27 segundos)

[XLS] 1er Cuat 2010

www.ing.unp.edu.ar/asignaturas/algebra/TERCER_PARCIAL.xls ▾

Para que veas los resultados más relevantes, omitimos ciertas entradas muy similares a las 1 que ya te mostramos.

Si lo deseas, puedes repetir la búsqueda e incluir los resultados omitidos.

Ejemplo Google Hacking (cont)

Listas de usuarios: 'inurl:admin inurl:userlist'

The screenshot shows a Google search results page. The URL in the address bar is <https://www.google.com.ar/search?q=Listas+de+usuarios%3A+inurl%3Aadmin+inurl%3Auserlist&oq=Listas+de+usuarios%3A+inurl%3Aadmin+inurl%3Auserlist>. The search query 'inurl:admin inurl:userlist' is typed into the search bar. Below the search bar, there are navigation links for 'Todos', 'Imágenes', 'Videos', 'Maps', 'Noticias', 'Más ▾', and 'Herramientas de búsqueda'. The main content area displays search results.

Cerca de 13,000 resultados (0.28 segundos)

[Index of /netwaresl/ADMIN/TOP20NET/USERLIST](#)

[cd.textfiles.com/netwaresl/ADMIN/TOP20NET/USERLIST/](#) ▾ Traducir esta página

Index of /netwaresl/ADMIN/TOP20NET/USERLIST. Parent Directory · CNET-BBS.VRP · CNET-BBS.ZZZ · FILE_ID.DIZ · USERLIST.DOC · USERLIST.

[Index of /userlist/admin/data](#)

[samhong.hk/userlist/admin/data/](#) ▾ Traducir esta página

Index of /userlist/admin/data. Parent Directory · sqldata/ · userpic/

[Index of /userlist/admin](#)

[samhong.hk/userlist/admin/](#) ▾ Traducir esta página

Index of /userlist/admin. Parent Directory · data/ · tp/

[Index of /admin/userlist/](#)

[thiagocajacity.50webs.com/admin/userlist/](#) ▾ Traducir esta página

Name, Last Modified, Size, Type. Parent Directory/ · - , Directory. colors.txt, 2008-Mar-15 23:27:35, 0.1K,

Ejemplo Google Hacking (cont)

Portales de autenticación WordPress gubernamentales:
inurl:wp-login.php site:gov.ar



- Todos Noticias Imágenes Videos Maps Más ▾ Herramientas de búsqueda
- Cerca de 17 resultados (0.29 segundos)
- Identificación de Usuario**
www.conicetdocumental.gov.ar/wp-login.php?redirect_to=http%3A%2F%2Fwww... ▾
Recomendaciones. Este servicio es exclusivo para usuarios registrados. Para acceder debe ingresar su Nombre de Usuario y su Contraseña y clickear ...
- Ministerio de Derechos Humanos > Log In**
desarrollohumano.salta.gov.ar/wp-login.php
Ministerio de Derechos Humanos. Nombre de usuario. Contraseña. Remember Me. ¿Olvidó su contraseña? ← Back to Ministerio de Derechos Humanos.
- <https://www.mpf.gov.ar/procurarte/wp-login.php?red...>
No hay descripciones de este resultado disponibles debido al archivo robots.txt de este sitio.
Más información

- Empresas // CERRITO.gob.ar > Contraseña perdida**
cerrito.gob.ar/empresas/wp-login.php?action=lostpassword ▾
Empresas // CERRITO.gob.ar. Por favor, introduzca su nombre de usuario y e-mail. Recibirá una nueva contraseña vía e-mail. Nombre de usuario: E-mail:.

Otros Ejemplos (cont)

()

Sitios:

site:.gob.ar site:.gob.es filetype:doc

subdominios:

-www site:unp.edu.ar

WebCam:

intitle:“webcam 7” inurl:‘/gallery.html’ inurl:“ViewerFrame?Mode=”

Impresoras:

inurl:webarch/mainframe.cgi

Información que no quieren que veamos:

“robots.txt” “disallow:” filetype:txt

Herramienta para automatizar los google dorks

Snitch.py

<https://github.com/Smaash/snitch>

Información o fallas potenciales . /snitch.py -U sitio.com -D all
-O info.txt ## Enumeración

Permite recolectar distintos registros de información que, por ejemplo, un servicio de consulta puede ofrecer. La información se presenta en forma ordenada. Se podría realizar enumeración sobre distintos protocolos y servicios:

- DNS
- Netbios
- ICMP. Enumeración de Hosts

Enumeración - netbios

```
root@kali:~# dnsenum --enum google.com  
dnsenum.pl VERSION:1.2.3
```

Host's addresses:

google.com.	62	IN	A	74.125.130.100
google.com.	62	IN	A	74.125.130.101
google.com.	62	IN	A	74.125.130.102
google.com.	62	IN	A	74.125.130.113
google.com.	62	IN	A	74.125.130.138
google.com.	62	IN	A	74.125.130.139

Name Servers:

ns1.google.com.	343227	IN	A	216.239.32.10
ns2.google.com.	343227	IN	A	216.239.34.10
ns3.google.com.	343227	IN	A	216.239.36.10
ns4.google.com.	343227	IN	A	216.239.38.10

The quieter you become, the more you are

Mail (MX) Servers:

aspmx.l.google.com.	17	IN	A	74.125.129.27
alt1.aspmx.l.google.com.	38	IN	A	74.125.142.26
alt3.aspmx.l.google.com.	178	IN	A	173.194.68.27
alt4.aspmx.l.google.com.	163	IN	A	74.125.131.27
alt2.aspmx.l.google.com.	293	IN	A	74.125.137.27

Enumeración - netbios

```
nicolas@poseidon:~$ smbclient -U nmacia -L NEPTUNO
```

