UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

"ANÁLISIS DE SISTEMA DE DETECCIÓN DE INTRUSOS EN REDES DE TRANSMISIÓN DE DATOS"

Autor:
Rodrigo Salvador Sarzosa Patiño

Tutor:
Ing. Marco Lituma

Cuenca – Ecuador

2011

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE RESPONSABILIDAD

Ing. Marco Lituma Orellana

Director de Tesis

CERTIFICA:

Que el presente trabajo de investigación “Análisis de Sistema de Detección de Intrusos en Redes de Transmisión de Datos”, realizado por el Sr. Rodrigo Salvador Sarzosa Patiño, egresado de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 7 de Noviembre de 2011

_____

Ing. Marco Lituma Orellana

DIRECTOR DE TESIS

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

ACTA DE SESIÓN DE DERECHOS

Yo, RODRIGO SALVADOR SARZOSA PATIÑO, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, 7 de Noviembre de 2011

_____

Rodrigo Salvador Sarzosa Patiño.

C.I: 010339648-7

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORÍA

Los contenidos, argumentos, exposiciones, conclusiones son de Responsabilidad del autor.

.

_____

Rodrigo Salvador Sarzosa Patiño

C.I: 010339648-7

DEDICATORIA

El presente trabajo de tesis lo dedico a las personas que siempre me han apoyado durante mis estudios, quienes con amor y comprensión me han dado fuerzas para superar los obstáculos que encontrado a lo largo de mi vida, mis padres Rafael y Senaida y a mis hermanos Wilson, Carmen, Rocío, Pablo y Karina. Por haberme brindado su apoyo incondicional para poder cumplir con esta etapa de mi vida tan importante.

AGRADECIMIENTOS

El agradecimiento es una de las virtudes más nobles del ser humano; por eso dedico la presente como agradecimiento al apoyo brindado durante estos años de estudio y como un reconocimiento de gratitud al haber finalizado esta carrera a todos los profesores de la Universidad Israel por haberme brindado su amistad, apoyo y conocimientos, también agradezco de manera muy especial a mi tutor el Ing. Marco Lituma Orellana, por su amistad y ayuda brindada durante el desarrollo de esta tesis.

RESUMEN

La seguridad de la información es algo de suma importancia para cualquier persona o empresa que puede ver comprometida su confidencialidad, es por eso que este trabajo trata sobre la seguridad que debe existir en las redes de transmisión de datos y cuál es el funcionamiento de Sistemas de Detección de Intrusos.

Las redes de transmisión de datos están basadas en características como funcionalidad y eficiencia, mas no en seguridad, partiendo desde este punto de vista describiremos, su estructura e identificaremos las vulnerabilidades que existen en las capas del protocolo TCP/IP.

Conociendo las vulnerabilidades que existen dentro de una de una red, analizaremos al firewall como filtro de seguridad de una red, para dar fiabilidad a la información que es transmitida y así mantener un óptimo rendimiento y funcionamiento de la red.

ABSTRACT

The information security is something very important for any person or company that confidentiality can be compromised that is why this paper deals with the safety that must exist in the transmission of data and what is the function of the systems Intrusion detection.

The data networks are based on characteristics such as functionality and efficiency, not security, starting from this point of view, describe, structure and identify the vulnerabilities that exist in the layers of TCP / IP.

Knowing the vulnerabilities that exist within a network, we analyze the firewall as a security filter network to provide reliability information that is transmitted and to maintain optimum performance and network performance.

Índice de Contenidos

Índice de gráficos

Capítulo I

1 Introducción

La seguridad es un aspecto primordial para cualquier empresa o persona que maneja información de contenido delicada, que no debe ser vulnerada o manipulada por terceras personas con el fin de alterar dicha información.

El presente trabajo trata sobre las vulnerabilidades que existen en las redes de transmisión de datos con protocolos TCP/IP, señalando algunas de sus vulnerabilidades y como los IDS (Sistemas de Detección de Intrusos), nos ayudan a protegernos de posibles ataques pudiéramos sufrir sobre nuestra red.

1.1 Planteamiento del problema

¿Cómo se podría identificar a las personas no autorizadas que ingresan a la red o redes?

1.2 Antecedentes

Desde tiempos inmemorables el hombre ha resguardado y protegido con celo sus conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades.

En la antigüedad surgen las bibliotecas, lugares donde se podía resguardar la información para trasmitirla y para evitar que otros la obtuvieran, dando así algunas de las primeras muestras de protección de la información.

En la actualidad, las computadoras se han convertido en las bibliotecas virtuales, en las cuales con ayuda de internet, encontramos todo tipo de información, de manera que las computadoras y el internet se han convertido en herramientas de trabajo.

Por lo tanto, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados (hacker), por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco se debe subestimar las fallas de seguridad provenientes del interior mismo de la organización.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el

impacto que puede tener. Una vez conocidos todos estos puntos, deberán tomarse las medidas de seguridad oportunas.

1.3 Sistematización

1.3.1 Diagnostico

El acceso de intrusos a redes de transmisión de datos es un problema que se presenta con más frecuencia, esto representa un grave problema para la confidencialidad de los datos que viajan a través de la red.

1.3.2 Causa Efecto

Todas las organizaciones dedicadas a dar servicio de seguridad informática deben estar a la vanguardia de los procesos de cambio, ya que cada día nos encontramos con nuevas tecnologías y hackers más experimentados, y tratando de robar información de empresas. Por tal motivo las personas encargadas de la seguridad de la red, deben estar en constante actualización de sus conocimientos, para evitar pérdidas de información valiosa para la empresa, y causar pérdidas irreparables o económicas cuantiosas.

“La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben

subestimarse las fallas de seguridad provenientes del interior mismo de la organización."[1] (Arcert, 1999)

1.3.3 Pronóstico y control de pronóstico

La seguridad en redes o en el ámbito informático se ha convertido en un problema grave el cual debemos solucionarlo. Ya que cada día somos más vulnerables por lo tanto debemos buscar alternativas para proteger nuestros datos.

La detección de intrusos es un proceso que permite buscar violaciones de seguridad en sistemas o redes de computadoras, esto ha permitido que los IDS sean implementados con mayor frecuencia en las empresas, e implementando políticas de seguridad, para acceso a la red, pero la propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van surgiendo.

Podemos decir también que para la protección de un sistema o sistemas es la constante vigilancia por parte de él o los responsables de administrar la red, en cuestión.

[1] Arcert (Coordinación de emergencias en redes teleinformáticas)[Manual de Seguridad, Seguridad en Redes, Noviembre de 1999.] http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

El acceso de intrusos a redes de transmisión de datos es un problema que se presenta con más frecuencia, esto representa un grave problema para la confidencialidad de los datos que viajan a través de la red.

El estudio de los sistemas de detección de intrusos nos permitirá mantener la seguridad de nuestra información ante posibles ataques de personas no autorizadas a la información.

1.4 Formulación de la problemática

1.4.1 Problema principal

La planificación de la seguridad en el diseño de la red es de suma importancia pues de esto depende el buen desempeño de la red, nos evita trabajo posterior, pérdida de datos y posibles daños a la red.

Podemos decir también que el nivel de seguridad de nuestra red dependerá de su tamaño e importancia de la información.

Como hemos visto la seguridad en las redes se ha convertido en un factor importante en el diseño e implementación de las redes. El administrador de la red debe estar constantemente implementando medidas de seguridad en la red con el fin de tener una red confiable y estable, en base a las exigencias del oficial de seguridad de la información y auditoria informática.

1.4.2 Problema secundarios

Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers. Es por eso que tenemos que tener una serie de precauciones y seguridades para evitar que alguien no deseado busque en nuestra información y seamos presa fácil de extorsiones, fraudes y pérdidas irreparables.

1.5 Objetivos

1.5.1 Objetivo general

Detectar y analizar el acceso de intrusos a redes TCP/IP con IDS y proponer soluciones de control y negación de acceso a usuarios no autorizados.

1.5.2 Objetivos específicos

- Conocer los conceptos relacionados con los Sistemas de Detección de Intrusos.
- Identificar las fallas de seguridad relacionadas con el protocolo TCP/IP
- Analizar los diferentes tipos de ataques utilizados por los intrusos para acceder a la red.
- Analizar las vulnerabilidades que ponen en peligro a la red.
- Investigar que herramienta de Hardware y Software, existen para tener una red segura.
- Reconocer las mejores alternativas para mantener una red segura.

1.6 Justificación

En la actualidad, la seguridad informática ha adquirido gran incremento, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Por otro lado el peligro más grande radica no en enviar la información sino una vez que esta información, unida a la de miles de clientes más, esto en caso de que sea una empresa, y también puede suceder en datos personales, etc. pero por lo general, toda información es valiosa, reposa en una base de datos de la compañía con las que se concretó el negocio. Con un único acceso no autorizado a esta base de datos, es posible que alguien obtenga no únicamente mis datos y los de mi tarjeta, sino que tendrá acceso a los datos y tarjetas de todos los clientes de esta compañía.

Capítulo II

2. Marco teórico

La seguridad en redes, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta.

"Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial."[2]

2.1 La Confidencialidad

La confidencialidad es lo que se debe mantener reservado o secreto previniendo la divulgación de información a personas o sistemas no autorizados.

La pérdida de la confidencialidad de la información puede adoptar muchas formas, como la infiltración y la penetración en ambas es posible el uso del soborno o el chantaje. También se tiene una pérdida de confidencialidad

[2] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

cuando alguien mira por encima de su hombro, mientras se tiene información confidencial en la pantalla.

2.2 La información contenida

El contenido de la información se ha convertido en uno de los elementos más importantes para cualquier organización. La seguridad informática debe ser establecida según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización.

2.3 La infraestructura computacional

La función de la seguridad informática en esta área es custodiar que los equipos funciones adecuadamente y de establecer planes de contingencia en caso de fallas, robos, incendios, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática.

2.4 Los usuarios

Son las personas que utilizan la estructura tecnológica, el área de telecomunicaciones, y que gestionan la información. La seguridad informática se encarga en establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de acceso, restricciones a determinados lugares, prohibiciones, perfiles de usuario, etc.

2.5 Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento o transmisión de información se consideran seguros, todavía se deben tener en cuenta las circunstancias que puedan afectar a los datos, los cuales son a menudo imprevisibles o inevitables.

En este mundo digitalizado, con sistemas informáticos que avanzan a pasos agigantados, y al saber que tener información es tener poder. Por estos motivos la seguridad informática es un punto importante para el futuro de organización o empresa, por tal motivo debemos decir que:

La seguridad informática debe ser garantizada en primera instancia los siguientes 4 puntos.

- La **Disponibilidad** de los sistemas de información.
- El **Recupero** rápido y completo de los sistemas de información.
- La **Integridad** de la información.
- La **Confidencialidad** de la información.

Sin embargo no podríamos decir que la seguridad informática está exenta de vulnerabilidades, pero en un rango más amplio de lo que es seguridad informática, diríamos que es un conjunto de métodos y herramientas destinadas a la protección de la información que se encuentra en los sistemas informáticos ante cualquier ataque o amenaza que se presente.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que es confidencial. La información no puede ser divulgada, mal utilizada, robada, borrada o alterada. Esto afecta su disponibilidad e integridad y la pone en riesgo.

Tomando en cuenta la importancia de la información podríamos decir que la información es poder, y la podríamos clasificar como:

Crítica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas.

Al identificar el tipo de información que tenemos, debemos analizar dos conceptos básicos que son riesgo y seguridad:

Riesgo: Es todo tipo de *"vulnerabilidades, amenazas que pueden ocurrir sin previo aviso"*[3], y causar gran pérdida o corrupción de la información.

Seguridad: Es una forma de protección contra los riesgos. La seguridad de la infSormación comprende varios aspectos entre los que podemos citar *"la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad*"[4], etc.

[3] http://yolopuedohacer.blogspot.com/2011/07/seguridad-de-la-informacion-parte-i.html

[4]CIDAGI(centro de investigación para el desarrollo archivístico y gestión de la información) http://www.cidagi.org.pe/index.php?option=com_content&view=article&id=1:bienvenido-a-cidagi&catid=1:latest-news

Comprendiendo que la reducción o eliminación de riesgos asociados a determinada información es el objetivo de la seguridad de la información y la seguridad informática.

Concretamente, la seguridad de la información tiene como objeto el control del acceso, divulgación, interrupción y destrucción no autorizada de información.

Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente por los administradores y encargado de seguridad, porque todos ellos persiguen una misma finalidad proteger la confidencialidad, integridad y disponibilidad de la información.

2.6 Protecciones lógicas y físicas

2.6.1 Seguridades Lógicas

La seguridad lógica hace referencia a la aplicación de mecanismos para mantener el resguardo y la integridad de la información dentro de un sistema informático.

La seguridad lógica de un sistema incluye:

Herramientas de protección de la información en el mismo medio en el que se genera o transmite.

- Protocolos de autenticación entre cliente y servidor.
- Aplicación de herramientas de seguridad en redes.

Medidas de prevención de riesgos y la creación de políticas de seguridad, de planes de contingencia, de recuperación ante desastres, aplicación de normativas, etc.

2.6.2 Seguridades Físicas

La Seguridad Física consiste en la *"aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"*[5] (HUERTA, 2000)

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos.

2.7 Tipos de ataques informáticos

Entre los distintos tipos de ataques informáticos, podríamos diferenciar a los ataques activos y pasivos.

a) **Los ataques activos**, son aquellos que producen cambios en la información y en la situación de los recursos del sistema.

[5] *HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.* http://www.kriptopolis.org

b) **Los ataques pasivos**, que se limitan a registrar el uso de los recursos o a acceder a la información almacenada o transmitida por el sistema.

La seguridad informática consiste en aquellas prácticas que se llevan adelante con respecto de un determinado sistema de computación, a fin de proteger y resguardar su funcionamiento y la información contenida.

Capitulo III

3.1 Metodología

3.2 Método de la Investigación

3.2.1 Método Bibliográfica-Documental

Puesto que el documento es la unidad básica para realizar una investigación o una indagación. Esta investigación gira entorno a documentos existentes para luego extraer lo más importante y también sacar, conclusiones, y hacer el trabajo lo más comprensible y sintético, en mayor medida en el que sea posible.

La metodología que se seguirá en esta investigación será bibliografía – documental. Ya que esta metodología indaga, interpreta, presenta datos e informaciones sobre un tema determinado.

3.2.2 Método Informativo (Expositivo)

Mediante este método se pudo obtener y recabar información concreta acerca de los estudios realizados sobre los IDS (Sistemas de Detección de Intrusos), publicaciones oficiales, artículos en revistas especializadas sobre la tecnología informática.

3.2.3 Fuentes de Investigación Documental

La fuente primaria para esta investigación fue la digital, en consulta a libros digitales, publicaciones que se realizan periódicamente, artículos de revistas especializadas sobre los IDS.

Capítulo IV

4.1 Historia de los IDS

Los sistemas de detección de intrusos dan inicio en los años 80 cuando James P. Anderson pública "Computer Security Threat Monitoring and Surveillance" (Anderson, 1980), dónde se inician las bases de la detección de intrusos en sistemas de computadores, principalmente mediante la consultas de ficheros de log.

