Sistema detector de intrusos (IDS) para redes WiFi usando JAVA

DIEGO JOSÉ LUÍS BOTIA VALDERRAMA*

* M.Sc.(c) en Software Libre, Universidad Oberta de Cataluña (España) – UNAB. Especialista en Construcción de Software para Redes, Universidad Autónoma de Colombia, D-Link Partner Certification D-Support For Wireless, D-Link Technology Institute, Ingeniero de Sistemas y Computación, Universidad Pedagógica y Tecnológica de Colombia, Profesor Catedrático UPTC, USTA Tunja y JDC - Tunja.

Resumen

Este trabajo muestra la forma más adecuada para proteger redes inalámbricas para entornos WLAN[1], debido a las vulnerabilidades de seguridad que presenta esta tecnología, ya sea por un mal diseño e implementación de la red, o por malas políticas de configuración de los Access Points y sus protocolos asociados. También se muestra que mediante la utilización de herramientas de Software Libre como JAVA, se puede desarrollar un software IDS para aumentar la seguridad y permitir la correcta configuración por parte del Administrador de Red.

Abstract

This work shows the most adequate method to protect wireless networks to environments WLAN, because of vulnerabilities of security that present this technology, by inadequate design and to implement the network, as well as bad politics of configuration of the Access Points and its join protocols. Also it shows that by means utilization of tools of free software as JAVA, we may to develop a software IDS to increase the security and to allow the correct configuration on the part of the network manager.

Palabras Claves: Seguridad en Redes, IDS, Redes WiFi, JAVA.
Key Words: Security in Networks, IDS, WiFi networks, JAVA.

1. Introducción

Actualmente, empresas y universidades se muestran más interesadas en el mundo del software libre, donde la principal herramienta es el sistema operativo GNU/Linux. Debido a sus características, este sistema operativo tiene gran aceptación y cuenta con muchas aplicaciones en colegios, hogares, oficinas, pymes, y grandes empresas, entre otros. Así mismo en el campo de desarrollo de software, ya aparecen herramientas que se han popularizado debido a su flexibilidad, desempeño, y portabilidad, entre las que se pueden mencionar: PHP, JAVA, Python, Perl, MONO, etc.

Actualmente y desde el inicio de Internet, han aparecido diversas tecnologías en redes en donde las más destacadas son las redes Inalámbricas, tanto para entornos WLAN(WiFi) como WMAN (WiMAX).

El activo más importante en cualquier empresa es la información, por lo tanto, y debido a la proliferación de redes inalámbricas, se deban buscar los mecanismos necesarios para proteger los recursos informáticos en una organización, sin embargo, aunque se sigan todas las recomendaciones de los expertos, siempre existen riesgos de posibles ataques.

Dentro de las soluciones tecnológicas que están disponibles para reforzar la seguridad de una red, los firewalls son muy populares. Un firewall es un sistema encargado del cumplimiento de las políticas de control de acceso a la red, lo cual se hace a través de reglas. Un firewall actúa como guardia perimetral de una red: protege una red de ataques que provengan del exterior de ésta. Pero el escenario se puede complicar de la siguiente forma:

1. Un atacante puede lograr pasar el firewall, dejando la red a su disposición.

2. Un firewall protege de los accesos no autorizados hacia la red interna, pero no protege a las máquinas ubicadas en la red perimetral como servidores Web, servidores de correo, servidores FTP, en otras palabras, de las bases funcionales de Internet.

3. Un firewall no protege contra ataques desde adentro.

En estos casos no queda más que detectar el ataque o la intrusión lo antes posible, para que cause el menor daño en el sistema, y lo más viable es evitar la agresión. Normalmente un intruso intenta:

- Acceder a una determinada información
- Manipular cierta información
- Hacer que el sistema no funcione de forma segura o inutilizarlo

Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades y brechas en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación.

Los accesos no autorizados son un riesgo tanto para las redes inalámbricas como para las cableadas. Las tecnologías informáticas que han ido apareciendo en el mercado han sido susceptibles de ser violadas, de una u otra forma , en su integridad, confidencialidad o autenticidad en los datos que contienen.

Así se tenga protegida la red por medio de un Firewall, el problema radica en que el AP (Access Point) puede irradiar la señal en un radio de 360 grados, lo cual implica que cualquier atacante potencial pueda interceptar la señal e intentar un acceso no autorizado, para lo cual puede hacer uso de diferentes herramientas que están a su disposición en Internet, como: Netstumbler, Kismet, AirCrack, entre otras.

A continuación se ven las salidas típicas de estas herramientas:

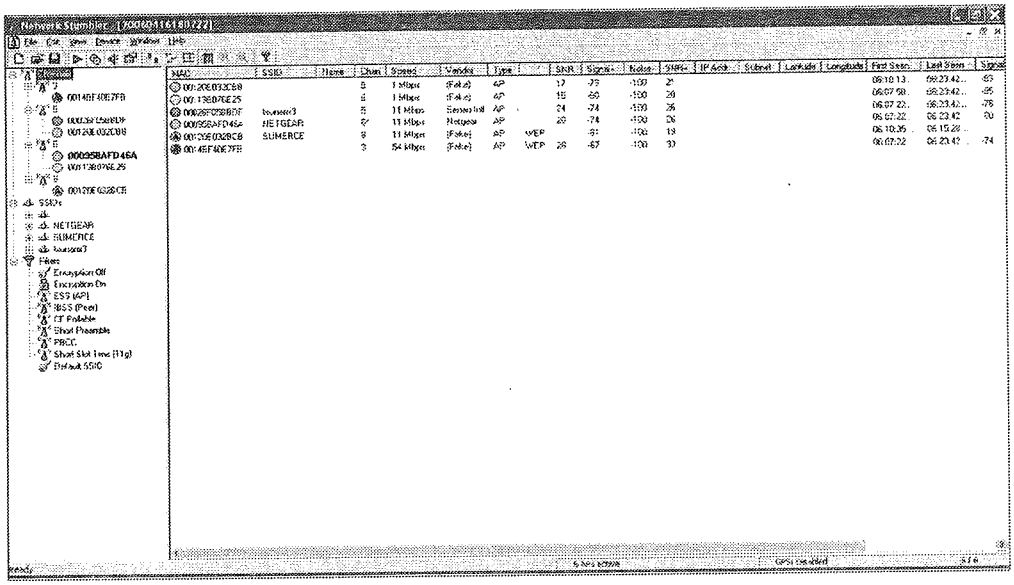

Figura 1. Herramienta NetStumbler.

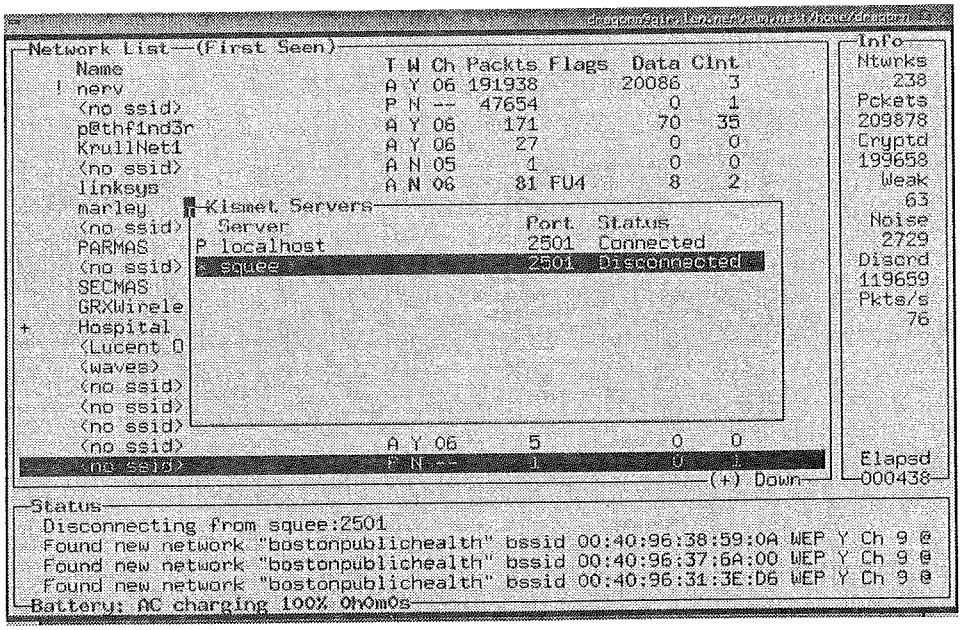

Figura 2. Herramienta Kismet.

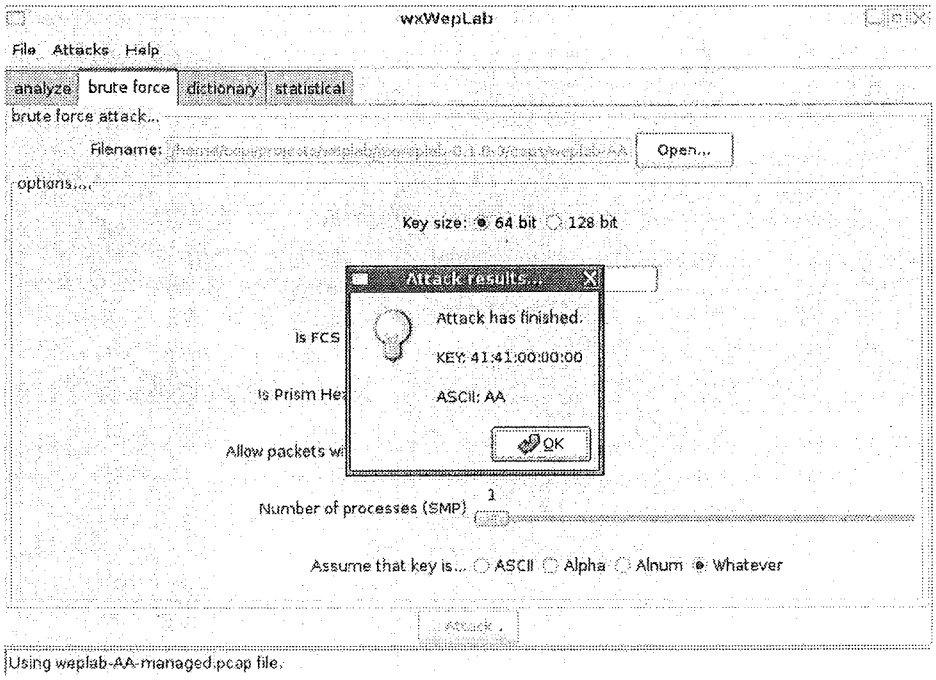

Figura 3. Herramienta WepLab.