Password:

Domain=[REDES] OS=[Unix] Server=[Samba 3.0.24]

Sharename	Type	Comment
IPC\$	IPC	IPC Service (neptuno server)
print\$	Disk	Printer Drivers
Voluntariado	Printer	Voluntariado
hp	Printer	hp

Domain=[REDES] OS=[Unix] Server=[Samba 3.0.24]

Server	Comment
LINTIDC	lintidc
NEPTUNO	neptuno server

```
nicolas@poseidon:~$ nbtscan 163.10.■■■■■/24
```

Doing NBT name scan for addresses from 163.10.■■■■■/24

Workgroup	Master	IP address	NetBIOS Name	Server	User	MAC address
REDES	LINTIDC	163.10.■■■■■	WSUS-UNLP	<server>	<unknown>	00:0c:29:09:96:77
		163.10.■■■■■	Sendto failed: Permission denied			
		163.10.■■■■■	EUROPA	<server>	<unknown>	00:15:c5:32:f5:04
		163.10.■■■■■	SERVIDORLIVIANO	<server>	SERVIDORLIVIANO	00:00:00:00:00:00
		163.10.■■■■■	PEPE	<server>	<unknown>	00:0b:6a:cd:12:59
		163.10.■■■■■	LINTIDC	<server>	LINTIDC	00:00:00:00:00:00
		163.10.■■■■■	NEPTUNO	<server>	NEPTUNO	00:00:00:00:00:00
		163.10.■■■■■	LIHUEN-008BF8	<server>	LIHUEN-008BF8	00:00:00:00:00:00
		163.10.■■■■■	Sendto failed: Permission denied			
		163.10.■■■■■	2003LIVIANO	<server>	<unknown>	00:0c:29:e9:b1:6a
		163.10.■■■■■	LIHUEN-E87C98	<server>	LIHUEN-E87C98	00:00:00:00:00:00
		163.10.■■■■■	A1	<server>	<unknown>	00:0a:e6:cd:cc:ac
		163.10.■■■■■	DEBIAN	<server>	DEBIAN	00:00:00:00:00:00
		163.10.■■■■■	CMP-E75F0890AE5	<server>	<unknown>	00:13:8f:a7:35:e8
		163.10.■■■■■	DEBIANII	<server>	DEBIANII	00:00:00:00:00:00

Utilidad Netbios.

Enumeración - Netbios

```
Command Prompt
C:\Rix World\Apps\nbtscan\nbtscan_1_0_3>nbtscan -r 10.0.0.0/24
Warning: -r option not supported under Windows. Running without it.

Doing NBT name scan for addresses from 10.0.0.0/24

IP address      NetBIOS Name    Server      User      MAC address
10.0.0.1          APP1           <server>   APP1       00-50-8b-a0-f7-c2
10.0.0.2          PRINT1          <server>   PRINT1     00-00-00-00-00-00
10.0.0.5          Recvfrom failed: Connection reset by peer
10.0.0.6          Recvfrom failed: Connection reset by peer
10.0.0.13         S-RWU2           <server>   <unknown>  00-53-45-00-00-00
10.0.0.8          EXCH-SRU          <server>   EXCH-SRU   00-08-c7-5d-1f-e2
10.0.0.9          PERVERSIVE-WEB1    <server>   ADC        00-e0-81-05-46-55
10.0.0.12         WEB3             <server>   ROGERSJ    00-00-24-c8-03-6f
10.0.0.38         BEN_XL_POWER      <server>   BEN_XL_POWER 00-a0-cc-26-79-09
10.0.0.54         SAMIAM           <server>   SAMIAM     00-a0-c9-5a-a7-fa
10.0.0.58         W-STEWARTF        <server>   STEWARIF   00-a0-cc-26-7b-56
10.0.0.65         L-CLARKET          <server>   CLARKET    00-10-a4-f8-2a-14
10.0.0.75         US0066114-WP01    <server>   JENKINST   00-50-04-e7-78-e6
10.0.0.81         W-RICARDS          <server>   RICHARDSE  00-a0-cc-26-78-cb
10.0.0.101        APP2              <server>   APP2       00-02-a5-37-7c-ad
10.0.0.104        W-WUEBKERC         <server>   WUEBKERC   00-c0-a8-f1-48-a8
10.0.0.108        W-MURCHJ           <server>   MURCHJ     00-c0-a8-f1-49-1c
10.0.0.109        W-MILLERJ          <server>   MILLERJ    00-c0-a8-57-74-f9
10.0.0.127        L-KDONAHUE         <server>   DONAHUEK   00-10-a4-7b-b5-d3
10.0.0.135        CAROLLAPTOP         <server>   CSTEBBINS  00-20-e0-e0-6e-82
10.0.0.203        Recvfrom failed: Connection reset by peer
10.0.0.204        Recvfrom failed: Connection reset by peer
```

