Taxonomia de la Banca Mexicana en Linea:

Amenazas y Mitigacion

Juan Carlos Guel Lopez

Temas

* Introducción

* El problema

* Elementos del problema

* Resultados

* Conclusiones

* Anexos

Introducción

* En la actualidad, cualquier computadora conectada a Internet es potencialmente blanco de un ataque.

* Existen varios factores que pueden afectar los ambientes de cómputo de las organizaciones y usuarios.

* Uno de estos factores: **La gestión del riesgo,** que se ha convertido en un problema para las organizaciones

* Especialmente complicado gestionar el riesgo en aquellas empresas cuyos procesos críticos reposan en tecnologías de la información, un ejemplo claro lo es la Banca en Línea.

Introducción

* Es necesario llegar a un equilibrio en la organización entre inversión y riesgo asumido voluntariamente, y éste es el objetivo principal de la gestión de los riesgos.

* Parte de este estudio se realizo para determinar el riesgo actual de la Banca Mexicana en línea y estudiar posibles soluciones con las cuales se puede ayudar a disminuir y gestionar la administración del riesgo en este sector.

Introducción

* En el estudio académico sobre la Banca en Línea en México fue realizado en diversas etapas y es un trabajo continuo.

1a. Etapa. Realizada en un período de cuatro meses efectuado del mes de Enero al mes de junio del 2005 por UNAM-CERT. Este estudio incluye a 25 instituciones financieras.

2da. Etapa. Análisis de tecnología existente (Teclados virtuales). Sept. 2005

3a. Etapa. Propuesta creación de Centro de Mando virtual conjuntamente con los Bancos, Policía y UNAM-CERT. (Oct. 2005)

Introducción

* La finalidad de este estudio no es proyectar alguna debilidad de las instituciones financieras, el presente documento analiza amenazas que podrían estar fuera de su alcance,

* Así mismo pretende fomentar e impulsar la creación de mecanismos de comunicación y coordinación para reducir los riesgos que impactan a las instituciones y anticipar a las nuevas formas del delito cibernético, así como la adopción de nuevas tecnologías en las organizaciones financieras.

Elementos del Problema

* El presente estudio se realizo tomando en cuenta las distintas amenazas existentes en Internet hoy en día como son:

- Key loggers. Son herramientas diseñadas para capturar todas las teclas ejecutadas, incluyendo contraseñas, nombre de usuario.

- Phishing Scam. Generalmente un intento por conseguir que un usuario confirme información personal como una cuenta bancaria, tarjeta de crédito o numero de servicio social.

Elementos del Problema (2)

* El estudio fue basado en el listado instituciones financieras disponible en la pagina de la Asociación de Bancos de México y se tomo en cuenta únicamente a aquellas instituciones bancarias que mantienen sitios Web o banca electrónica en México.

* Las pruebas realizadas, están basadas en pruebas realizadas en ambientes controlados desde los laboratorios de seguridad del Departamento de Seguridad y del UNAM-CERT. Es importante señalar que ***No son pruebas intrusivas*** y fueron ejecutadas desde 2 equipos Pentium IV con 512 MB en RAM, ejecutando sistemas operativos Windows y Linux.

Herramientas Utilizadas

* Navegadores: Internet Explorer, Mozilla y Firefox.

* Algunas de las herramientas y utilerías utilizadas son:

- host: Utilidad DNS lookup

```
$ host google.com
google.com has address 216.239.57.99
```

-Traceroute: Imprime la ruta que toman los paquetes a un host.

```
$ traceroute google.com
traceroute to google.com (216.239.39.99), 30 hops max, 38 byte packets
1  132.248.103.253 (132.248.103.253)  0.595 ms  0.424 ms  0.401 ms
2  * 132.248.103.254 (132.248.103.254)  1.501 ms  1.219 ms
```

- nslookup: Solicitud de nombres de Internet interactivo.

```
$ nslookup google.com
Non-authoritative answer
Name:   google.com
Address: 216.239.37.99
```

Herramientas Utilizadas (2)

* whois : Cliente para servicio Whois

    $ whois google

    [Preguntando whois.internic.net]

*Plushs –Pluf Simple escaneador de nombres de host en redes.

    192.168.78.1 ==> mail.dominio.com.mx

    192.168.78.2 ==> nomina.dominio.com.mx

    …

    192.168.78.253 ==> boveda.dominio.com.mx

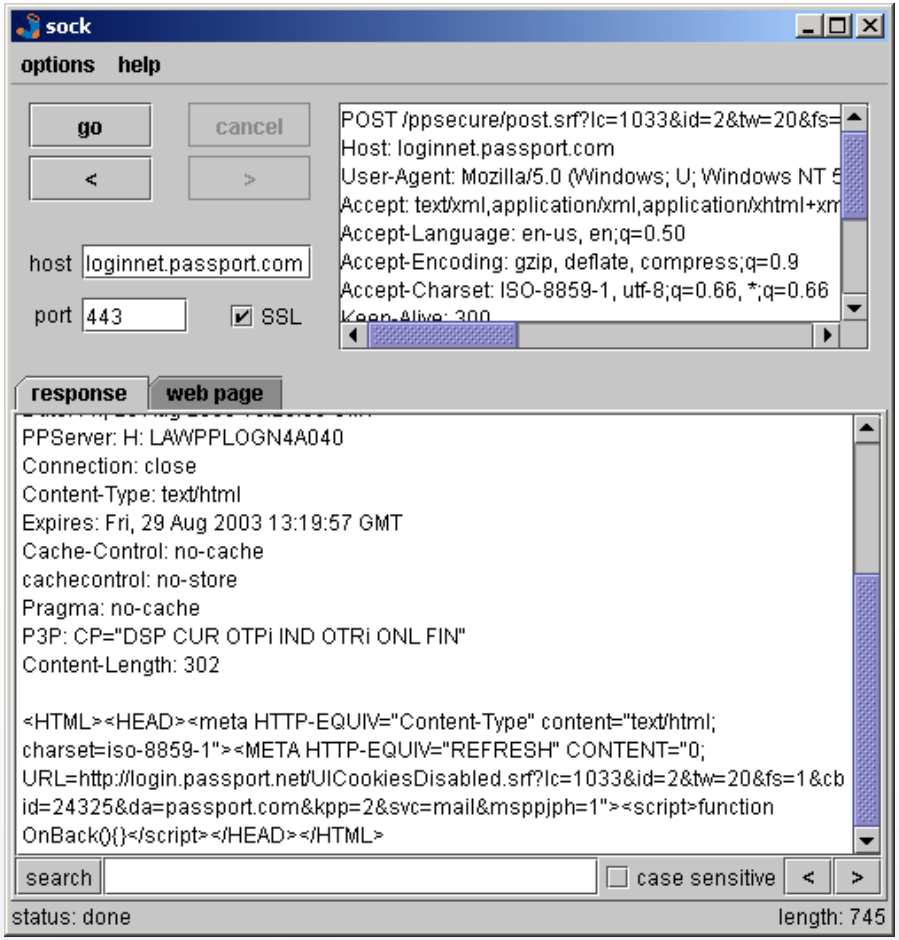
    192.168.78.254 ==> router.dominio.com.mx

