REDSE1301 – Redes & Seguridad (1)

Felipe Alfonso González L.
Continuidad en Ingeniería en Informática, IACC Chile., 2020-2021

Instituto Superior de Artes y
Ciencias de la Comunicación,
IACC
Av. Salvador 1318, Metro Santa
Isabel, Providencia, Santiago.
Chile.

f.alfonso@res-ear.ch – felipe.alfonso.glz@gmail.com – https://twitter.com/felipealfonsog
https://glzengrg.com - https://freeshell.de/felipe - https://linkedin.com/in/felipealfonsog

Amenazas según OWASP (S.F.)[1]

Una forma de mitigación de amenazas según OWASP (S.F.) podría definirse como todo un proceso para capturar y organizar y analizar la información, de esta forma permite generar decisiones relativas al riesgo de seguridad en las redes. Debido a la complejidad de las amenazas existentes existen organizaciones que trabajan en generar buenas normas y buenas practicas en la red:

- ISO: Gestiona normas para seguridad.
- OWASP: Organización que apoya y gestiona proyectos e infraestructuras Owasp.
- ISC2: Organización que certifica sistemas de información (ISC)2.
- NIST: I.N. de patrones de USA.
- CIS: Centro de seguridad de Internet.
- ISACA: Organización que apoya metodologías y certificaciones.
- INCIBE: I.N. de Ciberseguridad. Organización Española.

Clasificación de intrusos:

- Hacker: intrusos que toman como pasatiempo o reto técnico, pero no provocan daños, pero pueden tener acceso a información comercial, sin embargo, esto se considera como delito.
- Crackers: individuos que actúan con un cierto afán, que a la vez es un delito, de atacar sistemas con interés político, religioso, comercial, etc.
- Sniffers: descifrado de mensajes.
- Phreackers: sabotean redes telefónicas.
- Spammers: envío masivo de emails provocando colapso de servidores o con correos dañinos.
- Piratas informáticos: Pirateo de programas y contenidos digitales de forma ilegal.
- Creadores de virus o programas dañinos: informáticos que construyen virus y programas dañinos. Se han modernizado para obtener datos de cuentas bancarias y tarjetas de crédito
- Lammers: Personas que tienen determinados programas y los utilizan sin tener conocimientos técnicos.
- Amenazas de personal técnico: empleados que pueden generar ataques e incidentes, de manera involuntaria o voluntaria, por personal interno (Insiders) o externos (Outsiders).
- Ex Empleados: Ataques por ex empleados que actúan por despecho o venganza accediendo a cuentas. Generan bombas lógicas para dañar sistemas.
- Intrusos remunerados: Expertos contratados por un tercero para robo de información, y generar sabotajes.

Según isotools.org, los dominios activos que van a proteger y cumplir totalmente la seguridad. [i]

Su principal descripción es asegurar que los sistemas de información se cumplan.

- La norma NchISO 2700 (2014 – p.1) ha sido preparada para proporcionar requisitos como:
  - Establecer
  - Implementar
  - Mantener
  - Mejorar la gestión

Esta ofrece recomendaciones compuestas por 14 dominios:

- Políticas de seguridad: Restricción de pendrives.
- Aspectos organizativos: Persona responsable del respaldo.
- RR.HH. capacitaciones de seguridad.
- Gestión de activos: inventario de computadores y asignaciones.
- Control de accesos: personas con acceso de la sala de servidores.

[1] Alegre M. (2011). SEGURIDAD INFORMATICA ED.11. Madrid, España: Paraninfo.

- Cifrado: gestión de claves.
- Seguridad física y ambiental
- Seguridad de forma operativa: separación de entornos.
- Seguridad en las telecomunicaciones; segregación de redes.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con suministradores:
    - Supervisión.
    - Revisión de terceros.
- Gestión de incidentes en la seguridad de información
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Redundancia: Disponibilidad de instalaciones.
- Cumplimiento: identificación de la legislación aplicable, como, no usar software pirata.

Trabajo de investigación sobre Redes, seguridad en lugares públicos y recomendaciones para mantenerse seguros:

Sistemas abiertos: Existe una tendencia mundial en todos los campos de la actividad humanaii: económico, político, tecnológico, social, etc., hacia los sistemas abiertos, hacia la comunicación libre sin barreras de unos pueblos con otros en lo económico y político, de un individuo con otro en lo social y de una computadora con otra en lo tecnológico, sin importar la marca, la compañía o el país donde se fabrica. Ésta es una tendencia inexorable, que está más allá de la voluntad de líderes políticos, individuos, técnicos o empresarios.

El hecho de que existan cada vez mas dispositivos que actúan como tecnología IoT, significa que podrán existir barreras de seguridad que pueden ser explotadas. Es interesante pensar por ejemplo en el tipo de seguridad que podamos obtener en una conexión a internet en un restaurant McDonalds o Starbucks, que comúnmente entregan acceso a internet, pero con muy poca seguridad. Hoy en día se han sabido casos de robo de información importante en computadoras conectadas a estas redes abiertas. Es importante tomar recomendaciones de seguridad.[iii]

Riesgos de las wifis públicas
Cuando nos conectamos a una red wifi pública desconocemos quién es el administrador o qué medidas de seguridad utiliza para impedir acciones malintencionadas de otros usuarios conectados y por tanto, podemos exponernos sin necesidad a una serie de riesgos que describiremos a continuación.
Robo de datos transmitidos.
Si la conexión la realizamos sin contraseña, lo que conocemos como red "abierta", los datos que transmitimos pueden ser leídos por cualquiera, tanto el administrador como otros usuarios conectados a la red. La información está expuesta a cualquiera que sepa cómo leerla, y para ello no es necesario tener unos conocimientos técnicos muy elevados.

Si el sistema nos pide una contraseña y aparece un candado, como "red protegida", la información se transmite de forma cifrada. No obstante, esto está condicionado por el sistema de seguridad utilizado y la contraseña escogida. De menor a mayor seguridad, los sistemas son WEP, WPA y WPA2. Nunca debemos conectarnos a una red WEP ya que se ha demostrado que es vulnerable y que su seguridad equivale a una red abierta (sin contraseña).

Robo de datos almacenados en nuestro equipo
Al formar parte de una red pública en la que existen otros usuarios conectados, nuestro dispositivo está expuesto y visible a los demás usuarios presentes en la misma.
Por tanto, somos susceptibles de recibir cualquier tipo de ataque desde uno de estos equipos conectados.
Infección de los dispositivos.
Al conectarnos a una wifi ajena, un usuario malintencionado conectado a la misma red podría tratar de infectar nuestro equipo con algún tipo de virus.
Es importante mantener siempre nuestro equipo actualizado con las últimas actualizaciones de seguridad para el sistema operativo y para las aplicaciones que tengamos instaladas.
Equipos intermediarios malintencionados
Un usuario malintencionado conectado a la red podría configurar su equipo para hacer de intermediario de la comunicación entre nosotros y el servicio (por ejemplo, Facebook) modificando o eliminando la información intercambiada, que pasaría a través del ciberdelincuente.

El hacker "inocente"
En un momento dado, podemos sentir la tentación de conectarnos a una red ajena abierta o protegida utilizando herramientas de hacking wifi. Sin embargo, esta práctica constituye un uso ilícito de servicios de terceros que puede tener consecuencias legales. Además, puede darse el caso de que esa red wifi no presente contraseña o sea especialmente fácil de hackear precisamente para atraer víctimas a ella y así robar los datos al pícaro usuario.
Recomendaciones de seguridad
Nunca debemos utilizar redes wifi no confiables para acceder a servicios donde se intercambie información sensible: información bancaria, recursos corporativos, correo electrónico o acceso a las redes sociales.
Debemos evitar el uso de cualquier servicio en el que la información transferida tenga un componente importante de privacidad.
Nunca intercambiar información privada en redes no confiables.
Aunque podemos utilizar las redes públicas para otras acciones, como leer noticias en periódicos online o mirar la previsión del tiempo, no olvidemos que la mayor parte de los dispositivos mantienen un proceso de sincronización continua, por lo que el riesgo continúa existiendo.
Para protegernos de estos riesgos en redes donde los demás usuarios son desconocidos, contamos con una serie de medidas de seguridad que debemos aplicar:
Cortafuegos
Es muy importante tener instalado y habilitado un cortafuegos que no permita las conexiones entrantes a nuestro equipo por parte de otros usuarios de la red.
Muchos sistemas operativos actuales permiten escoger el modo de funcionamiento del cortafuegos cada vez que nos conectamos a una nueva red wifi.iv

Administración y seguridad de redes [v]

El gobierno norteamericano a tomado en cuenta la cita de Bruce Shneider: "The U.S. goverment likes to paint cryptography as a tool only for the four Horsemen of the information apocalypse: drug dealers, money launderers, child pornographers, and terrorists. This is deceitful; cryptography is an enabling technology for honest citizens. Privacy, accountability, credentials, identification, anonimity, integrity, these are not new ideas. Modern cryptography makes levels of security and privacy which were once the province of the rich, available to everybody. It enables commerce, fosters free speech, and facilitates communication in all forms by all the people. Cryptography is a technological equalizer.
bruce schneider, Applied Cryptography.

La administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. El objetivo de la administración es:
Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de re solución de problemas y de suministro de recursos.
Hacer uso eficiente de la red y utilizar mejor los recursos, como, por ejemplo, el ancho de banda.
Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
Hacer la red más segura, protegiéndola contra el acceso so no autorizado, haciendo imposible que personasvi

¿Qué son las tecnologías de interconexión?
Según su titularidad existen dos tipos de redes IP: LAN e Internet. Las redes LAN se conocen como redes privadas porque suelen emplear direcciones IP privadas y la red Internet se entiende como red pública porque normalmente emplea direcciones IP públicas. La diferencia entre ellas es que una dirección IP privada, en general, no puede emplearse en Internet, mientras que una dirección IP pública solo puede utilizarse en redes LAN que no tengan acceso directo a Internet. Así, los medios físicos y programas que hacen posible el tráfico de mensajes electrónicos entre los distintos tipos de redes se conocen como tecnologías de interconexión.vii

Mecanismos de seguridad En una red inalámbrica solo deberían poder acceder a la red los equipos autorizados. Además, la información que circula por ella no debería ser comprensible para los equipos no legítimos. Por ello, las redes inalámbricas deben cifrar las comunicaciones y controlar la forma en que los equipos se autentican en la red. Estos son los principales mecanismos de seguridad utilizados en redes inalámbricas: – WEP (Wired Equivalent Privacy). Es el mecanismo de seguridad utilizado por defecto por muchos puntos de acceso y routers inalámbricos en la actualidad. Presenta graves fallos de seguridad en el mecanismo de ci- frado (RC4), con lo que un atacante podría obtener la contraseña muy rápidamente, por lo que se desaconseja su uso. – WPA (Wireless Protected Access). Se le considera como un estadio inter- medio en el camino desde el WEP hacia la implementación completa del estándar 802.11i (WPA2). Ofrece una mayor protección que WEP, ya que proporciona una versión mejorada de RC4 e incorpora mecanismos de seguridad adicionales, como TKIP, pero se recomienda utilizar WPA2. – WPA2. Se considera el mecanismo de seguridad más adecuado para redes inalámbricas y ofrece mecanismos de cifrado robustos (AES, Advanced Encryption Standard). Existen dos tipos de WPA2 (Personal y Enterprise) que se diferencian en los mecanismos de autenticación: • WPA2 Personal o PSK. Su mecanismo de autenticación es PSK (Pre- Shared Key), en el que la contraseña se comparte entre el punto de acceso y los clientes de la red. Es la opción recomendada para redes domésticas. • WPA2 Enterprise. Proporciona una mayor flexibilidad para gestionar los mecanismos de autenticación, pudiendo utilizarse un servidor de contraseñas aleatorias (servidor RADIUS) o diferentes tipos de protocolos EAP como usuario y contraseña, certificados digitales, tarjetas inteligentes (smartcards), etc. Es la opción recomendada para empresas. Existen otras medidas que, en algunos casos, complican la gestión de la red o disminuyen el nivel de seguridad, por lo que pueden ser consideradas como falsas medidas de seguridad y se desaconseja su uso: – Filtrado de direcciones MAC. Esta medida crea una falsa sensación de seguridad, ya que puede ser fácilmente burlada mediante programas que cambien la dirección MAC del atacante. – Ocultación del SSID. El problema de esta medida es que en este tipo de redes si los puntos de acceso no difunden el SSID, son las estaciones cliente quienes continuamente envían peticiones preguntando si esa red se encuentra dentro de su alcance. Un atacante podría aprovechar esta situación para suplantar la red y establecer conexiones.[viiiixxxi]
Seguridad En Acceso A Dispositivos.

Es muy importante tomar en cuenta que los aparatos de comunicación, como móviles son propensos a ataques.