Utilidad nbtscan

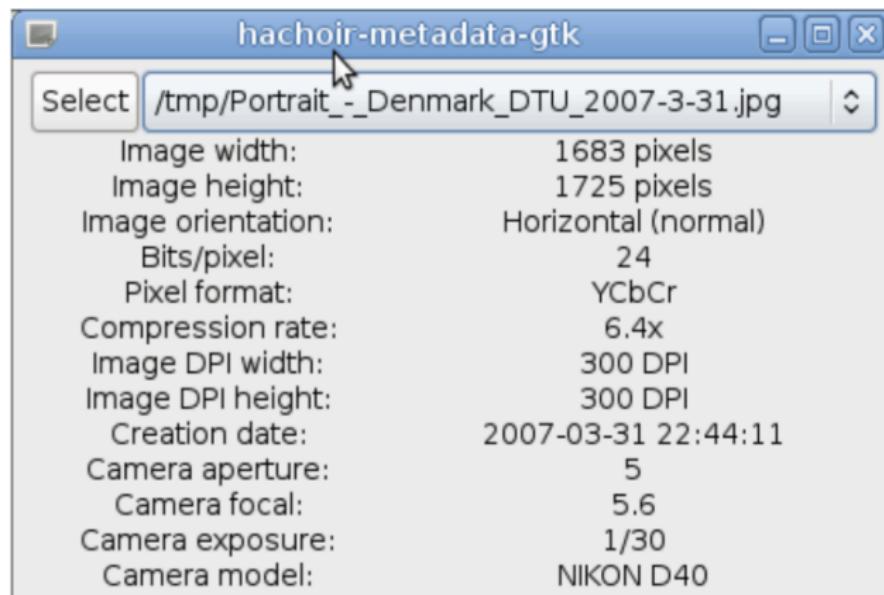
Análisis de campos meta

- Simplemente son datos de los datos
- Tienen distintas utilidades:
 - Análisis Forenses
 - Obtener información para un ataque
 - Aplicaciones que utilicen los mismos para realizar ordenaciones o categorías de cosas. Por ej:
 - Ordenación de fotos por fechas de la misma
 - Correlación de fotos por coordenadas geográficas

Análisis de campos meta

Algunas herramientas para extraer esta información de diferentes archivos:

metadata extraction Tool hachoir-metadata Exiftool



Análisis de campos meta

Foca

Es una herramienta que automatiza búsquedas de diferentes recursos de una organización y hace un análisis de campos meta en los recursos recolectados.



Fingerprinting

Son técnicas intrusivas que permiten el reconocimiento de la identidad del objetivo:

- Dispositivo de red (impresora, servidor, router, APs, centrales telefónicas, etc)
- Sistema Operativo
- Implementación de un servicio (por ej: apache o IIS o nginx)
- Versión de la implementación

nmap permite realizar fingerprint del OS y los servicios

Fingerprinting

- El sistema operativo puede ser descubierto en base a como cada implementación responde a distintos paquetes (TCP, UDP, ICMP, etc)

<http://nmap.org/book/osdetect.html>

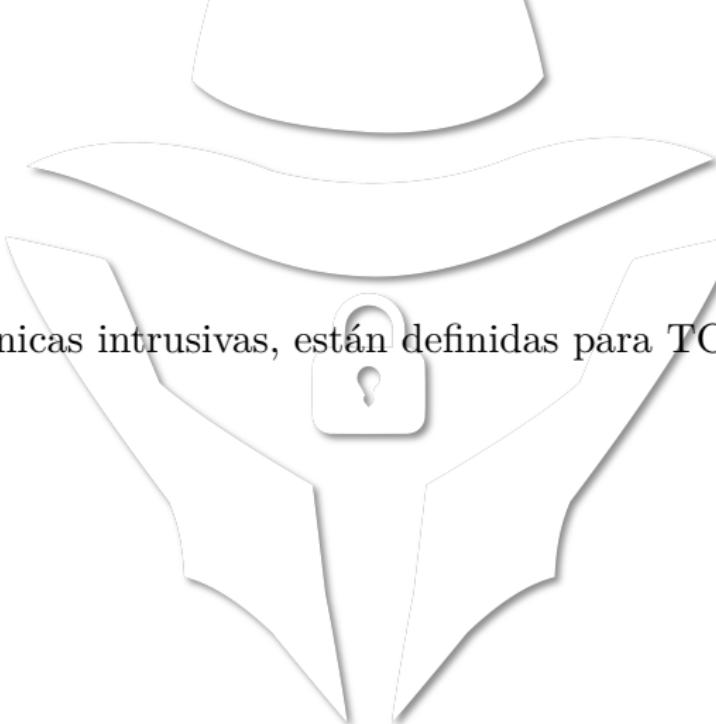
- Los servicios pueden ser inferidos en base a banners que presentan o a como responden en caso que los banners estén deshabilitados.

Escaneo de puertos

El objetivo es determinar qué puertos están abiertos en un host o servidor determinado.

Si el puerto está abierto, eso implica que hay un proceso atendiendo a los requerimientos que llegan al puerto. El proceso es software el cual puede estar desactualizado, por lo que puede tener vulnerabilidades que afecten su normal funcionamiento o la seguridad del sistema y sus datos.

Técnicas de escaneo de puertos



Son Técnicas intrusivas, están definidas para TCP y UDP.

Técnicas de scanning - TCP:

Open TCP scanning:

TCP Connect() Scanning (Vanilla connect scanning)

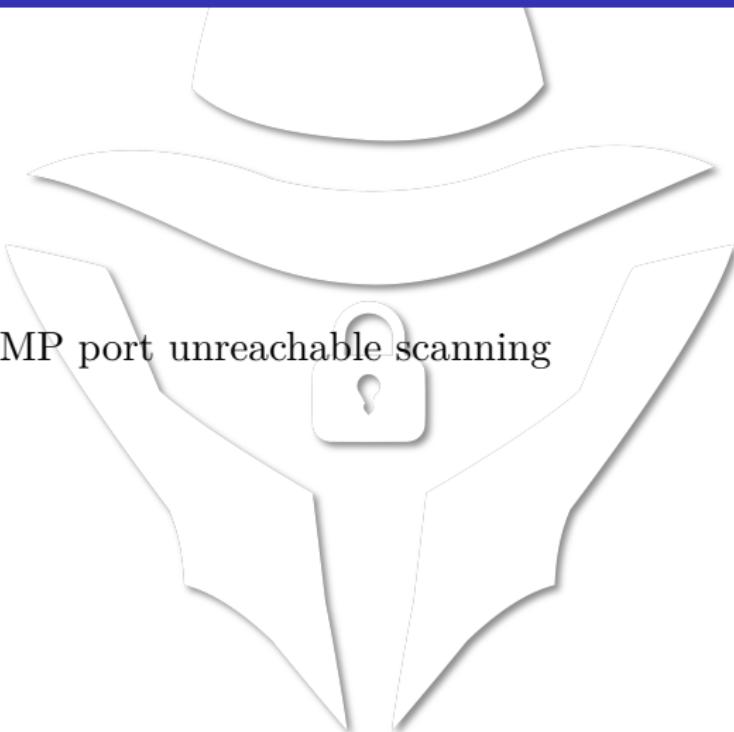
Stealth TCP scanning

- Half-open SYN flag scanning
- Inverse TCP flag scanning
- ACK flag probe scanning

