

TEMA 5

Asegurar la granja web

SWAP

¿Qué podemos hacer para proteger y
asegurar la granja web?
¿Evitará acciones maliciosas?



José Manuel Soto Hidalgo
Dpto. Arquitectura y Tecnología de Computadores
Universidad de Granada

jmsoto@ugr.es

Índice



- [1. Introducción]
- 2. Defensa en profundidad
- 3. Políticas de seguridad
- 4. Asegurar un servidor
- 5. Cortafuegos
- 6. Evitar ataques
- 7. Prácticas de seguridad recomendadas
- 8. Conclusiones

Introducción

Asegurar la granja web es una tarea muy importante para cualquier sitio web.

Puede permitir además, saber quién hizo cada cosa y en qué momento.

La seguridad es fundamental para proteger los datos propiedad de la empresa y la información de los usuarios.

El fin último es evitar (o al menos dificultar en lo posible) que un hacker malicioso realice cualquier acción que afecte al sistema.

Introducción

Se trata de **asegurar y mejorar la disponibilidad del sitio** y también de asegurarse de que las **operaciones** que se lleven a cabo en el sitio sean **seguras**.

Las políticas de seguridad y los procedimientos para implementar esas políticas son clave en el diseño de una granja web.

Introducción

Los objetivos de seguridad deben definirse correctamente y se basan generalmente en los siguientes conceptos:

- **Confidencialidad:** las comunicaciones deben ser secretas.
- **Integridad:** los mensajes enviados deben ser exactamente los recibidos.
- **Disponibilidad:** la comunicación con cualquier aplicación o servicio de la granja web debe estar disponible en el momento en que sea requerida.

Introducción

En este tema trataremos:

- Comprender el concepto de **defensa en profundidad** (diferentes capas de defensa).
- Establecer **políticas de seguridad**, incluyendo claves seguras, para todas las cuentas.
- Asegurar un servidor mediante la **eliminación de servicios innecesarios y vulnerabilidades**.
- **Usar un cortafuegos**: comprender el funcionamiento de los cortafuegos y los beneficios de estos.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Defensa en profundidad

Importancia de la arquitectura de seguridad.

Incluso en el mundo real, se controla el acceso a los recursos de un edificio o empresa con varias capas.

EJ: *en un banco hay varios niveles de seguridad para proteger el dinero (varios sistemas de seguridad de diferente tipo que superar para hacerse con el dinero):*

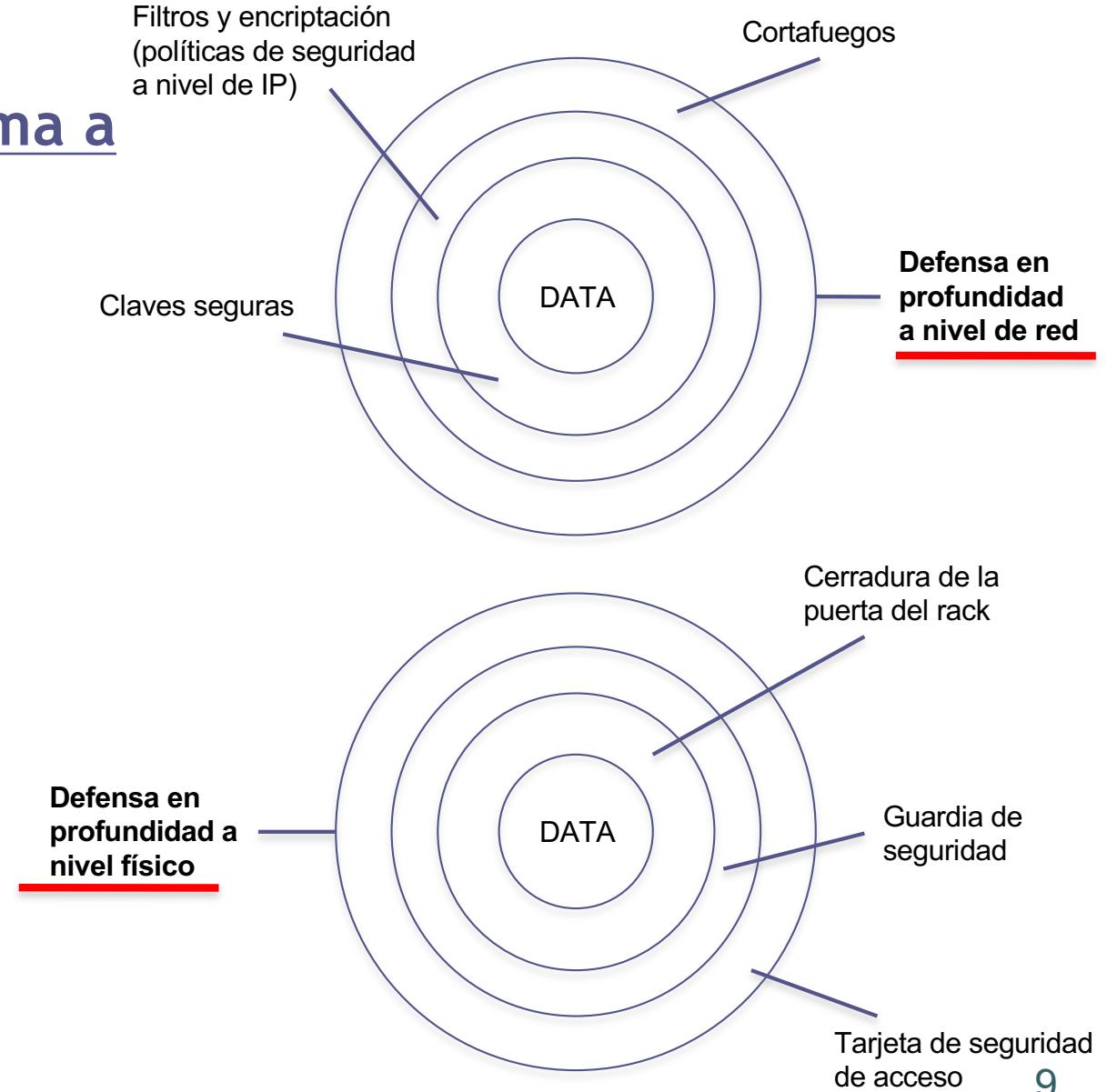
- (1) *el dinero está guardado en cajas fuertes. Para acceder a ese dinero, los clientes deben identificarse.*
- (2) *el banco utiliza video-vigilancia y mantiene registros detallados de todas las transacciones.*