ASEGURAMIENTO DE LA INFRAESTRUCTURA DE RED.

Debido a la gran cantidad de usuarios involucrados, se generan mas posibilidades de ataques. Además de que las redes se amplían constantemente. Esto genera acceso a situaciones de ataques. Es necesario que existan diversas formas de protección desplegadas. Existen las siguientes[2]:

- Sniffers.
- Spoofing.
- Ataques de contraseñas.
- Control de salida ilegal de información sensible.
- Ataques de hombre en el medio.
- Ataques de denegación de servicio, Denial of Service o ataques DoS.
- Ataques a nivel de aplicación tipo exploits.
- Caballos de Troya (Trojan Horses), virus y otros códigos con virus.

Los sistemas de defensa en ciertos ataques son:

[2] Datos importantes para la respuesta acerca de que se recomendaría para asegurar una infraestructura.

- IDS - Sistema de anti Intrusos, se refiere al monitoreo de una red para detectar e informar accesos no autorizados, así se puede prevenir que se vea afectada la integridad de la red. (Gutiérrez, 2015).
- IPS - Sistema de Prevención de Intrusos, es una herramienta similar a IDS, pero alerta sobre detecciones y puede bloquearlas o prevenirlas (Gutiérrez, 2015).
- Firewall: permite controlar el trafico de una red. Permite filtrar el tráfico de red entre internet y un dispositivo en particular, funciona:

- permitiendo controlar algunos paquetes en internet y bloquear los que parezcan intrusos; o bien, denegando ciertos paquetes (Gutiérrez, 2015).

En base a la solución al problema de la empresa acerca de ¿De qué manera recomendaría asegurar la infraestructura de la red de la empresa?:

- Fundamentalmente asegurar la infraestructura de red, en base lo detallado anteriormente. Articular también sistemas de defensa, detallados anteriormente.

MONITOREO Y ADMINISTRACIÓN DE DISPOSITIVOS DE RED

Existen protocolos que pueden ayudar a monitorear una red, Cisco (2018) entrega las siguientes definiciones sobre ellos:

- SNMP - Protocolo que de un modo simple permite administrar una red.

Es uno de los protocolos conocidos que permiten administrar elementos de red.

- SYSLOG: Standard para el registro de mensajes.

DETERMINACIÓN DEL TIPO DE ACCESO DE GESTIÓN

El protocolo SNMP, del inglés “Simple Network Management Protocol”, se idóneo para administrar, elementos en una red, sin importar el tipo de dispositivo. Esto genera un entorno ideal para una red Ethernet, por su heterogeneidad, ya que permiten tener un agente SNMP configurable (Cisco, 2018).

Según Cisco (2018) hay 5 modelos de administración:

- ADMINISTRACIÓN DE INCIDENTE: detecta fallas, genera un log e informa a los usuarios de problemas de red para resguardar y ejecutarse con eficacia, si existe un error se determina automáticamente.
- ADMINISTRACIÓN DE LA CONFIGURACIÓN: Aquí se configura el control de una red y la los datos de configuración del sistema, así mantenerse a pesar de situaciones fuera de control sobre la operación de la red.
- ADMINISTRACIÓN DEL RENDIMIENTO: monitoreo el rendimiento individual de cada dispositivo para mantener niveles aceptables de seguridad.
- ADMINISTRACIÓN DE SEGURIDAD: el objetivo aquí es controlar los recursos de la red y locales para evitar sabotajes.
- ADMINISTRACIÓN DE CONTABILIDAD: mide paramentos en la red y permite regular directivas a usuarios.

INTRODUCCIÓN Y OPERACIÓN PARA SYSLOG.

Según Leskiw (s. f.)
“Syslog es un tipo de protocolo en que los dispositivos envían mensajes de eventos a un determinado servidor. Es compatible con un sin fin de dispositivos “.

Leskiw (S. F.) También Indica Que:
“Al tener un Syslog en un servidor permite recibir mensajes syslog en una red. Esto incluye logs de los servers Unix/linux/Windows etc, firewalls, y dispositivos de red (routers, switches, etc)”.

Muchos tipos de dispositivos de red, pueden enviar mensajes de Syslog. En servidores Unix pueden generar y enviar mensajes de Syslog, así como firewalls e impresoras o tipos de servidores web como Apache. Los servidores con Windows no son compatibles con Syslog .

Respecto A La Consulta De La Empresa En Cuestión, Detallada En El Trabajo De La Semana Sobre: ¿Qué Protocolo De Monitoreo Y Administración Recomendaría Usar Para El Caso Mencionado? Explique.

- Cisco recomienda esencialmente dos tipos de monitoreo que son SNMP y SYSLOG, También determinar el tipo de acceso en cuestión, esto genera tal como se explica anteriormente en base a un resumen de la tarea semanal, un entorno ideal para una red Ethernet, por su heterogeneidad, ya que permiten tener un agente SNMP configurable (Cisco, 2018).

Chequear lo que según Cisco (2018) son los 5 modelos de administración:

- Administración De Incidente.
- Administración De La Configuración.
- Administración Del Rendimiento.
- Administración De Seguridad.
- Administración De Contabilidad.

-Las anteriores se encuentran explicadas anteriormente en un resumen del trabajo semanal.

1- Compara las diferentes técnicas del aseguramiento del plano de control y administración de los dispositivos de red.

SEGURIDAD EN EL PLANO DE CONTROL

Según Henao (2012, p. IX), "las intrusiones a las redes de datos, son un problema constante (…), es por eso que es necesario generar técnicas que permitan detectar los momentos vulnerables". Una de las amenazas más importantes es de tipo Spoofing.

- IP SPOOFING: Se realiza un enmascaramiento de la dirección IP y es el tipo de amenaza en el cual un atacante modifica paquetes en ciertos servidores y simula que son enviados de uno distinto.
- DNS SPOOFING: Aquí el atacante falsifica la DNS y busca equipos que tengan un re direccionamiento falso por medio de errores en nombres de dominio a direcciones IP.
- WEB SPOOFING: Se genera una falsa web y genera una copia exacta de otra copia en internet. La web falsa pareciera real, pero es puede así generar robo de datos y ataques.

Para evitar riesgos Hacking-ético.com, recomienda:

Generar filtros en la entrada y salida del Router es una buena defensa de spoofing. Se debe crear una lista de control de acceso que bloquea ciertas IP privadas en su propia interfaz.

PROTOCOLO DE ENRUTAMIENTO.

El protocolo IP no solo es para redes WAN, también permite conexión de redes locales LAN, así conectar diferentes equipos dentro y fuera de una organización donde estén conectadas. Casi todos los sistemas operativos que soportan este tipo de protocolos, Unix y Linux tienen sistemas que permiten un optimo rendimiento en redes locales o externas.

OPERACIONES DE DISPOSITIVOS DE RED.
Según Cisco (2018), los dispositivos que conforman una red LAN o WAN son:

- MÓDEM DE BANDA ANCHA: Es un modem digital que se utiliza con servicio de internet DSL.
- SWITCH: Es un dispositivo que usa varios puertos en redes de proveedores de servicios.
- ROUTER: entrega redes e interfaz de acceso WAN que se usan para conectarse a la red del proveedor de servicios.

VULNERABILIDADES DEL PLANO DE CONTROL Y GESTIÓN.

De acuerdo a EcuRed.cu (s. f.), la Gestión de Redes consiste en "la monitorización, el sondeo, configuración y control de los recursos de una red para conseguir niveles de trabajo adecuados a los objetivos de una instalación y una organización; mediante tareas de despliegue y coordinación de hardware, software y elementos".

En tanto, Torres (2006, p. 20) indica que la ventaja y resultado de la aplicación de un sistema de gestión de red puede ser resumido de la siguiente manera:

- INCREMENTO DE CONFIABILIDAD: Disminución de tiempo requerido bajo ciertos errores, diagnostico y corrección de error.
- INCREMENTO DE SEGURIDAD: Acceso a la red controlado y regulado para usuarios, autorizaciones y autenticaciones.
- NUEVOS SERVICIOS PROVISTOS A LOS USUARIOS DE RED: Adquisición de información de tarificación, de tráfico, etc.

MONITOREO COMPUTARIZADO EFECTIVO DE SISTEMA:
Se almacenan datos de tarificación, estadística, seguimiento y evaluación de carga y performance de la red, chequeo de errores, soporte de red, etc.

- Gestión de vulnerabilidades: Al respecto Hewlett Packard Enterprise (2010), indica que "es un ciclo continuo que abarca la supervisión, la clasificación y la reparación de las debilidades del sistema". El ciclo incluye:
- El desarrollo de políticas de seguridad.
- Detección e inventario de activos: Categorización de activos del sistema y uso de soluciones de automatización y gestión de activos.
- Supervisión de perímetros.

EVALUACIÓN Y PRIORIZACIÓN DE AMENAZAS: La importancia del chequeo de vulnerabilidades se llevan a cabo a través de escáneres de vulnerabilidades. Si el escáner no tiene un buen ranking propio puede hacer uso de terceros como Arcsight o idealmente del Common Vulnerability Scoring System(CVSS), un estándar de industria abierto y gratuito para evaluar la peligrosidad de la vulnerabilidad.

Respecto a la pregunta relacionada con la empresa en cuestión presentada durante esta semana, cuya pregunta es la siguiente: ¿De qué manera usted realizará la evaluación y priorización de la amenaza? Explique.

Chequear el plano de control, analizando el conocido Spoofing. Estas amenazas son:

- IP SPOOFING.
- DNS SPOOFING.
- WEB SPOOFING.

Analizar el protocolo de enrutamiento en la red WAN de la organización.
Todo lo anterior se detalla y se explica con mayor detalle en el resumen anterior a la pregunta.

El control de acceso es la forma de administrar a quién se le permite el ingreso a la red y qué servicios pueden usar una vez que tengan dicho acceso. Los componentes de seguridad de los servicios son:
Esta es una forma de administrar los ingresos a la red y servicios que esta tenga. En términos de seguridad los tipos son:

- Autenticación
- Autorización
- Contabilización

Estos dan un marco para configurar el acceso a un enrutador o servidor.
Según el sitio ccn-cert.cni.es (s. F.), los servicios tipo AAA son, herramientas, procedimientos y protocolos para garantizar las correspondientes tareas de autenticación, autorización y registro de actividad de las entidades con acceso al sistema de información".

Descripción general de AAA.
AAA es un "protocolo para autenticar usuarios en base a identidades verificables. Significa autorizar usuarios en sus correspondientes derechos y consumo de recursos en la red:

- Mayor flexibilidad y control.
- Escalabilidad.
- Métodos de autenticación estándar, tal como Radius y Tacacs+.
- Respaldo.

La autentificación sin AAA presenta dos protocolos para llevar a cabo el proceso de autentificación, estos son PAP y CHAP. Para clarificar el tema cisco.com (2005) indica que "el protocolo point-to-point protocol (PPP), actualmente admite dos protocolos de autenticación: protocolo de autenticación de contraseña (PAP) y protocolo de confirmación de aceptación de la autenticación (CHAP)", los que se detallan a continuación:
Sin autenticación AAA hay dos protocolos a tomar en cuenta, PAP y CHAP, según cisco (2005), el protocolo ppp – point to point – admite los siguientes protocolos de aceptación:

- PAP: genera un método simple para establecer una identidad bidireccional. Así el nodo remoto envía de manera repetida usuario y contraseñas, recibe estas hasta que finaliza la conexión.
- CHAP: es un protocolo de reto-respuesta para que el receptor de este genera una respuesta valida si es positiva, así de manera continua evita ataques -replay-.

En la denominada authentication es una forma de chequear que un usuario sea quien corresponde ser, su ingreso común vía contraseña. Es común también el uso de token, challenge and response, etc. Challenge y response son protocolos donde se genera una segunda pregunta para chequear un ingreso valido.

Autorización
Authorization, luego del ingreso y autenticación de un usuario, controla recursos de los cuales tiene derechos de acceso.

Contabilización
Accounting, registra como y el tiempo en que el usuario ingreso y tuvo acceso al sistema, es muy útil para chequeo y auditorias de red.
El proceso AAA chequea las siguientes preguntas:

- ¿quién es usted?: autentificación
- ¿qué se le permite hacer al usuario?: autorización
- ¿qué han estado haciendo los usuarios en la red?: auditoría

Modos de autenticación
Según Caroll (2004), los modos de autenticación son los siguientes:

- Modo carácter: acceso administrativo.
- Modo paquete: acceso remoto.

Autenticación AAA local
Configuración de AAA con autenticación local
La autenticación AAA local según -Ariganello y Barrientos-, utiliza una base local en sus procesos. Almacena usuario y contraseña en un router. Se puede mejorar con una autenticación en base a un servidor.