Third-party and spoofed TCP scanning

- TCP Idle Scanning (IP ID header scanning)
- FTP bounce scanning
- Proxy bounce scanning 7

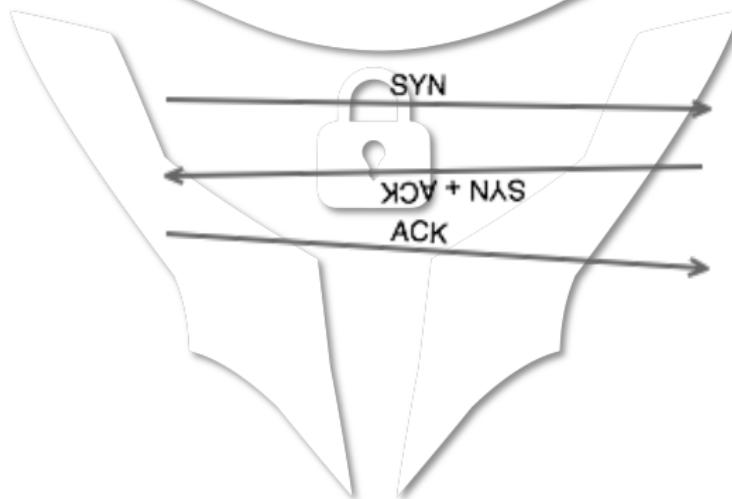
Técnicas de scanning - UDP:



UDP ICMP port unreachable scanning

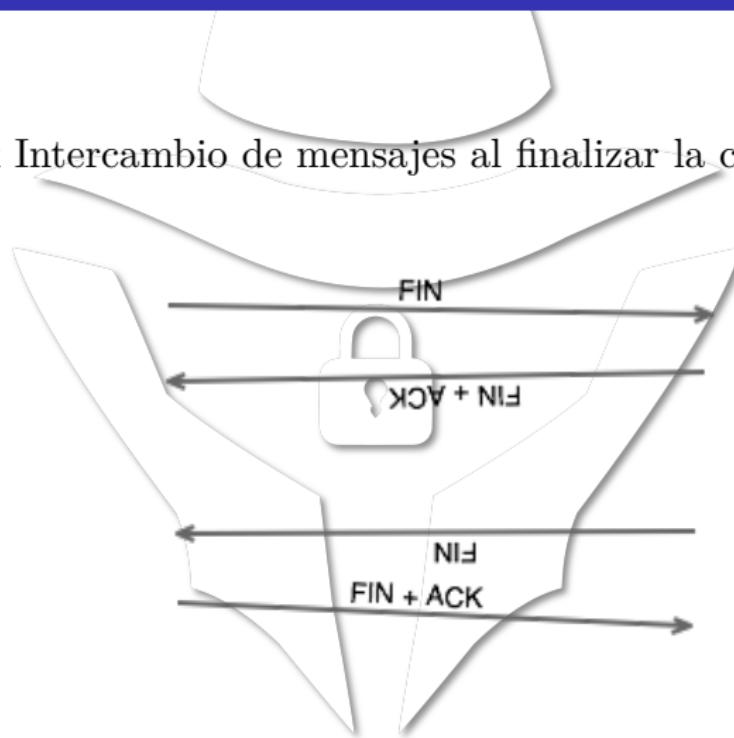
Sesiones TCP - Inicio de conexión

Saludo de tres vías Syn Intercambio de mensajes en el inicio de la conexión Syn/Ack



Sesiones TCP - Cierre de conexión

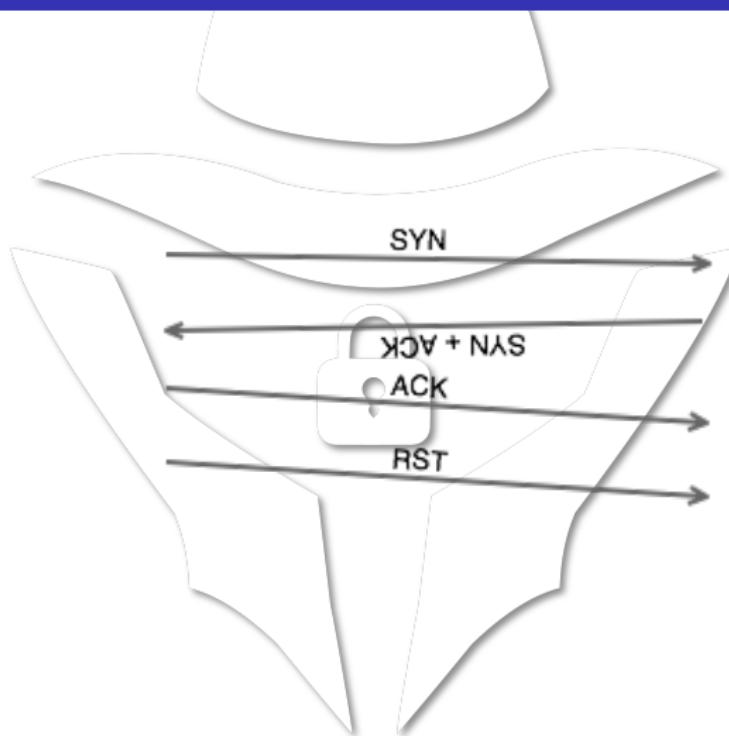
Fin Ack Intercambio de mensajes al finalizar la conexión