En la década de los 80 se diseñó el primer sistema (IDES), (Intrusion Detection Expert System) fue desarrollado por Dorothy Denning y Peter Neumann que funcionaba en tiempo real.

4.2 ¿Qué es un sistema de detección de intrusos?

Un sistema de detección de intrusos (IDS) es un tipo de sistema de gestión de seguridad de los computadores y redes. Un IDS reúne y analiza información de diversas áreas dentro de un computador o una red de computadores para identificar las posibles violaciones de seguridad, este análisis incluyen tanto las intrusiones que pueden ser externas (ataques desde fuera de la organización), como internas (ataques desde dentro de la organización).

Los IDS utilizan técnicas de análisis de vulnerabilidad (conocidos como scanning), el scanning es una tecnología desarrollada por los Hackers para

evaluar la seguridad de un sistema informático o red de transmisión de datos, en búsqueda de vulnerabilidades.

4.3 Clasificación de IDS

4.3.1 Por su localización

4.3.1.1 HIDS (HostIDS):

Los IDS basados en host, realizan su función protegiendo a un único sistema es un proceso que trabaja en background (o que se ejecuta periódicamente) buscando patrones que puedan indicar un intento de intrusión y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado.

Los modelos de IDS basados en Host han consistido por una parte en la utilización de herramientas automáticas de análisis de logs generados por diferentes aplicaciones o por el propio kernel del sistema operativo, prestando siempre especial atención a los registros referentes a los de red.

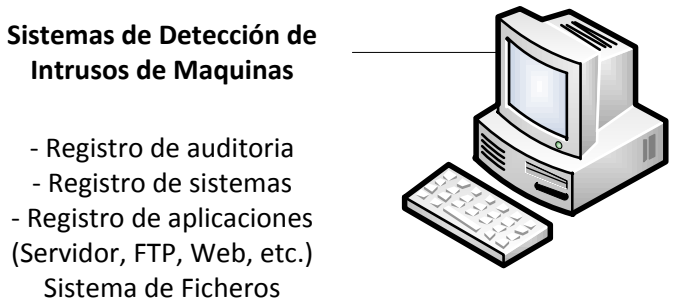


Gráfico N° 1 HIDS

4.3.1.2 NIDS (Network IDS)

Los IDS basado en red monitoriza los paquetes que circulan por nuestra red en busca de elementos que indiquen un ataque contra alguno de los sistemas ubicados en ellos; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador). Este donde este, monitorizara diversas máquinas y no una sola, esta es la principal diferencia con los sistemas de detección de intrusos basados en host.

Los sistemas de detección de intrusos basados en red son capaces de detectar ataques contra diferentes sistemas de una misma red, aunque generalmente se ejecuten en uno solo de los hosts de esa red. Para lograr su objetivo, al menos uno de los interfaces de red de esta máquina sensor trabaja en modo promiscuo, capturando y analizando todas las tramas que pasan por el en busca de patrones indicativos de un ataque.

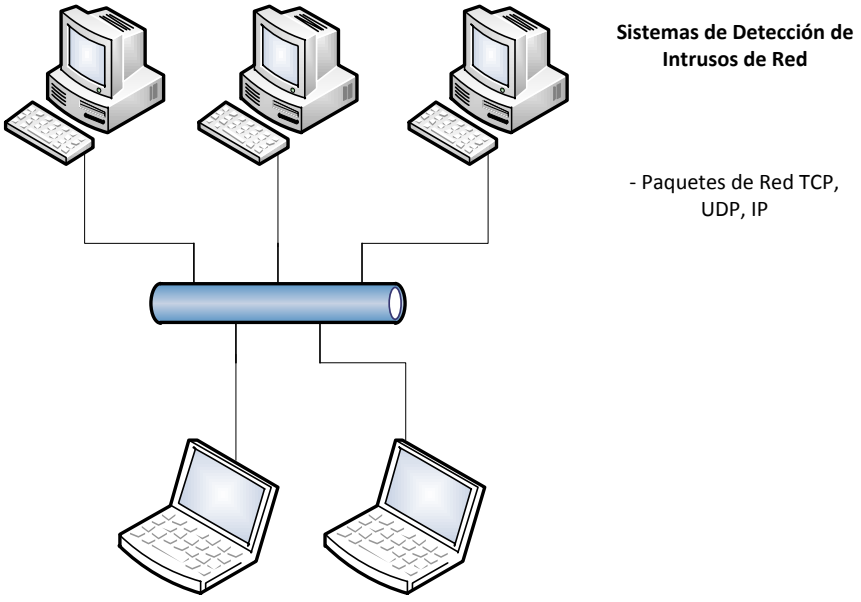


Gráfico N° 2 NIDS

4.3.2 Por su modo de detección

4.3.2.1 Detección de mal uso

Los IDS basados en detección de mal uso monitorizan las actividades que ocurren en un sistema y las compara con firmas de ataques, las cuales se encuentran almacenadas en una base de datos. Cuando las actividades monitorizadas coinciden con las firmas, genera una alerta. La detección de intrusos basada en mal uso se limita al conocimiento previo de las secuencias y actividades que forman un ataque.

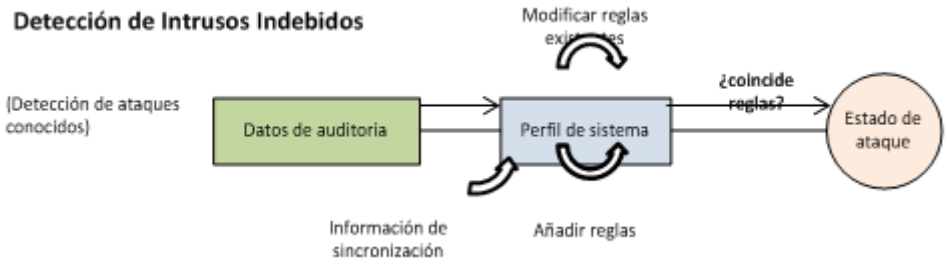


Gráfico N° 3 Detección de Intrusos Indebidos

4.3.2.2 Detección de uso anómalo

Los IDS basados en detección de anomalías se basan en la condición de que cualquier ataque o intento de ataque implica un uso anormal de los sistemas, en la detección por anomalías no se buscan señales de intrusiones conocidas, sino eventos anormales en el tráfico de una red, se puede definir como la incompatibilidad de una regla o de un uso, de ese modo, el primer paso de un sistema de detección de anomalías comienza por establecer lo que se considera comportamiento normal de un sistema (usuarios, redes, registros de auditoría, llamadas del sistema de los procesos, etc.). Una vez definido esto,

clasificará como sospechosas o intrusivas aquellas desviaciones que pueda detectar sobre el comportamiento normal.

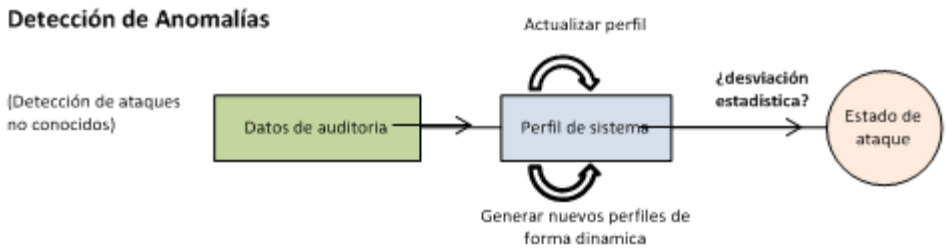


Gráfico N° 4 Detección de Anomalías

4.3.3 Por su naturaleza

4.3.3.1 Pasiva:

Los sistemas de respuesta pasiva responden por notificación a la autoridad que corresponde, y no trata de mitigar por sí mismos el daño realizado.

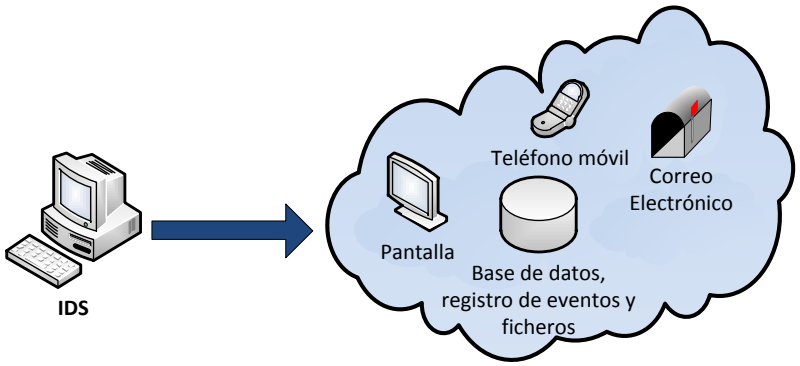


Gráfico N° 5 IDS con Respuesta Pasiva

4.3.3.2 Activa:

Los que ejercen control sobre el sistema atacado. En respuesta activa terminan con la sesión del usuario y bloquean la conexión del intruso.

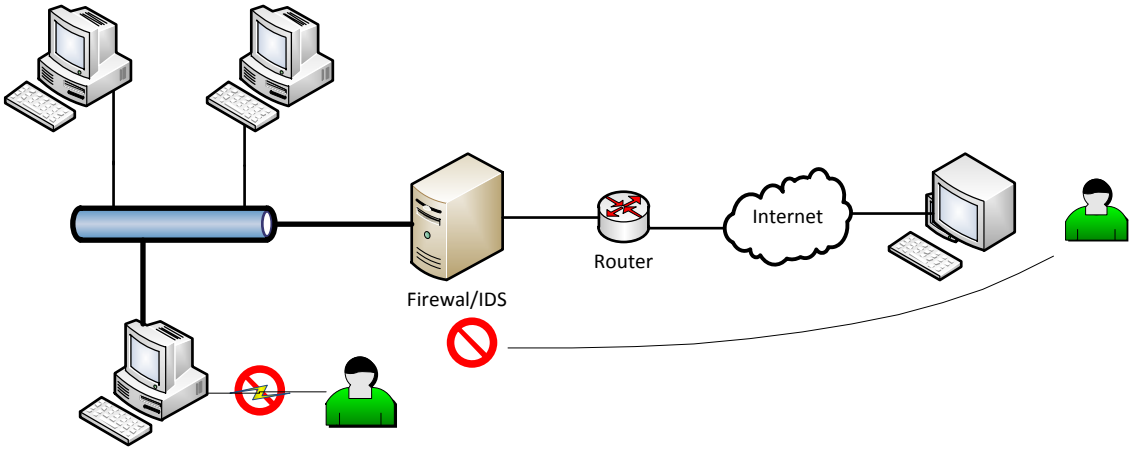


Gráfico N° 6 IDS con Respuesta Activa

4.4 Arquitectura de los IDS

Un sistema de detección de intruso (IDS), puede dramáticamente simplificar sus procedimientos de monitorear la red.

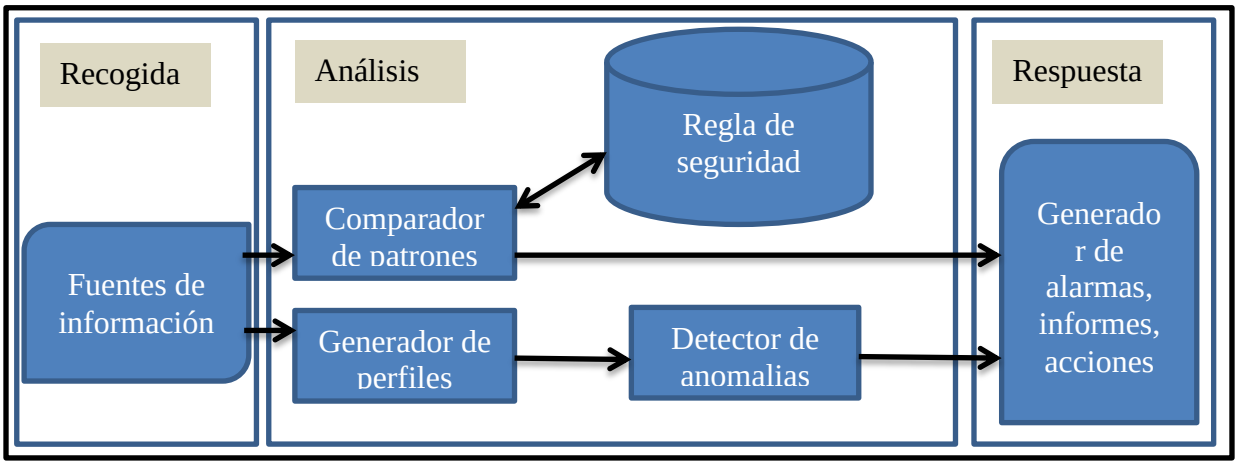


Gráfico N° 7 Arquitectura IDS

4.4.1 CIDF (Common Intrusion Detection Framework)

Fue desarrollado en los años 90 por DARPA (Defense Advanced Research Projects Agency), fue un primer intento de estandarización de la arquitectura de los IDS.

Se definen cuatro tipos básicos de equipos:

- **Equipos E**. Sensores: detectan eventos “interesantes” y emiten alertas (informes).
- **Equipos A:** Analizadores: reciben los informes de los equipos E y los analizan, emitiendo una recomendación.
- **Equipos D:** Componentes de bases de datos: correlación, estadísticas, análisis históricos, etc.
- **Equipos R:** Equipos de respuesta: responden al evento a partir de los datos generados por los equipos anteriores.

Los diferentes componentes de la arquitectura CIDF intercambia información en forma de GIDOS (Generalized Intrusion Detection Objects).

Un GIDO puede representar

- La ocurrencia de un cierto evento en un momento determinado.
- Una conclusión extraña de un conjunto de eventos.
- Instrucciones para ejecutar una acción (respuesta).

4.4.2 CISL (Common Intrusion Specification Language)

Lenguaje para expresar información acerca de eventos, ataques y respuestas en el entorno de detección.

Las etiquetas: SIDs (Semantic IDenti ers). Indican la interpretación del resto de la expresión, convirtiéndose en el corazón del lenguaje.

Los principales SIDs:

Verbos. Indican una acción o recomendación (borrar, bloquear, ejecutar).

Roles. Informan de los elementos implicados en el verbo (objetos o actores).

4.4.3 DIDS (Distributed Intrusion Detection System)

Los DIDS son sistemas basados en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada.

El análisis de los DIDS es tan o más complejo que el realizado con los NIDS, con lo que queda fuera de este trabajo aunque se cita la bibliografía correspondiente.

Su característica diferenciadora respecto a los sistemas NIDS tradiciones, es la presencia de dos elementos nuevos en su arquitectura

4.4.3.1 Central Analysis Server:

El centro del sistema DIDS y es el encargado de recibir toda la información procedente de los agentes y realizar un repositorio común de conocimiento. También realiza las funciones de control y sincronización de los diferentes nodos que forman parte del sistema.