2. Redes WiFi Estándar IEEE 803.11

Fue creado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos).

Este protocolo data de 1997, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican estos productos.

El término IEEE 802.11 se utiliza también para referirse al protocolo que ahora se conoce como "802.11legacy". La siguiente modificación apareció en 1999 y se designó como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, y trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a la cual resultó incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibió el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g. El paso siguiente se da con la norma 802.11n que subió el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen un primer borrador del estándar N con un máximo de 300 Mbps (80-100 estables). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializaron siguiendo el estándar 802.11g y la compatibilidad hacia el 802.11b.

Los estándares 802.11b y 802.11g utilizan bandas de 2,4 giga hercios (Ghz), que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda de 5 GHz. El estándar 802.11n

hará uso de ambas bandas, 2,4 GHz y 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz.

Entre los principales estándares que se han trabajado están:

- IEEE 802.11h es una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos interferentes. Está disponible desde el año 2003 y los productos están empezando a aparecer en el mercado en estos momentos.

- IEEE 802.11n, diseñado para aumentar la capacidad efectiva de transmisión hasta 100 Mbps, siendo compatible con los estándares anteriores.

- IEEE 802.1x. Estandar ya finalizado con disponibilidad de productos desde el año 2003, este mejora las prestaciones de seguridad (mecanismos de autenticidad y autorización).

- IEEE 802.11i. Estándar ya finalizado destinado a mejorar las prestaciones de seguridad y cifrado.

- IEEE 802.11e, diseñado para el soporte multimedia mejorado, garantizando la calidad de servicio (QoS) en comunicaciones de gran ancho de banda y tiempo real (p.e. vídeo).

3. Topologías Típicas

Antes de describir la seguridad de una red WiFi, es necesario conocer las diferentes topologías que se pueden utilizar, las cuales pueden generar ciertas vulnerabilidades, dependiendo de cómo se implementen.

3.1 Ad Hoc o Peer to Peer

En esta topología, cada estación posee una tarjeta de red inalámbrica mediante la cual se conecta con todos los demás. No existe un dispositivo que controle el acceso a la red y el alcance es limitado al cubrimiento de las Tarjetas. Es usado en redes sencillas y su seguridad es limitada.

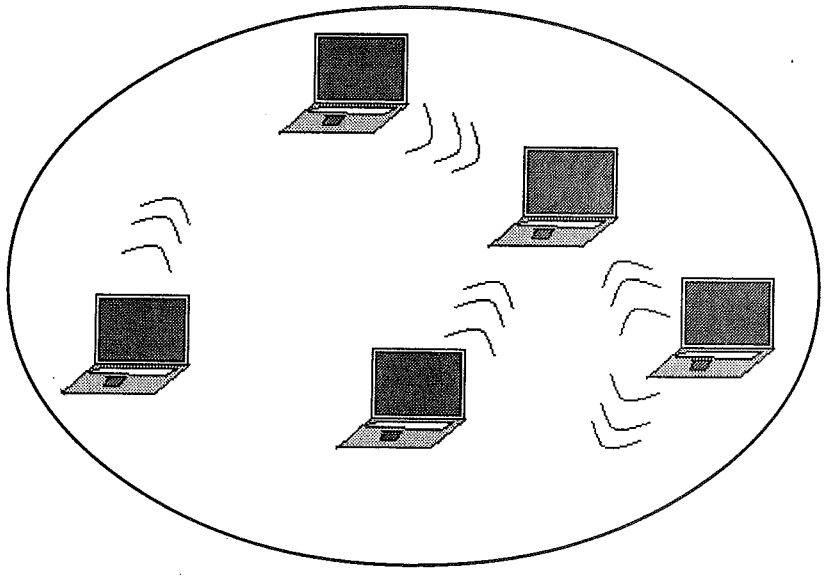

Figura 4. Topología Red Ad-Hoc.

3.2 Configuración Infraestructura

Los equipos se conectan a un AP que controla el acceso a la Red. Tiene mayor cobertura que la configuración Ad Hoc porque el AP actúa como repetidor y tiene mayor seguridad que la configuración AD-HOC. Su esquema es el siguiente.

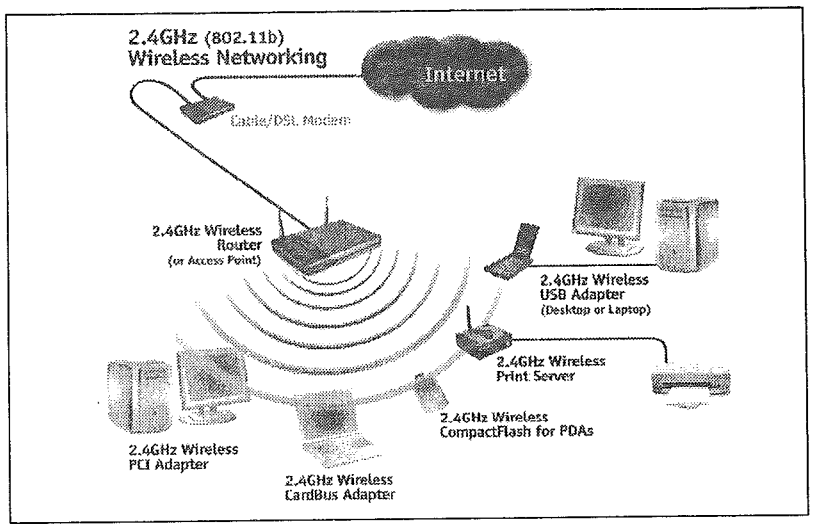

Figura 5. Topología Infraestructura.

