***Tecnológico Nacional de México*** **

INSTITUTO TECNOLÓGICO DE SALINA CRUZ

**FUNDAMENTOS DE REDES**

**SEMESTRE AGOSTO-DICIEMBRE 2014**

**REPORTE DE PRÁCTICAS.**

**PRACTICA No. 2 CONSULTAR SANS**

**UNIDAD: PROTOCOLOS DE CAPAS SUPERIORES Y CAPA DE TRANSPORTE.**

**NOMBRE: ZARATE LÓPEZ LEONARDO**

**FECHA: 23 DE SEPTIEMBRE DEL 2014.**

**OBJETIVOS**

MOSTRAR EL FUNCIONAMIENTO DE LOS PROTOCOLOS DE APLICACIÓN.

**INSTRUCCIONES**

DAR A CONOCER LOS RECURSOS DE SANS, COMO TAMBIÉN LOS OBJETIVOS DE LA APLICACIÓN, IDENTIFICAR LOS PROTOCOLOS QUE USA SANS, POSTERIOR MENTE IDENTIFICAR LAS AMENAZAS MÁS RECIENTES DENTRO DE SANS.

**MATERIALES:**

Internet, Computadora.

**SANS**



¿Qué es SANS?

Una red de área de almacenamiento, en inglés SAN (*Storage Area Network*), es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

* Una red de alta velocidad de canal de fibra o iSCSI.
* Un equipo de interconexión dedicado (conmutadores, puentes, etc).
* Elementos de almacenamiento de red (discos duros).

SANS es la más confiable y con mucho, la fuente más grande de formación en seguridad en el mundo. Ofrecemos formación a través de varios métodos de entrega - vivir y, como un aula virtual, en línea a su propio ritmo o por Internet con instrucción en vivo, estudio guiado con un mentor local o en el sitio en su lugar de trabajo, donde incluso sus colegas más remotas pueden unirse a través de Simulcast .

Nuestros cursos de seguridad informática son desarrollados por líderes de la industria en numerosos campos, incluyendo la formación ciber seguridad, seguridad de red, análisis forense, auditoría, el liderazgo de seguridad, y la seguridad de aplicaciones. Los cursos son impartidos por profesionales del mundo real que son los mejores a garantizar no sólo aprender el material, pero que se pueden aplicar inmediatamente cuando regrese a la oficina. Además de la formación de primera categoría, le ofrecemos la certificación a través de GIAC, una filial del Instituto SANS, un organismo de certificación que ofrece más de 20 manos, certificaciones técnicas en seguridad de la información, y los programas de maestría opcional Grado a través de la escuela de posgrado Instituto Tecnológico SANS, como así como numerosos recursos de seguridad gratuitas, que incluyen boletines, documentos técnicos y webcasts.

Protocolos

Existen tres protocolos básicos usados en una red de área de almacenamiento:

* FC-AL
* FC-SW
* SCSI

FC-AL: Protocolo Fibre Channel Arbitrated Loop, usado en hubs, en el SAN hub este protocolo es el que se usa por excelencia, el protocolo controla quién puede comunicarse, sólo uno a la vez.

FC-SW: Protocolo Fibre Channel Switched, usado en switches, en este caso varias comunicaciones pueden ocurrir simultáneamente. El protocolo se encarga de conectar las comunicaciones entre dispositivos y evitar colisiones.

SCSI: Usado por las aplicaciones, es un protocolo usado para que una aplicación de un equipo se comunique con el dispositivo de almacenamiento. En la SAN, el SCSI se encapsula sobre FC-AL o FC-SW. SCSI trabaja diferente en una SAN que dentro de un servidor, SCSI fue originalmente diseñado para comunicarse dentro de un mismo servidor con los discos, usando cables de cobre.. Dentro de un servidor, los datos SCSI viajan en paralelo y en la SAN viajan serializados.

Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Una red de canal de fibra es muy rápida y no está agobiada por el tráfico de la red LAN de la empresa. Sin embargo, es muy cara. Las tarjetas de canal de fibra óptica cuestan alrededor de $ 1000.00 USD cada una. También requieren conmutadores especiales de canal de fibra. iSCSI es una nueva tecnología que envía comandos SCSI sobre una red TCP / IP. Este método no es tan rápido como una red Fibre Channel, pero ahorra costes, ya que utiliza un hardware de red menos costoso.