* Netcat: Conexiones y escuchas arbitrarios de TCP Y UDP.

    nc 192.168.74.84 22

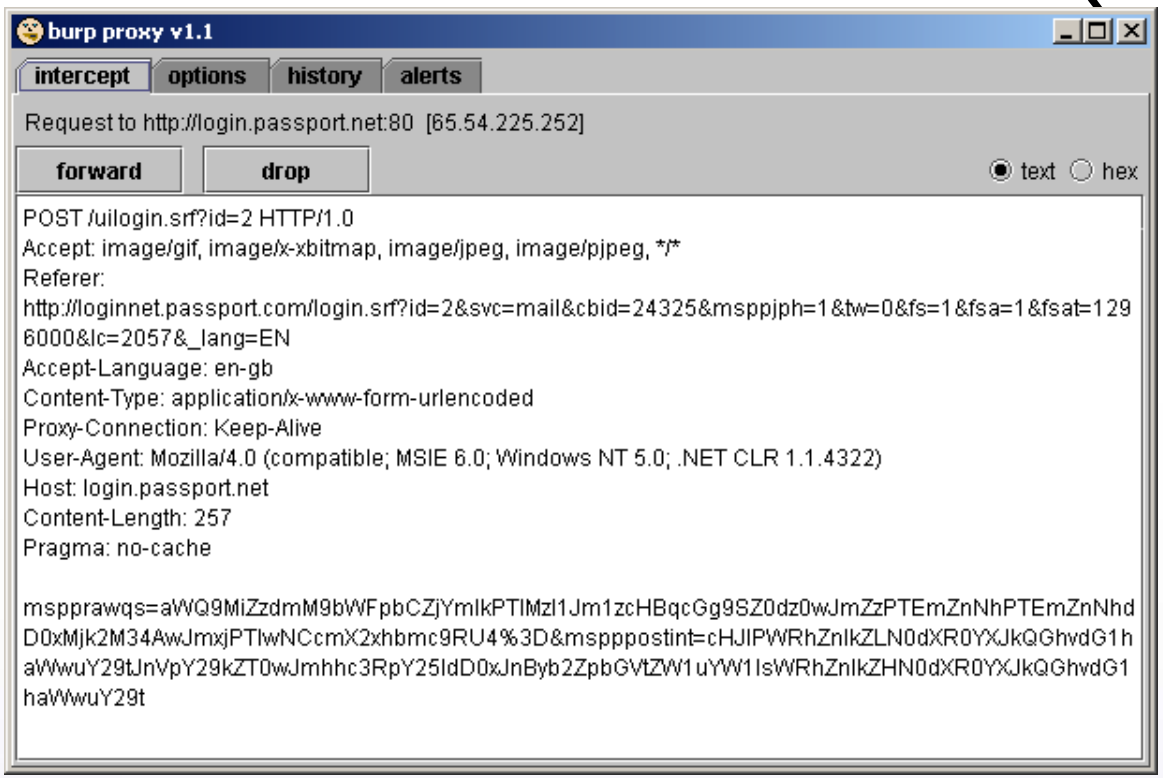
* SSH-1.99-OpenSSH_3.9

Herramientas Utilizadas (3)