3.3 Roaming

El uso de varios AP aumenta la cobertura de la red Wireless y es muy usado en entornos o edificios con varios pisos. En este esquema el AP da cobertura a una zona o celda. La función de Roaming le permite a un usuario móvil desplazarse entre celdas sin perder conexión. Los AP se conectan a la red, cableada típicamente en cable par trenzado o fibra óptica.

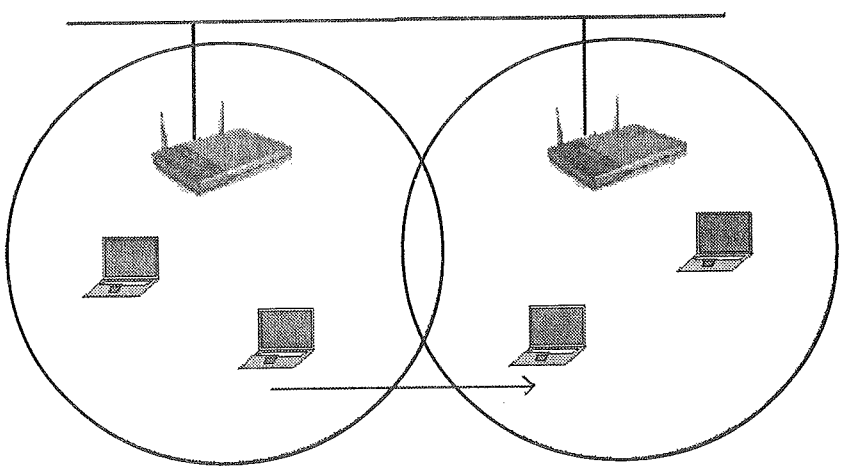

Figura 6. Esquema Roaming.

3.4 Alcance o cobertura

Para Redes internas (Indoor), el alcance de una red IEEE 802.11 b/g depende de:

- Tipo de construcción
- Materiales de paredes, divisiones, puertas, ventanas, pisos, muebles
- Potencia de Tx de los equipos y antenas
- Nivel de sensitividad de los receptores.

La cobertura puede estar entre 30 m (Oficinas con muros de ladrillo) y 200 m (Oficina abierta). También es importante tener en cuenta que la señal se deteriora por efecto de la atenuación, la reflexión multipath (cuando se producen múltiples trayectorias para llegar al receptor) y la interferencia o ruido.

4. Protocolos de Seguridad en redes WiFi

4.1 WEP (Wired Equivalence Privacity)

Es un mecanismo de seguridad para las redes inalámbricas, mediante el cual, la asociación de los dispositivos con el AP y la información transmitida por la red Wireless pueden encriptarse. Utiliza un algoritmo de encripción RC4, que emplea llaves de 64,128 o 256 bits.

En este método todos los dispositivos (Estaciones y AP) deben tener definida una palabra o llave de cifrado (WEP Key). Esta palabra debe ser la misma en todos los dispositivos de Red. La desventaja es que WEP presenta vulnerabilidad al ataque de Hackers mediante el uso de sniffers, debido a que la clave es estática, por lo que en la actualidad se están desarrollando e implementando nuevos mecanismos más seguros.

Consisten en aplicar a los datos originales la operación lógica XOR (O exclusiva) utilizando una clave generada de forma pseudoaleatoria. Los datos cifrados resultantes son los que se transmiten al medio.

Para generar la clave pseudoaleatoria, se utiliza una clave secreta definida por el propio usuario y un vector de inicialización (IV, Initialization Vector). La longitud de los datos cifrados excede en cuatro caracteres a la longitud de los datos originales. Estos cuatro caracteres reciben el nombre de ICV (Integrity Check Value, 'Valor de Comprobación de Integridad') y se utilizan para que el receptor pueda comprobar la integridad de la información recibida. Esto se hace mediante el algoritmo CRC-32.

Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta (distribuida a todas las estaciones) para generar la semilla que permitirá descifrar los datos mediante el algoritmo PRNG[2].

A continuación se presenta el esquema de asociación del AP con una estación en donde se puede ver la vulnerabilidad que aprovecha el atacante:

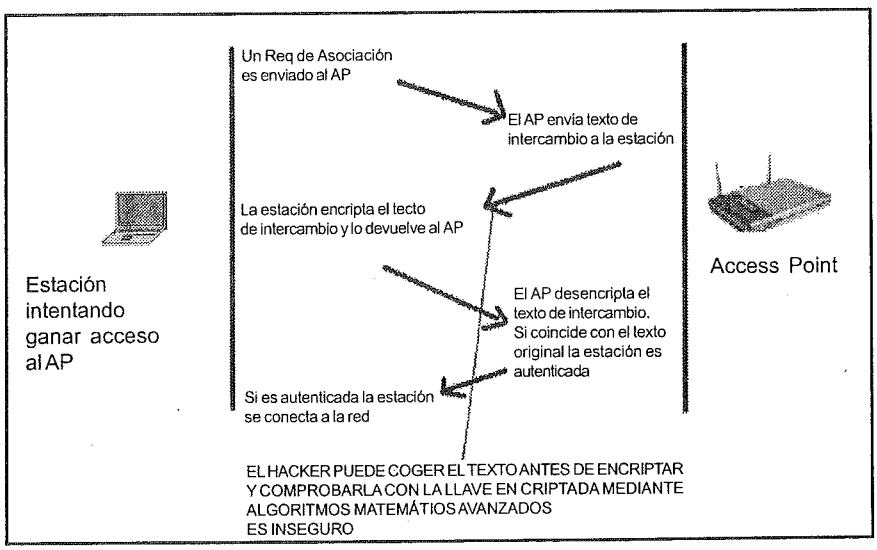

Figura 7. Esquema de vulnerabilidad en WEP.