Autentificando el acceso administrativo
Los administradores pueden tener acceso a todo a través de consola o una shell, y su puerto auxiliar es vtv.

Acceso remoto a la red
Los usuarios acceden a una red LAN, vía marcaciones NAS, o vía VPN.

Métodos de autenticación
Los principales son:

- Sin contraseña: algunos Sysadmins generan usuarios sin contraseña, no es la opción mas segura, ya cualquiera vía externa tendrá acceso total.
- Nombre de usuario y contraseña: es lo mas común, es lo mas ideal, los passwords varían entre débiles y fuertes.
- S/key one-time passwords (otp): otp significa tener varias contraseñas que se utilizan en las sesiones de terminales. En s/key se utiliza una frase secreta para generar el primer password,

y de esa manera continúa usando la anterior mediante cifrado.
- Token: aquí un usuario usa una tarjeta token y algo que tienen en su poder, como un PIN password. Los dispositivos token son aparatos como una pequeña calculadora, estos generan un pin y genera una password segura.

Opciones de depuración

- Los comandos debug muestran información sobre las operaciones del dispositivo y cualquier mensaje de error o lo que suceda en el trafico de esta.
- Según Andreu (2014), los routers tienen formas para generar un debug, son útiles para solucionar problemas de autenticación. Tiene varios comandos para estos propósitos.

Autenticación AAA basado en servidor

Permite mantener bases de datos con autenticaciones para cada router es inseguro. Aquí se recomienda un servidor AAA.

Protocolos de comunicaciones

Ariganello y Barrientos - (2015) - indican la utilización de una bbdd vía protocolos Radius, o Tacacs+. Ambos protocolos pueden ser usados en clientes AAA, aunque Tacacs+ es mas seguro. Tacacs+ como Radius son protocolos de administración, sin embargo, tiene diferentes capacidades. Su uso dependerá de lo que necesite una organización.

Introducción a Radius y Tacacs+.

En el caso de Radius se debe considerar lo siguiente, ya que hay comparaciones a considerar versus Tacacs+:
Radius cifra solamente la contraseña en su paquete de acceso, del cliente servidor. El resto no esta cifrado.
En el caso de Tacacs+ cifra todo el cuerpo del paquete, pero deja un encabezado estándar de Tacacs+.
Radius utiliza ADP. En el caso de Tacacs+., utiliza protocolo TCP.
Radius no permite los siguientes protocolos:

- Appletalk remote access (ARA).
- Netbios frame protocol control.
- Novell asynchronous services interface (nasi).
- Conexión x.25 PAD.

Y, en el caso de Tacacs+ es multiprotocolo.
Radius permite al mismo tiempo autenticación y autorización. En el caso de Tacacs+ utiliza arquitectura AAA. Permite autenticaciones separadas.
Los paquetes access-accept enviados por el servidor de Radius al cliente contienen datos de autorización.
En el caso de Tacacs+, es posible utilizar la autenticación de Kerberos y la autorización Tacacs+ y conteo.

AAA, es la representación de varios protocolos de seguridad con servidores de listas centralizadas, hay ventajas tales como la de entregar mayor flexibilidad y control en la configuración. Los métodos de autenticación Radius y Tacacs+, son ampliamente reconocidos como estándar.
Análisis en las redes wireless sensor networks, y redes locales inalámbricas.[xiixiii]

La revolución de la informática y ciencias de la computación a permitido también una revolución inalámbrica, esto significa entregar datos o información digital en todo aquello que esté disponible, en cualquier lugar y a costos bastante reducidos. La innovación en microcircuitos, ciclos cortos en desarrollo y costos bajos, han sido extendidos a las comunicaciones inalámbricas. *Cada vez más dispositivos se encuentran conectados a todo tipo de redes, como los aparatos electrodomésticos, automóviles, maquinaria industrial, dispositivos de comunicación personal, etc. En un sentido amplio, la revolución que de manera exponencial crece día a día, significará que se proveerá de sentidos a lo que alguna vez solamente tuvo cerebro.* Este será el papel que jugarán los sensores inalámbricos cooperando en redes de corto alcance con topologías dinámicas, en una clase especial de redes Ad hoc, es decir las WSN (Wireless Sensor Network). No obstante, igual que las redes convencionales como Internet, serán sujetas a ataques por usuarios mal intencionados, motivados por diferentes objetivos que pondrán en riesgo la información que ahí se curse, causando daños importantes. La suplantación de identidades es uno de los muchos ataques que pueden presentarse en estas redes, comprometiendo la confiabilidad y disponibilidad de la red, es por ello que en este trabajo se propone un esquema de autenticación de nodos, en consideración de las bajas prestaciones computacionales con las que disponen estos dispositivos.

Este manuscrito presenta los elementos que conforman las WSN, su arquitectura y topologías más comunes, así como las propuestas hechas para la autenticación de entidades. Luego se propone un protocolo de autenticación de nodos basado en el es- quema de secretos compartidos de Shamir. Finalmente se presentan las simulaciones del modelo propuesto para una red hipotética y se analizan los resultados de dicha simulación.

- WSN Las WSN están compuestas generalmente por un conjunto que puede ser considerablemente grande, de dispositivos sensores autónomos de bajo costo, que se comunican vía enlaces de radio de corto alcance.
- NODOS En una red de sensores existen diferentes tipos de nodos, los cuales son identificados de acuerdo con las funciones que realizan dentro del sistema. Los estándares relacionados, como el estándar IEEE 80215.4, distinguen los dispositivos basándose en complejidad de su hardware y en sus capacidades [15]. Dicho estándar define dos clases de dispositivos físicos: el Full Function Device (FFD) y el Reduced Function Device (RFD). Los nodos se definen en tres categorías: 1) coordinador de red, 2) nodo ruteador y 3) dispositivos terminales.
- Entre otros.

Las redes inalámbricas[xiv] *se extienden a todos los ámbitos de las redes*, desde el personal hasta el más extenso o mundial.

Según su alcance las redes in- alámbricas se clasifican del siguiente modo:

- Redes inalámbricas de ámbito personal (WPAN o wireless personal area networks): interconectan dispositivos en el entorno próximo de un usuario (pocos metros). Tecnologías: WPAN: bluetooth e infrarrojos (IrDA).
- Redes inalámbricas de ámbito local (WLAN o wireless local area networks): interconectan dispositivos en un local, piso, planta, edificio o campus. Tecnologías: WLAN: WiFi.
- Redes inalámbricas de ámbito metropolitano (WMAN o wireless metropolitan area networks): interconectan dispositivos y redes en un barrio, pueblo o ciudad. Tecnologías: WMAN: WiMax.
- Redes inalámbricas de ámbito extenso (WWAN o wireless wide area networks): interconectan dispositivos y redes en toda una región, país o conjunto de países. Tecnologías: WMAN: UMTS, GPRS, 3G, 4G…

Ventajas e inconvenientes respecto a las LAN cableadas. Principales ventajas

- Permiten la movilidad de usuarios y dispositivos: los usuarios pueden desplazarse con sus dispositivos inalámbricos a lo largo de toda la zona de cobertura de la WLAN sin perder la conexión.
- Menor coste: el hecho de necesitar muy pocos cables, o incluso ninguno si la red es pequeña, junto con el bajo coste de los componentes de la WLAN hacen que la instalación resulte muy económica.
- Menor tiempo de instalación: es más rápida porque no se tienen que instalar cables, canalizaciones, rosetas, etc. Principales inconvenientes
- Sensibilidad a las interferencias electromagnéticas y a la presencia de otras WLAN: la presencia de interferencias electromagnéticas y de otras WLAN que operen con frecuencias próximas a las de la nuestra puede influir negativamente en el rendimiento de la misma.
- Si en una zona aumenta el número de dispositivos, el rendimiento en dicha zona disminuye: en una misma zona e instante solo puede existir una transmisión para nuestra WLAN, pues sería como si todos los dispositivos de la zona estuvieran conectados a un mismo hub. Esto no ocurre en las redes cableadas basadas en switches.
- Velocidades de transmisión generalmente inferiores: aunque cada vez surgen tecnologías más veloces, todavía no se ha llegado a igualar la velocidad que ofrecen los medios cableados.
- Mayores requerimientos de seguridad: dado que no hace falta acceder físicamente a las WLAN para atacarlas, necesitan mayor seguridad. 2.3 > Situación actual de las WLAN Hoy en día encontramos WLAN en casi todas partes: en nuestros hogares, en oficinas, en centros educativos, en hoteles etc. También existen proyectos para compartir el acceso a Internet en espacios públicos como calles, plazas, etc. En algunas ciudades se pretende dotar de puntos de acceso inalámbrico a cada uno de los semáforos de la ciudad. Pero también hay iniciativas privadas, como Fon, que permite que los usuarios particulares puedan compartir su conexión a Internet a través de su WiFi.

En algunos países como España no es legal compartir la conexión a Internet a través de la WiFi fuera del domicilio concreto para el que el particular o empresa ha contratado los servicios del ISP, salvo que el contrato firmado con el ISP así lo permita o que el titular del contrato se registre como un operador de telecomunicaciones y pague los correspondientes gravámenes de la CMT (Comisión del Mercado de las Telecomunicaciones).

Seguridad en redes inalámbricas.[xv]

Las redes inalámbricas son muy vulnerables a la captura de información por parte de usuarios no autorizados, sobre todo porque cualquier equipo ubicado dentro del radio de acción de la red tiene capacidad de obtener los mensajes enviados por equipos que sí están autorizados Esta captura de trafico la pueden realizar los equipos que dispongan de adaptadores inalámbricos con capacidad para funcionar en modo promiscuo, además de tener instalado un programa de captura de trafico, El modo promiscuo consiste en que el adaptador de red recibe los mensajes y los procesa aunque éste no sea su destinatario Hay que tener en cuenta que no todos los adaptadores inalámbricos disponen de este modo de funcionamiento Para evitar los problemas de seguridad en la captura de trafico de las redes inalámbricas, es imprescindible utilizar mecanismos de cifrado de las comunicaciones, Los mecanismos utilizados para el cifrado de la información en redes inalámbricas son:

- WEP: utiliza una clave de cifrado de 64 o 128 bits (esta ultima es mas segura) que se establece, tanto en los puntos de acceso inalámbricos como en la configuración de los equipos de la red.
- WPA: utiliza una clave de cifrado que se asigna de forma dinámica a los puntos de acceso y a los equipos.
- WPA2: utiliza un método de cifrado mucho mas avanzado, además de que la clave de cifrado puede tener mayor longitud, por lo que se consigue una mayor seguridad, Sin embargo, este mecanismo es relativamente reciente (2004), por lo que muchos dispositivos inalámbricos del mercado pueden no soportarlo.

El inconveniente del cifrado WEP radica en que se establece una clave de cifrado estática que no cambia con el tiempo, a no ser que los administradores de la red se preocupen en cambiarla con determinada frecuencia, Un intruso puede utilizar programas especializados de fuerza bruta para obtener la clave de cifrado y acceder a la red, Uno de estos programas es la distribución de Linux Wifislax, que esta especializada en el acceso y descifrado de contraseñas de las redes inalámbricas (véase el ejemplo 11,1), Si se utiliza cualquiera de las variantes de cifrado WPA (TKIP, EAP o WPAZ), entonces el acceso a la red por usuarios no autorizados es mucho mas complejo, debido a que las claves de cifrado de la red cambian constantemente.

Seguridad en dispositivos de red.[xvixviixviiixixxxxxixxiixxiiixxiv]

Según Hernández y Salazar (2017), una Lista de Control de Acceso o ACL (Access Control List) "es una configuración de router que permite o deniega

paquetes según el criterio encontrado en el encabezado del mismo, comúnmente utilizadas (...) para seleccionar los tipos de tráfico para analizar, reenviar o procesar".

Listas de control de acceso estándar
Según Ariganello (2016), las listas de acceso IP estándar "verifican solo la dirección de origen de la cabecera del paquete IP. Las ACL estándar llevan un número que las identifica según sus características". El rango numérico de las listas de acceso es de 1 a 99 y el rango extendido es de 1300 a 1999.

Router(config)# Access-list {1-99} {permit | deny} source-address [sourcewildcard][3]

Donde:

- 1-99: Identifica numero de lista
- Permit-deny: se chequea si la entrada esta permitida o si será bloqueado el trafico de la dirección de origen.
- Source-address: identifica la dirección IP de origen.
- Source-wildcard: chequea bits del campo de la dirección que serán comprobados.
- Finalmente, el autor indica que la lista de acceso estándar puede eliminarse anteponiendo un "no" al comando.

Finalmente, el autor indica que la lista de acceso estándar puede eliminarse anteponiendo un "no" al comando.