¿Por qué no en una granja web?

Defensa en profundidad

Protección del sistema a diferentes niveles.

Habría que superar cada una de las capas independientemente para acceder a los datos



Defensa en profundidad

¿Son necesarios tantos niveles?

Sí

Ningún sistema de seguridad es totalmente seguro...

La forma de complicarle la tarea a un hacker malicioso es poner más de un nivel de seguridad.

Incrementar el tiempo necesario para superar cada nivel hace que sea más probable detectar un ataque, y así evitar que las últimas defensas se vean comprometidas.

Defensa en profundidad

Importante estar al día en cuanto a temas de seguridad en todos los frentes.

El administrador responsable de la seguridad informática debe conocer los temas relativos a la seguridad así como las vulnerabilidades a nivel de red, de cortafuegos, de sistema operativo y de las aplicaciones en el sistema web.

Defensa en profundidad

Hay que estar pendientes a los grupos de noticias, listas de correo, blogs y foros sobre estos temas.

Cuando se identifica una vulnerabilidad, los administradores de seguridad deben tomar **medidas de prevención** ya que siempre habrá quien esté atento para aprovecharla...

Estas investigaciones y estudios sobre seguridad en ciertas organizaciones suelen **revelar los puntos débiles** de los sistemas web de otras en las que no aplican políticas de seguridad.



Índice

1. Introducción
2. Defensa en profundidad
- 3. Políticas de seguridad**
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Políticas de seguridad

Las políticas de seguridad definen cómo se les permite interaccionar a los usuarios con los servidores y el hardware del sistema web.

Todas las políticas definen:

- procedimientos de identificación y acceso
- o privilegios de uso (qué acciones puede llevar a cabo cada tipo de usuario).

Políticas de seguridad

Los procedimientos de identificación comienzan solicitando una identificación (nombre de usuario + clave). De la validez de esta identificación dependerá que se permita o deniegue el acceso.

¿Qué se suele utilizar?

- Una clave o PIN
- Una tarjeta física que incluirá la clave
- Un escáner de retina, huella dactilar o ADN

...del menos efectivo al más efectivo.

Usar dos, especialmente si el primero es una simple clave.

Políticas de seguridad

retina / huella / tarjeta



Políticas de seguridad

Ejemplo: algunas empresas usan dos factores:

El primero, una **tarjeta de identificación** con la que se le permite a los empleados acceder a ciertas áreas.

El segundo suele ser una **identificación** (usuario y clave) en la red de ordenadores. Con ella podrá acceder a ciertos recursos, aunque a ciertas otras máquinas no.

En los **dominios de seguridad** los administradores definen listas de control de acceso (usuarios o grupos que pueden acceder a ciertos recursos concretos).

Políticas de seguridad

Formas de usar la huella dactilar...

The screenshot shows a news article from the website <https://www.elsiglodetorreon.com.mx/noticia/163290.asesina-a-su-marido-y-le-corta-el-dedo-para-c.html>. The article is categorized under 'SUCESOS' and published by 'El Siglo de Torreón' on Monday, August 8, 2005, at 11:22 am. It is the 4th of 7 articles in the series. The main headline reads: 'Asesina a su marido y le corta el dedo para cobrar pensión'. Below the headline are social sharing buttons for Facebook, Twitter, Google+, and LinkedIn.