4.4.3.2 Co-operative Agent network:

Es un sistema autónomo encargado de la monitorización de una red. Detecta posibles incidentes e informa al servidor central para que comunique a todos los nodos el ataque detectado así como las contra-medidas a realizar. Dependiendo de la implementación, el agente puede llegar a tomar contra-medidas de forma autónoma (aunque siempre informando y supeditándose al servidor central).

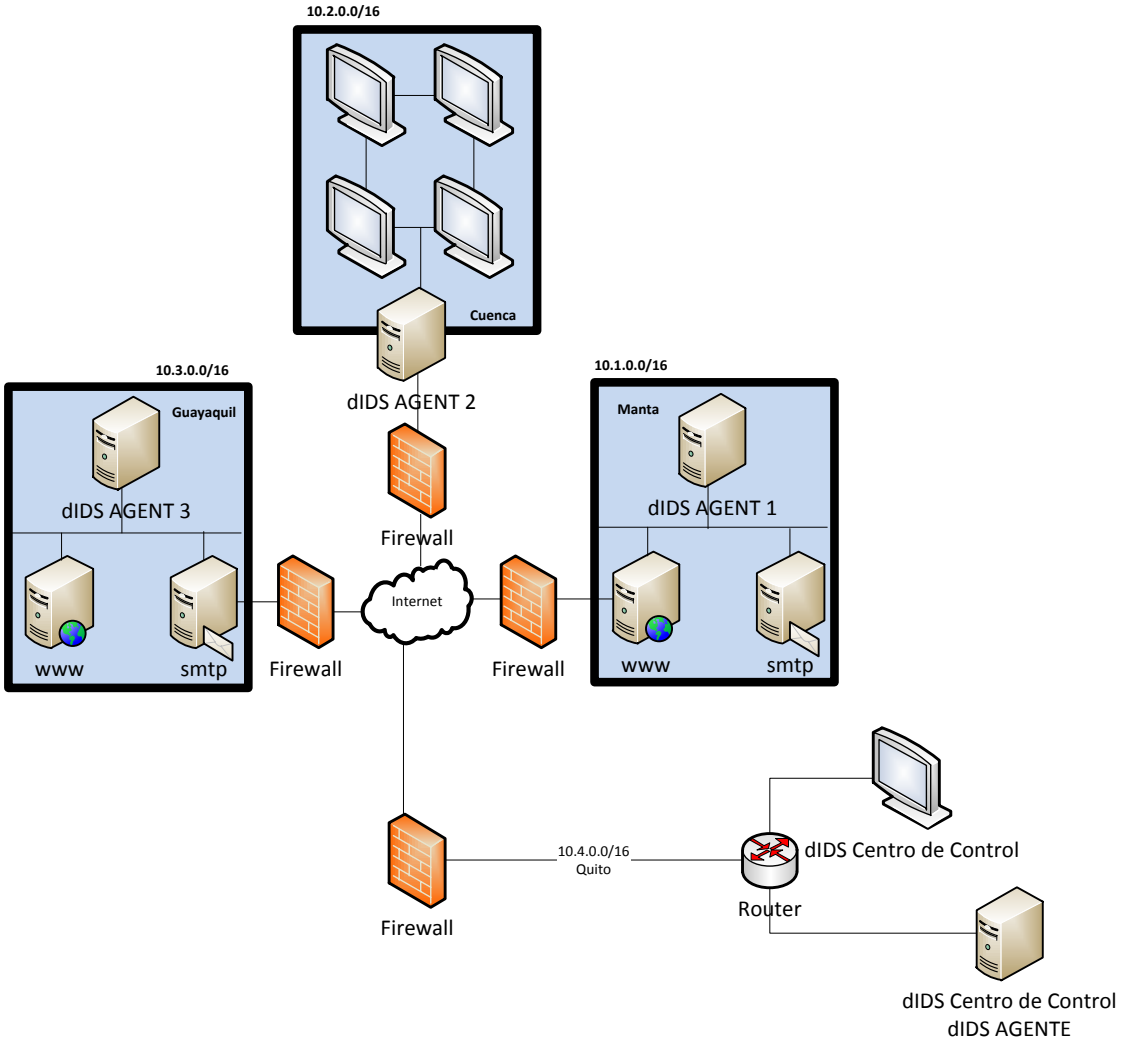


Gráfico N° 8 DIDS

4.4.4 IDWG (Intrusion Detection Working Group)

El propósito de la identificación de intrusos de Grupo de trabajo, es definir los formatos de datos y procedimientos de intercambio para compartir información de interés para la detección de intrusos y sistemas de respuesta.

Los resultados de este grupo de trabajo serán los siguientes:

- Documentos que describan los requerimientos funcionales de alto nivel para la comunicación entre sistemas de detección de intrusos y entre los sistemas de detección de intrusos y sus sistemas de gestión.
- Un lenguaje común de especificación que describa el formato de los datos.
- Un marco de trabajo que identifique los mejores protocolos que se pueden usar para la comunicación entre los IDS y que defina como se mapean en éstos lo formatos de datos.

4.5 Limitaciones de los IDS

4.5.1 Limitaciones de los NIDS

Uno de los problemas más importantes de los NIDS es su incapacidad de reconstruir exactamente lo que está ocurriendo en un sistema que están monitorizando, los detectores de intrusos basados en firmas funcionan examinando el contenido de los paquetes que se están transmitiendo por la red. El análisis consiste básicamente en un análisis pasivo del protocolo utilizado, lo cual hace a esta técnica no intrusiva y extremadamente difícil de detectar o evadir. Algunos de los ataques que los IDS pueden detectar se pueden ver simplemente analizando los paquetes IP; un intento de ocultar un ataque fragmentando paquetes IP se puede observar examinando el desplazamiento del fragmento dentro de su paquete IP correspondiente.

4.6.1 Estructura de la red TCP/IP

4.6.1 Protocolo IP

Ip es un protocolo que permite a las aplicaciones ejecutarse transparentemente sobre diferentes redes conectadas. Es de esta forma se permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega. Es aquí donde el protocolo IP procesa datagramas IP de manera independiente sin definir su representación, ruta o envío. Es así como el protocolo IP puede determinar el destinatario del mensaje mediante 3 campos:

- Campo de dirección IP: Está dada por la dirección del equipo.
- Campo de máscara de subred: La cual permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red.
- Campo de pasarela predeterminada: La cual permite al protocolo IP saber a qué equipo enviar un datagrama.

4.6.2 Protocolo TCP

TCP es un protocolo que asegura que los datos sean recibidos de la misma forma que fueron enviados, estableciendo una comunicación entre 2 o más equipos, por lo tanto, es un protocolo orientado a la conexión que permite la unión de dos equipos, en donde existe un cliente y un servidor que responde a las solicitudes generadas de forma simultánea. El protocolo TCP en conjunto con los equipos de soporte, se encargan de manejar la velocidad de los mensajes emitidos, debido a la capacidad que tiene de manipular los mensajes en diferentes tamaños (segmentos).

Las principales características del protocolo TCP son las siguientes:

- Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- Permite el monitoreo del flujo de los datos para así evitar la saturación de la red.
- Permite que los datos se formen en segmentos de longitud variada para entregarlos al protocolo IP.
- Permite multiplexar los datos, es decir, permite que la información que viene de diferentes fuentes pueda ser transmitida en una misma línea (circulación simultáneamente).
- Permite comenzar y finalizar la comunicación amablemente.

Bajo su funcionamiento, se transfieren datos mediante el ensamblaje de bloques de datos conocidos como paquetes. Cada paquete comienza con una cabecera que contiene información de control y validación, seguido de los datos.

Cuando se envía un archivo por la red TCP/IP, su contenido se envía utilizando una serie de diferentes paquetes. Es así como se establece la forma de operación general bajo estos dos protocolos.

Debido a lo mencionado anteriormente, se puede señalar que éste modelo es fundamental para comenzar el análisis de los puntos defectuosos de la red.

Es así como ésta estructura o modelo representa la forma en que la información circula por la red, donde cada etapa le da soporte a la capa superior, y así posteriormente a la familia de protocolos TCP/IP que necesita para establecer la comunicación.

4.6.3 Modelo TPC/IP

El primer modelo de protocolo en capas para comunicaciones de internet se creó a principios de la década de los setenta por el departamento de defensa de los EEUU porque necesitaban una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear, este define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas.

Este problema de diseño de difícil solución fue lo que llevó a la creación del modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló Internet.

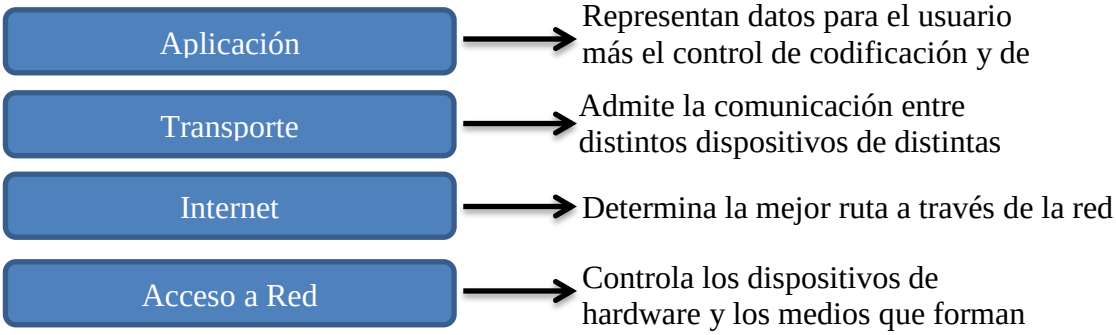


Gráfico N° 9 Modelo TCP/IP

4.6.4 Familia de protocolos TCP/IP

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel (ejmp. la transmisión de flujos de bits a un medio físico) hasta aquellas de más alto nivel (ejmp. el compartir o transferir información desde una computadora a otra en la red).

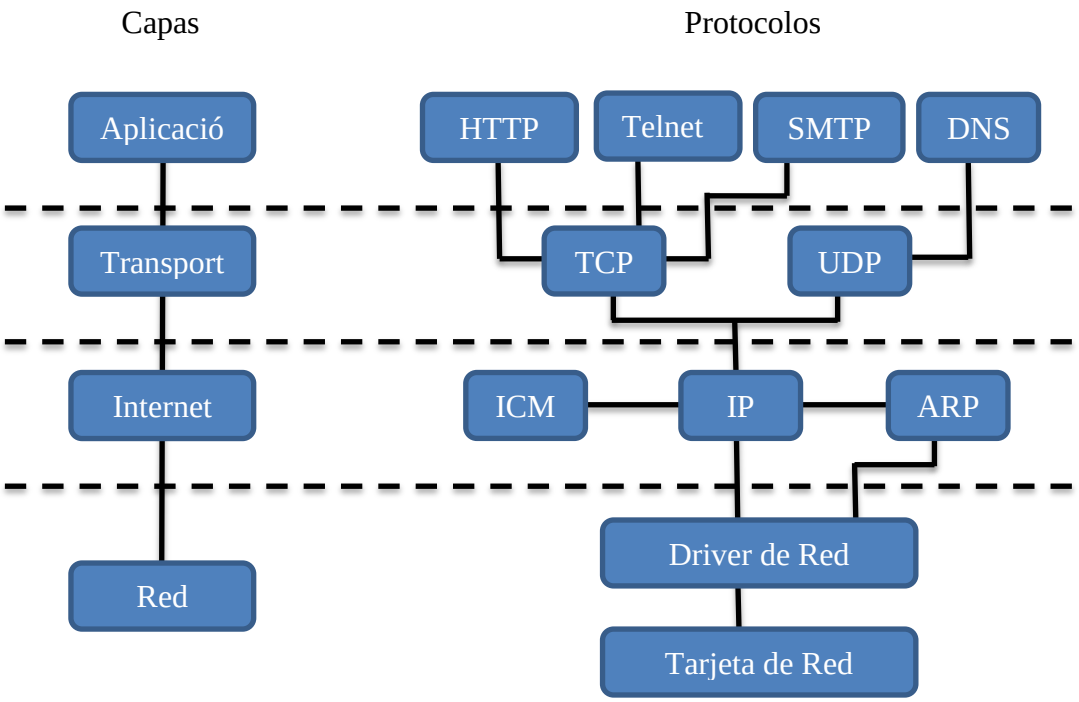


Gráfico N° 10 Familia de protocolos TCP/IP

Tarjeta de Red:

La Tarjeta de red, también conocida como Tarjeta de Interfaz de Red (NIC), es un Hardware necesario para poder establecer una comunicación entre 2 o más equipos Una tarjeta de red, convierte los datos enviados por un equipo a un formato que pueda ser utilizado por el cable de red, transfiere los datos a otro equipo y controla a su vez el flujo de datos entre el equipo y los cables

conectores (RJ45). Se encarga de traducir los datos que ingresan por el cable a la unidad conocida bytes para que el CPU del equipo pueda leerlos.

La función de la tarjeta de red es la de preparar, enviar y controlar los datos en la red. Esta tarjeta de red puede ser orientada para una conexión física o de tipo inalámbrica.

Driver de Red:

El Driver de Red es un Software que sirve de intermediario entre un dispositivo (Hardware) y el sistema operativo que tiene el equipo. Su funcionamiento en el Modelo TCP/IP está basado en permitir una sincronización a través de Software entre el Protocolo IP y la Tarjeta de Red.

Protocolo ARP:

El Protocolo de Resolución de Dirección (ARP) permite que se conozca la dirección física de una Tarjeta de Interfaz de Red por medio de una dirección IP y los Driver de Red

Protocolo ICMP:

El Protocolo de Control de Mensajes de Internet (ICMP) se encarga de realizar un control de flujo de datagramas IP que circulan por la Red, es decir, se encarga de realizar las notificaciones de posibles errores y de situaciones anormales que se presenten en el envío o recepción de información a través del protocolo IP.

Protocolo UDP:

El Protocolo de Datagramas de Usuario (UDP) es el que permite crear una interfaz en las aplicaciones IP existentes, es una forma de multiplexar y demultiplexar los datagramas IP enviados a través de la red.

Protocolo HTTP:

El Protocolo de Transferencia de Hyper Texto (HTTP) está orientado en permitir la transferencia de archivos en lenguaje de marcación de Hyper Texto (HTML) entre un navegador (el cliente) y un servidor Web localizado mediante una cadena de caracteres denominados dirección de Localización Uniforme de Recursos (URL). Este protocolo se encarga de, en una página Web, proyectar los elementos de texto, imágenes, enlaces, inserciones multimedia de audio, entre otros. Al tener un buen manejo de este protocolo, se permite tener un entorno más ameno y agradable a los usuarios.

Protocolo Telnet:

El Protocolo de Comunicaciones de red (Telnet) es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor). Actualmente, éste protocolo ha evolucionado a un sistema más seguro conocido como SSH (interprete de órdenes seguras).

Protocolo SMTP:

El Protocolo Simple de Transferencia de Correo (SMTP) es el que permite la transferencia en línea de correos desde un servidor a otro mediante una conexión punto a punto.