Listas de control de acceso extendidas.
Según Ariganello (2016), las listas de acceso IP extendidas "pueden verificar otros muchos elementos, incluidas opciones de la cabecera del segmento de la capa 4, como los números de puerto".
Es posible que las ACL extendidas puedan ser granulares y se les configuren para filtrar trafico por criterios:
 Protocolo.
 Números de puerto.
 Valor de punto de código de servicios diferenciados (DSCP).
 Valor de precedencia.
 Estado del bit de número de secuencia de sincronización (SYN).
Además, el autor indica que "las ACL extendidas llevan un número que las identifica según sus características. El rango numérico de las listas de acceso extendidas es de 100 a 199 y el rango extendido es de 2.000 a 2.699".
Además, el autor indica que "las ACL extendidas llevan un número que las identifica según sus características. El rango numérico de las listas de acceso extendidas es de 100 a 199 y el rango extendido es de 2.000 a 2.699".

Donde:
 100-199: Identifica el rango y número de lista.
 Permit – deny: Indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección de origen.
 Protocol: Como por ejemplo IP, TCP, UDP, ICMP.
 Source-address: Identifica la dirección IP de origen.
 Source-wildcard: Identifica los bits del campo de la dirección que serán comprobados.
 Operator port: Compara los puertos de origen o de destino. Operados posibles son It (menor que), gt (mayor que), eq (igual), neq (no igual) y range (rango).
 Established: Se usa solo para TCP de entrada. Esto permite que el tráfico TCP pase si el paquete utiliza una conexión ya establecida (si, por ejemplo, posee un conjunto de bits ACK).

Como ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet. Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

Según Geovanny (2016).
Un firewall de nueva generación (NGFW por sus siglas en inglés). Aparte de poseer metodologías de chequeo y protección de datos, mantienen un optimo rendimiento y baja latencia para que redes de alto trafico se mantengan en funcionamiento.
Además, proporcionan un único punto de control para diferentes características:
 Dirección IP: De origen o de destino.
 Número de Puerto: De origen o de destino.
 Dominio: Integración con el servicio de nombres de dominio (DNS), para simplificar el acceso a recursos que resultarían más difíciles de definir por otros medios.
 Tipo de aplicación: Con técnicas de inspección profunda de paquetes, para controlar el funcionamiento de las aplicaciones web.
 Traducción de direcciones IPv4 por NAT: En sentido de salida, y acceso IPv6 nativo a internet. Control del acceso remoto a redes corporativas.
 Control del acceso: Control de acceso remoto a redes corporativas.

Según Cisco (s. f.) "un firewall es un dispositivo de seguridad de la red que controla el tráfico de la red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad".
Un firewall normalmente se encuentra en un punto

[3] Ejemplo obtenido de documento IACC (2019). Implementación de Firewall. Redes y Seguridad. Semana 4.

medio entre 2 redes. Estas. Pueden marcar el perímetro necesario entre una red privada y otras.

Firewall con estado.
Según Symantec (2018), los firewalls que trabajan con estados pueden mantener un seguimiento de las direcciones IP tanto de origen como de destino, los puertos, apps, etc. Mucho antes de que el cliente pueda dar un vistazo a las normas de firewall, esta toma decisiones sobre el flujo de trafico que se basa en la información de conexión.
Si una norma de firewall entrega un permiso a un equipo para que se conecte a un servidor web, el firewall registra información sobre la conexión. Cuando el servidor contesta, el firewall detecta que se espera una respuesta del servidor al equipo.

Firewall de nueva generación.
Según Geovanny (2016), un firewall de nueva generación (NGFW por sus siglas en inglés). Aparte de poseer metodologías de chequeo y protección de datos, mantienen un optimo rendimiento y baja latencia para que redes de alto trafico se mantengan en funcionamiento.

Visión general de los firewalls basados en zona.
Comúnmente, la división se realiza en 3 zonas distintas:
Inside: La zona inside o zona verde es donde se encuentran los equipos corporativos.
Outside: La zona outside o zona roja, es la conexión hacia redes como Internet (red WAN).
DMZ: Es el acrónimo de "Demilitarized Zone" y conocida como zona naranja, es donde se encuentran los servicios extranet, correo, web, etc.

Colomés (2015) indica lo siguiente:
La DMZ es una subred independiente, aparte de la red LAN y de Internet o 'Outside'. Al crear una DMZ se puede configurar un firewall para crear reglas específicas tanto de seguridad como NAT que permitan el tráfico desde Internet hacia esa zona. *Así, si un hacker vulnera la seguridad de uno de los servidores, no tendrá acceso a la red LAN de la organización. Para eso es clave entender cómo se deben crear reglas de tráfico y el cómo se definen los perfiles de seguridad entre las zonas outside, LAN (o inside) y DMZ.*
En 2006, Cisco System un nuevo modelo de configuración en firewalls. Con este nuevo modelo, cada interfaz es asginada a una zona y después una política de inspección es aplicada al tráfico que se mueve entre las zonas. También tiene la opción de denegar el tráfico a través de una política que por defecto no permite ingresos todo entre zonas del firewall. Con este tipo de firewall se pueden emplear zonas, permitiendo que en un Router existan distintas zonas, declarando a una de ellas como origen y la otra como destino. Se establecen fronteras de seguridad de una red. Una zona define un límite donde el tráfico está sujeto a restricciones de políticas cuando cruza a otra región de su red. *Hay varios pasos para configurar ZPF. A continuación, He creado una lista y se explicará su configuración.*
1. Crear las zonas vía comando zone security.
2. Definir clases vía comando class-map type inspect.
3. Especificar políticas del firewall con el comando policy-map type inspect.
4. Aplicar políticas a pares de zonas origen y destino usando zone-pair security.
5. Definir interfaces del Router a zonas usando zone-member security.

Crear las zonas
FW (config) # zone security Inside
FW (config-sec-zone) # description Inside network
FW (config) # zone security Outside
FW (config-sec-zone) # description Outside network
Definir clases de tráfico
FW (config) # class-map type inspect FOREXAMPLE
FW (config-cmap) # match access-group 101
FW (config-cmap) # exit
FW (config) # access-list 101 permit ip 10.0.0.0.0.0.0.255 any
Especificar políticas firewall
FW (config) # policy-map type inspect InsideToOutside
FW (config-pmap) # class type inspect FOREXAMPLE
FW (config-cmap-c) # inspect
Aplicar políticas firewall
FW (config) # zone-pair security insidetooutside source inside destination outside
FW (config-sec-zone-pair) # description Internet Access
FW (config-sec-zone-pair) # service-policy type inspect InsideToOutside
FW (config-sec-zone-pair) # interface F0/0
FW (config-if) # zone-member security Inside
FW (config-if) # interface S0/0/0.100 point-to-point
FW (config-if) # zone-member security Outside.

Las actividades principales en la seguridad, lógica y, o física es monitorear. Esto significa que existe un sistema de control en una red, en laptops o computadores, software, etc. anomalías posibles.
Esto significa que habrá un sistema que podrá retroalimentar parámetros, situaciones a detectar, etc., habrá seguramente correcciones fijadas en parámetros que se establecen en un sistema IDS/IPS.
"Un sistema de detección de intrusiones ("Intrusion Detection System" – IDS) o sistema de prevención de intrusiones ("Intrusion Prevention System" – IPS) es un elemento que monitoriza el comportamiento de redes, host y/o aplicaciones en búsqueda de patrones de comportamiento malicioso". Acosta. (2014).

Tecnología del sistema de prevención de intrusos (IPS)
Según Securizando.com (s. f.):
Los sistemas de detección de intrusos (IDS, Intrusion Detection System) y los sistemas de protección de intrusos (IPS, Intrusion Prevention System), estos son

una evolución de sistemas basados en un firewall. Se utilizan por Sysadmins para detectar anomalías o situaciones de riesgo, para el chequeo de puertos, direcciones IP, etc.

Características IDS
Según Segu-info.com.ar (2009) las características principales de los IDS son:

- Estos deben funcionar sin el chequeo humano o supervisión, el sistema es fiable por si mismo, para que este corriendo como un servicio en el sistema operativo.
- Deben ser tolerantes a fallos, pueden tolerar una caída de sistema.
- Es importante que sea resistente a situaciones de errores, podría ser monitoreado por si mismo.
- Debe minimizar sobrecargas; un sistema que no debe generar una latencia.
- Debe chequear situaciones de desvío, bajo un comportamiento típico.
- Debe ser de fácil adaptación, al momento que se encuentre ya instalado. Cada sistema tiene un patrón, todos funcionan de manera diferente y bajo un mecanismo de defensa a patrones incluso sencillos.
- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
- Debe ser fácil de que sea 'invisible', indetectable.

Debilidades de los IDS:
- Generan falsas alarmas.
- Producen fallos en las alarmas.
- No pasa a ser un sustituto para un Firewall standard, auditorias en seguridad son regulares y estrictas como política de seguridad.

Características IPS
CertSi (2017, p. 31) indica que los IPS se asemejan el comportamiento de los cortafuegos, ya que "ambos toman decisiones sobre la aceptación de paquetes en un sistema". Sin embargo, "los cortafuegos basan sus decisiones en los encabezados de paquetes entrantes, capas de red y de transporte, mientras que los IPS basan sus decisiones tanto en los encabezados como en el contenido de datos del paquete".

Además, CertSi (2017, p. 32) indica que las características principales de los IPS son:
- Capacidad de reacción automática ante incidentes.
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Bloqueo automático frente a ataques efectuados en tiempo real.
- Disminución de falsas alarmas de ataques a la red.
- Protección de sistemas no parcheados.
- Optimización en el rendimiento del tráfico de la red.
- Es posible distinguir dos generaciones históricas de los IPS:
- Los IPS de primera generación, al detectar un ataque proveniente de una dirección IP determinada, descartaban todos los paquetes de esa dirección, estuvieran o no involucrados en el ataque.
- La evolución de los IPS se debe a la capacidad de descartar únicamente los paquetes relacionados con el ataque identificado, permitiendo el tráfico de otros paquetes provenientes de la IP del atacante, siempre y cuando no estuvieran relacionados con el ataque.

Es posible distinguir dos generaciones históricas de los IPS:
Se pueden distinguir dos tipos de generaciones a través del tiempo en los IPS:
- Bajo los IPS de primera generación, interceptar ataques de una IP determinada, se desacertaban todos los paquetes de esa dirección, estuvieras o no bajo en el ataque.
- Mientras ha existido una evolución de los IPS, esta es gracias a que se puede descartar atacantes que puedan venir de un atacante, mientras no exista algún tema con el ataque.

Diferencias entre IPS e IDS
CertSi (2017) indica que existen diferencias entre IPS e IDS, y son:
- Mientras el IDS esta limitado a verificar y detectar intrusiones y que la detiene de algún modo predefinido. A través de esto, el nivel de alertas de un IPS es considerado menor que el nivel de alertas producido por un IDS.
- La diferencia total entre IDS y IPS es fundamentalmente que estos últimos están en capacidad de dejar bajo total inutilización paquetes que hayan sido interceptados en un ataque, siendo modificados.

Formas de detección de IPS/IDS
En el sitio PCI Hispano (Acosta, 2014) indica lo siguiente:

Formas de detección de los IPS/ IDS
Según el tipo de información cuya fuente analizada:
- Red (Network IDS/IPS): Analiza lo que sucede en una red de datos, mientras captura trafico basándose en técnicas de análisis de paquetes. 'Sniffing', también. Bajo Wireless IDS-IPS.
- Host (Host IDS/IPS): Chequea el como un equipo en cuestión – por lo usual el Sistema Operativo- y eventos relacionados con la seguridad.

Dependiendo del tipo de análisis ejecutado:
Según el tipo de análisis:

- Firmas: Se estructura en paquetes de ataques, usualmente como lo gestiona un antivirus.
- Heurística: Esta tomado en cuenta según el análisis y forma de comportamiento.

Según el tipo o forma de respuesta activada:

- Pasiva: No habrá una alteración activa del entorno. Son catalogados como IDS.
- Activa: Aparte de una alerta, se genera una forma de detección correctiva que puede alterar el entorno, puede finalizar una conexión o un proceso, bloqueando trafico que pueda estar relacionado. Son catalogados como IPS.

Implementación ips basada en red (NIPS)
En relación a este tema, el sitio Mit.edu (s.f. b). indica lo siguiente:
Los sistemas para detectar intrusos, que operan en la red diferente a IDS/IPS basados en host. La filosofía detrás de un diseño IDS/IPS va por el hecho de que escanea a nivel de enrutador, o host, escanear cualquier paquete sospechoso, en un archivo de registros especiales con información amplia. La red puede escanear su propia BBDD de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete. Bajo niveles críticos son bastante altos, en varios niveles para chequear cualquier tipo de anomalía.