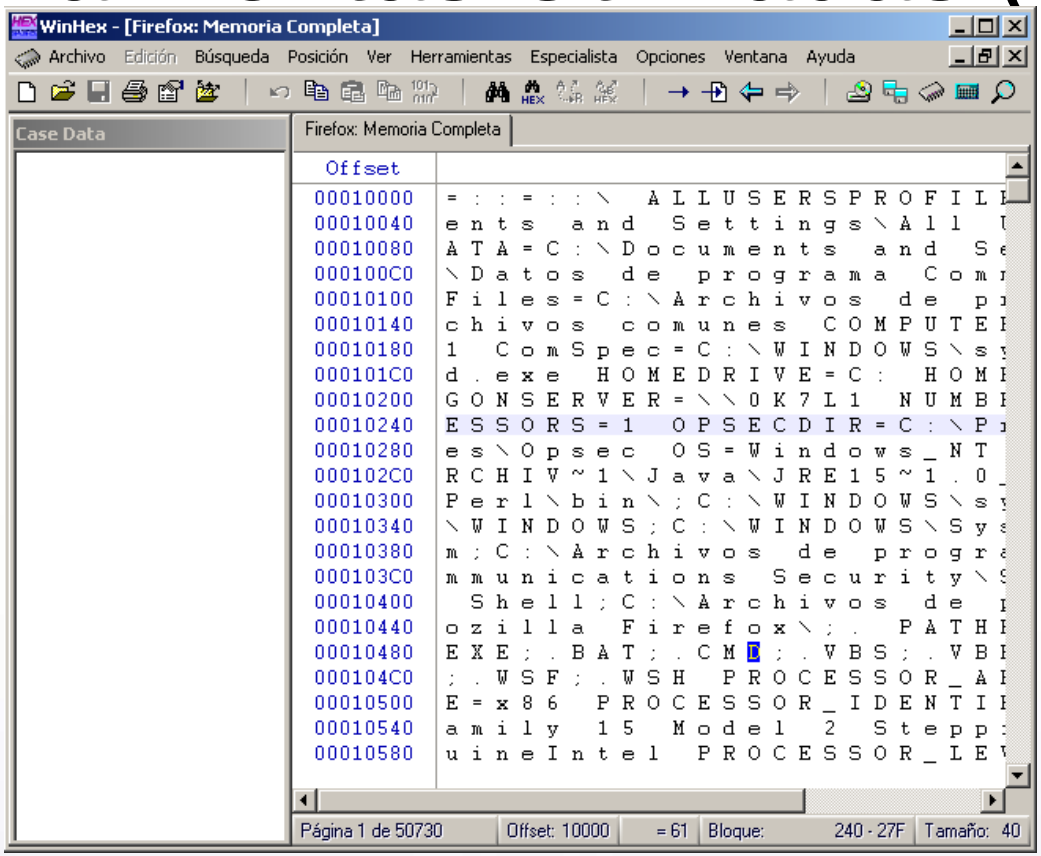
- Sock. Herramienta simple para atacar manualmente aplicaciones basadas en web. Este permite una simple solicitud http/s que es manipulada y republicada repetidamente de la misma ventana.

Herramientas Utilizadas (4)



* Burp Proxy. Un servidor Proxy interactivo para atacar y analizar aplicaciones basadas en web este opera como man-in-the-middle entre el navegador y el sitio web y permite interceptar, modificar e inspeccionar el trafico entre ambos.

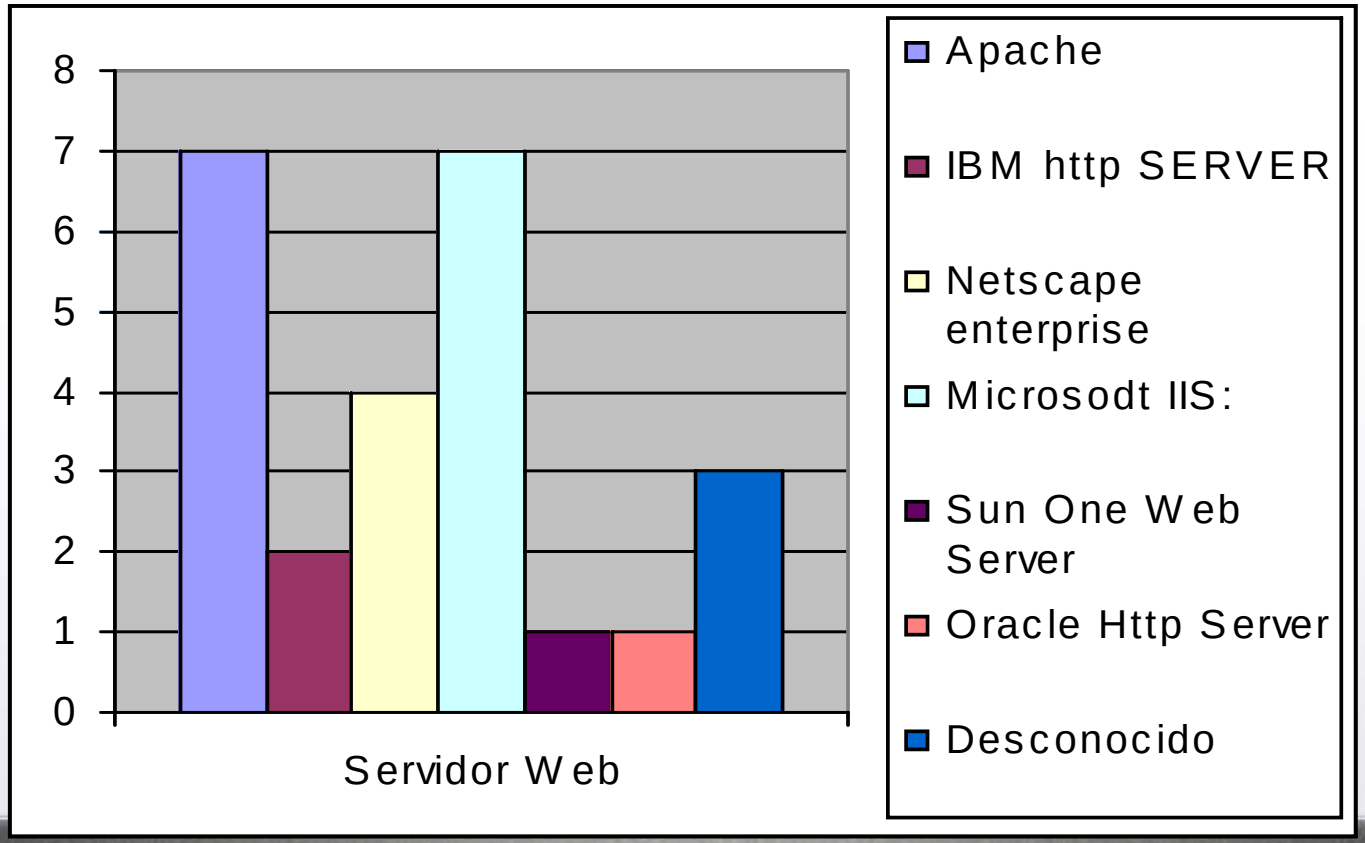
Herramientas Utilizadas (5)



* WinHex. Es un editor hexadecimal permite editar discos, RAM lo que permite editar otros procesos, memoria virtual, analizar y comparar archivos, una excelente herramienta para análisis forense.