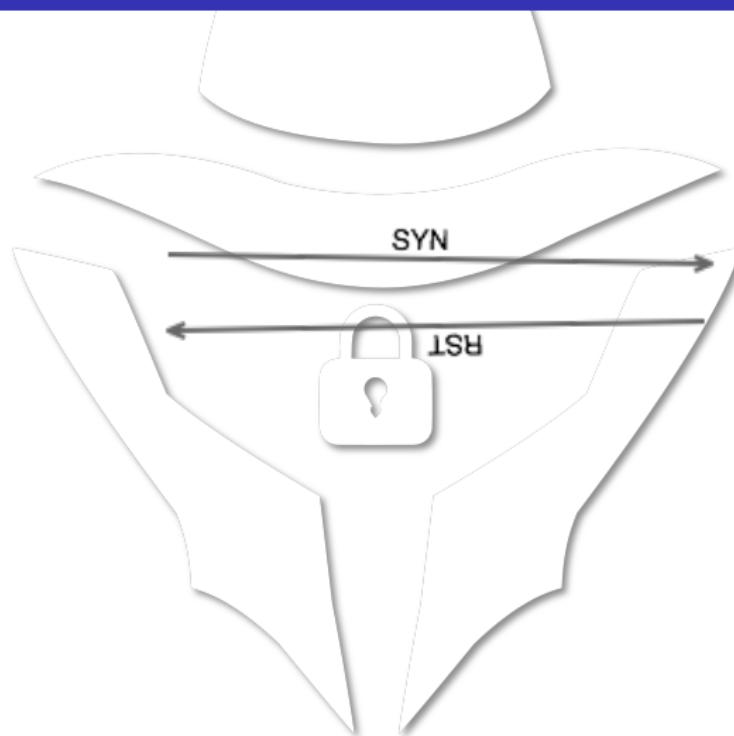
TCP Connect() Scanning



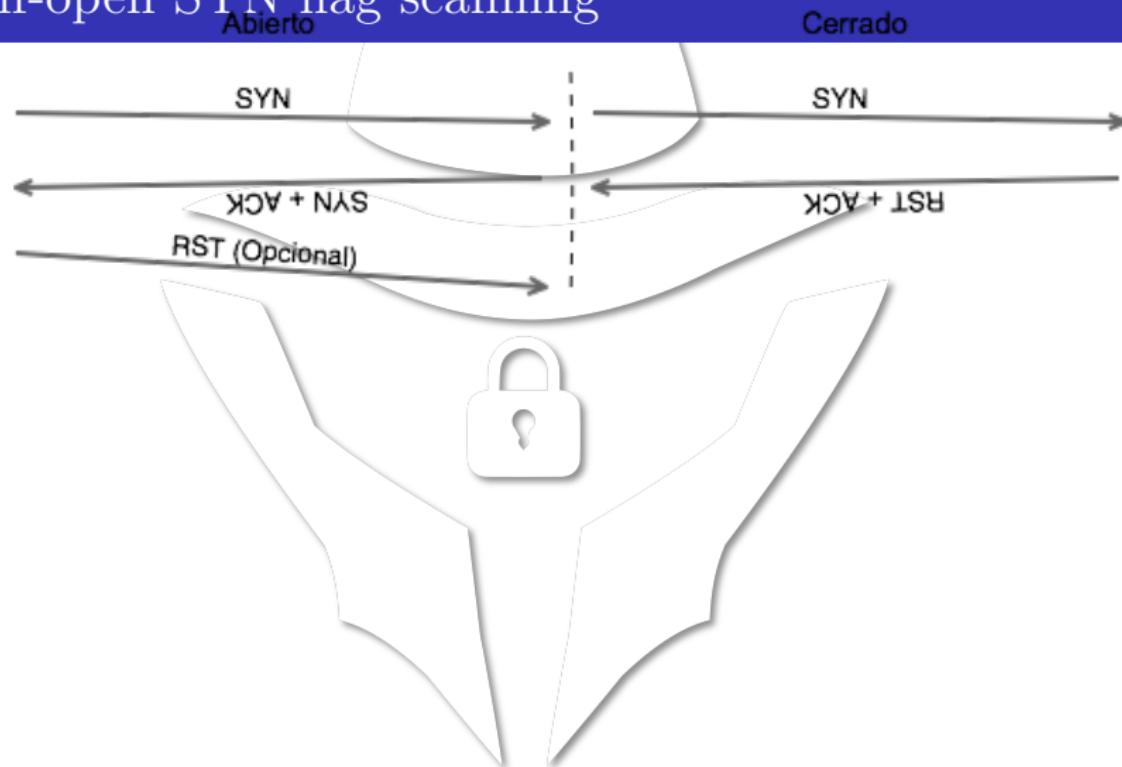
Abierto



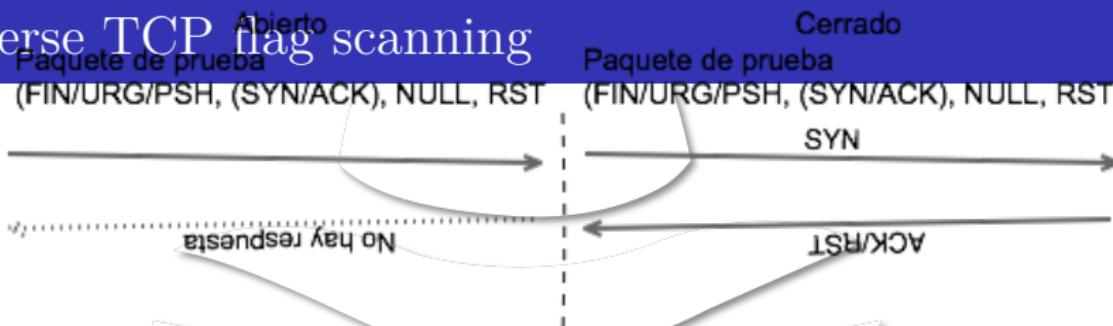
TCP Connect() Cerrado



Half-open SYN flag scanning



Inverse TCP flag scanning



Idle Scan

Permite el scan de puertos sin que el dispositivo escaneado reciba paquetes provenientes de nuestra IP. Se distinguen los siguientes actores:

- Atacante
- Víctima
- Zombie

El zombie deberá ser una estación en la red con:

- Poco tráfico
- IP ID predecible

TCP idle scan - Zombie

Para que el zombie sirva a nuestro propósito, el mismo debe cumplir con los siguientes requisitos:

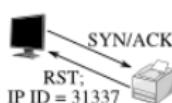
Debe tener poco tráfico
Debe ser predecible el valor del campo IP ID de los paquetes que éste envía

```
hping3 -S -p 80 -S 192.168.0.2
```

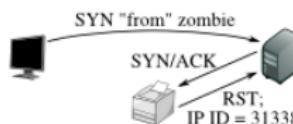
```
HPING 192.168.0.2 (eth0 192.168.0.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.2 ttl=64 id=7 sport=80 flags=SA seq=0 win=65535