Los IDS/IPS basados en la red se han vuelto muy populares a medida en que internet ha crecido en tamaño y tráfico. Los IDS/IPS que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escáneres, husmeadores y otras herramientas de auditoría y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

- Engaño de direcciones IP (IP Spoofing).
- Ataques de rechazo de servicio (DoS).
- Envenenamiento de caché arp.
- Corrupción de nombres DNS.
- Ataques de hombre en el medio.

IPS basados en HOST (HIPS)

El Mit.edu (s.f. a), indica lo siguiente respecto al tema:
EL uso basado en HOST analiza diferentes áreas, para testear actividades maliciosas, intrusiones, etc. Estos sistemas consultan diferentes tipos de registros de archivos (Kernel, sistemas servidores, etc.) Los sistemas basados en Linux y UNIX utilizan mucho Syslogs para separar eventos y registrarlos por severidad.
Los sistemas basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Estan en archivos confidenciales, y crea una suma de verificaciones en una base de datos de archivos confidenciales y crea una suma de verificación de cada archivo con una utilidad de resumen de archivos de mensajes tal como MD5 (algoritmo de 128-bit) o SHA1 (algoritmo de 160-bit) generados mediante “Funciones Hash”.

Tablas de enrutamiento
Según redes locales y globales (s. f.) “cada host y cada router mantienen el conjunto de correspondencias entre direcciones IP de destino y las direcciones IP de los routers del próximo salto para esos destinos en una tabla denominada tabla de enrutamiento IP”.

El router resuelve rutas de paquetes según su destino, y si se encuentran en algún tipo de interfaz de red.

El sitio indica:
Que como un router es incapaz de tener un interfaz de red por cada red de destino, entonces, si no delega en otros routers, sería incapaz de resolver el destino de la mayor parte de los paquetes. Así cuando un router recibe un paquete, si no encuentra la dirección destino en su tabla de rutas, encamina el paquete hacia un router de orden superior confiando en que él sepa resolverlo.

Se pueden encontrar tres tipos de correspondencia en las tablas de enrutamiento:
Correspondencias en tablas de enrutamiento

Rutas directas:

- Para redes conectadas localmente. En ese caso está conectada a la misma red y se pone como Gateway (puerta de enlace) 0.0.0.0.

Rutas Indirectas:

- Para redes alcanzables vía uno o más routers. Se pone como gateway la ip del router en el que se delega la búsqueda. Es decir, el próximo salto.

Una ruta por defecto:

- Que contiene la dirección IP de un router que se usa para todas las direcciones IP que no cubren las rutas directas e indirectas. Se señaliza poniendo en el destino 0.0.0.0.

Tipos de tablas de enrutamiento
Los tipos de tablas de enrutamiento según Oracle.com (s. f.), son los siguientes:

Tipos de tablas de enrutamiento

Estático:

- Hosts y redes de tamaño pequeño obtienen rutas de enrutados predeterminados. Estos necesitan, solo conocer uno o dos enrutadores en los consiguientes saltos.

Dinámico:
- Interredes de mayor tamaño, enrutadores, con múltiples hosts y hosts de sistemas autónomos de gran tamaño. El enrutamiento dinámico es la mejor opción para los sistemas en la mayoría de las redes.

Estático y dinámico combinados:
- Enrutadores que conectan una red con enrutamiento estático y una red con enrutamiento dinámico, y enrutadores de límite que conectan un sistema autónomo interior con redes externas. La combinación del enrutamiento estático y dinámico en un sistema es una práctica habitual.

Volviendo al tema de los IPS, comprueban valores HASH del host que está monitoreando. Si alguna se modifica, el sistema tomará las medidas correspondientes para corregir la situación, o tomará medidas.

Firmas del sistema de prevención de intrusos (IPS)

Características de la firma IPS

La detección basada en firmas analiza el tráfico en busca de patrones coincidentes con una base de datos de firmas. Es un funcionamiento similar al de los antivirus.
- Pro: Pocos falsos positivos, permite detectar exploits u otro código malicioso.
- Contra: Hay que actualizar las firmas frecuentemente.

Alarmas de firma IPS
Según Cybsec.com (s. f., p.1 3), "los IPS reaccionan de forma automática a las alarmas, por ejemplo, reconfigurando firewall, actualizando la lista negra del firewall, bloqueando puertos, etc.".

Y Cisco.com (s.f. b) indica que:
Un IPS seguro acciona una alarma cuando un paquete o una secuencia dado de paquetes se iguala a las características de los perfiles del ataque conocido definidos en las firmas seguras de IPS". Un criterio de diseño crítico de la firma IPS es minimizar el acontecimiento del falso positivo y de las alarmas negativas falsas.

En este sitio también se indica que los falsos positivos (activadores benignos) o avisos falsos ocurren cuando el IPS señala cierta actividad benigna como malévola. Esto requiere la intervención humana diagnosticar el evento. Un gran número de falsos positivos pueden drenar perceptiblemente los recursos, y las habilidades especializadas requeridas analizarlos son costosas y difíciles de encontrar.

Acciones de firma IPS

Gómez (s. f., p. 20) indica que "las respuestas que proporcionan estos sistemas son acciones automatizadas tomadas cuando se detectan ciertos tipos de intrusiones. Se tienen tres categorías de respuestas activas".

Acciones de los sistemas IPS
Incrementar la sensibilidad de las fuentes de información:
- Cuando se sospecha de información que pueda significa run ataque, podría incrementarse la el nivel de sensibilidad y fuentes, así como activaciones, para capturar lo no restringido solamente a un puerto, o pc.

Cambiar el ambiente:
- Esto consiste en detener un ataque en progreso a través de la reconfiguración de dispositivos como routers o sistemas de protección perimetral parabloquear el acceso del atacante.

Tomar acciones contra el atacante:
- Significa lanzar ataques en contra del intruso o intentar activamente, obteniendo onformacion acerca de la computadora del atacante o del sitio donde se encuentra. Sin embargo, este tipo de respuesta no es recomendable, debido a que los atacantes utilizan direcciones IP falsas.

Aplicaciones de Criptografía[xxv]: Seguridad, Firma digital Certificados, SSL, etc.

Mediante técnicas criptográficas, pueden garantizarse tres propiedades vitales para la seguridad: confidencialidad (cifrado simétrico y asimétrico), autenticación (cifrado asimétrico) e integridad (funciones hash).

En el caso de la firma digital, se trata de resolver el problema de la autenticidad del mensaje, es decir, que el mensaje recibido es exactamente igual al original (integridad) y que además proviene de quien dice venir (autenticación de origen). A esto hay que añadir también la necesidad de garantizar el no repudio, es decir, que el emisor no pueda negar haber sido él quien generó el mensaje.

Los mecanismos de cifrado por sí mismos no son

capaces de garantizar la autenticidad, por lo que se han tenido que desarrollar otros métodos. La solución es la utilización de la firma digital, también denominada firma electrónica. La firma digital es un conjunto de datos que se añaden a un mensaje original y que permiten asegurar la identidad de la persona que ha firmado el mensaje, así como que el contenido de este no ha sido modificado por terceras personas.

Clases de firma digital:

- Firma electrónica: es el conjunto de datos en forma electrónica que pueden ser utilizados como medio de identificación del firmante. Por ejemplo, sería cifrar un mensaje con nuestra clave privada.
- Firma electrónica avanzada: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Firma electrónica reconocida: es avanzada basada en un certificado re- conocido y generada mediante un dispositivo seguro de creación de firma. Por ejemplo, es la firma mediante el DNIe. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Certificados digitales
Para solucionar el problema de la autenticación en las transacciones por Internet se buscó algún sistema identificativo único de una entidad o persona.
Ya existían los sistemas criptográficos de clave simétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, solo conocida por el propietario. El problema era asegurar que, efectivamente, la clave pública que se recibía era de la persona correcta y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin lugar a dudas a su emisor. La solución a este problema vino con la aparición de los certificados digitales o certificados electrónicos, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales. La misión principal de un certificado digital es garantizar, con toda confianza, el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Existen varios tipos de certificados, pero los más usados se rigen por el estándar UIT-T X.509.
Su estructura es la siguiente:

– Certificado:
• Versión.
• Número de serie.
• ID del algoritmo.
• Organismo emisor.
• Periodo de validez.
• Información de la clave pública del usuario.
• Otros campos opcionales (ID del emisor, ID del usuario, etc.).

– Algoritmo usado para firmar el certificado.
– Firma digital del certificado.

SSL y TLS SSL y TLS
Son protocolos que proporcionan comunicaciones seguras en una red insegura, como Internet.
– SSL: Secure Sockets Layer o protocolo de capa de conexión segura.
– TLS: Transport Layer Security o seguridad de la capa de transporte.

En ambos casos existe un sistema híbrido que usa un canal seguro con cifrado asimétrico (Diffie Hellman) para intercambiar las claves simétricas dinámicas (van cambiándose cada cierto tiempo) negociadas entre ambas partes. El cifrado de estos protocolos se produce sobre la capa de transporte. Una de las principales aplicaciones prácticas de estos protocolos es formar https junto a http, garantizando el envío y recepción de información de forma segura mediante un navegador web. Todo esto permite confidencialidad en las comunicaciones, manteniendo la integridad de los datos al tiempo que se garantiza la identidad de las partes. Toda comunicación mediante SSL o TLS consta de dos fases: – Fase de saludo, correspondiente con los sistemas de criptografía de clave asimétrica, en la que se negocia entre las partes el algoritmo que se usará en la comunicación. También se produce el intercambio de claves públicas, autenticándose cada una de las partes mediante certificados digitales X.509. Los dos interlocutores eligen una clave de sesión. – Fase de comunicación, correspondiente con los sistemas de criptografía de clave simétrica, en la que se produce el cifrado del tráfico basado en cifrado simétrico a partir de la clave de sesión y se van generando nuevas claves de forma dinámica.

En cuanto a las características de cada uno de estos protocolos, SSL es un protocolo abierto que puede ser empleado por cualquier fabricante de aplicaciones para Internet para asegurar la privacidad en el envío de información a través de la web. Se suele utilizar en servidores web y permite que la información transmitida entre un navegador web (cliente) y un servidor web esté cifrada. El servidor debe utilizar un par de claves, así como un certificado. SSL presenta las versiones 1 y 2 (en las que se proporciona autenticación de servidor) y 3 (en que se añade autenticación del cliente por medio de certificados digitales del cliente y servidor). En cuanto al TLS, es un protocolo basado en SSL mejorado. Existen

diferentes versiones que van corrigiendo vulnerabilidades detectadas en versiones anteriores. La última versión es TLS 1.2, definida en el RFC 5246.

Clasificación de los IPS[xxvi] e IPS de Nueva Generación.

Los IPS se pueden clasificar de diferentes maneras. Por un lado, dependiendo de su método para realizar detecciones de amenazas y por otro, basados en la tecnología que los implementa.

Clasificación de acuerdo al método de detección:

- IPS basado en firmas o signaturas: cuentan con una base de datos de "firmas", en la cual se reflejan patrones conocidos de ataques a la seguridad de un dispositivo o una red. Esta información se adhiere al dispositivo que realizará la detección para que así, mediante una búsqueda de coincidencias, se pueda establecer si existe o no un posible ataque y reaccionar en consecuencia.
- IPS basado en anomalías: también conocido como basado en "perfil", esta funcionalidad intenta identificar un comportamiento diferente que se desvíe de lo que, de alguna forma, se ha predefinido como una "actuación normal" de un dispositivo o una red. Para garantizar este comportamiento se hace uso de un potente análisis estadístico de indicadores de tráfico.
- IPS basado en políticas: se requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico definido por el perfil establecido, permitiendo o descartando paquetes de datos, por lo que su manera de actuar ocurre de forma muy similar al funcionamiento de un *firewall*.
- IPS basados en detección por *Honey Pot* (Pote de Miel): funciona usando un equipo configurado para que, a primera vista, parezca ser vulnerable e interesante para un ataque, de forma tal, que al ocurrir estos, se deja evidencia de la forma de actuar, con lo cual posteriormente se pueden implementar políticas de seguridad.

Clasificación de acuerdo a su tecnología:

- IPS basado en host: monitorea las características de un dispositivo de un abonado de la red en particular, para detectar actividades dentro del mismo. Entre las características que supervisa se encuentran: el tráfico de red cableada o inalámbrica, registros del sistema, acceso de los usuarios, ejecución de procesos y modificaciones de archivos; las acciones de contingencia lanzadas, actúan igualmente solo sobre el host en el cual trabaja. Este tipo de IPS se emplea con frecuencia en la protección de servidores y dispositivos con aplicaciones de servicios ininterrumpidos.
- IPS basado en la red: con esta tecnología, se realiza el monitoreo sobre el tráfico que fluye a través de segmentos particulares, y se analizan los protocolos de la red, de transporte y de aplicación para identificar actividades sospechosas. Su funcionamiento se caracteriza por el análisis en tiempo real de los paquetes de datos del tráfico (cableado o inalámbrico), en busca de patrones que puedan suponer algún tipo de ataque. Una solución recomendada para la detección de intrusos que proceden de redes no fiables, es que el sistema IPS resida junto con el *firewall* en el mismo dispositivo.