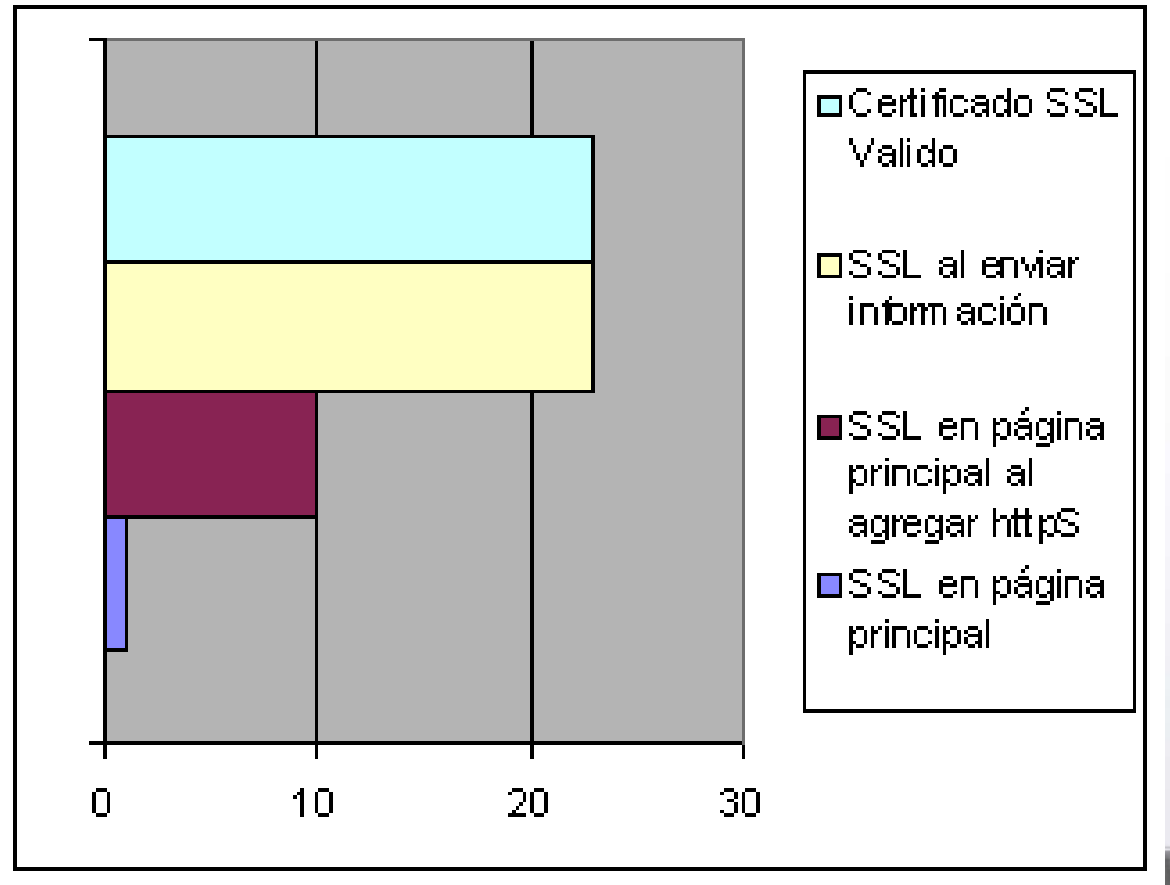
Resultados Encontrados

* Versión de Servidor Web. Uno de los pasos para conocer sobre vulnerabilidades especificas que pueda tener un servidor web es a través de la versión del servicio.



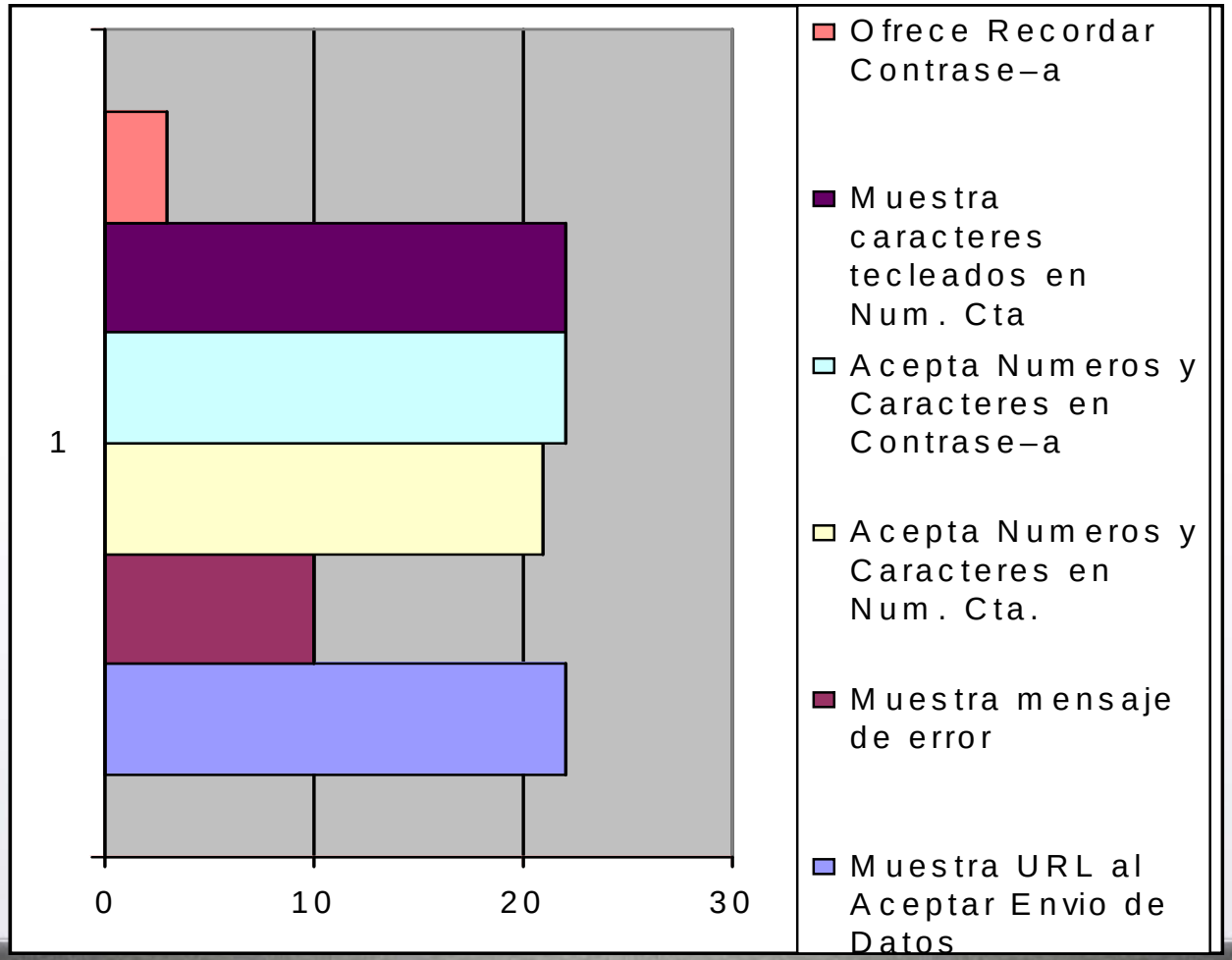
Resultados Encontrados (2)