len=46 ip=192.168.0.2 ttl=64 id=8 sport=80 flags=SA seq=1 win=65535
len=46 ip=192.168.0.2 ttl=64 id=9 sport=80 flags=SA seq=2 win=65535
len=46 ip=192.168.0.2 ttl=64 id=10 sport=80 flags=SA seq=3 win=65535
len=46 ip=192.168.0.2 ttl=64 id=11 sport=80 flags=SA seq=4 win=65535
len=46 ip=192.168.0.2 ttl=64 id=12 sport=80 flags=SA seq=5 win=65535
```

TCP Idle Scanning Abierto

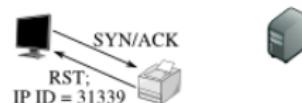
Step 1: Probe the zombie's IP ID.



Step 2: Forge a SYN packet from the zombie.



Step 3: Probe the zombie's IP ID again.



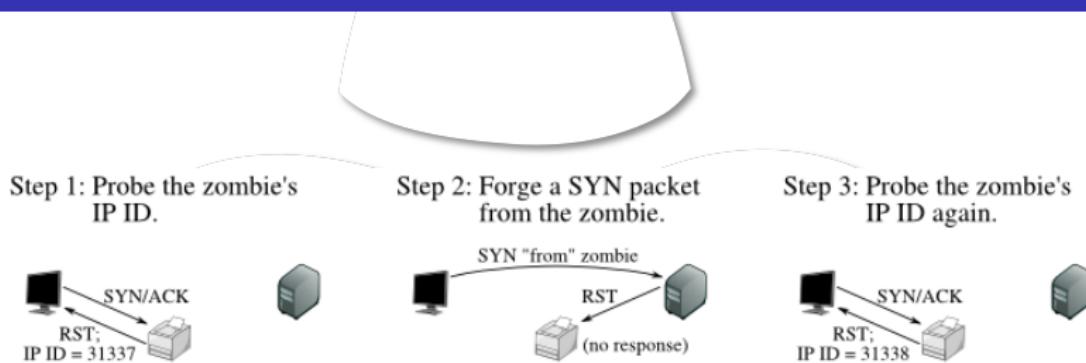
The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

Figura 14: idle-scan-open

TCP Idle Scanning Cerrado



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

Figura 15: idle-scan-closed

TCP Idle Scanning Filtrado



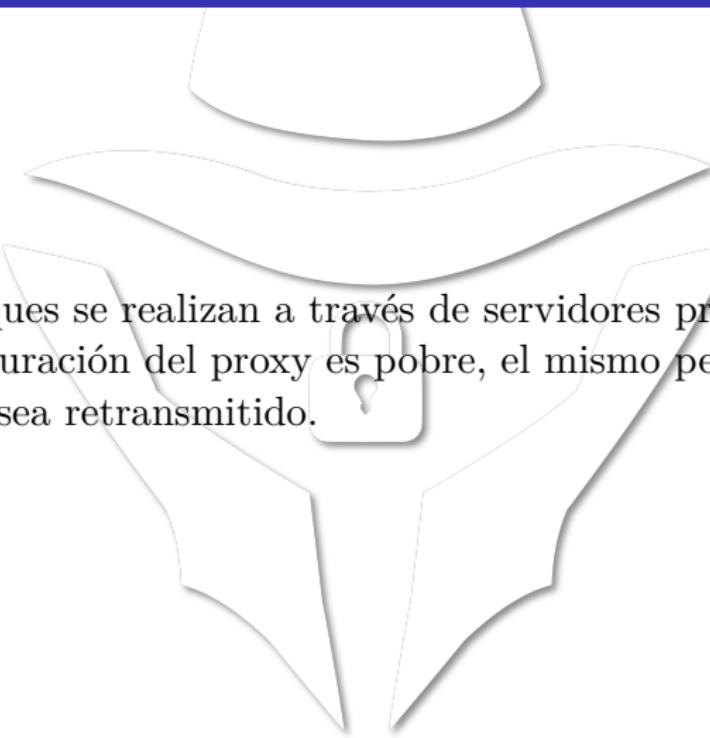
Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