Funcionamiento

El procesamiento de un IPS está basado en un conjunto de instrucciones altamente especializadas, que permiten inspeccionar de forma total cada bit de un paquete de datos intercambiado.

El tráfico de datos es clasificado e inspeccionado en su totalidad por todos los filtros relevantes antes de que se permita su salida, lo que se realiza analizando la información del encabezamiento de cada paquete, como puertos y direcciones IP de fuente y destino, y los campos de aplicación.

Cada filtro consta de un conjunto de reglas que definen las condiciones que deben cumplirse para llegar a saber si un paquete o flujo es malicioso o no. Cuando se clasifica el tráfico, el dispositivo debe ensamblar la carga útil del flujo y pasarla a campos que sean de utilidad para hacer luego un análisis contextual.

A fin de impedir que un ataque alcance su objetivo, en el instante en que se determina que un flujo es malicioso, se detiene el avance de los paquetes, así como de aquellos que lleguen posteriormente y que pertenezcan a dicho flujo.

Puede ocurrir, además, un ataque multiflujo, dirigido a desactivar una red inundándola de paquetes, por lo que se requieren filtros que realicen estadísticas e identifiquen anomalías en varios flujos agregados.

Los IPS más avanzados, combinan procesamiento masivo de paquetes en paralelo, para realizar chequeos simultáneamente. El procesamiento en paralelo generalmente se implementa sobre hardware, porque las soluciones de software convencionales, disminuyen por lo general el rendimiento.

Adicionalmente, los IPS pueden incorporar técnicas de redundancia y tolerancia a errores (*failover),* para asegurar que una red continúe operando en el caso de que se produzca un fallo. De la misma manera, agregan control sobre las aplicaciones que no son de misión crítica, para proteger el ancho de banda.

IPS de Nueva Generación

El dinamismo de las redes actuales, provoca la aparición constante de nuevas tecnologías, dispositivos y sistemas, lo que incrementa la exposición a mejoradas técnicas para vulnerar la seguridad de la información y evidencia la necesidad de mecanismos que tengan cierta inteligencia para poder hacerle frente, propiciando el desarrollo de IPS de Nueva Generación.

Un IPS de Nueva Generación, debe cumplir con los siguientes elementos:

- Siempre en Línea: nunca entorpecer o interrumpir el funcionamiento de una red.
- Conciencia de Aplicaciones: capacidad para poder identificar aplicaciones e implementar políticas de seguridad de red en la capa de aplicación.
- Conciencia del Contexto: las decisiones de detección y enfrentamiento de las amenazas, debe basarse en el análisis complejo de circunstancias que rodean un ataque específico, que permitan decidir automáticamente la prioridad específica a la respuesta que el equipo deba dar ante un incidente de seguridad inminente.
- Conciencia del Contenido: debe ser capaz de inspeccionar y clasificar los tipos de archivos reflejados en los paquetes de datos.
- Agilidad: debe ser capaz de incorporar nuevos mecanismos de retroalimentación para enfrentar amenazas futuras.

Esta nueva generación de IPS puede tener visibilidad sobre el comportamiento de la red, los perfiles de los equipos dentro de la infraestructura de comunicación, y la identidad de los usuarios y las aplicaciones que están en uso, de tal forma que esa información le sirva de insumo para poder realizar un proceso de afinamiento automático.

El termino dispositivo final se refiere a una parte del equipamiento se puede ser el origen o destino de mensajes en una red. Otro termino es que el dispositivo final que envía o recibe mensajes es el Host, que puede ser parte de varias partes de una amplia estructura de funciones.

Medidas de seguridad para dispositivos finales

Protocolos:

- Los dispositivos configurables que se utilicen deben usar la versión segura del protocolo que exista.

En técnicas como Fuzzing, se puede testear la implementación de protocolos para verificar vulnerabilidades de desborde en buffer, de enteros o bucles infinitos. Así se determinan si todo opera bajo protocolos de seguridad en todas las capas de red, y así evitar ataques.

Puertos e interfaces:

- Los dispositivos finales cuentan con una interfaz física, (RJ45, WIFI, Zigbee, CAN, USB, etc.) y, usualmente, entregan también el firmware. Estas deben controlarse tanto físicamente con protección anti-tampering, como lógicamente deshabilitando aquellos que no son utilizados y proporcionando un mecanismo de control de acceso a usuarios unívocos.

Acceso al hardware:

- Uno de los grandes problemas de la seguridad de los dispositivos finales es el acceso físico al mismo, un atacante puede estudiar esto en detalle. Para prevenir esto es necesario una estructura anti-tampering (anti-manipulación) que bloquee física y lógicamente la apertura del dispositivo.

Firmware:

- Para valorar lo vulnerable que puede llegar a ser el hardware de los dispositivos, es necesario disponer de una infraestructura en la que poder valorar y certificar la seguridad e integridad a nivel hardware de toda la maquinaria, chips o sistemas.

- Hace años era difícil obtener el firmware de un dispositivo, ya que había que extraerlo del propio dispositivo, pero hoy por hoy se puede encontrar en la web de quienes lo han fabricado o puede ser descargado a través de la misma aplicación.

Software:

Un software tiene la posibilidad la habilidad para calcular y ejecutar muchas tareas o aplicaciones a la vez. Es importante evaluar y verificar bugs.

- Es muy importante revisar la configuración de todos los aplicativos, bases de datos, almacenes de contraseñas, accesos remotos, etc., para aplicar las medidas de seguridad

adecuadas en todos los aspectos de la infraestructura de software.

Antes de explicar este ataque se verá cómo funciona un switch. De acuerdo al sitio Computerhoy.com (2016), "básicamente, los switchs crean una especie de canal de comunicación exclusiva entre el origen y el destino".

En capa 2 del modelo OSI los equipos son visibles unos a otros mediante una dirección física MAC. El tráfico entre equipos es administrado por un switch, el cual permite el uso de los recursos de la red de manera eficiente. El uso de switches ha creado algunos mitos, como son:

- La dirección MAC de un equipo es física por lo tanto no puede ser cambiada o falsificada.
- El switch no es vulnerable a Sniffing de tráfico.
- Si creo una VLAN aíslo completamente el tráfico ente equipos.

Comparativo funcionamiento hub / switch

Hub:

- Envía los paquetes de datos recibidos a todos los equipos que estén conectados a sus puertos.

Switch:

- Envía los paquetes de los datos recibidos solo a una dirección MAC específica, la cual está indicada en las cabeceras de los paquetes de datos.

Un switch guarda la asociación entre MAC y el puerto físico donde está conectado un equipo en una tabla que se llama CAM, la cual tiene un tamaño fijo.

Ataque

El ataque "consiste en inundar con direcciones MAC falsa la tabla CAM hasta sobrepasar su almacenamiento y así conseguir que el conmutador se comporte como un hub e inunde todos los puertos del conmutador con tráfico" (Networkingbasico.blogspot.com, 2011).

Esto se usa comúnmente en el mundo del hacking para capturar trafico de la red, o pueden llegar a botar un sistema en una red, completamente.

Para mitigar una situación como la entregada en la pregunta 2, es importante considerar la seguridad de los puertos que Cantone.com.ar[xxvii] (2018) indica lo siguiente:

La seguridad de puertos para administradores permite, logrará encontrar una especificación de manera estática a las direcciones MAC y permitir al Switch aprender en forma dinámica un número limitado de direcciones MAC. Esto permite limitar direcciones MAC permitidas en un puerto, la seguridad de puerto puede ser utilizada para controlar la expansión no autorizada de la red.

Una vez que las direcciones MAC son asignadas a un puerto seguro, dicho puerto no reenvía tramas cuyas direcciones MAC de origen no se encuentren en el grupo de direcciones definidas. Cuando un puerto configurado con seguridad recibe una trama, se compara la dirección MAC de origen de la trama contra la lista de direcciones de origen seguras que fueron configuradas en forma manual o automática (aprendidas) en el puerto.
Si la dirección MAC de un dispositivo conectado al puerto no se encuentra en la lista de direcciones seguras, el puerto puede apagarse hasta ser habilitado nuevamente por un administrador (modo por defecto) o bien puede descartar las tramas provenientes de hosts no seguros (modo "restrict").

Mitigación de ataques de VLAN

Ataques VLAN Hopping

Guedez (2018) indica que:
El VLAN Hopping se puede evitar desde la prevención, significa generar un refuerzo a la seguridad de capas primarias del modelo OSI, *se protege datos y monitoreo de actividad en los sistemas*. En cualquier caso, se requiere de un plan de trabajo bien estructurado que permita la detección de eventos amenazantes durante las 24 horas del día.

Esta vulnerabilidad se puede eliminar con una estrategia temprana que combine la fuerza de trabajo del equipo de IT y el apoyo de software de Security Management.

Entrega al equipo IT, la compresión de métodos y las intenciones de forma de actuar de hackers o cyber-atacantes. Se pueden lograr que las aplicaciones de procesos o tareas automatizadas de manera efectiva, en protocolos, reforzando áreas especificas en los sistemas.

Para esa tarea, el modelo ATT&CK (Tácticas, Técnicas y Conocimiento Común de Adversarios), es un marco de trabajo o base de conocimientos para definir técnicas y tácticas de ataque para describir modelos de comportamiento, cómo se comporta un usuario o equipo y las claves para corregirlo, de modo que los proveedores puedan probar sus tecnologías antes de lanzarlas.

Doble etiquetado de VLAN

El mejor método para mitigar los ataques de etiquetado doble es asegurar que la VLAN nativa de los puertos de enlace troncal sea distinta de la VLAN de cualquier puerto de usuario.

Mitigación de ataques de DHCP

Ataque de DHCP Spoofing

El DHCP *Spoofing* es una funcionalidad que es capaz de diferenciar entre dos tipos de puertos en un entorno conmutado: por un lado, puertos confiables (trusted port) y, por otro, puertos no confiables (untrusted host).
Los primeros no tendrán restricciones de cara al tipo de mensajes DHCP que puedan recibir, puesto que serán aquellos conectados a un entorno controlado (en este caso al servidor/servidores DHCP). Sin embargo, los segundos únicamente podrán enviar aquellos paquetes que en condiciones normales un cliente necesita enviar para conseguir su configuración DHCP (DHCPDiscover, DHCPRequest, DHCPRelease). Los untrusted port por tanto serán configurados en aquellos puertos conectados a los usuarios finales y en el caso de que dicho puerto reciba un paquete suplantado serán bloqueados (Iesharia.org, s. f.).

Mitigación de ataques de ARP

Ataque de ARP Spoofing

Para evitar a este tipo de ataques se recomienda trabajar con rutas estáticas en los dispositivos conectados a red. *Mora, M. (s. f.) indica que, "Esto permite invalidar los mensajes ARP, debido a que las IP se asocian una dirección MAC y esta no cambia en el tiempo"*. Esto es una simple solución implementado un camino predefinido hacia la puerta de enlace evitando que los datos entregados en la red sean recibidos por un atacante.

Criptología[xxviii] es la ciencia que se relaciona con los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre puntos de emisores y receptores en comunicaciones digitales – computadores, servidores, etc.-
Esta ciencia está dividida en dos grandes ramas:

- Criptografía: se relaciona con el cifrado de mensajes criptosistemas.
- Criptoanálisis: descifra mensajes en clave, rompiendo así el criptosistema (Rediris.es, 2002).

Hashes criptográficos
"Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija" (Kaspersky.com, 2014).

Respecto a las funciones hash

- A pesar de cualquier largo de entrada, una función Hash siempre entrega una salida con longitudes constantes.
- En las funciones Hash no es posible revertir su resultado de forma directa. Son irreversibles.

Adslzone.net (2017) presenta en su Web la siguiente explicación respecto al uso con archivos:
Verifica si un archivo es original al que se entrego. Verifica infecciones de malware, así como descargas incompletas o corruptas.

Integridad con md5, sha1 y sha2
La integridad es definida por la RAE como la "propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada".
Para garantizar integridad en la información se han creado funciones Hash, como:

- MD5[xxix] El algoritmo toma un mensaje de longitud sin definir y emite un resumen de mensaje de 128 bits.
- SHA1: El algoritmo toma un mensaje de entrada de cualquier longitud inferior a los 264 bits y genera un resumen de mensaje de 160 bits.
- SHA2 E Está compuesta por diferentes versiones, por ejemplo, SHA-224, SHA-256, SHA-384, SHA-512. Por ejemplo, SHA-256 tiene una longitud de 256 bits.