La mayoría de las SAN usa el protocolo SCSI para la comunicación entre los servidores y los dispositivos de almacenamiento, aunque no se haga uso de la interfaz física de bajo nivel. En su lugar se emplea una capa de mapeo, como el estándar FCP.

una SAN permite a varios servidores acceder a varios dispositivos de almacenamiento en una red compartida.

 

 SAN vs NAS vs DAS esquema



Posibles configuraciones híbridos sans-nas

**Las Top 25 errores de software se enumeran a continuación en tres categorías:**

* [**Software Error Categoría: Interacción insegura entre los componentes**](http://www.sans.org/top25-software-errors/#cat1)**(6 errores)**

### Interacción Inseguro Entre Componentes

Estas deficiencias están relacionadas con formas de inseguridad en que se envían y reciben datos entre distintos componentes, módulos, programas, procesos, hilos o sistemas.

| **CWE ID** | **Nombre** |
| --- | --- |
| [CWE-89](http://cwe.mitre.org/top25/index.html#CWE-89) | La neutralización inadecuada de elementos especiales utilizados en un comando SQL ('SQL Injection') |
| [CWE-78](http://cwe.mitre.org/top25/index.html#CWE-78) | La neutralización inadecuada de elementos especiales utilizados en un ('Inyección de comandos OS') Comando OS |
| [CWE-79](http://cwe.mitre.org/top25/index.html#CWE-79) | La neutralización inadecuada de entrada Durante Web Página Generada ('Cross-site Scripting') |
| [CWE-434](http://cwe.mitre.org/top25/index.html#CWE-434) | Cargar sin restricciones de archivo con el tipo peligroso |
| [CWE-352](http://cwe.mitre.org/top25/index.html#CWE-352) | Cross-Site Request Forgery (CSRF) |
| [CWE-601](http://cwe.mitre.org/top25/index.html#CWE-601) | URL de redirección a un sitio no confiable ('Open Redirect') |

* [**Software Error Categoría: Risky Gestión de Recursos**](http://www.sans.org/top25-software-errors/#cat2)**(8 errores)**

### Gestión de Recursos Risky

Los puntos débiles de esta categoría están relacionadas con las formas en que el software no administra correctamente la creación, uso, transferencia, o la destrucción de los recursos importantes del sistema.

| **CWE ID** | **Nombre** |
| --- | --- |
| [CWE-120](http://cwe.mitre.org/top25/index.html#CWE-120) | Buffer Copia sin Comprobación de Tamaño de entrada ('Classic Buffer Overflow') |
| [CWE-22](http://cwe.mitre.org/top25/index.html#CWE-22) | Limitación indebida de un nombre de ruta de un directorio restringido ('Transversal Camino') |
| [CWE-494](http://cwe.mitre.org/top25/index.html#CWE-494) | Descargar de Código Sin Integrity Check |
| [CWE-829](http://cwe.mitre.org/top25/index.html#CWE-829) | La inclusión de la funcionalidad de control que no se confía Esfera |
| [CWE-676](http://cwe.mitre.org/top25/index.html#CWE-676) | Uso de la Función Potencialmente Peligrosos |
| [CWE-131](http://cwe.mitre.org/top25/index.html#CWE-131) | Cálculo incorrecto de Tamaño de búfer |
| [CWE-134](http://cwe.mitre.org/top25/index.html#CWE-134) | Cadena de formato no controlada |
| [CWE-190](http://cwe.mitre.org/top25/index.html#CWE-190) | Desbordamiento de enteros o Wraparound |

* [Software Error Categoría: Defensas porosos](http://www.sans.org/top25-software-errors/#cat3) (11 errores)

### Defensas porosos

Los puntos débiles de esta categoría están relacionadas con las técnicas defensivas que a menudo uso, abuso, o simplemente ignoradas llanura.