4.2 WI-FI PROTECTED ACCESS (WPA)

Son especificaciones basadas en el estándar IEEE 802.11i que mejora fuertemente el nivel de protección de datos y el control de acceso de las redes inalámbricas Wi – Fi. La gran ventaja de WPA es que puede aplicarse a las redes Wi – Fi existentes y que es completamente compatible con el sistema de seguridad integrada proporcionado por IEEE 802.11i.

Se puede instalar en los equipos Wi-Fi existentes de una forma tan sencilla como instalar un pequeño software en los equipos. Una vez instalado, el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados puedan acceder a la red y que los datos transmitidos permanezcan completamente inaccesibles para cualquier usuario que no sea el destinatario.

Las mayores ventajas que aporta WPA frente a WEP son dos:

- Mejoras en el cifrado de datos mediante TKIP (Temporal Key Integrity Protocol 'Protocolo Temporal de Integridad de Clave'). Este sistema asegura la confidencialidad de los datos.

- Autentificación de los usuarios mediante el estándar 802.11x y EAP (Extensible Authentication Protocol, 'Protocolo Extensible de autentificación'). Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red. No obstante, si desea, permite el acceso de usuarios anónimos[3].

5. Sistemas Detectores de Intrusos (IDS)

Una de las principales herramientas que tienen los administradores de red para incrementar la seguridad de sus sistemas son los IDS (Sistemas de Detectores de Intrusos). Un IDS es un sistema que intenta detectar y alertar sobre el intento de intrusiones en un sistema o en una red, considerando intrusión a toda actividad no autorizada o que no debería ocurrir en ese sistema. Es importante anotar que el Firewall no realiza estas funciones y no debe confundirse con un IDS, sino que a este debe considerarse como un complemento del Firewall.

Los FW filtran los paquetes y permiten su paso o los bloquean por medio de una tabla de decisiones basadas en el protocolo de red utilizado. Las reglas se verifican contra una base de datos que determina si está permitido un protocolo determinado el cual permite o no el paso del paquete basándose en atributos tales como las direcciones de origen y de destino, el número de puerto, etc. Esto se convierte en un problema cuando un atacante enmascara el tráfico que debería ser analizado por el FW o utiliza un programa para comunicarse directamente con una aplicación remota. Estos aspectos se escapan a las funcionalidades previstas en el diseño inicial de los cortafuegos. Es aquí dónde entran los IDS, ya que estos son capaces de detectar cuando ocurren estos fallos.

Algunas de las características deseables para un IDS son:

- Deben estar continuamente en ejecución con un mínimo de supervisión.

- Se deben recuperar de las posibles caídas o problemas con la red.

- Debe analizarse él mismo y detectar si ha sido modificado por un atacante.

- Debe utilizar los mínimos recursos posibles.

- Debe estar configurado acorde con la política de seguridad seguida por la organización.

- Debe de adaptarse a los cambios de sistemas y usuarios, y ser fácilmente actualizable.

5.1 Arquitectura general de un IDS

Generalmente un IDS esta conformado por los recolectores de información, los procesadores de eventos, las unidades de respuesta y por los elementos de almacenamiento, este esquema se puede ver en la siguiente gráfica.

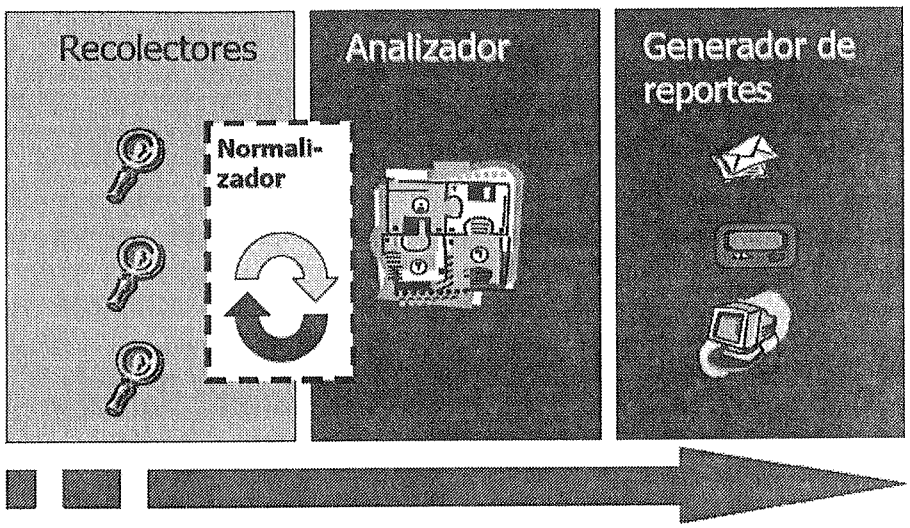

Figura 8. Elementos básicos de un IDS[4].