Asesina a su marido y le corta el dedo para cobrar pensión

✉ ENVIAR
★ FAVORITO
🖨 IMPRIMIR
💬 COMENTAR

Bogotá, (Notimex).- La policía colombiana capturó a una mujer que asesinó a su esposo en el año 2000 y luego le cortó y congeló el dedo índice derecho para poder estampar mensualmente su huella digital en un poder para cobrar su pensión.

Políticas de seguridad

Tipos de sensores biométricos:

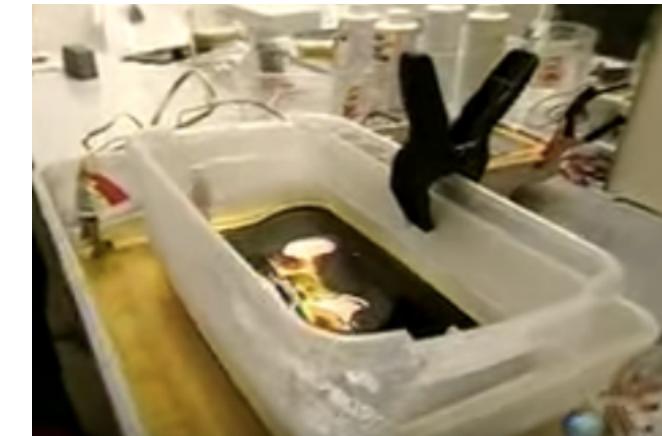
	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Vascular dedo	Vascular mano	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

<http://www.interempresas.net/Seguridad/Articulos/50527-Lectores-de-reconocimiento-biometrico-seguridad-y-control-de-acceso.html>

Políticas de seguridad

¿se puede engañar a un sensor biométrico?

YouTube^{ES}



Políticas de seguridad

¿se puede engañar a un sensor biométrico?

 clipset.20minutos.es/se-puede-enganar-al-iphone-5s-con-un-dedo-cortado/

¿Se puede engañar al iPhone 5s con un dedo cortado?

Por Juan Castromil (@castromil) el 17/09/2013 | 10 comentarios

Tus dedos son tu identidad digital para el iPhone 5s, pero ¿están a salvo tus dedos?

La respuesta corta es no. La respuesta larga es que el sistema de reconocimiento utilizado en el iPhone 5s, desarrollado por **AuthenTec** y basado en un **sensor capacitivo RF**, utiliza tecnología capacitiva para determinar patrón eléctrico formado por las huellas dactilares de cada dedo. Esto significa que, a diferencia de los escáneres ópticos que sólo ven la imagen formada por el contorno de los surcos sub epidérmicos, el sistema de Apple localiza algunos puntos clave del 'circuito eléctrico' que forma la huella dactilar.

Políticas de seguridad

¿se puede engañar a un sensor biométrico?

<https://www.youtube.com/watch?v=C2cVAQmcMf0>



How to make the fakefingerprints (VIRDI)
VIRDI Biometric
187.963 visualizaciones



Falsificación de Huellas Digitales en Control de Acceso
Cybertronics Security
31.561 visualizaciones



Con huellas dactilares falsas checaba por compañeros - El Universal
Miguel Angel Sanchez Pacheco
11.437 visualizaciones



Seguridad Fisica - Duplicacion de Huellas y Acceso
Lockpick AR
7.420 visualizaciones

Políticas de seguridad

Aplicar políticas a diferentes niveles:

- 1. Seguridad a nivel físico:** asegurarnos de que no entren en las salas y roben las máquinas o los discos; ambiente refrigerado, cerradura de seguridad, vigilancia; contraseñas de BIOS y de consola...
- 2. Seguridad a nivel de red:** cortafuegos; subred privada, ACL.
- 3. Seguridad a nivel de administrador:** administradores por tipo de servicio.
- 4. Cuentas de servicios (o aplicaciones):** accesos controlados desde Internet (usuario “apache” o “www” + cuentas de aplicaciones).

Políticas de seguridad

Toda organización con un gran sistema web debe tener un **equipo de ingenieros con dedicación exclusiva** a desarrollar, investigar, responder y arreglar temas de **seguridad** del sistema a todos los niveles.

Ética profesional. Si soy un extrabajador de una empresa, conozco la política de seguridad y podría “fácilmente” tener acceso no permitido...

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
- 4. Asegurar un servidor**
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Asegurar un servidor

Proceso en el que eliminamos

- características no necesarias,
- servicios,
- configuraciones e
- información de seguridad del servidor,

de forma que sólo se dejen las aplicaciones, servicios y puertos realmente necesarios.