DNS:

Es un Servidor de Dominio de nombres de servicios que permite traducir de nombre de dominio a dirección IP. De ésta forma, DNS sería una base de datos, en donde se encuentran las direcciones necesarias solicitadas por los usuarios para establecer sus peticiones de conexión en un servidor determinado.

4.7 Historia de las vulnerabilidades

En los primeros años, los ataques involucraban poca sofisticación técnica. Los ataques internos se basaban en utilizar los permisos para alterar la información. Los externos se basaban en acceder a la red simplemente averiguando una clave válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar vulnerabilidades en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevaron a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automáticos, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita un conocimiento técnico básico para realizarlos. El aprendiz de intruso, *script-kiddie,* [6] aprendiz de *hacker*[7], o *wannabee*[8], tiene acceso hoy en día a numerosos programas y scripts (exploits) que se aprovechan de las vulnerabilidades, disponibles desde numerosas fuentes underground, como hacker newsgroups, mailing-lists y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Bruce Schneier[9], ha definido y clasificado las generaciones de ataques en la red existentes a lo largo del tiempo.

La primera generación: ataque físico

Ataques que se centraban en los componentes electrónicos: ordenadores y cables. El objetivo de los protocolos distribuidos y de la redundancia es la tolerancia frente a un punto único de fallo. Son mayormente problemas para los que actualmente se conoce la solución.

La segunda generación: ataque sintáctico

Las pasadas décadas se han caracterizado por ataques contra la lógica operativa de los ordenadores y las redes, es decir, pretenden explotar las vulnerabilidades de los programas, de los algoritmos de cifrado y de los

[6] http://es.wikipedia.org/wiki/Script_Kiddie
[7] http://es.wikipedia.org/wiki/Hacker
[8] http://es.wikipedia.org/wiki/Wannabe
[9] http://www.schneier.com/

protocolos, así como permitir la denegación del servicio prestado. En este caso se conoce el problema, y se está trabajando en encontrar soluciones cada vez más eficaces.

La tercera generación: ataque semántico

Se basan en la manera en que los humanos asocian significado a un contenido. El hecho es que en la sociedad actual la gente tiende a creerse todo lo que lee (medios informativos, libros, la Web...). El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o e-mails, por ejemplo, para beneficiarse de las inversiones dentro de la bolsa financiera. También pueden llevarse a cabo modificando información caduca.

4.8 Vulnerabilidades

4.8.1 Vulnerabilidades en Capas de Modelo TCP/IP

4.8.1.1 Capa de Red

Los principales inconvenientes en esta capa pueden ocurrir si alguien tuviera acceso a los equipos con los que la red opera, es decir, acceso al cuarto de telecomunicaciones, al cableado o a los equipos remotos establecidos para la comunicación (ataques realizados en la capa de red pueden ser los que ocurren en líneas de cableado, desvío de cableado, interceptación de comunicación entre equipos), es por ello que los principales inconvenientes que pudiesen presentarse en esta capa, están asociados al grado de confidencialidad y control de acceso que pueda tener o manejar una persona.

En esta capa están tres aspectos muy importantes que se debe precautelar.

La Confidencialidad:

Es la privacidad que posee cualquier documento enviado por la red o mecanismos que necesiten un control de acceso, es así que se debe garantizar que éstos estarán disponibles únicamente para la persona autorizada a acceder a dicha información.

Autenticidad:

La autenticación es el proceso de verificación de identidad digital en una comunicación que permitirá conocer la validez de los usuarios y datos que se manipulan.

Integridad:

Es la garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta, refiriéndose principalmente a la fidelidad de la información que debe mantenerse entre el emisor y el receptor.

4.8.1.2 Capa de Internet

Es la capa de donde mayor información se puede obtener para vulnerar un sistema. Lo fundamental para acceder a ésta es tener acceso a los datagramas IP los que se pueden encontrar en cada paquete que circula por la red, mediante Software espía. Este Software permite recolectar información

mediante un proceso que se conoce como Sniffing, el cual es un término asociado a la captura de información que circula por la red, en donde se puede hacer una separación de la información, para discriminar si es relevante.

4.8.1.3 Capa de Transporte

Las principales vulnerabilidades están asociadas a la autenticación de integración y autenticación de confidencialidad. Estos términos se relacionan con el acceso a los protocolos de comunicación entre capas, permitiendo la denegación o manipulación de ellos.

4.8.1.4 Capa de Aplicación

Los posibles inconvenientes a presentarse pueden ser ocasionados por cuatro puntos, principalmente los que están asociados a la autenticación de datos y los protocolos presentes en ésta capa.

1: Se establecen las deficiencias del servicio de nombres de dominio. Este servicio, es que se encarga de generar las solicitudes de cada usuario que circulan por la red, es decir, en el momento que una persona solicita una conexión a un servicio determinado, se solicita una dirección IP y un nombre de dominio, se envía un paquete UDP (Protocolo de Comunicación el cual envía los datos del usuario) a un servidor DNS (Dominio de Nombre de Servicio). Lo que hace el servidor DNS es responder a ésta solicitud y entregar los datos que fueron pedidos, donde éste servidor DNS funciona como una base de datos en donde se encuentran las direcciones que solicitan los usuarios, por lo tanto,

cuando se tiene acceso a esta especie de base de datos se presenta un inconveniente, el cual hace vulnerable al sistema, ya que puede ser modificada a gusto de la persona que le quiere sacar provecho a esa información, pudiendo entregar direcciones incorrectas o recepcionar las peticiones de los usuarios para obtener información acerca de sus cuentas.

2: Está dado por el servicio Telnet, el cual se encarga de autentificar la solicitud de usuario, de nombre y contraseña que se trasmiten por la red, tanto por el canal de datos como por el canal de comandos.

3: Está dado por File Transfer Protocol (FTP), el cual al igual que el servicio Telnet, se encarga de autentificar. La diferencia se encuentra en que el FTP lo hace más vulnerable ya que es de carácter anónimo.

4: Está dado por el protocolo HTTP, el cual es responsable del servicio World Wide Web. La principal vulnerabilidad de este protocolo, está asociado a las deficiencias de programación que puede presentar un link determinado [7], lo cual puede poner en serio riesgo el equipo que soporta este link, es decir, el computador servidor.

4.8.2 Escuchas de red

Se trata de un ataque realmente efectivo, puesto que permite la obtención de una gran cantidad de información sensible.

Mediante aplicaciones que se encargan de capturar e interpretar tramas y datagramas en entornos de red basados en difusión, conocidos como escuchas de red o sniffers, es posible realizar el análisis de la información contenida en los paquetes TCP/IP que interceptan para poder extraer todo tipo de información.

5.3.2.1 Sniffing

Las técnicas de sniffing también se conocen como técnicas de eavesdropping y técnicas de snooping. La primera, eavesdropping, es una variante del sniffing, caracterizada por realizar la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la información.

Por otra parte, las técnicas de snooping se caracterizan por el almacenamiento de la información capturada en el ordenador del atacante, mediante una conexión remota establecida durante toda la sesión de captura. En este caso, tampoco se modifica la información incluida en la transmisión.

5.3.2.2 Suplantación ARP

El protocolo ARP es el encargado de traducir direcciones IP de 32 bits, a las correspondientes direcciones hardware, generalmente de 48 bits en dispositivos Ethernet. Cuando un ordenador necesita resolver una dirección IP en una dirección MAC, lo que hace es efectuar una petición ARP (arp-request)

a la dirección de difusión de dicho segmento de red, FF:FF:FF:FF:FF:FF, solicitando que el equipo que tiene esta IP responda con su dirección MAC.

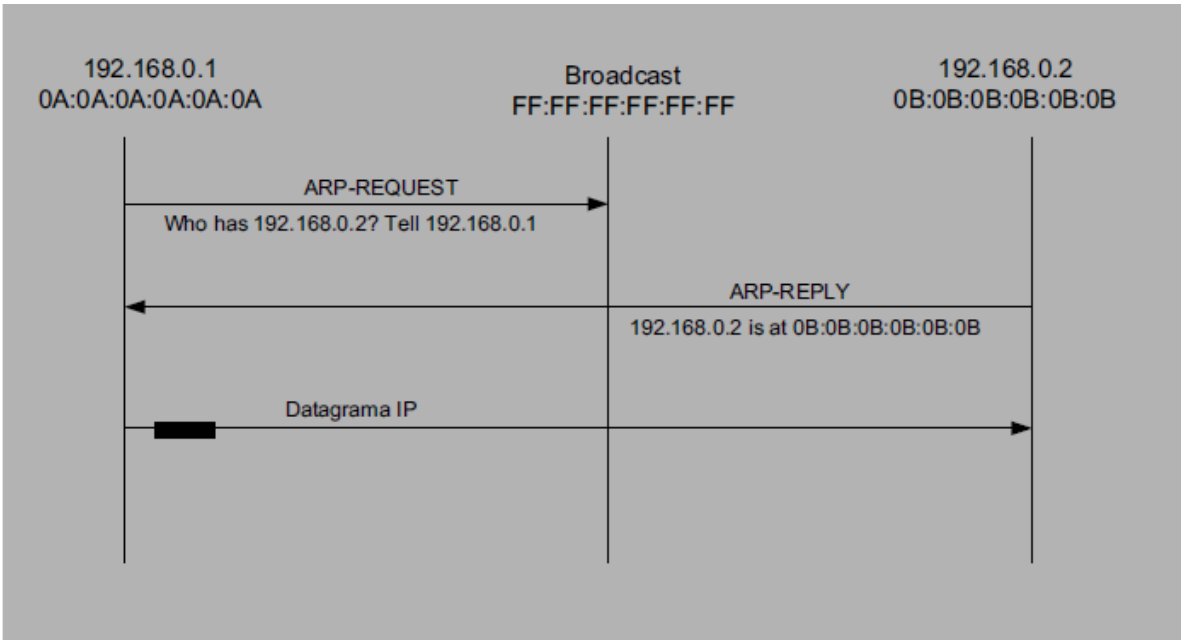


Gráfico N° 11 Suplantación ARP

Con el objetivo de reducir el tráfico en la red, cada respuesta de ARP (arp-reply) que llega a la tarjeta de red es almacenada en una tabla caché, aunque la máquina no haya realizado la correspondiente petición. Así pues, toda respuesta de ARP que llega a la máquina es almacenada en la tabla de ARP de esta máquina. Este factor es el que se utilizará para realizar el ataque de suplantación de ARP.

5.3.2.3 Desactivación de filtro Mac

Una de las técnicas más utilizadas por la mayoría de los sniffers de redes Ethernet se basa en la posibilidad de configurar la interfaz de red para que desactive su filtro MAC (poniendo la tarjeta de red en modo promiscuo).

Las redes basadas en dispositivos Ethernet fueron concebidas en torno a una idea principal: todas las máquinas de una misma red local comparten el mismo medio, de manera que todos los equipos son capaces de ver el tráfico de la red de forma global.

Cuando se envían datos es necesario especificar claramente a quién van dirigidos, indicando la dirección MAC. De los 48 bits que componen la dirección MAC, los 24 primeros bits identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante. Esto garantiza que dos tarjetas no puedan tener la misma dirección MAC.

Para evitar que cualquier máquina se pueda apropiar de información fraudulenta, las tarjetas Ethernet incorporan un filtro que ignora todo el tráfico que no les pertenece, descartando aquellos paquetes con una dirección MAC que no coincide con la suya. La desactivación de este filtro se conoce con el nombre de modo promiscuo.

Con el uso adecuado de expresiones regulares y otros filtros de texto, se podrá visualizar o almacenar únicamente la información que más interese; en

especial, aquella información sensible, como nombres de usuario y contraseñas.

El entorno en el que suele ser más efectivo este tipo de escuchas son las redes de área local configuradas con una topología en bus. En este tipo de redes, todos los equipos están conectados a un mismo cable. Esto implica que todo el tráfico transmitido y recibido por los equipos de la red pasa por este medio común.

4.8.3 Fragmentación de IP

4.8.3.1 Fragmentación en redes Ethernet

La MTU (unidad de transmisión mixta), por defecto de un datagrama IP para una red de tipo Ethernet es de 1500 bytes. Así pues, si un datagrama IP es mayor a este tamaño y necesita circular por este tipo de red, será necesario fragmentarlo por medio del enrutador que dirige la red. Los fragmentos pueden incluso fragmentarse más si pasan por una red con una MTU más pequeña que su tamaño.

Para que el equipo de destino pueda reconstruir los fragmentos, ´estos deben contener la siguiente información:

- Cada fragmento tiene que estar asociado a otro utilizando un identificador de fragmento común. Este se clonará desde un campo de la cabecera IP, conocido como identificador IP (también llamado ID de fragmento).

- Información sobre su posición en el paquete inicial (paquete no fragmentado).
- Información sobre la longitud de los datos transportados al fragmento.
- Cada fragmento tiene que saber si existen más fragmentos a continuación. Esto se indica en la cabecera, dejando o no activado el indicador de más fragmentos (more fragments, MF) del datagrama IP.

Toda esta información irá en la cabecera IP, colocada en el datagrama IP. Esto afectará a todo el tráfico TCP/IP puesto que IP es el protocolo responsable de la entrega de los paquetes.

4.8.2. Fragmentación para enmascaramiento de datagramas IP

La fragmentación IP puede plantear una serie de problemáticas relacionadas con la seguridad de nuestra red.

Aparte de los problemas de denegación que veremos con más detenimiento en la siguiente sección, una de las problemáticas más destacadas es la utilización de fragmentación IP malintencionada para burlar las técnicas básicas de inspección de datagramas IP.

En este caso, un atacante tratará de provocar intencionadamente una fragmentación en los datagramas que envía a nuestra red con el objetivo de que pasen desapercibidos por diferentes dispositivos de prevención y de

detección de ataques que no tienen implementado el proceso de fragmentación y reensamblado de datagramas IP.

4.8.4 Denegación de servicios

Un ataque de denegación de servicio es un incidente en el cual un usuario o una organización es privada de los servicios de un recurso que esperaba obtener. Normalmente, la pérdida de servicio se corresponde con la imposibilidad de obtener un determinado servicio de red como, por ejemplo, el acceso a una página web.

Los ataques de denegación de servicio pueden ser provocados tanto por usuarios internos en el sistema como por usuarios externos. Dentro del primer grupo podríamos pensar en usuarios con pocos conocimientos que pueden colapsar el sistema o servicio inconscientemente.

Por ejemplo, usuarios que abusan de los recursos del sistema, ocupando mucho ancho de banda en la búsqueda de archivos de música o de películas, usuarios malintencionados que aprovechan su acceso al sistema para causar problemas de forma premeditada, etc.

En el segundo grupo se encuentran aquellos usuarios que han conseguido un acceso al sistema de forma ilegítima, falseando además la dirección de origen con el propósito de evitar la detección del origen real del ataque (mediante ataques de suplantación).

El peligro de los ataques de denegación de servicio viene dado por su independencia de plataforma. Como sabemos, el protocolo IP permite una comunicación homogénea (independiente del tipo de ordenador o fabricante) a través de espacios heterogéneos (redes Ethernet, ATM). De esta forma, un ataque exitoso contra el protocolo IP se convierte inmediatamente en una amenaza real para todos los equipos conectados a la red, independientemente de la plataforma que utilicen.