A continuación se hace una breve descripción:

1. Recolectores de información o sensores:

Son elementos pasivos que examinan todo el tráfico de su segmento de red en búsqueda de eventos de interés. Es decir que monitoriza su segmento en busca de tráfico sospechoso.

Pueden tener como fuentes un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.

2. Procesadores de eventos

También conocidos como analizadores, son los encargados de procesar la información obtenida de los sensores y realizar su análisis. Se admite como ampliación de su funcionalidad la capacidad de realizar recomendaciones al operador e incluso de actuar proactivamente. Entre los principales tipos están el esquema basado en usos indebidos y el modelo de detección de anomalías que se explican más adelante.

Además, se encargan de enviar el resultado a un almacén de datos (típicamente una base de datos) para otro posterior análisis y para generar informes. También pueden coexistir procesadores monitorizando el mismo sistema (en paralelo).

3. Unidades de respuesta

Este elemento es el encargado de proporcionar una respuesta ante los eventos obtenidos de los demás elementos o sugerir acciones al operador de consola (bloquear el acceso desde una dirección IP, limitar el número de conexiones nuevas aceptadas por segundo, entre otras). Dentro de las unidades de respuesta se pueden encontrar las de respuesta pasiva y activa. Los

pasivos detectan una posible violación de la seguridad, registran la información y genera una alerta.

Los activos están diseñados para responder ante una actividad ilegal, por ejemplo, sacando al usuario del sistema o mediante la reprogramación del FW para impedir el tráfico desde una fuente hostil.

4. Elementos de Almacenamiento

Esta entidad simboliza la base de datos (o base de conocimiento) dónde se almacenan los informes, firmas y patrones detectados en la red por el IDS. El objetivo de mantener esta información es doble:

1. Obtener la posibilidad de generar informes históricos y permitir el uso de técnicas de *Business Intelligence* y *Data Warehouse* (BI/DW) para la extracción de información y obtención de nuevo conocimiento.

2. Proactividad del sistema. Conseguir una respuesta rápida del IDS ante un ataque nuevo consultando otros ataques similares registrados.

Como se puede observar las ventajas son evidentes y se pueden resumir en tres:

- **Eficiencia:** varios componentes podrían manejar el mismo tipo de datos.

- **Operatividad:** los datos de los sensores podrían ser accesados con una simple consulta SQL.

- **Rendimiento:** la detección de complicados ataques a gran escala podría ser posible mediante el conocimiento y el manejo de los datos por todos los detectores.

5.2 Tipos de Sensores

Los principales tipos de Sensores son:

- Sensores basados en Red
- Sensores basados en Host
- Sensores basados en Aplicación

Los basados en Red analizan el tráfico de la red completa, examinando los paquetes individualmente, comprendiendo todas las diferentes opciones que pueden coexistir dentro de un paquete de red y detectando paquetes armados maliciosamente y diseñados para no ser detectados por los Firewalls.

Entre sus principales ventajas están las siguientes:

- Detectan accesos no deseados a la red.

- No necesitan instalar software adicional en los servidores en producción.

- Fácil instalación y actualización por que se ejecutan en un sistema dedicado.

Como principales desventajas se encuentran:

- Examinan el tráfico de la red en el segmento en el cual se conecta, pero no puede detectar un ataque en diferentes segmentos de la red. La solución más sencilla es colocar diversos sensores.

- Pueden generar tráfico en la red.

- Ataques con sesiones encriptadas son difíciles de detectar.

En cambio, los sensores basados en Host analizan el tráfico sobre un servidor o un PC, se preocupan de lo que está sucediendo en cada host y son capaces de detectar situaciones como los intentos fallidos de acceso o modificaciones en archivos considerados críticos.

Las ventajas que aporta son:

- Registra comandos utilizados, archivos abiertos, etc.

- Tiende a tener menor número de falsos-positivos que los sensores de red, entendiendo falsos-positivos a los paquetes etiquetados como posibles ataques cuando no lo son.

- Menor riesgo en las respuestas activas que los de red.

Los inconvenientes son:

- Requiere instalación en la máquina local que se quiere proteger, lo que supone una carga adicional para el sistema.

- Tienden a confiar en las capacidades de auditoria y logging de la máquina en sí.

Por último están los sensores basados en aplicación que es un caso especial de los host y es posible integrarlo en sensores híbridos.

5.3 Esquemas de detección basados en usos indebidos y en anomalías.

El uso indebido involucra la verificación de tipos ilegales de tráfico de red, por ejemplo, combinaciones dentro de un paquete que no se podrían dar legítimamente. Este tipo de detección puede incluir los intentos de un usuario por ejecutar programas sin permiso (por ejemplo, "sniffers"). Los modelos de detección basados en usos indebidos, se implementan observando como se pueden explotar los puntos débiles de los sistemas, describiéndolos mediante unos patrones o una secuencia de eventos o datos ("firma") que serán interpretados por el IDS. Una de las ventajas que se tienen al usar un analizador basado en transiciones de estado, es que los diagramas de transición permiten realizar una representación a alto nivel de escenarios de intrusión, ofreciendo una forma de identificar una serie de secuencias que conforman el ataque, con esto es posible aumentar la potencia del motor de análisis.