| **CWE ID** | **Nombre** |
| --- | --- |
| [CWE-306](http://cwe.mitre.org/top25/index.html#CWE-306) | Autenticación Falta de función crítica |
| [CWE-862](http://cwe.mitre.org/top25/index.html#CWE-862) | Autorización Missing |
| [CWE-798](http://cwe.mitre.org/top25/index.html#CWE-798) | El uso de Credenciales no modificable |
| [CWE-311](http://cwe.mitre.org/top25/index.html#CWE-311) | Missing cifrado de datos sensibles |
| [CWE-807](http://cwe.mitre.org/top25/index.html#CWE-807) | La confianza en que no se confía entradas en una Decisión de Seguridad |
| [CWE-250](http://cwe.mitre.org/top25/index.html#CWE-250) | Ejecución con privilegios innecesarios |
| [CWE-863](http://cwe.mitre.org/top25/index.html#CWE-863) | Autorización incorrecta |
| [CWE-732](http://cwe.mitre.org/top25/index.html#CWE-732) | Asignación incorrecta Permiso para recursos críticos |
| [CWE-327](http://cwe.mitre.org/top25/index.html#CWE-327) | El uso de un algoritmo criptográfico roto o Risky |
| [CWE-307](http://cwe.mitre.org/top25/index.html#CWE-307) | Restricción inadecuado de intentos de autenticación excesivos |
| [CWE-759](http://cwe.mitre.org/top25/index.html#CWE-759) | El uso de un cifrado de una vía sin sal |

Análisis de software de aplicación para seguridad.

* **Software:** ModSecurity
* **URL:**[**www.modsecurity.org**](http://www.modsecurity.org/)
* **S.O.:**Windows, Linux, BSD… etc
* **Tipo:**Seguridad servidor web
* **Licencia:**GPL
* **Descripción:**

ModSecurity es una herramienta para la detección y prevención de intrusiones para aplicaciones web, lo que podríamos denominar como “firewall web”. Este motor funciona como módulo de Apache, incrementando la seguridad del servidor web frente a ataques de tipo tanto conocido como desconocido. Ayuda a evitar, entre otros tipos de ataque:

• Técnicas anti-evasión

• Supervisa código HTML y cookies

• Análisis de los contenidos pasados al servidor mediante el método POST

• Permite realizar completas auditorías de los POSTs realizados

• Soporta HTTPS

• Soporta contenidos comprimidos

• etc..



La instalación y configuración en Apache no resulta excesivamente complicada, para lo cual sólo es necesario instalarlo como módulo y activar unas ciertas reglas en el fichero de configuración httpd.conf, y puede ser usado con otros módulos (como Snort o mod\_rewrite) para obtener una mayor funcionalidad.

Comprensión del protocolo HTTP: al comprender el protocolo HTTP, ModSecurity puede realizar filtrados específicos y granulares.

Toda la información que facilites y una buena descripción ayudarán a realizar un mejor catálogo. Aceptamos también que referenciéis simplemente el software que uses (sin descripción ni otros datos), pero esto ralentizará la creación del listado.  El software puede ser tanto libre como propietario, siendo especialmente valioso el software libre para que pueda ser usado sin restricciones. No importa para qué sistema operativo sea, ni que sea de sobra conocido: la idea es que el listado pueda ser consultado tanto por usuarios nóveles como expertos.

**CONCLUSIÓN**

Esta práctica fue realizada con la finalidad de poder entender los aspectos, recursos, objetivos e identificar que protocolo utiliza sans, y Sus principales objetivos son Reunir información sobre todo lo referente a seguridad informática ([sistemas operativos](http://es.wikipedia.org/wiki/Sistema_operativo), [routers](http://es.wikipedia.org/wiki/Router%22%20%5Co%20%22Router), [firewalls](http://es.wikipedia.org/wiki/Firewall), [aplicaciones](http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica), [IDS](http://es.wikipedia.org/wiki/IDS), etc.), Ofrecen capacitación y certificación en el ámbito de la seguridad informática Igualmente, el SANS Institute es una universidad formativa en el ámbito de las tecnologías de seguridad.

No hay duda de que hay Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Curiosamente me he dado cuenta d que El tipo de tráfico en una SAN es muy similar al de los [discos duros](http://es.wikipedia.org/wiki/Disco_duro) como [ATA](http://es.wikipedia.org/wiki/ATA), [SATA](http://es.wikipedia.org/wiki/SATA) y [SCSI](http://es.wikipedia.org/wiki/SCSI).

Más adelante me servirá esta investigación como base fundamental de mis estudios en la cual me desempeñare sin problemas y gracias a las investigaciones realizadas.

Espero que esta información sirva de ayuda para los lectores y demás personas que tengan interés sobre la práctica y queda a disposición de críticas en la cual me beneficiara en el futuro.