Asegurar un servidor

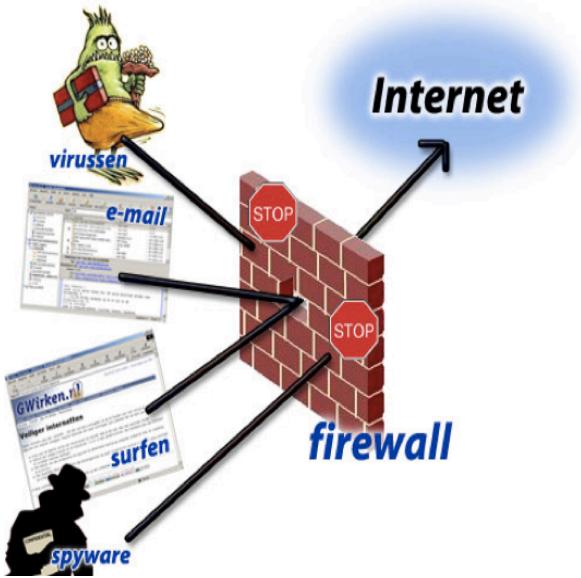
Dos fases:

(1) una vez que el servidor ha sido montado hacer **cambios de configuración** (instalación limpia).

- Eliminar cuentas y grupos de usuarios no necesarios
- Renombrar las cuentas de administrador e invitado
- Eliminar servicios no necesarios
- Poner filtros TCP/IP
- Equipo de seguridad al día

(2) mantenimiento continuo para proteger de los ataques que van surgiendo.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Cortafuegos

Un cortafuegos protege el sistema de accesos indebidos.

En un sistema sin cortafuegos, otros elementos del sistema quedarán expuestos a diferentes riesgos.

Es el guardián de la puerta al sistema, permitiendo el tráfico autorizado y denegando el resto.



Cortafuegos

El cortafuegos más efectivo:



Cortafuegos

Colocados entre subredes para realizar diferentes tareas de manejo de paquetes.

Tareas que realizan:

- **Bloquear y filtrar paquetes** de red inspeccionando las direcciones y puertos de cada paquete enviado entre las subredes que separa y controla.
Por defecto, un cortafuegos debería prohibir el tráfico, y en el proceso de configuración se establecerán reglas para permitir cierto tipo de tráfico.

Cortafuegos

Tareas que realizan:

- **Controlar protocolos de aplicación**, como HTTP, FTP, ssh o telnet. Esto se consigue configurando reglas relativas a ciertos puertos.
- **Control del tráfico de red a nivel de protocolo de red** (TCP o UDP). Así, si las reglas permiten la comunicación entre dos servidores, el tráfico (paquetes) fluirán entre ambos mientras la conexión permanezca abierta.

Cortafuegos

Tareas que realizan:

- **Ocultar la verdadera dirección del servidor**, actuando como un proxy. De esta forma traduce la información de dirección de los mensajes entrantes y salientes reenviándolos a su destino.
- **Proteger los servidores y aplicaciones de ataques y uso indebido** controlando el flujo de información. Sin el cortafuegos, todos los servidores de la red serían accesibles para cualquier usuario

Cortafuegos

La implementación y configuración del cortafuegos es **compleja**, pero aporta beneficios:

- Evita el consumo excesivo de recursos, reduciendo el tráfico global que un servidor recibirá.
- Oculta los servidores finales a otras redes.
- Protege los servidores de múltiples ataques.
- Oculta información de los servidores a otras redes (evitamos escaneo de puertos).
- Avisa de posibles ataques.

Cortafuegos

Construir el conjunto de reglas de la siguiente forma:

- Crear grupos de reglas para conjuntos de servidores que deben responder a diferente tipo de tráfico.
- **Por defecto**, establecer reglas para **denegar el tráfico** que no esté permitido explícitamente.
- **Permitir el tráfico en el sentido necesario** (un servidor web no necesita navegar por Internet).

Cortafuegos

Recomendaciones:

1. Configurar el cortafuegos completamente independiente del resto de recursos.
2. La máquina cortafuegos no debe ejecutar otro software salvo el del cortafuegos.
3. Eliminar cualquier servicio accesorio en el cortafuegos.

Cortafuegos

Recomendaciones:

4. Blindar el cortafuegos para que no acepte conexiones directas a él (se comporte como un paso más en el camino y el atacante no se dé cuenta de que está ahí).
5. No registrar la IP del cortafuegos en ningún servicio de DNS, ya que su IP no es necesaria para que los clientes accedan a la granja web.
6. No permitir acceso desde Internet para administrar el cortafuegos, ya que un hacker podría conseguir acceso al mismo → VPN

Cortafuegos

Configurar el cortafuegos en Linux con iptables

<http://www.cyberciti.biz/tips/linux-iptables-examples.html>

<http://bit.ly/17Vqwi3>

http://www.linuxtotal.com.mx/?cont=info_seyre_002

<https://openwebinars.net/como-configurar-en-linux-firewall-basico-con-iptables/>