La detección basada en anomalías se apoya en estadísticas y el uso de heurísticas tras comprender cual es el tráfico "normal" en la red del que no lo es. Un claro ejemplo de actividad anómala sería la detección de tráfico fuera de horario de oficina o el acceso repetitivo desde una máquina remota (rastreo de puertos). Este modelo de detección se realiza detectando cambios en los patrones de utilización o comportamiento del sistema generado a partir de un perfil definido. Esto se consigue realizando un modelo estadístico que contenga una métrica definida para compararlo con los datos reales analizados en busca de desviaciones estadísticas significantes, además es posible potenciar el motor de análisis usando algoritmos genéticos, o técnicas más avanzadas como el uso de redes neuronales, por lo que es muy importante integrar técnicas de inteligencia artificial que harán al IDS más "inteligente".

La ventaja principal es que puede detectar ataques desconocidos, debido a que si el hacker realiza actividades que se desvían del perfil normal del usuario legal, el procesador de eventos enviará una alarma sobre la intrusión.

6. Librería JPCAP

Esta es una clase de Java que permite a las aplicaciones desarrolladas capturar y/o enviar los paquetes a la red.

Jpcap esta basado en el libpcap/winpcap y API. Por consiguiente, se supone que Jpcap trabaja en cualquier SO en que libpcap/winpcap se lleve a cabo. Actualmente, Jpcap se ha probado en FreeBSD 3.x, Linux RedHat 6.1, Red Hat 4, Solaris, y Microsoft Windows 2000/XP.

Jpcap apoya los tipos siguientes de paquetes: Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, e ICMPv4. Se capturan otros tipos de paquetes como los paquetes crudos (es decir, instancia de clases de paquetes) qué contienen los datos enteros de los paquetes. Esto permite a las aplicaciones de Java, analizar los tipos de paquete.

Características:

- Los errores que ocurren en la capa del jpcap se transmiten en la aplicación como excepciones de Java.
- El jpcap usa un evento de notificación dónde los clientes interesados en los paquetes receptores registran la captura del paquete en el sistema para las notificaciones.
- El sistema contiene una jerarquía y una herencia basada en el packet/protocol.
- La interfaz captura un nivel más alto donde recibe los objetos del paquete.

El sistema captura paquetes fabricados con diferente protocolo de codificados donde la mayoría pueden ser instanciados de un paquete reconocido[5].

7. Diseño de la Herramienta

Para el diseño de una herramienta se deben tener en cuenta varias características como las siguientes:

- Tipo de claves que detecta: WEP y WPA.
- Tipo de IDS: nIDS.
- Tipo de analizador. Reconocimiento de patrones.

Teniendo en cuenta estos elementos, se procede a elegir las herramientas de software libre para realizar las primeras pruebas entre las que se pueden destacar las siguientes.

- JCreator o Netbeans 6
- JSDK 1.6.0
- Librería JPCAP 0.4
- Base de Datos Postgres SQL 8.1

7.1 Arquitectura lógica del IDS

Cumpliendo con una arquitectura típica de un sistema IDS, se puede tener en cuenta la distribución de los distintos módulos tal como se muestra en la figura 10:

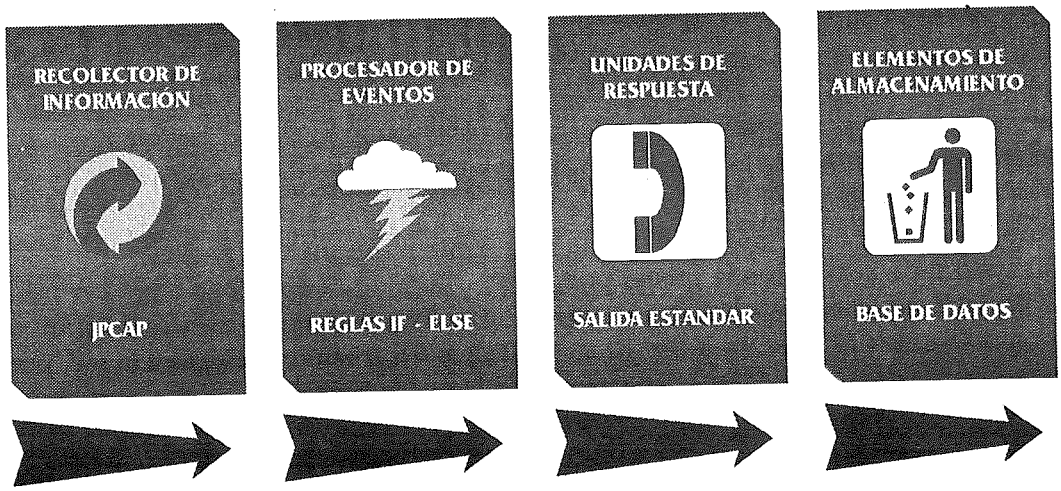

Figura 9: Arquitectura Lógica del IDS desarrollado.

8. Elementos desarrollados con Java

A continuación se presentan algunos ejemplos de la forma en que se integran los módulos de un IDS estándar con el uso de sentencias en JAVA utilizando la librería JPCAP.

8.1 Recolector de información o Sensor

```
1 public void captura() throws IOException{
2 String[] devices = Jpcap.getDeviceList();
3 for (int i = 0; i < devices.length; i++) {
4 System.out.println(devices[i]);
5 }
6 System.out.println("Capturando con la interfaz..."+ devices[2]);
7 String deviceName = devices[2];
8 Jpcap jpcap = Jpcap.openDevice(deviceName, 1024, false, 1);
9 capturar c = new capturar();
10 jpcap.loopPacket(-1, c);
11 }
12 static class capturar implements JpcapHandler {
13 .....
```

Entre las principales líneas, se ve que en la número 2 se almacenan los dispositivos activos para capturar paquetes. En la línea 8 se utiliza la librería especial de java llamada Jpcap, por medio de la cual se le envía el dispositivo escogido para la captura y en la línea 10 se procede a realizar la captura mediante un ciclo o loop.