Autenticación con hmac
Es un algoritmo que entrega una integridad utilizando clave secreta, funciones HMAC -algoritmo que utiliza clave secreta y funciones Hash, para garantizar y proteger la seguridad e integridad de los datos.
Los objetivos del algoritmo HMAC son los siguientes (Ocad, 2015):

- Genera autenticidad, e integridad de la información.

- Utilizar técnicas de hash existentes.
- Preservar rendimiento del hash que se hace generado y utilizado.
- Permitir reemplazar fácilmente el algoritmo Hash usado.

Diferencias entre HASH y HMAC.
Ofrecen integridad: Ofrecen integridad y autenticidad.
Solo utiliza funciones Hash: Utiliza funciones Hash y clave secreta para proteger la información.

En los años 70, En USA se genero un standard -DES-, para datos digitales. Son sistemas de cifrado que ofrecen clave simétrica.

Winrar[xxx] es un ejemplo común en computadores, además de comprimir permite cifrar y proteger con passwords datos o archivos. El sitio Winrar.es (s. f.) indica que "los archivos RAR están codificados con AES-256 en modo CBC para los archivos con formato RAR 5.0 y con AES-128 en modo CBC para RAR 4.x. La función de derivación de la clave en archivos RAR 5.0 está basada en PBKDF2 usando HMAC-SHA256".

Cifrado Clave Cantidad Claves distintas posibles
- DES 64 bits. 264
- 3DES 192 bits. 2192
- Blowfish 128 bits. 2128
- IDEA 128 bits. 2128

Algoritmo de cifrado alterno o clave asimétrica
Estos algoritmos de clave publica o asimétrica, se conciben con dos llaves distintos. Emisor y receptor, todo encriptado.
Respecto a las claves asimétricas[xxxi] Ecured.cu (s. f.), indica lo siguiente:
La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Ventajas y desventajas de la criptografía asimétrica
Ventajas:

- Distribución de claves más fácil, en este caso denominada clave pública.

Desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

Protocolos de cifrados de datos

De acuerdo al sitio de la empresa IBM[xxxii] (s. f. 3), "los protocolos de cifrado SSL (Secure Sockets Layer) y TLS (Transport Layer Security) proporcionan conexiones seguras, permitiendo que dos partes se comuniquen con privacidad e integridad de datos".

Estos protocolos entregan la posibilidad que los servidores y clientes web compartan información de manera segura, trabajen juntos entre las capas 4 y 7 del modelo OSI.

Características y similitudes de los protocolos SSL y TLS:

Protocolo: SSL
- Característica: Considerando un modelo OSI (Arquitectura de redes por capas), el protocolo SSL se utiliza entre la capa de aplicación y la capa de transporte.
- Se utiliza para la transferencia de hipertexto (sitios web) de manera segura.
- En el protocolo SSL se utiliza tanto en criptografía asimétrica como simétrica. La primera se utiliza para realizar el intercambio de las claves que, a su vez, serán usadas para cifrar la comunicación mediante un algoritmo simétrico.
- En el caso de los sitios web, para el funcionamiento de este protocolo lo que se necesita utilizar es un certificado SSL.

Similitudes: Mientras que SSL y TLS:
- Proporcionan una funcionalidad similar, no son intercambiables.
- Sin embargo, el protocolo TLS es compatible con SSL, lo que significa que funciona con conexiones cliente-servidor que requieren SSL.
- Otro detalle de interés es que SSL no funciona con conexiones cliente-servidor que requieren TLS.

TLS:
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- Se implementa sobre un protocolo de transporte fiable como el TCP.
- Los extremos se autentican mediante certificados digitales e intercambian las

claves para el cifrado, según la negociación.

- *Compara los diferentes protocolos de integridad para los datos.*

El protocolo IPsec (Internet Protocol security. Es la intersección de distintos protocolos que consideran como objetivos proteger las comunicaciones sobre el protocolo IP. Funcionan sobre la capa 3 del modelo OSI, a diferencia de SSL y TLS que trabajan entre las capas 4 a la 7 (Laurel.datsi.fi.upm.es, 2012).

Modos de Funcionamiento protocolo IPsec:

- Únicamente los datos del paquete son cifrados.
- El enrutamiento y la cabecera se mantienen.
- Las capas son sometidas a funciones HASH.
- Generan una comunicación entre dos hosts y sobre un canal inseguro.

Modo Túnel:

- El paquete completo es cifrado y/o Autentificado.
- Se utiliza para comunicaciones red a red, es decir, para formar túneles seguros entre routers para levantar VPNs.
- Su fin es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro.

Desde los tiempos de los romanos hasta la criptografía cuántica, nuestros secretos han sido resguardados por técnicas criptográficas. En la actualidad se están presentado una gran cantidad de amenazas las cuales van creciendo exponencialmente, por lo tanto, se deben utilizar todas las herramientas disponibles para asegurar que la información mantenga su confidencialidad, disponibilidad e integridad. En resumen, que esté segura.

Una situación importante entre Windows / contraseñas y funciones Hash, son:

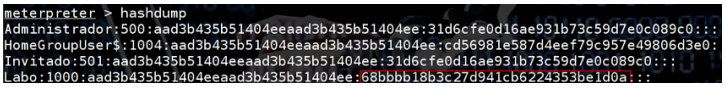
- *¿Cómo roban contraseñas en Windows? Importancia de una autenticación robusta*[xxxiii]
- *¿Cómo se almacenan las contraseñas en Windows?*

Para que un sistema operativo Windows permita la autenticación una vez que ingresamos, debe comparar lo ingresado con una cadena de caracteres almacenada en la computadora. Esta cadena contra la que compara no está almacenada en texto plano, pues un acceso indebido al sistema dejaría la contraseña fácilmente expuesta. Por lo tanto se utiliza una función de hash para almacenarla con un grado mayor de seguridad.
Para sistemas operativos Windows, el hash de las contraseñas de los usuarios de cada máquina se encuentran en el archivo SAM (Security Account Manager) y se utiliza, dependiendo de la versión del sistema operativo, uno de dos algoritmos: LM o NTLM.
El cifrado LM (Lan Manager) es un algoritmo débil por la forma en que está diseñado, ya que por ejemplo divide la contraseña en dos bloques de 7 bytes, convierte todos los caracteres a mayúsculas y rellena con ceros los bytes no utilizados; todo esto facilita un ataque de fuerza bruta. Cuando fue reemplazado por NTLM (NTLan Manager) se corrigieron estos errores, pero aún así muchos sistemas por compatibilidad siguen almacenando las contraseñas en los dos formatos, lo cual es una clara falla de seguridad.

Cómo los atacantes obtienen y descifran las contraseñas de Windows

Son múltiples las formas en las que un atacante podría llegar a hacerse con los hashes relacionados con las contraseñas de Windows, por ejemplo, a través del uso de un Iframe en un sitio web que aproveche una vulnerabilidad en un navegador o sus complementos.

Con el uso de un exploit un atacante podría obtener todos los nombres de usuario y los hashes asociados a una computadora en particular, tal como se puede ver en la siguiente imagen:



Con esta información, el atacante podría utilizar múltiples herramientas para a través de fuerza bruta llegar a obtener la clave que está utilizando la víctima. Sin embargo, y dado que muchos usuarios generalmente utilizan contraseñas débiles, una búsqueda en Internet basta para conocer la contraseña.

Protocolos en Banca, Fábrica de robots, Aerolíneas[xxxiv]*:*

Otros de los aspectos más importantes de los Sistemas Distribuidos son los protocolos de comunicación que se detallan a continuación.
Definición:
Un protocolo de comunicación es un conjunto de reglas

y formatos que se utilizan para la comunicación entre procesos que realizan una determinada tarea. Se requieren dos tipos de especificaciones:

- Especificación de la secuencia de mensajes que se han de intercambiar.
- Especificación del formato de los datos en los mensajes.

La finalidad de los protocolos es permitir que componentes heterogéneos de sistemas distribuidos puedan desarrollarse independientemente, y por medio de las capas que componen el protocolo, exista una comunicación transparente entre ambos componentes. Es conveniente mencionar que estas capas del protocolo deben presentarse tanto en el receptor como en el emisor.

Dentro de los protocolos más utilizados en los sistemas distribuidos se encuentran:

- IP: Protocolo de Internet.- Protocolo de la capa de Red, que define la unidad básica de transferencia de datos y se encarga del direccionamiento de la información, para que llegue a su destino en la red.
- TCP: Protocolo de Control de Transmisión.- Protocolo de la capa de Transporte, que divide y ordena la información a transportar en paquetes de menor tamaño para su envío y recepción.
- HTTP: Protocolo de Transferencia de Hipertexto.- Protocolo de la capa de aplicación, que permite el servicio de transferencia de páginas de hipertexto entre el cliente Web y los servidores.
- SMTP: Protocolo de Transferencia de Correo Simple.- Protocolo de la capa de aplicación, que procesa el envío de correo electrónico por la red.
- POP3: Protocolo de Oficina de Correo.- Protocolo de la capa de aplicación, que gestiona los correos en Internet, es decir, permite a una estación de trabajo recuperar los correos que están almacenados en el servidor.

Ventajas de un Sistema Distribuidos
Las ventajas de los sistemas distribuidos con respecto de los centralizados son:

- Economía. Los microprocesadores ofrecen mejor proporción precio/rendimiento que los mainframes, pues se pueden reunir un gran número de CPU's baratos en un mismo sistema y dado el avance tecnológico de estos, se puede dar un mejor rendimiento que un sólo mainframe.
- Velocidad. Un sistema distribuido puede tener mayor poder de cómputo que un mainframe.
- Distribución inherente. Algunas aplicaciones utilizan computadoras que están separadas a cierta distancia. Por ejemplo, trabajo cooperativo apoyado por computadora, juegos cooperativos apoyados por computadora.
- Confiabilidad. Si una computadora se descompone, el sistema puede sobrevivir como un todo.
- Crecimiento por incrementos. Se puede añadir poder de cómputo en pequeños incrementos.

Ventajas de los sistemas distribuidos con respecto a las computadoras personales aisladas

- Datos compartidos. Permiten que varios usuarios tengan acceso a una base de datos común.
- Dispositivos compartidos. Permiten que varios usuarios compartan periféricos caros como scanners o impresoras a color.
- Comunicación. Facilita la comunicación de persona a persona; por ejemplo, mediante correo electrónico, FAX, chats, foros, etc.
- Flexibilidad. Difunde la carga de trabajo entre las computadoras disponibles en la forma más eficaz en cuanto a costos.

Desventajas de un Sistema Distribuido
- Software. Existe poco software para los sistemas distribuidos en la actualidad.
- Redes. La red se puede saturar o causar otros problemas.
- Seguridad. Un acceso sencillo también se aplica a datos secretos.

La principal dificultad en el desarrollo de un sistema distribuido es el software, dado que el diseño, la implantación presenta numerosas interrogantes: Tipos de sistemas operativos y Lenguajes de Programación adecuados para estos sistemas Niveles de Transparencia Responsabilidades del sistema y de los usuarios

Otro problema potencial es la configuración de las redes dado que es necesario considerar:
perdidas de mensajes saturación en el trafico extensión de la red configuración de la topología
Aplicaciones Distribuidas.

- Una red de computadoras con una pila de procesadores
- Una aerolínea
- Fábrica de robots
- Un banco con sucursales
- Internet
- Multimedia y conferencias

Seguridad en redes telemáticas

En los últimos meses no sólo la prensa especializada en informática, sino todos los medios de difusión han hecho eco del futuro de las autopistas de la información, cuyo embrión está representado por la red Internet. A raíz de la interconexión del mundo

empresarial a esta red, viaja por ella y se almacena información de todo tipo, que abarca desde noticias o cotilleos, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas de seguridad que garanticen la confidencialidad, la integridad y el origen de los datos.

Pero, ¿cómo controlar el acceso indebido a aplicaciones y a la información almacenada?, ¿cómo garantizar la integridad o la confidencialidad de la información que viaja a través de las redes?, ¿cómo comprobar de manera fiable que el emisor y el receptor de una información son realmente quienes dicen ser?, o ¿cómo garantizar que el emisor no niegue haber enviado algo y el receptor no niegue haberlo recibido?

La criptografía como herramienta base de la seguridad[xxxv]

El criptosistema de clave secreta más utilizado es el Data Encryption Standard (DES) [1] desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977. Este criptosistema consiste en un algoritmo de cifrado-descifrado de bloques de 64 bits basado en permutaciones, mediante una clave, también de 64 bits. El algoritmo es fácil de implementar tanto en hardware como en software, sin embargo presenta problemas respecto a la distribución de claves, ya que dos usuarios que quieren comunicarse deben seleccionar una clave secreta que deberá transmitirse de uno a otro y respecto al manejo de claves, ya que en una red de n usuarios, cada pareja necesita tener su clave secreta particular, lo que hace un total de n(n-1)/2 claves para esa red.