<http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/>

Configurar el cortafuegos en Linux con ufw

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-16-04>

<https://ubuntuforums.org/showthread.php?t=1876124>

Usar nmap

<http://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know/>

<https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/>

Configurar el cortafuegos con iptables

(proteger un servidor web):

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

```
iptables -t nat -F
```

Eliminar todas las
reglas (configuración
 limpia)

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

Política por defecto:
denegar todo el
tráfico

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```

Permitir cualquier
acceso desde localhost
(interface lo)

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
```

Abrir los puertos
HTTP (80) de
servidor web

Configurar el cortafuegos con iptables

(reiniciar configuración):

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

```
iptables -t nat -F
```

Eliminar todas las
reglas (configuración
 limpia)

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

Permitir cualquier
acceso (todo el tráfico
está permitido)

```
iptables -L -n -v
```

Examinar las reglas
que hay establecidas

Cortafuegos: iptables

Configurar el cortafuegos con iptables (ejemplos):

Examinar las reglas configuradas en este momento:

```
iptables -L -n -v
```

Guardar/restaurar las reglas configuradas en este momento:

```
iptables-save > ~/reglas.iptables  
iptables-restore < ~/reglas.iptables
```

Evitar el acceso a www.facebook.com:

```
iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
```

También se puede usar el nombre de dominio:

```
iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP  
iptables -A OUTPUT -p tcp -d facebook.com -j DROP
```

Cortafuegos: ufw

Configurar el cortafuegos con ufw:

Para hacer una configuración lo más segura posible, dejando acceso a SSH, HTTP, HTTPS:

```
ufw default deny incoming  
ufw default allow outgoing  
ufw allow ssh  
ufw enable  
ufw allow http  
ufw allow https  
ufw status verbose
```

Para comprobar la configuración de la red, podemos usar netstat, lsof, nc, nmap

```
netstat -natopu  
lsof -i -P -n  
nc -vn -w 1 105.21.19.6 22  
nmap 105.21.19.6  
nmap -O 105.21.19.6  
nmap -sL 105.21.19.0/24
```

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Comprobación del funcionamiento del cortafuegos

Con la siguiente orden, comprobaremos qué puertos hay abiertos y cuáles cerrados:

```
netstat -tulpn
```

Para asegurarnos del estado del puerto 80 (abierto/cerrado), ejecutar:

```
netstat -tulpn | grep :80
```

Para ver las conexiones abiertas en el puerto 80 ejecutar:

```
netstat -an | grep :80 | sort
```

```
netstat | grep http | wc -l
```

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Comprobación del funcionamiento del cortafuegos

```
[jmsoto@m3-jmsoto:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 0.0.0.0:80                0.0.0.0:*              LISTEN    820/nginx: master p
tcp      0      0 127.0.0.53:53              0.0.0.0:*              LISTEN    656/systemd-resolve
tcp      0      0 0.0.0.0:22                0.0.0.0:*              LISTEN    816/sshd
tcp      0      0 0.0.0.0:443               0.0.0.0:*              LISTEN    820/nginx: master p
tcp6     0      0 :::22                   ::::*                  LISTEN    816/sshd
udp      0      0 127.0.0.53:53              0.0.0.0:*              LISTEN    656/systemd-resolve
udp      0      0 192.168.56.103:68            0.0.0.0:*              LISTEN    654/systemd-network
udp      0      0 10.0.2.15:68                0.0.0.0:*              LISTEN    654/systemd-network
[jmsoto@m3-jmsoto:~$ 
[jmsoto@m3-jmsoto:~$ 
[jmsoto@m3-jmsoto:~$ sudo netstat -tulpn | grep :80
tcp      0      0 0.0.0.0:80                0.0.0.0:*              LISTEN    820/nginx: master p
```

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Comprobación del funcionamiento del cortafuegos