8.2 Procesador de eventos

```
1 while(rsip.next()){
2 if(packete.contains(rsip.getString(1).trim())==true){
3 consultarip.executeUpdate("insert into historial_usuario values('" + fec + "','" + hor + "','" + packete + "','" + rsip.getString(1) + "')");
4 }
5 else{
6 band=1;
7 }
```

Para poder actualizar la base de datos es necesario el uso del componente JDBC (Java Data Base Connectivity), que es el elemento que proporcionará el acceso a la capa de datos, para las operaciones más importantes sobre la Base de Datos como inserts, updates, deletes y selects. En la línea 2 se tiene un ejemplo del procesador de eventos tipo reglas if – else, donde se verifica información del paquete capturado con los datos almacenados en la base de datos; en el caso que se encuentre alguna diferencia entre ellos, en la línea 6 se activa una bandera para generar la alarma.

8.3 Unidades de respuesta

```
1 System.out.println("***** ALERTA DE ATAQUE *****");
2 System.out.print(fec+" ");
3 System.out.println(hor);
4 System.out.println(packet);
```

Estas líneas muestran información sobre el ataque o intrusión realizada a la red, por medio de la salida estándar.

8.4 Elementos de almacenamiento

```
1 if(band==1){//Genera alarma
2 Statement consultar = conec.con.createStatement();
```

3 consultar.executeUpdate("insert into historial values('" + fec + "','" + hor +
"','" + packete + "')");

Sí la alarma se genera, inmediatamente se realiza una inserción de los datos de intrusión a la base de datos, para mantener un historial.

Conclusiones

Como se ha visto en este artículo, la combinación de sistemas IDS en redes tanto inalámbricas como alámbricas es un complemento esencial junto con los Firewalls, para incrementar la seguridad perimetral y así poder monitorear el tráfico de una forma más sencilla.

Es recomendable el uso de herramientas basadas en Software Libre no sólo por sus obvias ventajas, sino por su portabilidad, con lo cual no importa si el core (núcleo) de la red es basado en sistemas tipo Windows o Linux.

La librería JPCAP, es el API (Interfaz de Programación de Aplicaciones), más utilizado para el rastreo, y filtrado de paquetes y además debido a sus características ha sido implementado en muchas aplicaciones de Red, como: nmap, wireshark, snort, tcpdump; entre otras.

Citas bibliográficas

[1] WLAN (Wireless Local Area Network).

[2] CARBALLAR, José A. Wi-Fi como construir una red inalámbrica; Madrid España. p. 185.

[3] CARBALLAR, José A. Wi-Fi como construir una red inalámbrica; Madrid España. pp. 186-187.

[4] Fuente:http://www.virusprot.com/Archivos/Implementación%20y%20configuración%2ode%20IDS%20-%2025oct=-FINAL.pdf.

[5] The wonderful world of Linux. [On - line]. < https://help.ubuntu.com/6.10/kubuntu/about-kubuntu/C/wonderful-linux.html>

Bibliografía e Infografia

[1] BOBADILLA, Jesús. Comunicaciones y bases de datos con java a través de ejemplos. Alfaomega. México. 2003.

[2] CARBALLAR, José A. Como construir una red inalámbrica. Alfaomega. México. 2004.

[3] KAEO, Merike. Diseño de seguridad en redes. Pearson. Madrid. 2003. Pág. 448 - 449.

[4] STALLING, William. Comunicaciones y Redes de Computadores. 6 ed. Madrid. Prentice Hall. 2000. p. 421-427, 467-472, 605-636.

[5] TANENBAUM, Andrew s. Redes de Computadores. 4 ed. Prentice Hall. p. 21-23, 68-71, 100-108, 267-270, 292-302, 553-555, 776-783.

[6] HERRERA R., Omar A. jefe de seguridad informática, Banco de México. Implementación y configuración de sistemas de detección de intrusos. Octubre 2003. Disponible desde World Wide Web: <http://www.virusprot.com/Archivos/Implementación%20y%20configuración%20de%20IDS%20-%2025oct03-FINAL.pdf>

[7] INSYS. Soluciones integrales de seguridad en TI [online]. Texinfo. México. Disponible desde World Wide Web: <http//www.insys-corp.com.mx/Productos de detección de intrusos.htm>.

[8] MADRID MOLINA, Juan Manuel. Seguridad en redes inalámbricas [online]. Universidad Icesi, abril 20 de 2004. Disponible desde World Wide Web: <www.icesi.edu.co>.

[9] Sistemas de detección de intrusos: carencias actuales y nuevas tecnologías. Javier Fernández – Sanguino Peña. Jefe de proyecto. División de seguridad de Germinus Solutions. Junio. 2002. Disponible para la World Wide Web: <http://www.germinus.com/sala_prensa/articulos/Sistemas%20de%20deteccion%20de%20intrusos,%20carencias%20actuales%20y%20nuevas %20tecnologias,%20(Abril%202002).pdf>

[10] Fuentes en Java de JPCAP. [on-line] http://jpcap.sourceforge.net.

[11] Fuentes de PCAP para Unix usando lenguaje C. [onl ine] http://www.tcpdump.org