* SSL: Muchos sitios web utilizan SSL para obtener información confidencial como números de tarjetas de crédito.



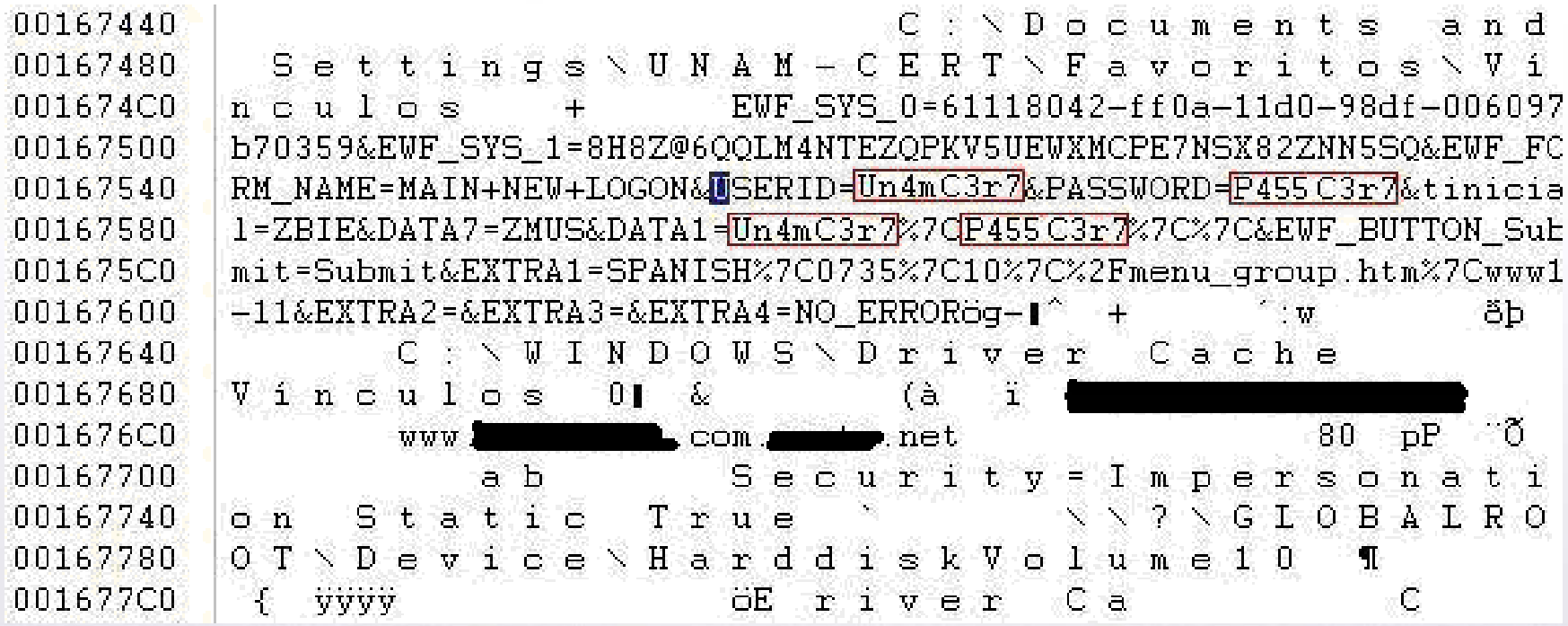
Resultados Encontrados (3)