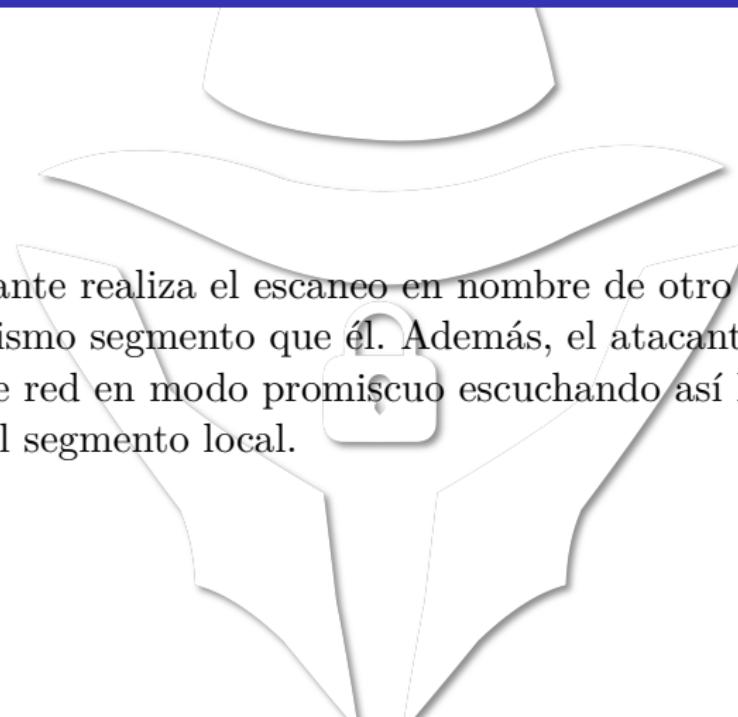
Figura 16: images/idle-scan-filtered

Proxy bounce scanning



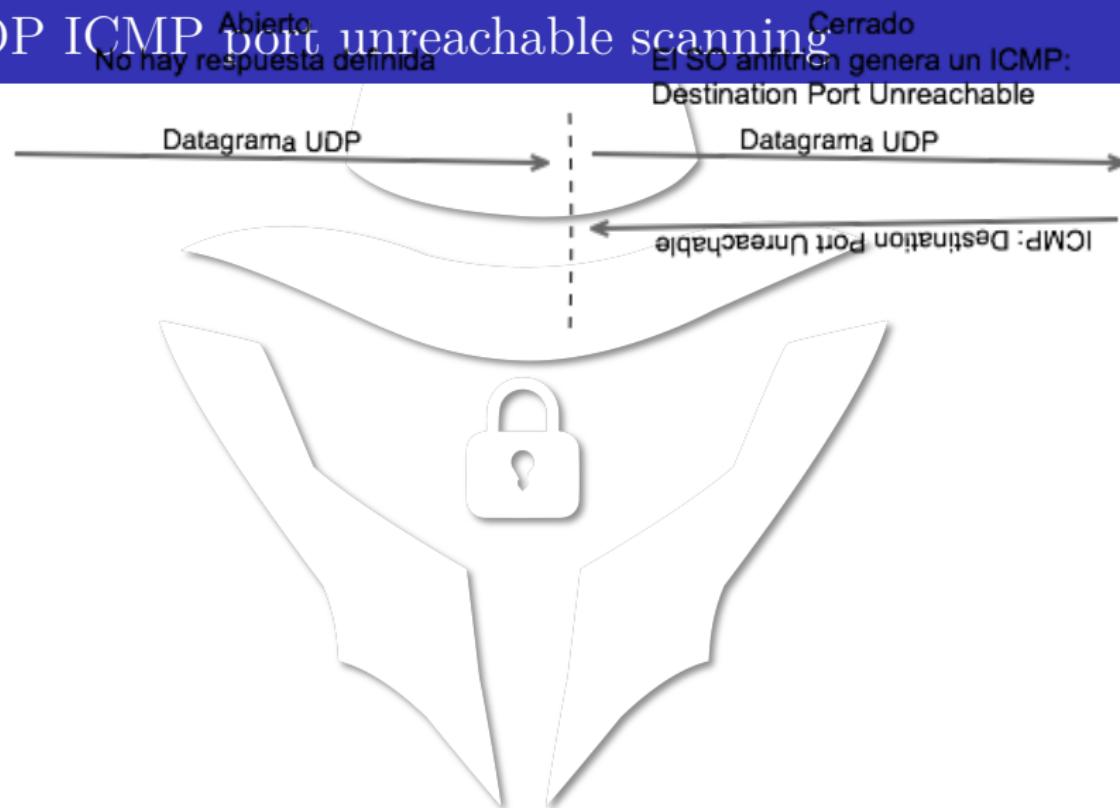
Los ataques se realizan a través de servidores proxy abiertos. Si la configuración del proxy es pobre, el mismo permitirá que el escaneo sea retransmitido.

Sniffer-based spoofed scanning



El atacante realiza el escaneo en nombre de otro host ubicado en el mismo segmento que él. Además, el atacante coloca su placa de red en modo promiscuo escuchando así las respuestas dadas al segmento local.

UDP ICMP port unreachable scanning



Escaneadores de vulnerabilidades

Además de implementar la funcionalidad de un escaner de puertos, realizan una tarea adicional.

- Escanean los puertos del host testeado la aplicación que está brindando el servicio descubierto.
- Intentan determinar la versión de la aplicación (banners, respuestas conocidas)
- Determinan si las aplicaciones descubiertas tienen vulnerabilidades conocidas
- Para ésto contrastan lo encontrado con una base de datos que se debe actualizar periódicamente.