```
[jmsoto@m1-jmsoto:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp    0      0 0.0.0.0:111                0.0.0.0:*
                                         LISTEN     464/rpcbind
tcp    0      0 127.0.0.53:53              0.0.0.0:*
                                         LISTEN     647/systemd-resolve
tcp    0      0 0.0.0.0:22                0.0.0.0:*
                                         LISTEN     804/sshd
tcp6   0      0 :::111                   ::::*
                                         LISTEN     464/rpcbind
tcp6   0      0 :::80                    ::::*
                                         LISTEN     845/apache2
tcp6   0      0 :::22                    ::::*
                                         LISTEN     804/sshd
tcp6   0      0 :::443                  ::::*
                                         LISTEN     845/apache2
tcp6   0      0 :::3306                 ::::*
                                         LISTEN     844/mysqld
udp    0      0 127.0.0.53:53              0.0.0.0:*
                                         LISTEN     647/systemd-resolve
udp    0      0 192.168.56.101:68            0.0.0.0:*
                                         LISTEN     646/systemd-network
udp    0      0 10.0.2.15:68               0.0.0.0:*
                                         LISTEN     646/systemd-network
udp    0      0 0.0.0.0:111                0.0.0.0:*
                                         LISTEN     464/rpcbind
udp    0      0 0.0.0.0:640                0.0.0.0:*
                                         LISTEN     464/rpcbind
udp6   0      0 :::111                   ::::*
                                         LISTEN     464/rpcbind
udp6   0      0 ::::640                 ::::*
```



Índice

1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Evitar otros tipos de ataques

El balanceador de carga puede evitar cierto tipo de ataques:

- denegación de servicio
- TCP SYN
- *ping of death*
- *Teardrop*
- *Smurf*
- *IP spoofing*
- Phishing

Para saber más sobre el funcionamiento de estos ataques:

https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
http://es.ciberseguridad.wikia.com/wiki/Ataques_TCP/IP

Tipos de ataques

Denegación de servicio:

- denegación de servicio por saturación
- denegación de servicio por explotación de vulnerabilidades

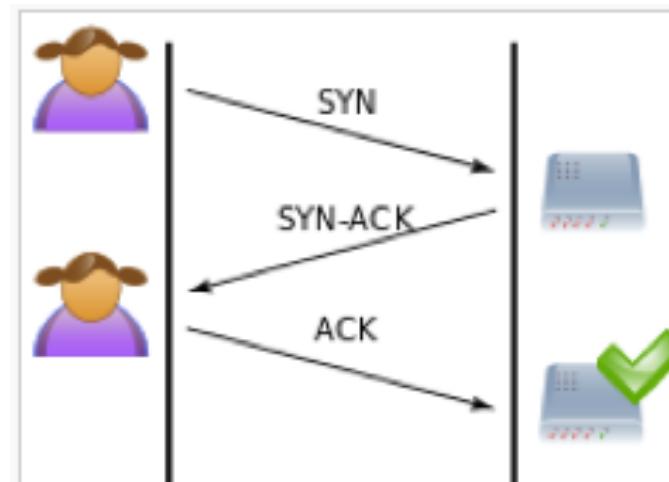
Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos raros que saturan los equipos de destino o los vuelven inestables.

DDoS, Distributed Denial of Service: sistema distribuido de denegación de servicio (participan varios equipos en la denegación de servicio).

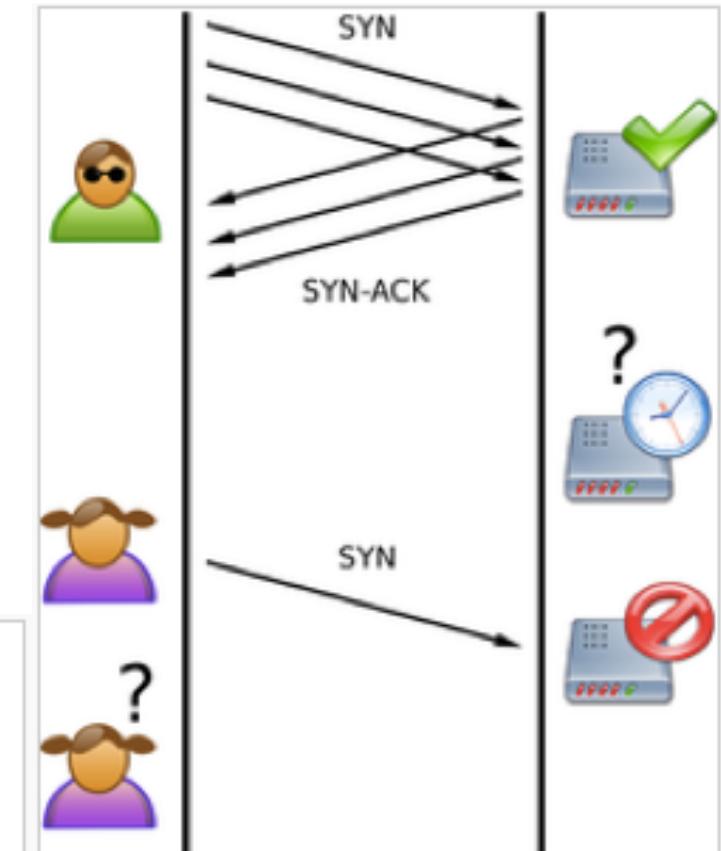
Tipos de ataques

TCP SYN o SYN flood (denegación de servicio):