Número de cuenta y contraseña



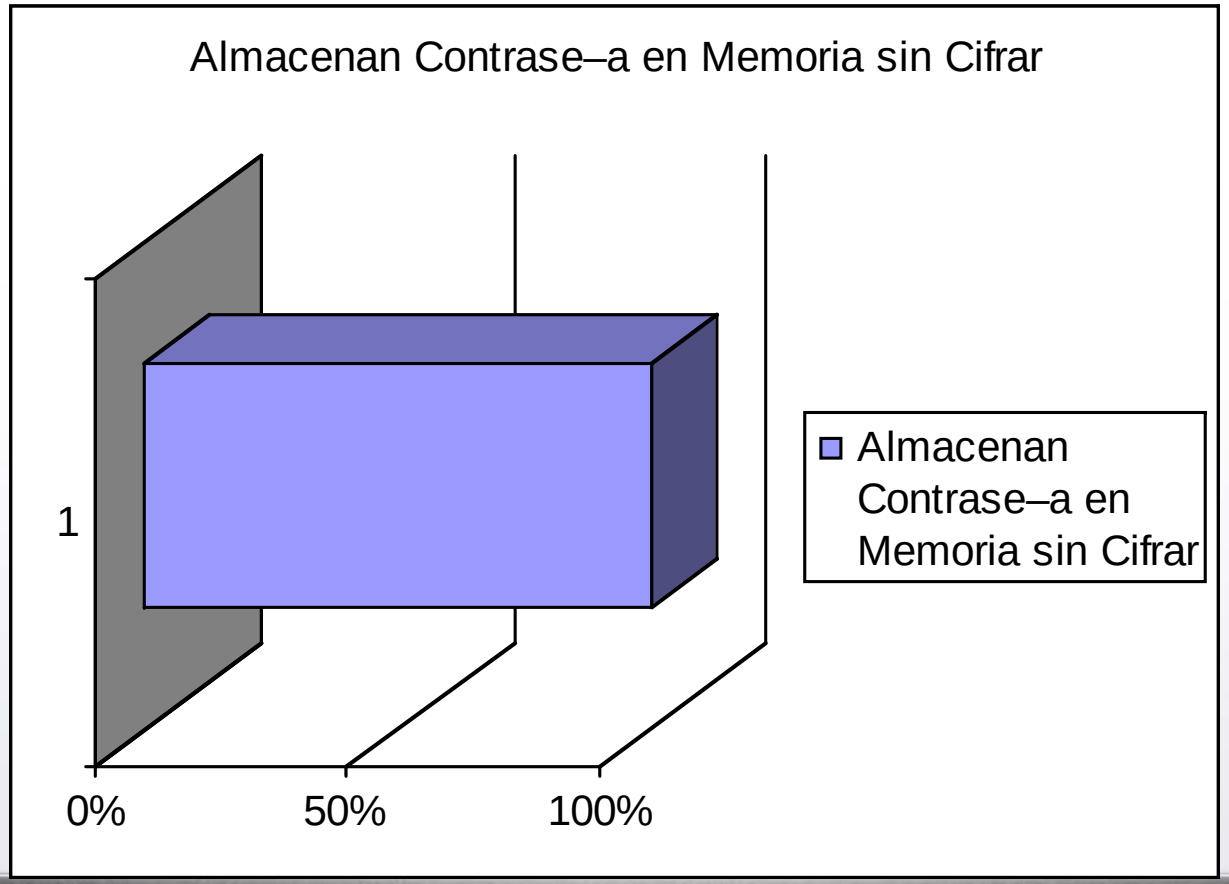
Resultados Encontrados (4)

Cualquier atacante que obtenga acceso al sistema podría leer la información en memoria y realizar búsquedas de contraseñas que se encuentren almacenadas por los navegadores de Internet, mediante un troyano, shell remoto realizando un vaciado de memoria.



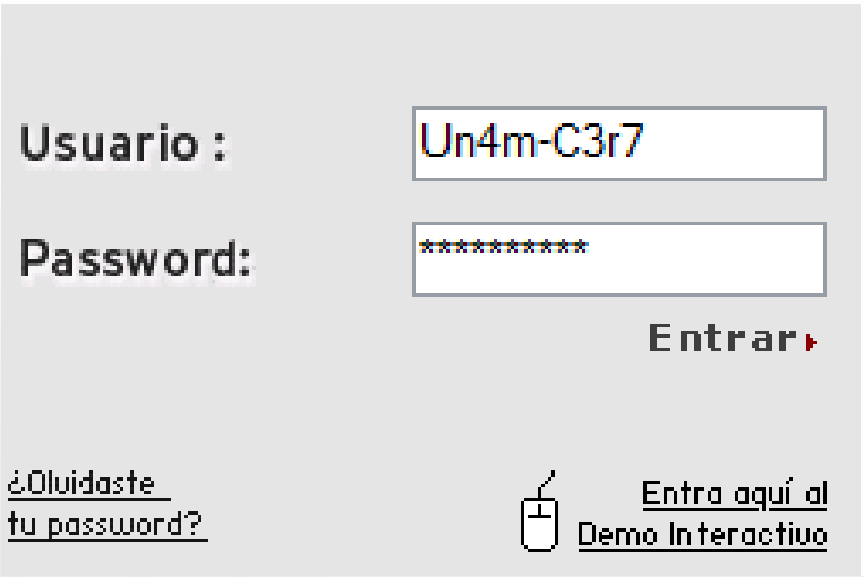
Resultados Encontrados (5)

Almacenamiento de contraseñas en memoria.



Resultados Encontrados (6)

Teclado Virtual



Resultados Encontrados (7)