4.8.4.1 IP Flooding

El ataque de IP Flooding se basa en una inundación masiva de la red mediante datagramas IP.

Este ataque se realiza habitualmente en redes locales o en conexiones con un gran ancho de banda. Consiste en la generación de tráfico basura con el objetivo de conseguir la degradación del servicio. De esta forma, se resume el ancho de banda disponible, ralentizando las comunicaciones existentes de toda la red.

Podemos pensar en la utilización de este ataque principalmente en redes locales cuyo control de acceso al medio es nulo y cualquier máquina puede ponerse a enviar y recibir paquetes sin que se establezca ningún tipo de limitación en el ancho de banda que consume.

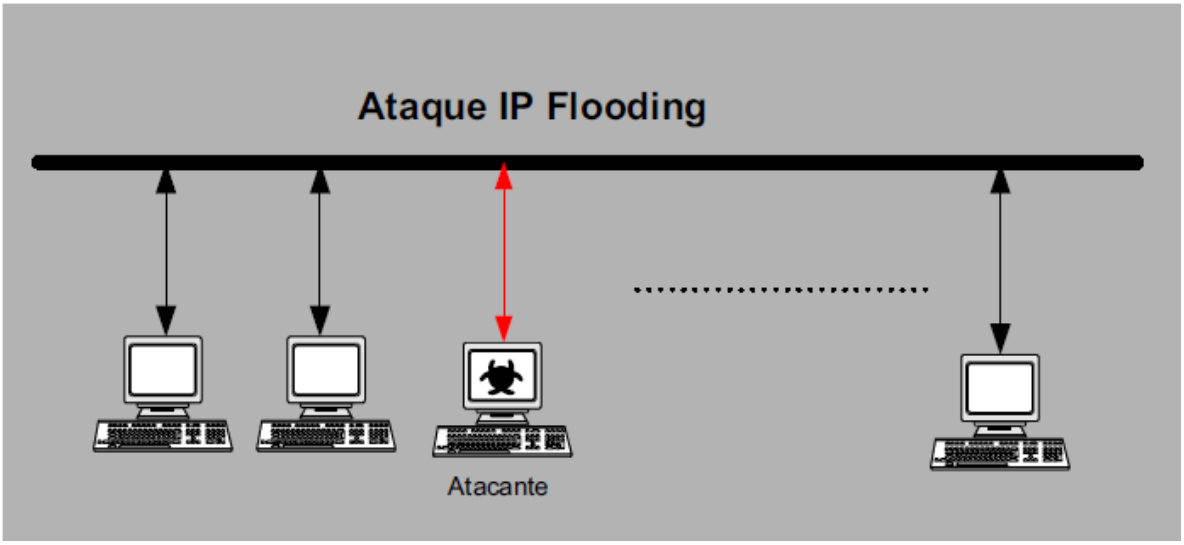


Gráfico N° 12 IP Flooding

El tráfico generado en este tipo de ataque puede ser:

- Aleatorio. Cuando la dirección de origen o destino del paquete IP es ficticia o falsa.

  Este tipo de ataque es el más básico y simplemente busca degradar el servicio de comunicación del segmento de red al que está conectado el ordenador responsable del ataque.
- Definido o dirigido. Cuando la dirección de origen, destino, o incluso ambas, es la de la máquina que recibe el ataque. El objetivo de este ataque es doble, ya que además de dejar fuera de servicio la red donde el atacante genera los datagramas IP, también tratará de colapsar al equipo de destino, sea reduciendo el ancho de banda disponible, o bien saturando su servicio ante una gran cantidad de peticiones que el servidor será incapaz de procesar.

Los datagramas IP utilizados podrían corresponder a:

- UDP. Con el objetivo de generar peticiones sin conexión a ninguno de los puertos disponibles. Según la implementación de la pila TCP/IP de las máquinas involucradas, las peticiones masivas a puertos específicos UDP pueden llegar a causar el colapso del sistema.
- ICMP. Generando mensajes de error o de control de flujo.
- TCP. Para generar peticiones de conexión con el objetivo de saturar los recursos de red de la máquina atacada.

Una variante del IP Flooding tradicional consiste en la utilización de la dirección de difusión de la red como dirección de destino de los datagramas IP. De esta forma, el enrutador de la red se verá obligado a enviar el paquete a todos los ordenadores de la misma, consumiendo ancho de banda y degradando el rendimiento del servicio.

También existen otras variantes en las que se envían peticiones ICMP de tipo echo-request a varios ordenadores suplantando la dirección IP de origen, sustituida por la dirección de difusión (broadcast) de la red que se quiere atacar. De esta forma, todas las respuestas individuales se ven amplificadas y propagadas a todos los ordenadores conectados a la red.

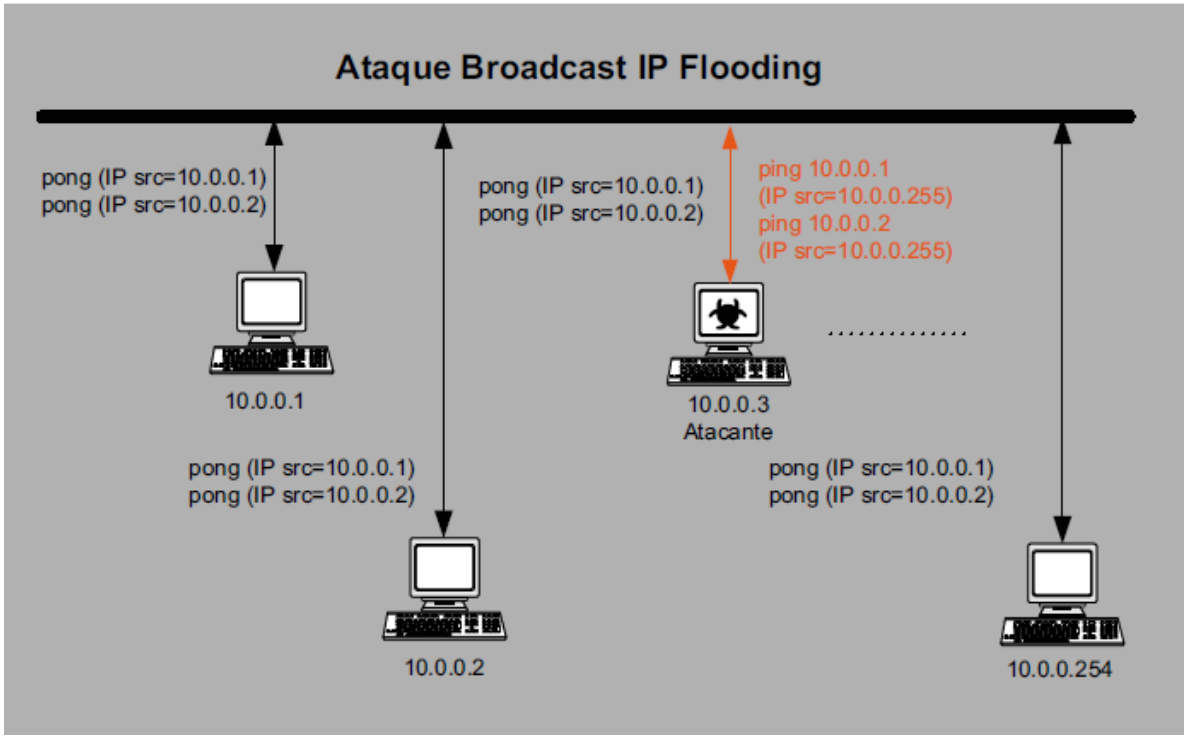


Gráfico N° 13 Ataque Broadcast IP Flooding

4.8.4.2 Smurf

Este tipo de ataque de denegación de servicio es una variante del (IP Flooding), pero realizando una suplantación de las direcciones de origen y destino de una petición ICMP del tipo echo-request:

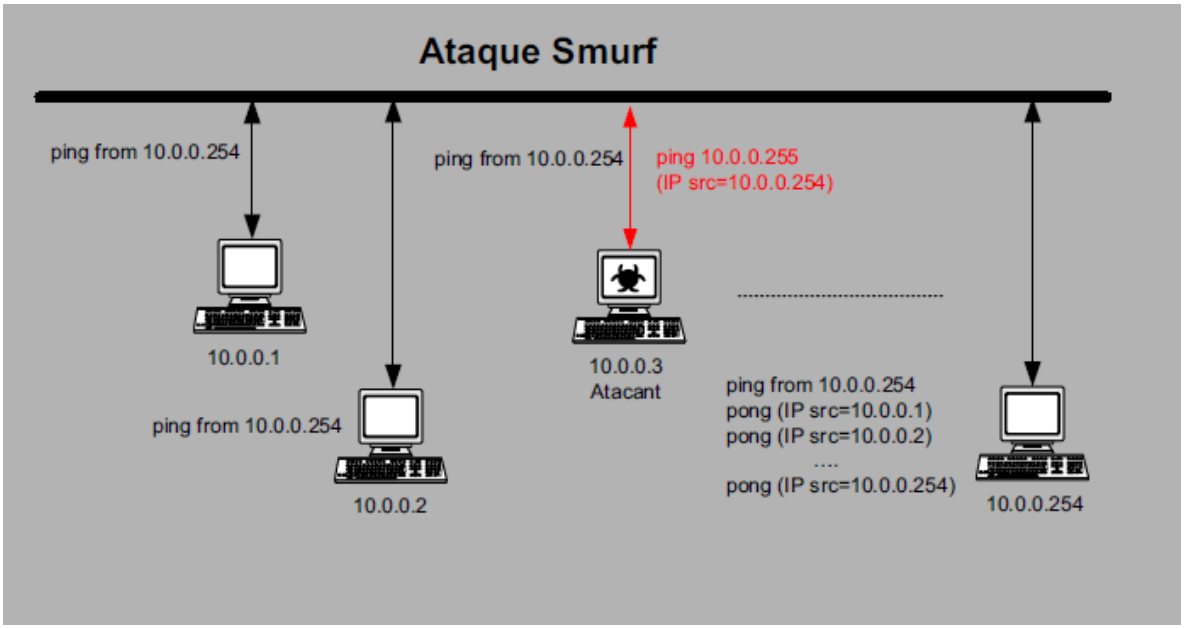


Gráfico N° 14 Smurf

Como dirección de origen se pone la dirección IP de la máquina que debe ser atacada. En el campo de la dirección IP de destino se pone la dirección de difusión de la red local o red que se utilizará como trampolín para colapsar a la víctima.

Con esta petición fraudulenta, se consigue que todas las máquinas de la red respondan a la vez a una misma máquina, consumiendo todo el ancho de banda disponible y saturando el ordenador atacado

4.8.4.3 TCP/SYN Flooding

El ataque de TCP/SYNFlooding se aprovecha del número de conexiones que están esperando para establecer un servicio en particular para conseguir la denegación del servicio.

Cuando un atacante configura una inundación de paquetes SYN de TCP, no tiene ninguna intención de complementar el protocolo de intercambio, ni de establecer la conexión. Su objetivo es exceder los límites establecidos para el número de conexiones que están a la espera de establecerse para un servicio dado.

Esto puede hacer que el sistema que es víctima del ataque sea incapaz de establecer cualquier conexión adicional para este servicio hasta que las conexiones que estén a la espera bajen el umbral.

Hasta que se llegue a este límite, cada paquete SYN genera un SYN/ACK que permanecerá en la cola a la espera de establecerse. Es decir, cada conexión tiene un temporizador (un límite para el tiempo que el sistema espera, el establecimiento de la conexión) que tiende a configurarse en un minuto.

Cuando se excede el límite de tiempo, se libera la memoria que mantiene el estado de esta conexión y la cuenta de la cola de servicios disminuye en una unidad. Después de alcanzar el límite, puede mantenerse completa la cola de servicios, evitando que el sistema establezca nuevas conexiones en este puerto con nuevos paquetes SYN.

Dado que el único propósito de la técnica es inundar la cola, no tiene ningún sentido utilizar la dirección IP real del atacante, ni tampoco devolver los

SYN/ACK, puesto que de esta forma facilitaría que alguien pudiera llegar hasta ´el siguiendo la conexión. Por lo tanto, normalmente se falsea la dirección de origen del paquete, modificando para ello la cabecera IP de los paquetes que intervendrán en el ataque de una inundación SYN.

6.3.4.4 Teardrop

El ataque Teardrop intentará realizar una utilización fraudulenta de la fragmentación IP para poder confundir al sistema operativo en la reconstrucción del datagrama original y colapsar así el sistema.

4.8.4.5 Snork

El ataque Snork se basa en una utilización malintencionada de dos servicios típicos en sistemas Unix: el servicio CHARGEN (CHARacter GENerator, generador de caracteres) y el servicio ECHO.

El primer servicio se limita a responder con una secuencia aleatoria de caracteres a las peticiones que recibe. El segundo servicio, ECHO, se utiliza como sistema de pruebas para verificar el funcionamiento del protocolo IP.

Así, esta denegación de servicio se basa en el envío de un datagrama especial al ordenador de destino, que una vez reconocido, enviará una respuesta al equipo de origen.