Saturar el tráfico de la red aprovechando el mecanismo de negociación de tres vías del protocolo TCP.



A normal connection between a user (Alice) and a server. The three-way handshake is correctly performed.



SYN Flood. The attacker (Mallory) sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

Tipos de ataques

TCP SYN o SYN flood:

aprovecha el mecanismo de negociación de tres vías del protocolo TCP:

Se envía una gran cantidad de solicitudes SYN a través de un ordenador con una dirección IP inexistente o no válida, de forma que el equipo atacado no puede recibir un paquete ACK. Así, quedarán las conexiones abiertas en cola en la estructura de memoria esperando la recepción de un paquete ACK.

Tipos de ataques

Ping de la muerte (ping of death):

El principio de este ataque consiste simplemente en crear un datagrama IP cuyo tamaño total supere el máximo autorizado (65.536 bytes). Cuando un paquete con estas características se envía a un sistema que contiene una pila vulnerable de protocolos TCP/IP, éste produce la caída del sistema.

Los sistemas actuales ya no son vulnerables a este ataque.

Tipos de ataques

Ataque por fragmentación (teardrop):

Se aprovecha del protocolo para fragmentar paquetes grandes en varios paquetes IP más pequeños. Cada uno de ellos tiene un número de secuencia y un número de identificación común para ensamblarlos.

El ataque se basa en introducir información falsa en los paquetes fragmentados para que queden fragmentos vacíos o superpuestos que pueden desestabilizar el sistema.

Los sistemas actuales ya no son vulnerables a esto.

Tipos de ataques

Ataque pitufo (Smurf):

Se basa en el uso de servidores de difusión (capacidad de duplicar un mensaje y enviarlo a todos los equipos de una misma red).

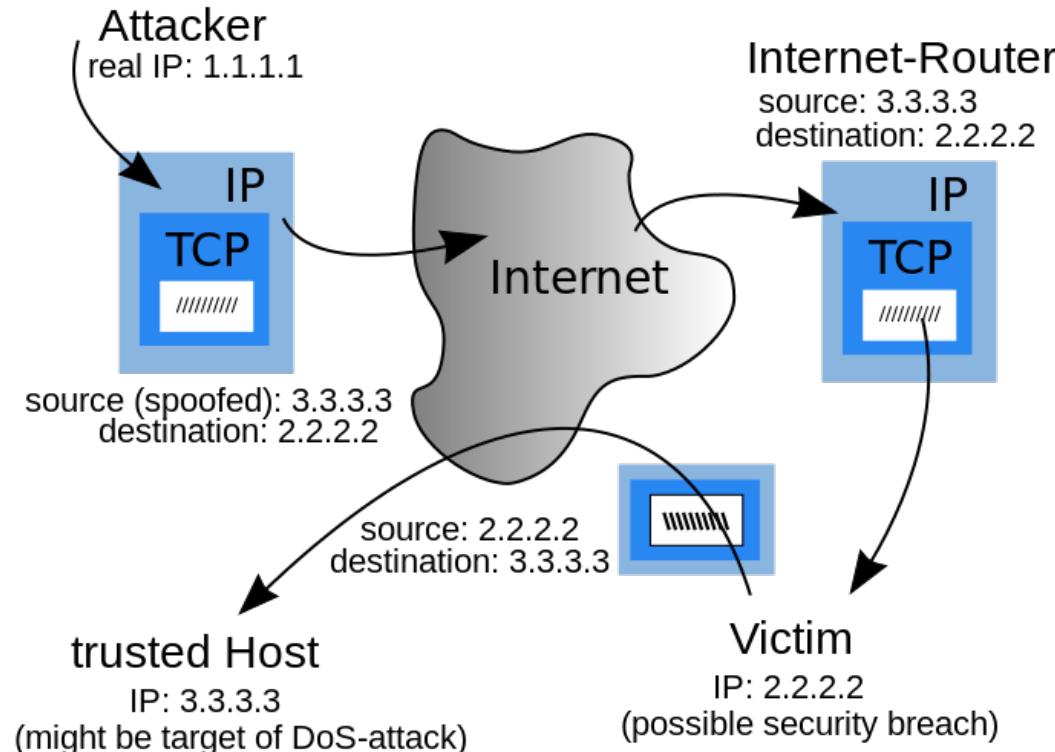
El equipo atacante envía una solicitud de ping a varios servidores de difusión falsificando las direcciones IP de origen y proporciona la dirección IP de un equipo de destino (atacado). El servidor transmite la solicitud a toda la red. Todos los equipos de la red envían una respuesta al servidor de difusión, que redirecciona las respuestas al equipo de destino.

Tipos de ataques

IP spoofing:

Consiste en crear paquetes con la IP de origen falsa.

Así se consigue que las respuestas que genere el equipo de destino vayan a otro equipo (el objetivo del ataque).



Tipos de ataques

Suplantación de identidad (Phishing):

Es una técnica de "ingeniería social", lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un "fallo humano" al engañar a los usuarios de Internet con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página Web bancaria o corporativa.

¿Cómo de difícil es hacer un ataque?

¿Alguien ha pensado en hacer un ataque?

Código C:

<http://www.binarytides.com/syn-flood-dos-attack/>