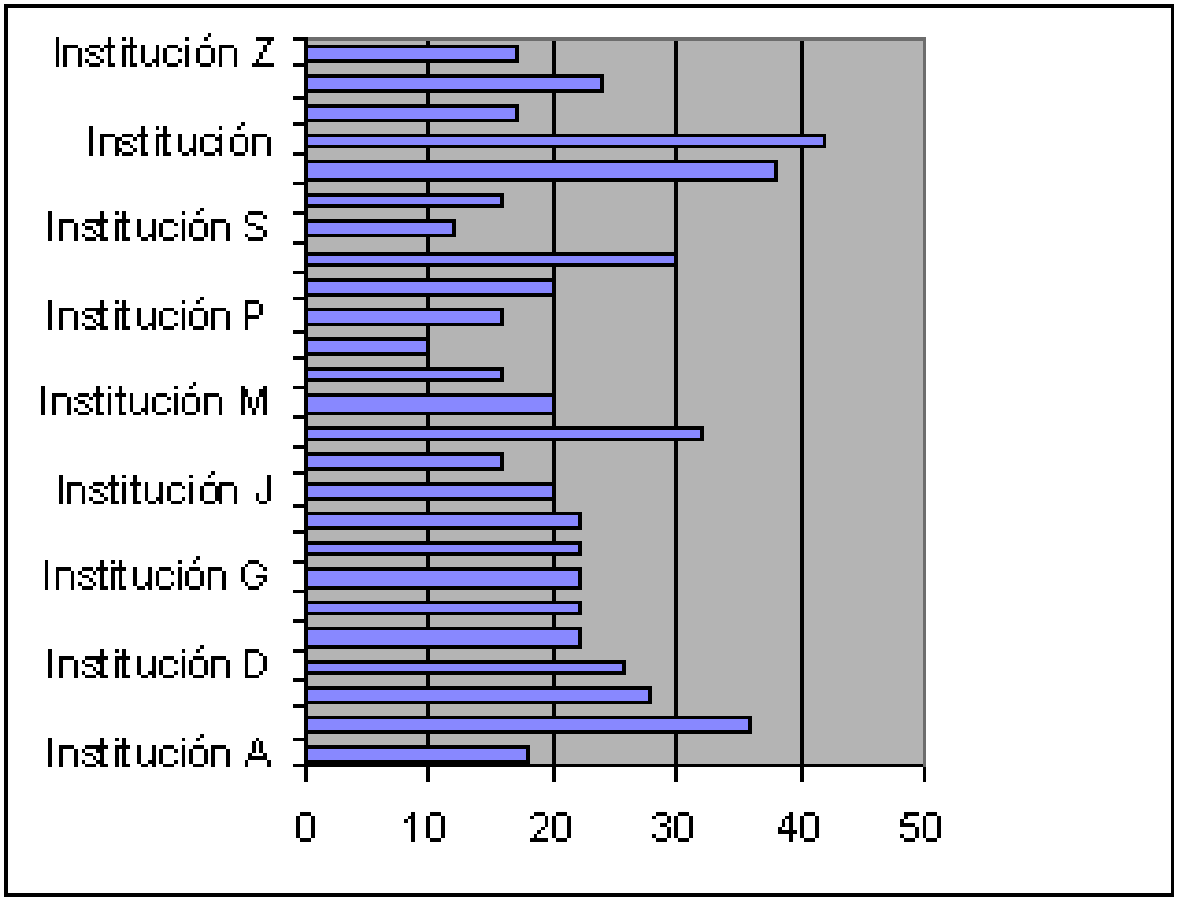
Domain Name Typo Generator

Toma el dominio especificado y crea una lista de dominios similares que podrían ser erróneamente tecleados para ese dominio.

foogle.com
hoogle.com
giogle.com
gpogle.com
goigle.com
gopgle.com
goofle.com
goohle.com
googke.com
googoe.com
googlr.com
googlw.com

Resultados Encontrados (8)

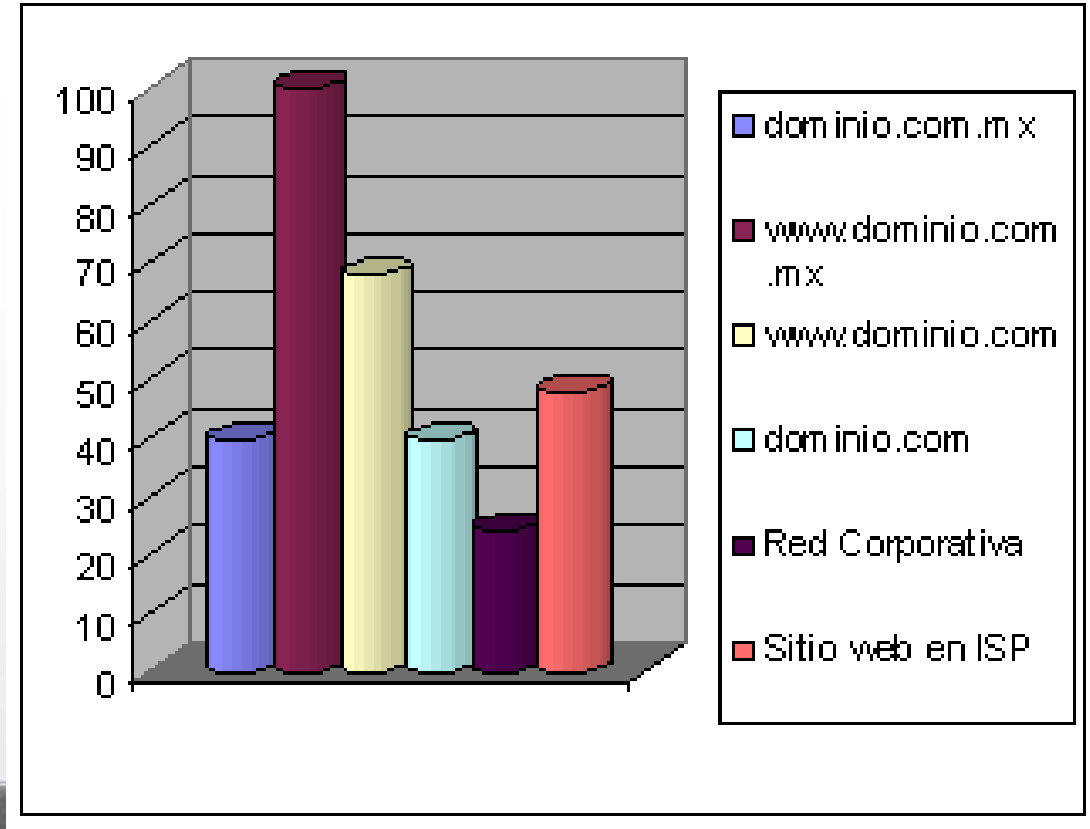
Domain Name Typo Generator - Dominios Generados



Resultados Encontrados (9)

Nombres de Dominio

Los hostnames de las instituciones deberían apuntar a un solo dominio y no deberían existir equipos en el mismo dominio.