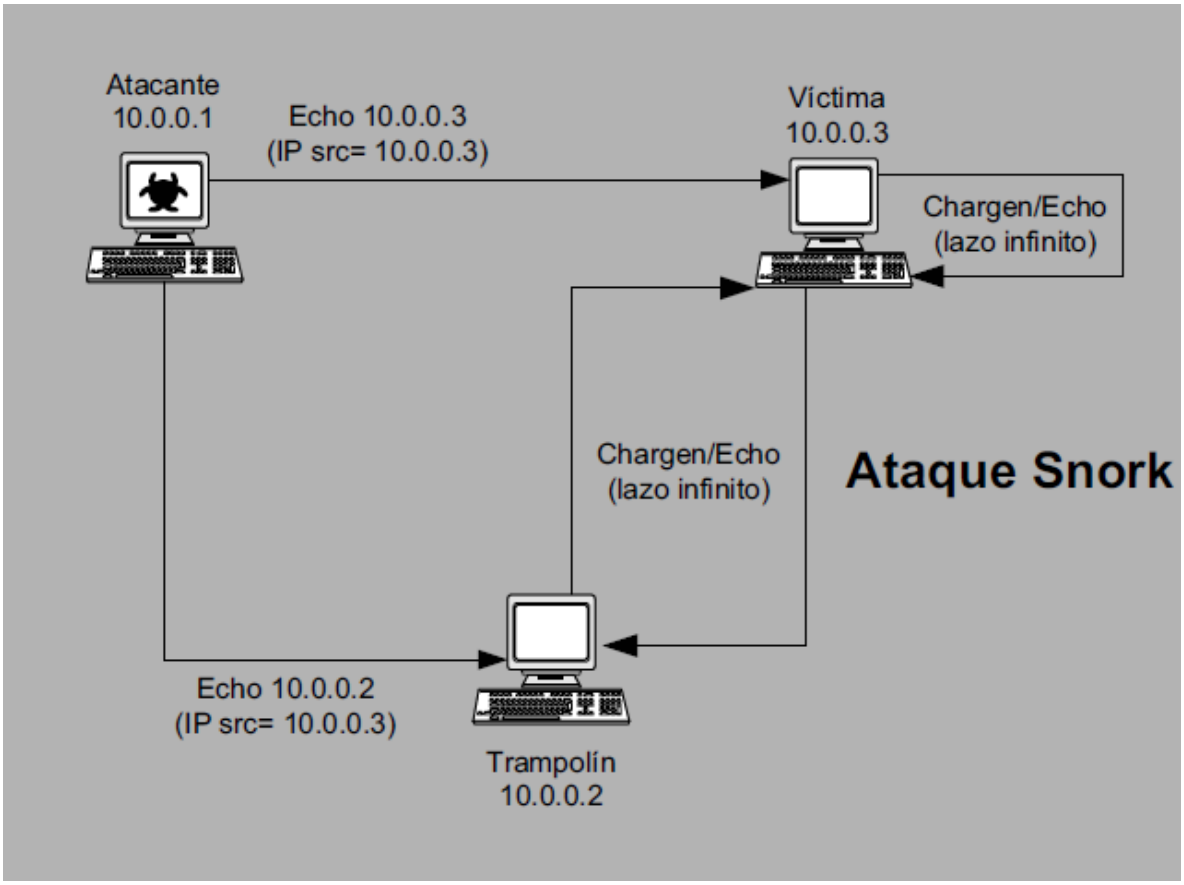


Gráfico N° 15 Ataque Snork

El ataque Snork consiste en el cruce de los servicios ECHO y CHARGEN, mediante el envío de una petición falsa al servicio CHARGEN, habiendo colocado previamente como dirección de origen la dirección IP de la máquina que hay que atacar (con el puerto del servicio ECHO como puerto de respuesta). De esta forma, se inicia un juego de ping-pong infinito.

Este ataque se puede realizar con distintos pares de equipos de la red obteniendo un consumo masivo de ancho de banda hasta degradar el rendimiento de la misma. También se puede realizar contra una misma

máquina (ella misma se envía una petición y su respuesta) consiguiendo consumir los recursos (especialmente CPU y memoria) de este equipo.

4.8.4.6 Ping of death

El ataque de denegación de servicio (ping of death) es uno de los ataques más conocidos. Al igual que otros ataques de denegación existentes, utiliza una definición de longitud máxima de datagrama IP fraudulenta.

La longitud máxima de un datagrama IP es de 65535 bytes, incluyendo la cabecera del paquete (20 bytes) y partiendo de la base de que no hay opciones especiales especificadas. Por otra parte, recordemos que el protocolo ICMP tiene una cabecera de 8 bytes. De esta forma, si queremos construir un mensaje ICMP tenemos disponibles 65535 - 20 - 8 = 65507 bytes.

Debido a la posibilidad de fragmentación de IP, si es necesario enviar más de 65535 bytes, el datagrama IP se fragmentará y se reensamblará en el destino con los mecanismos que comentados anteriormente.

El ataque ping de la muerte se basa en la posibilidad de construir, mediante el comando ping, un datagrama IP superior a los 65535 bytes, fragmentado en N trozos, con el objetivo de provocar incoherencias en el proceso de reensamblado.

4.8.4.7 Ataques distribuidos

Un ataque de denegación de servicio distribuido es aquél en el que una multitud de sistemas (que previamente han sido comprometidos) cooperan entre ellos para atacar a un equipo objetivo, causándole una denegación de servicio. El flujo de mensajes de entrada que padece el equipo atacado le dejará sin recursos y será incapaz de ofrecer sus servicios a usuarios legítimos.

Así pues, podemos definir los ataques de denegación de servicio distribuidos como un ataque de denegación de servicio en el que existen múltiples equipos sincronizados de forma distribuida que se unen para atacar un mismo objetivo.

En la siguiente figura podemos observar el diagrama de tres capas que conforma un ataque ejecutado mediante TRIN00. Vemos cómo a partir de un único ordenador, el atacante podrá llegar a obtener toda una red de equipos a su disposición para la realización del ataque distribuido:

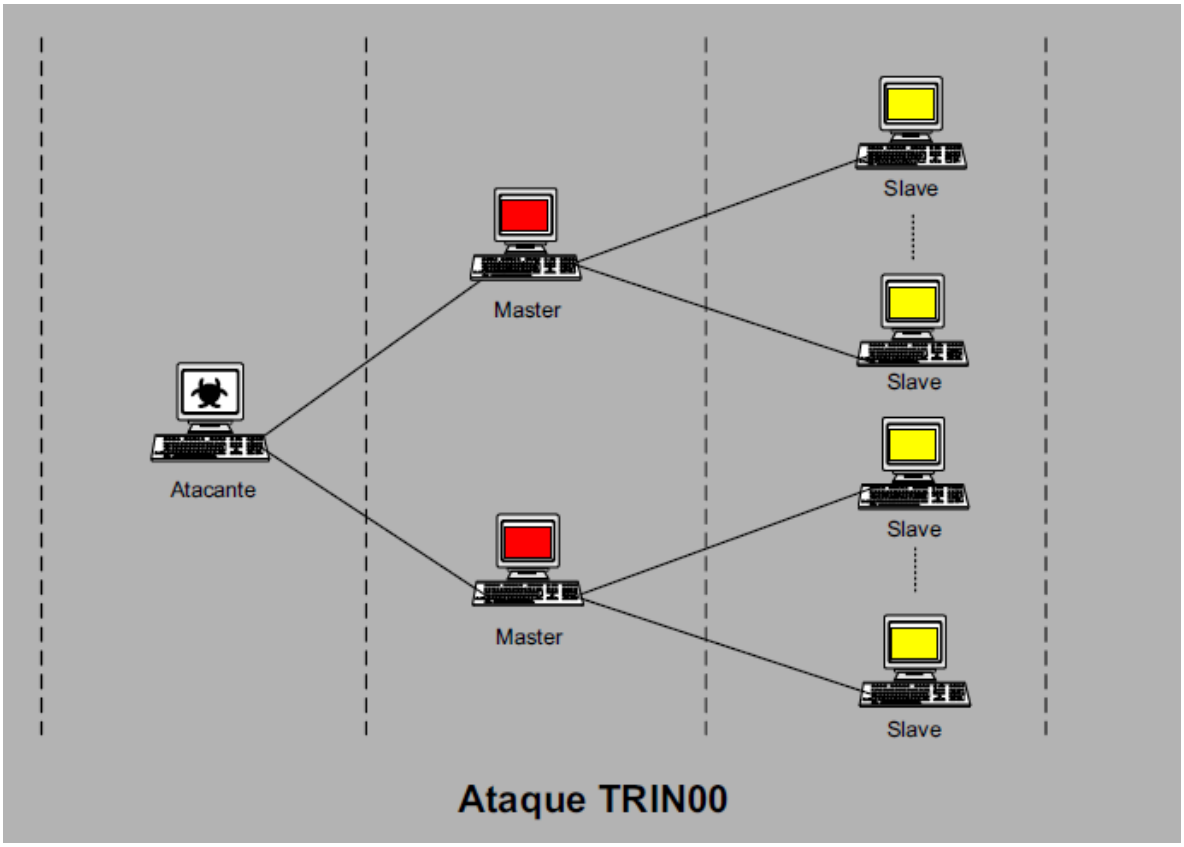


Gráfico N° 16 Ataque TRIN00

La comunicación entre las distintas capas se realiza mediante conexiones TCP (fiables) para la parte atacante-master, y conexiones UDP (no fiables) para la parte master-slave y slave-master, en puertos específicos de cada máquina.

4.8.5 Deficiencias de programación

4.8.5.1 Buffer-overflows

Un ataque de desbordamiento de *buffer* se basa en la posibilidad de escribir información más allá de los límites de una tupla almacenada en la pila de ejecución. A partir de esta tupla, asociada a una llamada a función dentro del programa, se puede conseguir corromper el flujo de la ejecución modificando el

valor de regreso de la llamada a la función. Si este cambio en el flujo de ejecución es posible, se podrá llevar la ejecución a una dirección de memoria arbitraria (introducida en los datos de la pila a partir del mismo ataque) y ejecutar un código malicioso.

El éxito de este ataque será posible en aquellos programas que utilizan funciones de manipulación de buffers que no comprueban los límites de las estructuras de los datos.

4.8.5.2 Format strings

Los ataques que explotan deficiencias de programación mediante cadenas de formato se producen en el momento de imprimir o copiar una cadena de caracteres desde un buffer sin las comprobaciones necesarias.

4.9 Seguridades de red

4.9.1 Firewall

Es un hardware o software ubicado entre dos redes que ejecuta políticas de seguridad establecidas para dar acceso o negación a un equipo determinado.

Es el encargado de proteger una red de otra q no lo es. (Internet)

Gráfico N° 17 Firewall

4.9.2 Tipos de Firewall

4.9.2.1 Filtrado de Paquetes

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

1. Protocolos utilizados.
2. Dirección IP de origen y de destino.
3. Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir

navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
- Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

4.9.2.2 Proxy-Gateways de Aplicaciones

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las

conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastión Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

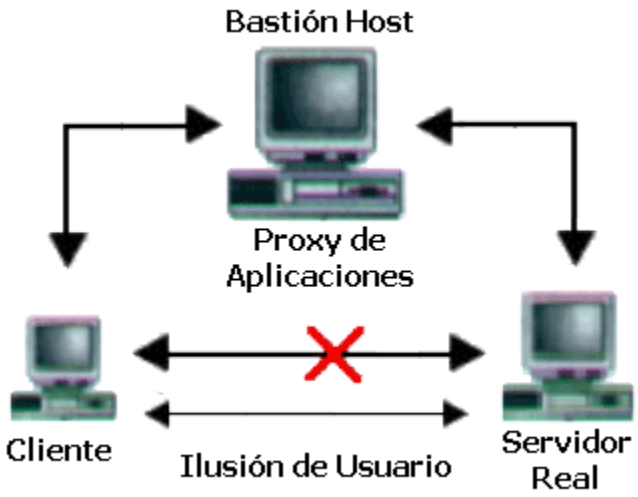


Gráfico N° 18 Bastión Host

4.9.2.3 Dual-Homed Host

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

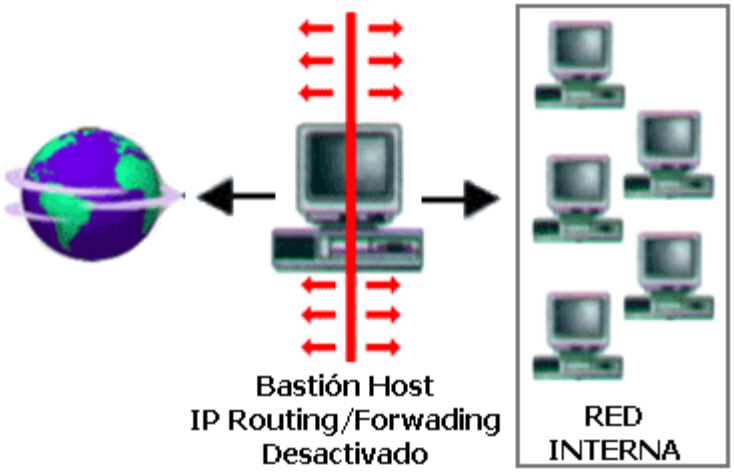


Gráfico N° 19 Dual-Homed Host

4.9.2.4 Screened Host

En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

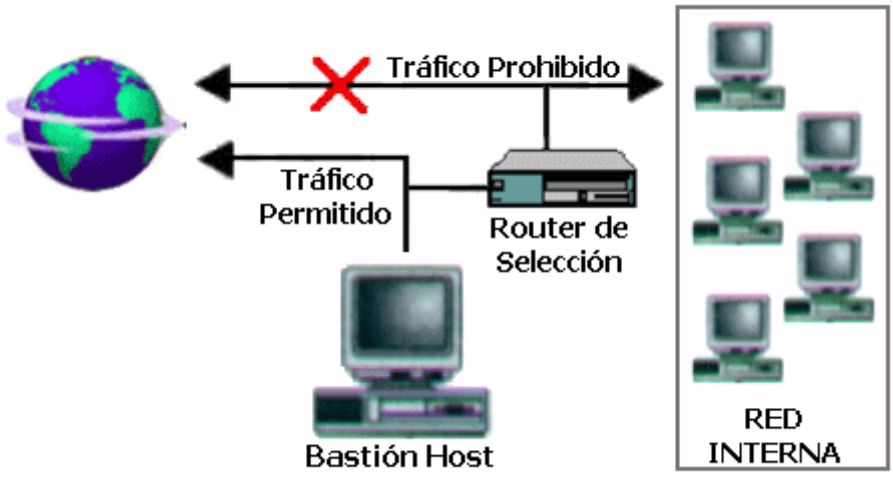


Gráfico N° 20 Screened Host

4.9.2.5 Screened Subnet

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.

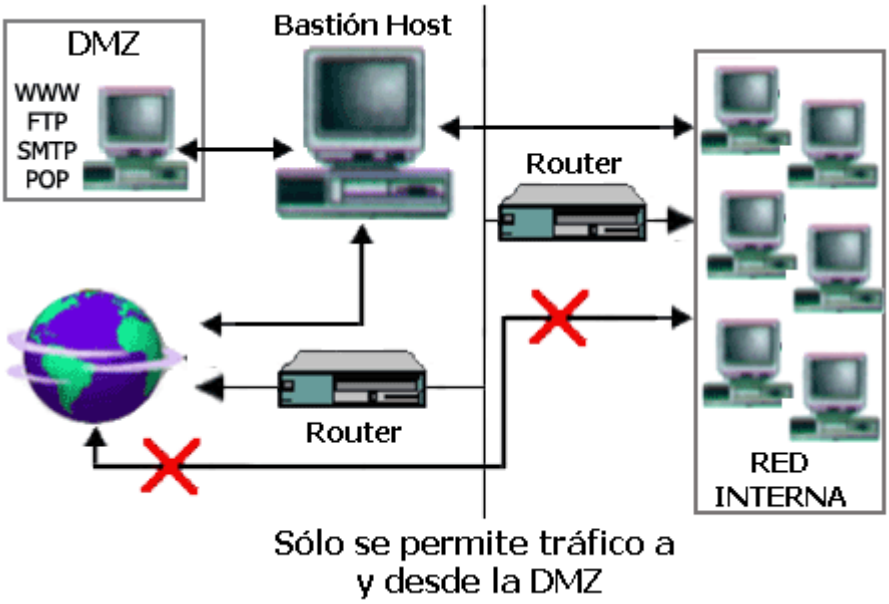


Gráfico N° 21 Screened Subnet

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, n o existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.

2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

4.9.2.6 Inspección de Paquetes

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

4.9.2.7 Firewalls Personales

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

Capítulo V

Conclusiones

El estudio realizado del funcionamiento de los IDS, nos presenta una amplia gama de opciones para prevenir de ataques a nuestra red de computadores, ya que constamos con IDS que están basados en hardware y software.