Escanners de vulnerabilidades

- OpenVAS <http://www.openvas.org/> Es un fork open-source de Nessus
- Nessus <http://www.nessus.org/nessus/> Paso a ser comercial en 2008
- Languard [<http://www.gfi.com/lannetscan/>] Producto comercial para Windows
- Retina [<http://go.beyondtrust.com/community>] Producto comercial para Windows
- Nikto [<http://www.cirt.net/nikto2>] Open source Web Server Scanner

Nes



Es un scanner de vulnerabilidades que cuenta con una arquitectura cliente/servidor cuyos componentes son:

- El servidor Nessus, que ejecuta el escaneo
- El cliente Nessus que presenta los resultados al usuario.
- Los plugins Nessus
- La base de datos de conocimiento Nessus.

Los resultados los presenta en reportes con distintos formatos: texto plano, XML, HTML y LaTeX.

Provee funcionalidad adicional para testear el nivel de vulnerabilidad de la red (como por ej. Ejecutar auditoría de passwords usando métodos de diccionario o ataques de fuerza bruta). Desde el 31 de julio de 2008 se volvió comercial

OPENVAS

(Open Vulnerability Assessment System) es distribuido bajo licencia GNU GPL.

Deriva de Nessus que pasó a ser un producto propietario en el año 2008.

Componentes:

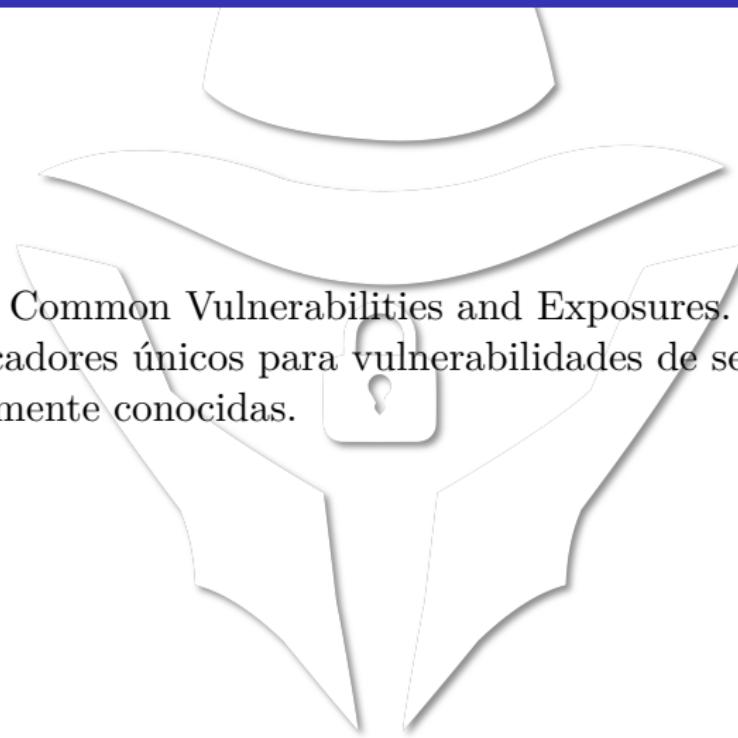
- OpenVAS-Server: Es el núcleo de OpenVAS
- OpenVAS-Client: El cliente se conecta con el OpenVAS-Server, procesa los resultados de los escaneos y los muestra al usuario
- OpenVAS-Libraries: Librerías que contienen funcionalidad que es utilizada por el OpenVAS - Server.
- OpenVAS-LibNASL: Este módulo contiene la funcionalidad requerida para que el OpenVAS-Server interactúe con NASL (Nessus Attack Scripting Language).

Escaner de propósito específico: Nikto

Es un scanner de vulnerabilidades de servidores WEB opensource (GPL). Está orientado a examinar servidores Web para descubrir:

- Configuraciones no adecuadas
- Archivos y scripts por defecto
- Archivos y scripts con problemas de seguridad
- Software desactualizado

Identificación de las vulnerabilidades



CVE = Common Vulnerabilities and Exposures. Son identificadores únicos para vulnerabilidades de seguridad públicamente conocidas.

Ejemplos

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0222>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160>

Cada CVE incluye: Un número identificador (por ej. “CVE-2013-1667”). Una breve descripción de la vulnerabilidad. Otra información relacionada (Alerta inicial, recomendaciones del equipo de respuesta, recomendaciones del fabricante)

Resultados de los análisis: Códigos

Dependiendo del origen del reporte, identificadores de distintos orígenes que generalmente mapean con un CVE:

Ejemplos: * USN-432-1 Ubuntu Security Notice USN-432-1 que se corresponde con el CVE-20071263

- MDKSA-2007:055 Mandriva Linux Security Advisory
MDKSA-2007:055 con el CVE2007-1246
- MS13-079 Microsoft Security Bulletin MS13-079 con el
CVE-2013-3868

Ataques de fuerza bruta

Cualquier servicio que permita la autenticación de usuarios puede ser afectado por ataques de fuerza bruta. Los ataques de fuerza bruta pueden intentar:

- Probar todas las combinaciones de contraseñas posibles o Utilizar un diccionario de claves (lo más usual)
- Se pueden encontrar diccionarios con determinadas características (palabras en algún idioma en particular o alguna temática determinada)

Ejemplos

- <http://boingboing.net/2009/01/02/top-500-worst-passwo.html>
- <http://blog.g0tmi1k.com/2011/06/dictionaries-wordlists.html>
- <http://www.skullsecurity.org/wiki/index.php/Passwords>
- <http://cyberwarzone.com/cyberwarfare/password-cracking-mega->