Propuestas de trabajo conjunto

* Reuniones Mensuales

* Análisis de Tecnología

* Propuesta de capacitación a personal técnico

*Creación Centro de Mando Virtual (Policía, Bancos y UNAM-CERT)

* Capacitación a Ministerio Publico para casos especificos relacionados a Fraudes Financieros

Propuestas de trabajo conjunto (2)

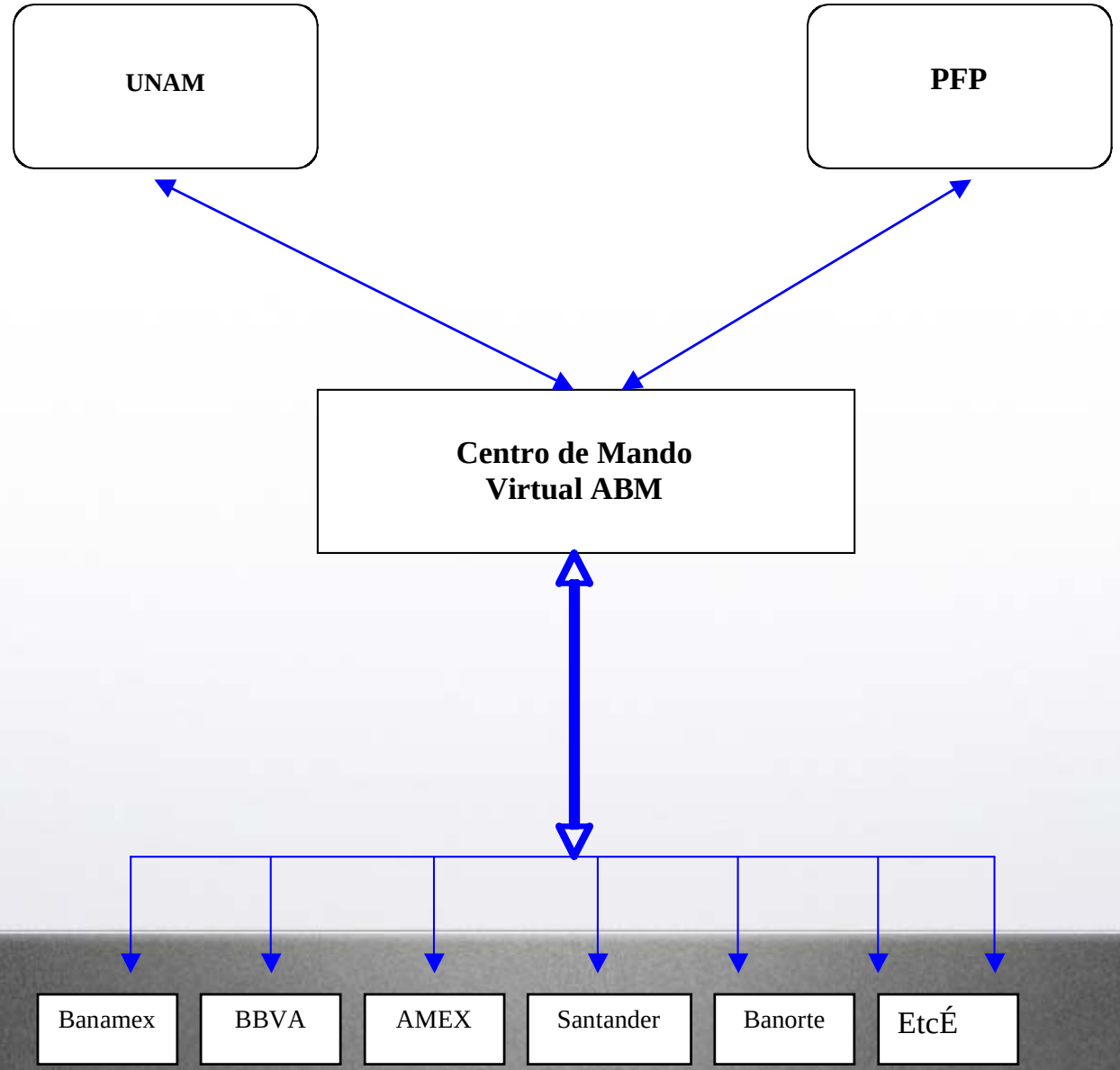
* Análisis de código Malicioso

* Intercambio de información y gestión de incidentes de seguridad.

* Generación de información enfocada al usuario final (Folletos en estados de cuenta, tips, como navegar seguro, etc).

* Impulsar por una legislación Informática

Propuestas de trabajo conjunto (3)



Propuestas de trabajo conjunto (4)

* Análisis de Tecnología de Teclado Virtual con personal técnico y Operativo de los Bancos

Conclusiones

* Gestión del riesgo en la Organización

* Implementación de mecanismos de seguridad en varios niveles.

* Implementar estándares de seguridad en la corporación. ISO1779, BS7799, ITIL.

* Implementación de análisis de riesgo y planes de contingencia.

* Implementar canales de información al usuario claros y concisos en la prevención del fraude.

Conclusiones (2)

* Crear su propio estándar mediante unión de todas las instituciones financieras.

* Compartir conocimiento y experiencias entre bancos

* Impulsar un IRT en las instituciones financieras.

* Evitar confusión al usuario final en creación de nuevos dominios.

* Analizar otros modelos P. Ej. Estándares en Bancos de UK.

Conclusiones (3)

* No olvidar que seguridad es un proceso en la organización

* Seguridad de la información es mucho más que la seguridad informática tradicional, y es fácilmente observable como, a la hora de hablar de seguridad de la información, en la que todo gira en torno a un eje temático: La gestión del riesgo.

* Entender que la adopción de estándares de seguridad provoca un cambio climático en nuestra organización y debemos entender nuestro entorno y adaptarnos a nuestro ecosistema.

¿¿Preguntas??

http://www.seguridad.unam.mx

http://www.cert.org.mx