Las vulnerabilidades que presentan los protocolos TCP/IP nos generan una gran vulnerabilidad y pone en riesgo nuestro bien más preciado que para nosotros sería la información.

La seguridad que nos puede brindar los firewall está ligada al tipo de protección para el que le configuremos a nuestro firewall.

En fin diríamos que para mantener una red segura contra ataques de personas inescrupulosas se debe tener en cuenta todas las medidas de seguridad posibles que en la actualidad la tecnología nos brinda tanto en hardware como de software, de estas maneras podremos tener una red con mayor fiabilidad para la trasmisión de datos.

Recomendaciones

Para tener un entendimiento más profundo sobre las vulnerabilidades y seguridades que existen para la transición de datos a través de redes de computadores, se podría aplicar los siguientes criterios:

- Implementación de los distintos tipos de software IDS que existe.
- Comparar la eficacia de cada uno.
- Identificar las variaciones que puedan tener los ataque a las redes.

Bibliografía

Arcert. (Noviembre de 1999). Manual de Seguridad, Seguridad en Redes. Argentina.

HUERTA, A. V. (Octubre de 2000). Seguridad en Unix y Redes.

Ko, C. C. (1996). Execution Monitoring of Security-Critical Programs in a Distributed System. California, EE.UU.

Montagnier, J.-L. (1995). Administración UNIX: System V y redes TCP/IP. Barcelona: Gestión 2000.

Montagnier, L. (1996). Administracion unix.system V & redes tcp/ip. Barcelona: Gestion 2000.

Jumes, G. (1999). Microsoft windows nt 4.0: seguridad, auditoría y control. Madrid: McGraw-Hill.

Rodríguez, L. (1995). Seguridad de la información en sistemas de cómputos, México: Ventura.

Fisher, P (1988). Seguridad en los sistemas informáticos. Madrid: Díaz de Santos.

Wasserman, Joseph J. *The Vanishing Trail*. Bell Telephone Magazine 47, no. 4, July - August 1968: 12 - 15

Links consultados

- http://articulos.astalaweb.com/Seguridad%20y%20Virus/Problemas%20de%20seguridad%20más%20habituales%20en%20Internet.asp
- http://ceres.ugr.es/~jedv/descargas/2005_jitel05-n3.pdf
- http://dk4nno.wordpress.com/2008/01/22/ids-sistemas-de-detecion-de-intrusos/
- http://es.kioskea.net/contents/detection/ids.php3
- http://es.kioskea.net/contents/secu/secuintro.php3
- http://es.wikipedia.org/wiki/Seguridad_informática
- http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
- http://fmc.axarnet.es/redes/indice.htm
- http://gost.isi.edu/cidf/
- http://kahit.wordpress.com/2008/03/13/sistemas-de-deteccion-de-intrusos-ids/
- http://programoweb.com/72230/desactivacion-de-filtro-mac/
- http://protegete.jccm.es/protegete/opencms/Administracion/Seguridad/SeguridadInformacion/seguridadredes.html
- http://seguridadyredes.wordpress.com/2007/12/28/sistemas-de-deteccion-de-intrusos-y-snort-i/
- http://ufpr.dl.sourceforge.net/project/librosperpinan/LibrosFCLD/Libro-Seguridad-GNU-Linux-Antonio-Perpinan-2011.pdf
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-netprot.html
- http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf
- http://www.acis.org.co/index.php?id=225
- http://www.biblioteca.co.cr/pdf/network-intrusion-detection.pdf
- http://www.biblioteca.co.cr/seguridad-ids.shtml
- http://www.criptored.upm.es/guiateoria/gt_m481a.htm
- http://www.fi.upm.es/docs/servicios/seguridad_informatica/371_recomendaciones.pdf
- http://www.gont.com.ar

- http://www.govannom.org/seguridad/10-ids-idp/127-arquitectura-y-comunicacion-en-un-ids-pdf.html
- http://www.idssoftware.com
- http://www.isoc.org/seinit/portal/index.php?option=com_content&task=view&id=29&Itemid=26&limit=1&limitstart=1&lang=es
- http://www.prnewswire.com/news-releases/problemas-de-seguridad-en-la-red-amenazan-la-integridad-de-las-redes-de-comunicaciones-116732844.html
- http://www.scirus.com/srsapp/sciruslink?src=web&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIIJNSI%2FIIIENSI.ppt
- http://www.segu-info.com.ar/ataques/ataques.htm
- http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- http://www.segu-info.com.ar/logica/seguridadlogica.htm
- http://www.segu-info.com.ar/proteccion/deteccion.htm
- http://www.seguridadenlared.org/es/
- http://www.slideshare.net/pcorcuera/principales-problemas-de-seguridad-en-redes-corporativas-e-institucionales
- http://www.virusprot.com/Art40.htm
- https://escert.upc.edu/content/sistemas-de-detección-de-intrusiones
- http://datatracker.ietf.org/wg/idwg/charter/
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html
- http://www.rediris.es/cert/doc/unixsec/node26.html

Glosario

ARP: Address Resolution Protocol (protocolo de resolución de direcciones)

Background: toda tarea o trabajo que se realiza en segundo plano, es decir, algo que se está llevando a cabo con una prioridad baja.

CIDF: El Marco Común de detección de intrusiones

CISL: (Common Intrusion Specification Language) Especificación del lenguaje común de intrusiones

DIDS: (Distributed Intrusion Detection System) System distribution de detection de intrusion.

DNS: Domain Name System o DNS (sistema de nombres de dominio)

Ethernet: Red de área local (LAN) desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN.

Firewall: se trata de cualquier programa que protege a una red de otra red

FTP: (File Transfer Protocol) Protocolo de Transferencia de Archivos

Gateway: Dispositivo conectado a múltiples redes TCP/IP físicas y capaz de enrutar o transportar paquetes IP de unas a otras.

Hardware: Corresponde a todas las partes tangibles de un sistema informático sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Host: Un host es un computador que permite a los usuarios comunicarse con otros sistemas centrales de una red.

HTTP: Hypertext Transfer Protocol o HTTP (protocolo de transferencia de hipertexto).

ICMP: (Internet Control Message Protocol) Protocolo de Mensajes de Control de Internet.

IDS: (Intrusion Detection System) Sistema de detección de intrusos.

Internet: Es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.

Log: Archivo que registra movimientos y actividades de un determinado programa.

MAC: (media access control) Control de Acceso al Medio.

Network: series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí.

NIDS: (Network Intrusion Detection System o IDS) Sistema de detección de intrusos en una Red..

Proxi: Servidor encargado de centralizar la comunicación entre Internet y una red privada

Scanning: evalúa la seguridad de un sistema informático o red de transmisión de datos, en búsqueda de vulnerabilidades

Sistema: Conjunto de procesos o elementos interrelacionados con un medio para formar una totalidad encauzada hacia un objetivo común.

SMTP: (Simple Mail Transfer Protocol), Protocolo Simple de Transferencia de Correo.

Software: Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático.

TCP/IP: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP).

Telnet: (Telecommunication Network) se utiliza para acceder a una computadora y manejarla de forma remota.

Tupla: una tupla corresponde a una fila de una tabla.

UDP: (User Datagram Protocol) Protocolo de Datagrama de Usuario.

Anexos

IDS de Hardware

Cisco Secure IDS 4230

El sensor Cisco Secure IDS 4230 es un "dispositivo" de seguridad de red que detecta cualquier actividad anómala que se transmite por la red, por ejemplo ataques de hackers, que realizan un análisis del tráfico en tiempo real, el sensor cisco permitiendo responder con rapidez ante las amenazas de seguridad.

Cuando el sensor detecta una actividad anómala, el sensor puede enviar alarmas a la consola de administración con detalles de la actividad y puede controlar otros sistemas, como los routers, para terminar las sesiones no autorizadas.

Su aplicación esta optimizada para trabajar sobre redes de 100 Mbps y es ideal para el control de tráfico de puertos SPAN (Switched Port Analyzer).

IDS Software

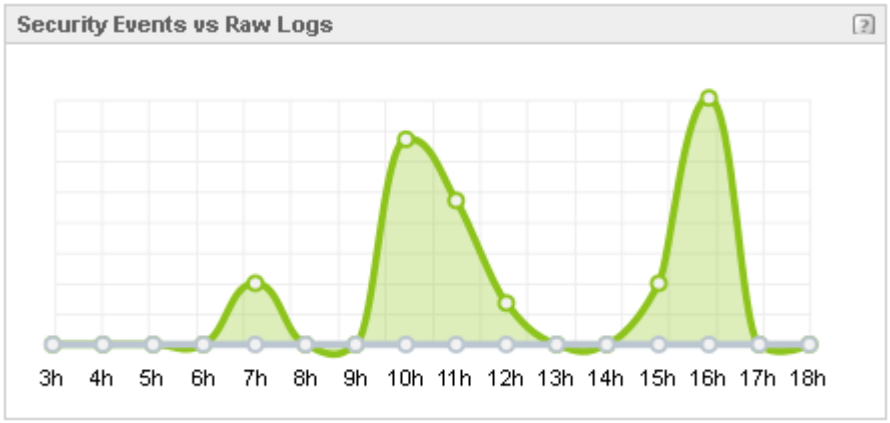
AlienVault Open Source SIEM (OSSIM)

Es un software de gestión de seguridad disponible sin costo alguno, AlienVault OSSIM proporciona toda la funcionalidad necesaria para detectar perfiles de ataques y proporciona una plataforma completa e inteligente gestión de seguridad.

AlienVault incluye una serie de herramientas (Snort, Ntop, Tcptrack, Arpwatch…) que permiten analizar todo el tráfico de red en busca de problemas de seguridad y anomalías. Para poder sacar provecho de esta funcionalidad de AlienVault es imprescindible que el Sensor de AlienVault sea capaz de ver todo el tráfico de la red, bien sea utilizando un concentrador, o configurando un port mirroring o port Span en la electrónica de red.

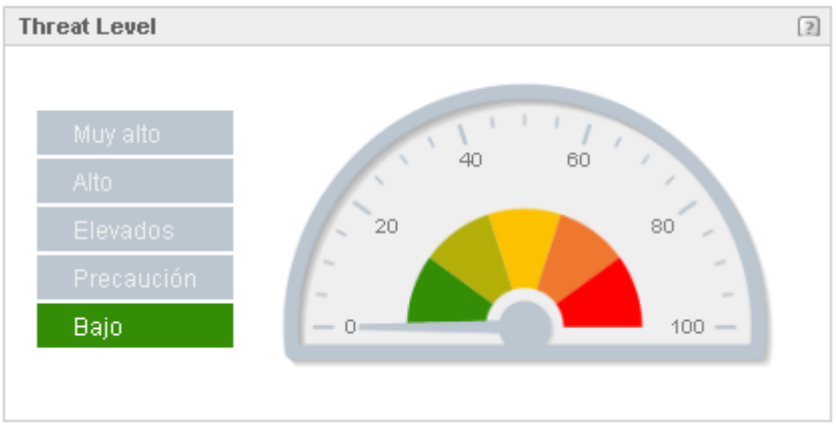
Todos los sensores de AlienVault envían sus eventos a un único servidor que se encarga de efectuar una valoración del riesgo para cada evento, y en el que también tendrá lugar el proceso de correlación. Una vez estos dos procesos han tenido lugar, los eventos son almacenados en la base de datos.

Eventos de registros frente a registros losg

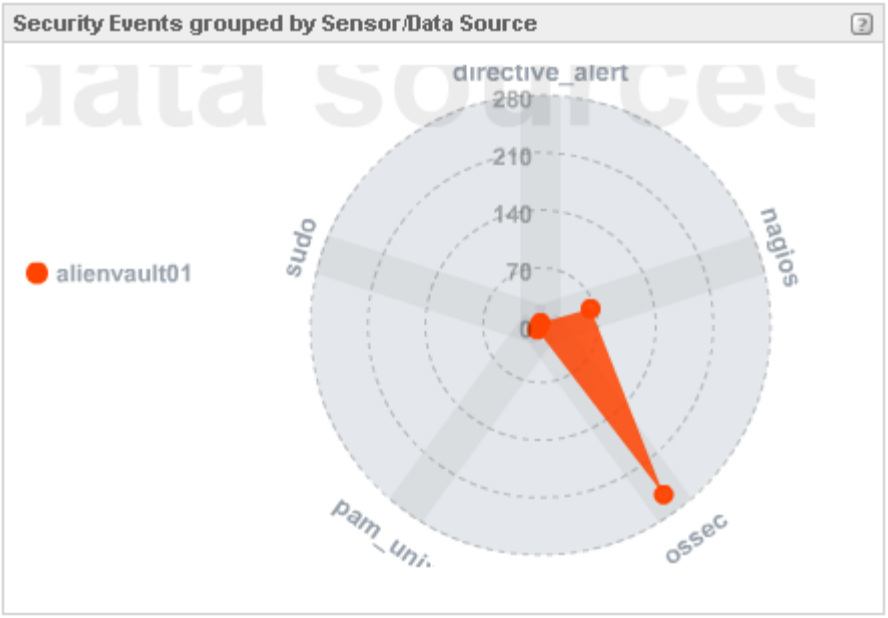


Aquí podemos aprecios que no tenemos registros de logs porque no hemos sufrido ninguna amenaza y solo nos muestra los eventos que han sucedido.