```
118 //Uncomment the loop if you want to flood :)
119 //while (1)
120 //{
121     //Send the packet
122     if (sendto (s,      /* our socket */
123                 datagram, /* the buffer containing
```

Código Perl:

<http://www.binarytides.com/perl-syn-flood-program-raw-sockets-linux/>

La herramienta hping:

<http://www.binarytides.com/tcp-syn-flood-dos-attack-with-hping/>

```
sudo apt-get install hping3
```

```
sudo hping3 -i u1 -S -p 80 192.168.1.1
```

Evitar otros tipos de ataques

El balanceador puede mantener **listas negras**.

Limitar o denegar completamente el acceso a listas de IP monitorizando el origen, destino o puerto del tráfico.

Se pueden incluir **rangos completos de IP**.

Se pueden evitar ataques de sitios concretos, actuando como sistema adicional de detección de intrusos.

Evitar otros tipos de ataques

Posibilidad de **crear listas de control de acceso** (access control list, ACL) y realizar filtrado a partir de ellas.

Definir las aplicaciones (servicios o puertos) a los que puede acceder un grupo. El administrador de red puede permitir o denegar el acceso a ciertas funcionalidades (aplicaciones) a rangos de IP.

- El balanceador sólo **complementa/ayuda al cortafuegos**, ya que tiene capacidad limitada para bloquear o filtrar.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Prácticas de seguridad recomendadas

Copias de seguridad:

 menéame ▾ login registrarse ☰

183 meneos
menéalo
2568 clics

Gitlab.com fundido por borrar un directorio incorrecto, los backups fallan [ENG]

por **ccguy** a **theregister.co.uk** 09:08
publicado: 11:50



Gitlab.com, una empresa de gestión de código fuente, ha perdido datos de producción. Un administrador cansado ejecutó un rm -rf sobre un directorio incorrecto que contenía 300 GB. Cuando se dio cuenta sólo quedaban 4.5 GB de datos. Los sistemas de backups que tienen no estaban probados y no han servido para nada. Se están recuperando los datos de un snapshot con algunas horas de antigüedad que además no es completo. La pérdida afecta a la base de datos (incidencias y merge requests) pero no a los repositorios.

etiquetas: gitlab, rm, backup, directorio, datos

Prácticas de seguridad recomendadas

Copias de seguridad:

Tener un sistema de **copias de seguridad automatizado** es indispensable para asegurar la disponibilidad de los datos en nuestro sistema.

El software de copia de seguridad debe verificar los datos una vez grabados.

Las copias de seguridad deben guardarse en un lugar seguro, en un local diferente al que alberga los servidores.

Prácticas de seguridad

Copias de seguridad:



Ejemplos de funcionamiento:

<https://www.youtube.com/watch?v=d-eWDuEo-3Q>

<https://www.youtube.com/watch?v=GwMn7YpF8r8>

Prácticas de seguridad recomendadas

Imágenes de los servidores:

También conviene disponer de **imágenes de instalación** de los propios sistemas.

Podremos restaurar una máquina rápida y fácilmente.

Opciones: desde usar el comando dd de Linux hasta usar software propietario como Intelligent Disaster Recovery (Veritas Backup-Exec) o Take Two (Adaptec).

Prácticas de seguridad recomendadas

Imágenes de los servidores. Intelligent Disaster Recovery

Backup Exec Intelligent Disaster Recovery
for Windows (2000/XP/Server 2003/Vista/7/Server 2008/Server 2008 R2)
Copyright (c) 2011 Symantec Corporation. All rights reserved.

You have successfully loaded a Backup Exec Disaster Recovery CD/Tape image.

If you are testing the bootable media, the computer successfully booted the image. Remove the boot media and press <Esc> to stop the recovery.
DO NOT PRESS <ENTER>.

If you are performing a disaster recovery, press <Enter> to start the disaster recovery process, which will repartition and reformat the computer's hard disks and **DESTROY ALL EXISTING DATA**. The Windows setup program and the Backup Exec Disaster Recovery Wizard are then loaded.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
- [8. Conclusiones]**

Conclusiones

El éxito de un sitio web depende de la seguridad.

La seguridad no se puede pasar por alto !

Aspecto crítico en un sistema web para mantener a salvo de ataques los recursos de la empresa.

Hay que establecer unas **políticas de seguridad**, y **mantenerse al día** de vulnerabilidades del software, de posibles ataques, de actualizaciones de software, etc.

Conclusiones

La defensa en profundidad implica mantener diferentes capas de seguridad, independientes entre ellas, de forma que si un atacante consigue pasar una, tendrá otra que superar.

Así se dificulta en gran medida la consecución final de un ataque.

Se diseñarán **diferentes tipos de acceso** y se configurará el sistema para facilitar esos accesos exclusivamente, denegando cualquier otro.