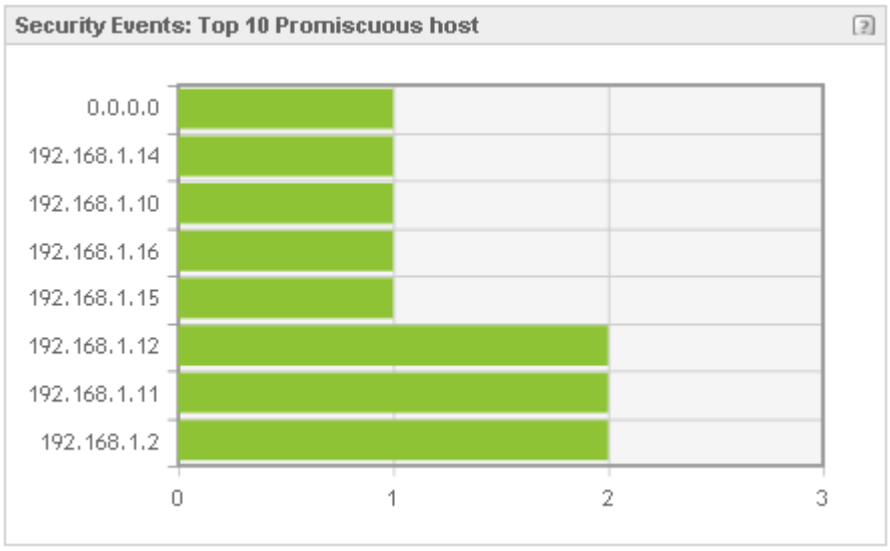
Nivel de amenaza

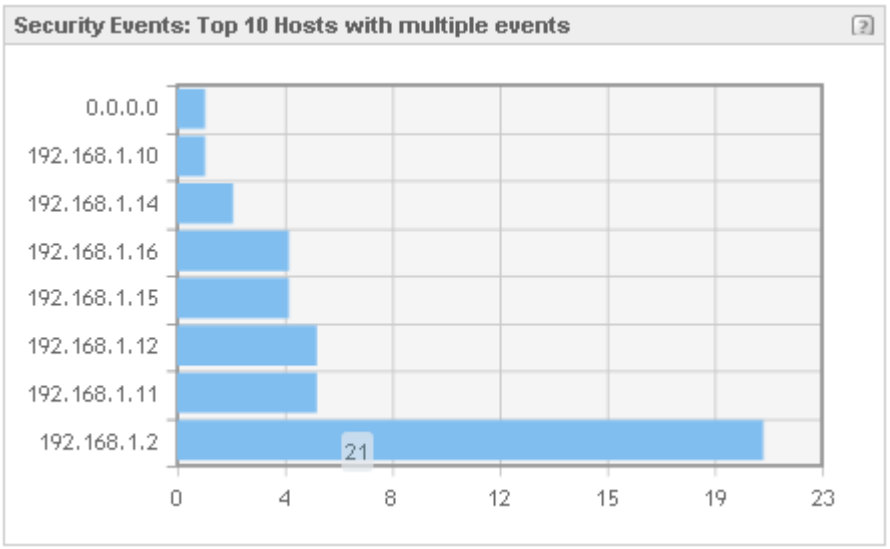


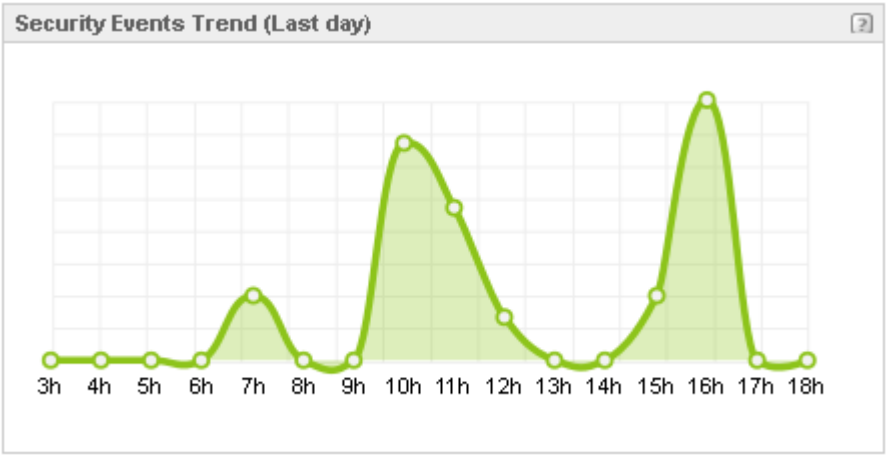
Eventos de seguridad agrupados por fuente / sensor de datos

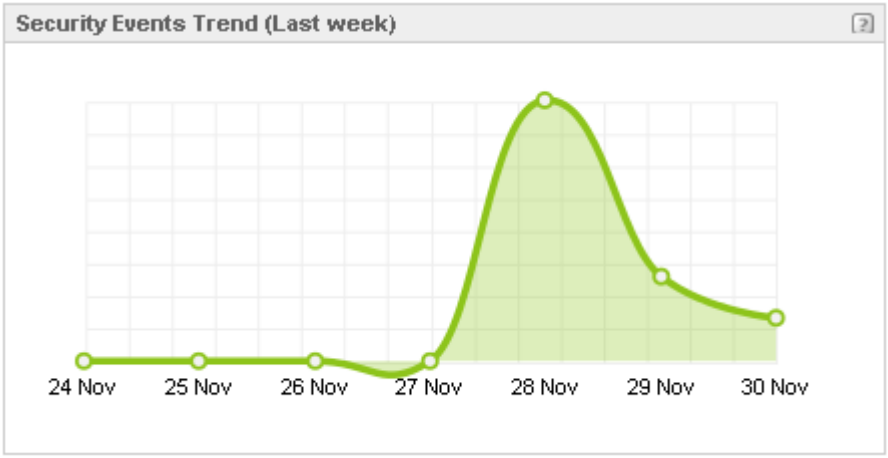


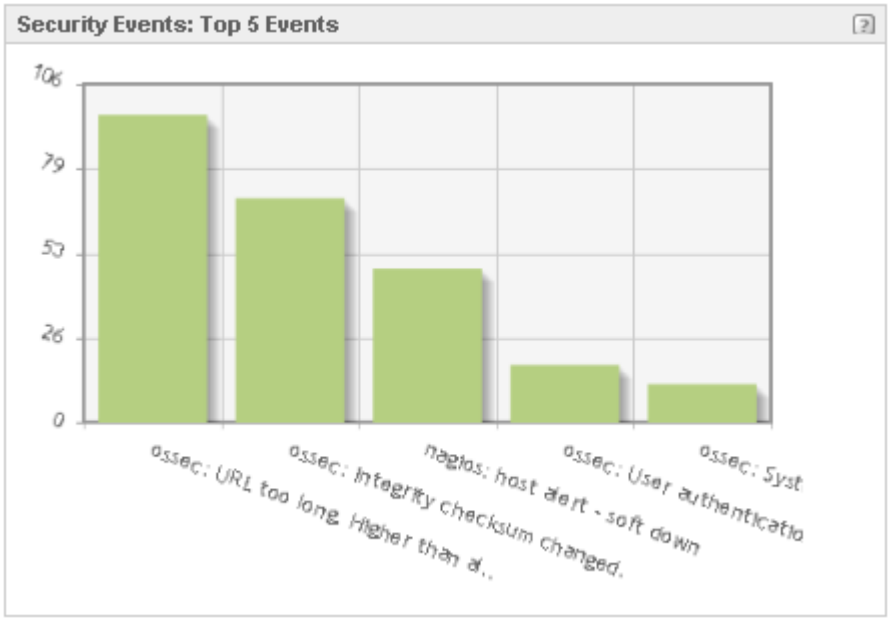
Seguridad


Security Events: Top 10 Promiscuous host
0.0.0.0
192.168.1.14
192.168.1.10
192.168.1.16
192.168.1.15
192.168.1.12
192.168.1.11
192.168.1.2
0
1
2
3

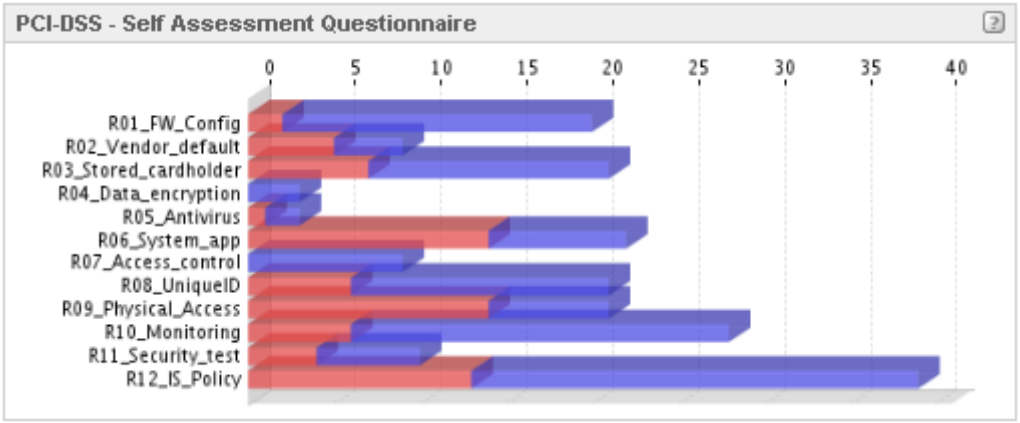

Security Events: Top 10 Hosts with multiple events
0.0.0.0
192.168.1.10
192.168.1.14
192.168.1.16
192.168.1.15
192.168.1.12
192.168.1.11
192.168.1.2
21
0
4
8
12
15
19
23


Security Events Trend (Last day)
3h
4h
5h
6h
7h
8h
9h
10h
11h
12h
13h
14h
15h
16h
17h
18h





Conformidad



Disponibilidad

View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
7	1	0	0

All Problems	All Types
1	8

Service Status Totals

Ok	Warning	Unknown	Critical	Pend
7	0	0	0	0

All Problems	All Types
0	7

Service Overview For All Host Groups

123 (123)

Host	Status	Services	Actions
administrador	UP	No matching services	
pc01	UP	No matching services	
pc02	UP	No matching services	
pc04	DOWN	No matching services	
pc05	UP	No matching services	
pc06	UP	No matching services	

All Servers (all)

Host	Status	Services	Actions
administrador	UP	No matching services	
gateway	UP	1 OK	
localhost	UP	6 OK	
pc01	UP	No matching services	
pc02	UP	No matching services	
pc04	DOWN	No matching services	
pc05	UP	No matching services	
pc06	UP	No matching services	

Debian GNU/Linux Servers (debian-servers)

Host	Status	Services	Actions
localhost	UP	6 OK	

HTTP servers (http-servers)

Host	Status	Services	Actions
localhost	UP	6 OK	

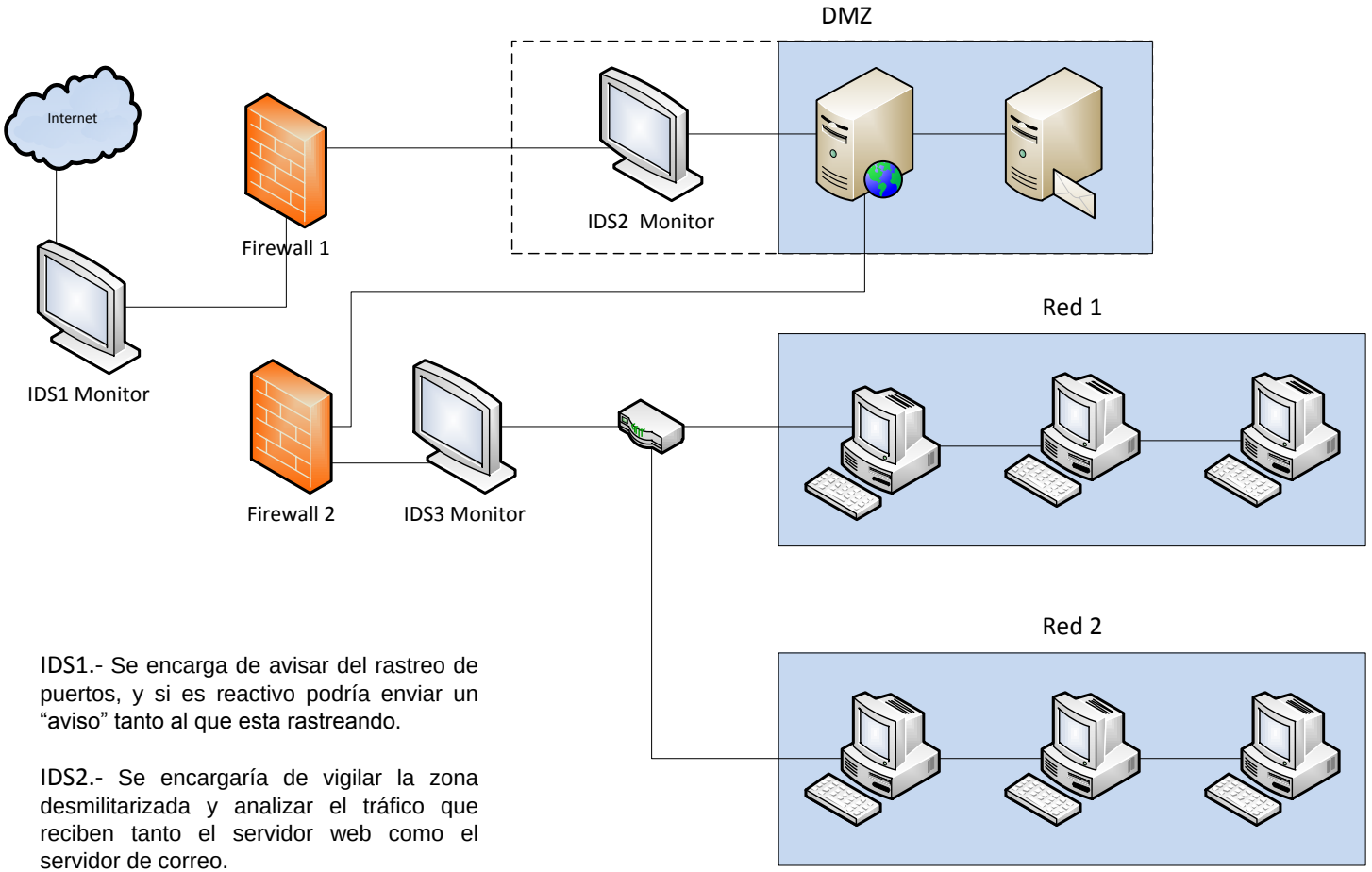
Pingable servers (ping-servers)

Host	Status	Services	Actions
gateway	UP	1 OK	

SSH servers (ssh-servers)

Host	Status	Services	Actions
localhost	UP	6 OK	

Diseño de red segura



IDS1.- Se encarga de avisar del rastreo de puertos, y si es reactivo podría enviar un “aviso” tanto al que esta rastreando.

IDS2.- Se encargaría de vigilar la zona desmilitarizada y analizar el tráfico que reciben tanto el servidor web como el servidor de correo.

IDS2.- Totalidad de trafico de la red

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Carlos Bautista **(miembro del tribunal)**
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 4 de diciembre 2011

Por medio de la presente certifico que el pregradista Rodrigo Salvador Sarzosa Patiño con CI No.010339648-7 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **"ANÁLISIS DE SISTEMA DE DETECCIÓN DE INTRUSOS EN REDES DE TRANSMISIÓN DE DATOS"**, del título de Ingenieros en Sistemas Informáticos

Atentamente

Ing. Carlos Bautista
(miembro del tribunal)

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Esteban Cáceres **(miembro del tribunal)**
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 4 de diciembre 2011

Por medio de la presente certifico que el pregradista Rodrigo Salvador Sarzosa Patiño con CI No.010339648-7 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **"ANÁLISIS DE SISTEMA DE DETECCIÓN DE INTRUSOS EN REDES DE TRANSMISIÓN DE DATOS"**, del título de Ingenieros en Sistemas Informáticos

Atentamente

Ing. Esteban Cáceres
(miembro del tribunal)

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Alberto Valencia **(miembro del tribunal)**
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 4 de diciembre 2011

Por medio de la presente certifico que el pregradista Rodrigo Salvador Sarzosa Patiño con CI No.010339648-7 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **"ANÁLISIS DE SISTEMA DE DETECCIÓN DE INTRUSOS EN REDES DE TRANSMISIÓN DE DATOS"**, del título de Ingenieros en Sistemas Informáticos

Atentamente

Ing. Alberto Valencia
(miembro del tribunal)