Los servicios de seguridad
El documento de ISO que describe el Modelo de Referencia OSI, presenta en su Parte 2 una Arquitectura de Seguridad. Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes servicios de seguridad:

Autenticación de entidad par. Este servicio corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra.

Control de acceso. Este servicio se utiliza para evitar el uso no autorizado de recursos.

Confidencialidad de datos. Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Integridad de datos. Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

No repudio. Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación. Puede ser de dos tipos:

Con prueba de origen. Cuando el destinatario tiene prueba del origen de los datos.

Con prueba de entrega. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del Modelo de Referencia OSI los siguientes mecanismos de seguridad:

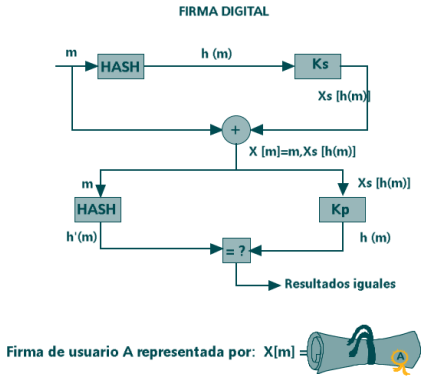
Cifrado. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

El mecanismo de cifrado soporta el servicio de confidencialidad de datos al tiempo que actúa como complemen to de otros mecanismos de seguridad.

Firma digital. Se puede definir la firma digital como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

La firma digital descrita por ITU y OSI en el Entorno de Autenticación del Directorio [4] utiliza un esquema criptográfico asimétrico. La firma consiste en una cadena que contiene el resultado de cifrar con RSA aplicando la clave privada del firmante, una versión comprimida, mediante una función hash unidireccional y libre de colisiones, del texto a firmar.

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.



El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

Control de acceso. Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de accesoa recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el enviante está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

Integridad de datos. Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una infomración suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

El mecanismo de integridad de datos soporta el servicio de integridad de datos.

Intercambio de autenticación. Existen dos grados en el mecanismo de autenticación:

Autenticación simple. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.

Autenticación fuerte. Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado.

Un certificado es un documento firmado por una Autoridad de Certificación, válido dunte el período de tiempo indicado, que asocia una clave pública a un usuario.

A la hora de plantearse en que elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

Protección de los sistemas de transferencia o transporte. En este caso, el administrador de un servicio, asume la responsabilidad de garantizar la transferencia segura de la información de forma bastante transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs seguras, o la instalación de un cortafuego, (firewall), que defiende el acceso a una parte protegida de una red.

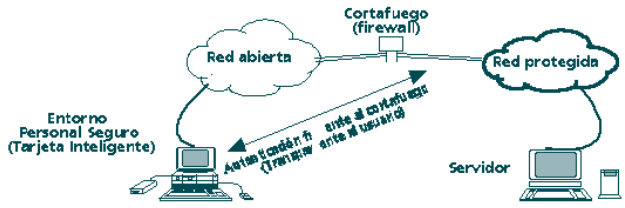
Aplicaciones seguras extremo a extremo. Si pensamos por ejemplo en correo electrónico consistiría en construir un mensaje en el cual en contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío, de forma que este mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de securizar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Este mismo

planteamiento, se puede usar para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

Uso de cortafuego con autenticación fuerte

En ambos casos, un problema de capital importancia es la gestión de claves. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).

Una manera de abordar esta gestión de claves está basada en el uso de los ya citados Certificados de Clave Pública y Autoridades de Certificación. El problema de la vigencia de la clave seresuelve con la generación de Listas de Certifados Revocados (CRLs) por parte de las CAs.



Un poco de historia: La Criptografía en la Primera guerra mundial.[xxxvi]

En enero de 1917, la Primera Guerra Mundial iba ya por su tercer año y no se divisaba un final en un corto plazo. El Kaiser Guillermo II, que había prometido una rápida victoria cuando se inició la contienda, veía ahora a sus tropas atascadas en el frente francés en una guerra de trincheras. Su poderosa armada había sido superada por la Royal Navy, y, como consecuencia de ello, Alemania se encontraba sometida a un bloqueo marítimo por parte de Inglaterra. Además, nuevos países habían decidido participar en la guerra al lado de los aliados. El Kaiser no anunciaba ya un triunfo inmediato. Ni siquiera estaba claro que la victoria fuese a caer del lado de las potencias de la Europa Central; a no ser, que los submarinos alemanes reanudasen la que se llamó «guerra sin restricciones». Consistía en que cualquier barco, de guerra o mercante, enemigo o neutral, hallado en una zona de exclusión próxima a las costas de Inglaterra, sería hundido sin previo aviso. Con ello, Inglaterra pasaría a ser el país bloqueado y tal situación asfixiaría a los ingleses y les obligaría a pedir la paz. Esa era la estrategia que conducía a la deseada victoria rápida. Alemania ya había declarado antes, a comienzos de 1915, la guerra sin restricciones. Sus ataques indiscriminados hundieron buques mercantes americanos, algunos con miles de pasajeros. Estas acciones estuvieron a punto de llevar a Estados Unidos a una declaración de guerra. Temerosos de que América entrara en la guerra al lado de los aliados, los alemanes abandonaron la guerra sin restricciones en otoño de 1915. Muy posiblemente su reanudación traería consigo la declaración de guerra por parte de Estados Unidos.

Eso no importaba ahora al alto mando militar germano. Estaba convencido de su victoria antes de que los grandes contingentes de tropas americanas pudiesen des- embarcar en Europa. Pero no era tan optimista el gobierno alemán, quién pensaba que la participación en la guerra de Estados Unidos daría el triunfo a los aliados. Por ello, prepararon un atrevido plan que, de salir adelante, evitaría la presencia del ejército americano en el frente europeo. El plan pasaba por una alianza con Méjico y Japón y consistía en que, si Estados Unidos declaraba la guerra a Alemania, esos dos países atacarían a los norteamericanos en su propio territorio. Alemania ayuda- ría económica y militarmente a dichas naciones.[xxxvii]

La Primera Guerra Mundial marcó un punto de inflexión en la historia de la Criptografía Militar. Antes de ella, únicamente el ejército francés contaba con oficiales formados en códigos y cifras. Después de la guerra, todos los ejércitos crearon unidades especializadas en Criptografía. Por otra parte, en la lucha que mantuvieron diseñadores de cifras y códigos con sus adversarios criptoanalistas, es clara la victoria de estos últimos. A pesar de la variedad de códigos y cifras que se emplearon, el triunfo de los criptoanalistas fue contundente. Y eso que la mayoría de ellos eran ajenos a la Criptografía antes de la guerra. Claro, que contaron con un par de ayudas inestimables: la primera, la gran cantidad de texto cifrado que proveían las interceptaciones del telégrafo y, sobre todo, la radio; la segunda, más importante, la falta de una seria instrucción criptográfica en las personas que manejaban la información encriptada.

Alan Turing en la Historia y en WW2.

Quisiera darle un pequeño honor a Alan Turing[xxxviii] *en estas líneas ligadas a los textos anteriores sobre criptografía en WWI. Ya que Turing fue un pionero desde el momento en que logro descifrar Enigma en WW2 y que nos dio el futuro que todos conocemos, al menos quienes somos amantes de la tecnología.*

Alan Mathison Turing, (Paddington, Londres; 23 de junio de 1912-Wilmslow, Cheshire; 7 de junio de 1954), fue un matemático, lógico, informático teórico, criptógrafo, filósofo, biólogo teórico, maratoniano y corredor de ultradistancia británico.

Es considerado uno de los padres de la ciencia de la computación y precursor de la informática moderna. Proporcionó una influyente formalización de los conceptos de algoritmo y computación: la máquina de Turing. Formuló su propia versión que hoy es ampliamente aceptada como la tesis de Church-Turing (1936).

Durante la segunda guerra mundial, trabajó en descifrar los códigos nazis, particularmente los de la máquina Enigma, y durante un tiempo fue el director de la sección Naval Enigma de Bletchley Park. Se ha estimado que su trabajo acortó la duración de esa guerra entre dos y cuatro años.6 Tras la guerra, diseñó uno de los primeros computadores

electrónicos programables digitales en el Laboratorio Nacional de Física del Reino Unido y poco tiempo después construyó otra de las primeras máquinas en la Universidad de Mánchester.

En el campo de la inteligencia artificial, es conocido sobre todo por la concepción de la prueba de Turing (1950), un criterio según el cual puede juzgarse la inteligencia de una máquina si sus respuestas en la prueba son indistinguibles de las de un ser humano.

La carrera de Turing terminó súbitamente tras ser procesado por homosexualidad en 1952. Dos años después de su condena, murió —según la versión oficial por suicidio; sin embargo, su muerte ha dado lugar a otras hipótesis, incluida la del envenenamiento accidental —. El 24 de diciembre de 2013, la reina Isabel II del Reino Unido promulgó el edicto por el que se exoneró oficialmente al matemático, quedando anulados todos los cargos en su contra.

El avance tecnológico: La era cuántica[xxxix]

¿Qué hay del día de mañana? Sabemos que los avances tecnológicos ponen a nuestra disposición herramientas más capaces. Al contar con éstas, el cripto-análisis se torna aún más poderoso y, como consecuencia, la criptografía también tiene que evolucionar.

Hoy en día, podríamos estar acercándonos a una era que marcaría una gran línea en la historia de la humanidad: La era del cómputo cuántico. En términos generales, ¿a qué se refiere el cómputo cuántico? Para empezar, el principio de incertidumbre nos dice que hay un límite en la precisión con la cual podemos determinar la información de una partícula, también llamado estado cuántico o simplemente Qubit.

Los qubits son estados cuánticos que representan simultáneamente ceros y unos (del código binario). Antes de que se considere que el número de resultados computados es siempre igual a las combinaciones posibles que se pueden hacer con los qubits (256 para 8 bits), se sabe que esto no es así. La máquina cuántica posee un elevado paralelismo capaz de romper los cripto-sistemas más usados hoy en día; es decir, la capacidad de una computadora cuántica es mayor que aquella que se basa en las leyes clásicas de la física.

El cómputo cuántico y los criptosistemas actuales

Supongamos que hoy existieran las computadoras cuánticas. En primer lugar, sucedería que algunos de los cripto-sistemas actuales se volverían inseguros. La capacidad de la máquina cuántica es tal, que rompería cualquier sistema criptográfico cuya seguridad provenga de álgebra modular (pues ya existe un algoritmo cuántico que rompería la misma), como el esquema de RSA, uno de los más usados hoy en día. Esto representa, a nivel mundial, un peligro potencial y habría consecuencias tanto económicas como científicas.

Podría ser que un algoritmo matemático resista un ataque cuántico durante su tiempo de vida promedio (5 a 25 años). Incluso se podrían asumir medidas simples, como duplicar el tamaño de la llave, entonces los algoritmos clásicos podrían seguir resistiendo un ataque cuántico como sucede hoy entre los cripto-sistemas matemáticos y los ataques no cuánticos.

Aunque hablamos de que la computación cuántica ya tiene su algoritmo para descifrar los sistemas basados en álgebra modular, también es importante mencionar que los esquemas que no se basan en este tipo de álgebra quedan exentos del algoritmo que termina con la seguridad en el álgebra modular, aunque no de la capacidad de procesamiento de la computadora cuántica.

De hecho, no se sabe si otros esquemas, diferentes a los del álgebra modular (como los de redes y los basados en código), se rompan ante un ataque cuántico. Estos alcanzan la complejidad necesaria para resistir el cómputo cuántico al duplicar el tamaño de sus llaves.

Es una realidad que el cómputo cuántico aumenta el poder de procesamiento. Sin embargo (empleado en criptoanálisis), no garantiza la vulnerabilidad de los otros criptosistemas (los no modulares), la razón: aún no hay algoritmo cuántico (más simple que la fuerza bruta) contra estos modelos, pero tengamos presente que la falta de este algoritmo ha sido siempre la problemática, en la esfera del cómputo cuántico o fuera de ella.

VPN de acceso remoto

Esta implementación entrega un acceso a la red LAN de la organización y sus recursos tecnológicos, es decir, archivos, bases de datos, etc. «Este acceso a través de internet de forma segura permite la movilidad del trabajador e incluso interconectar sedes separadas geográficamente» .

VPN punto a punto

Esta arquitectura de VPN se utiliza en la conectividad de oficinas remotas utilizando un servidor VPN conectado a internet, el cual se encarga de la seguridad de las comunicaciones.

Tunneling PPTP

Su funcionamiento es muy parecido a las VPN punto a punto con la diferencia de que se forma un túnel mediante PPTP o Protocolo de Túnel Punto a Punto (en inglés, Point-to-Point Tunneling Protocol). Es usado tanto por empresas como usuarios domésticos. Para acceder a la VPN, los usuarios inician sesión con una contraseña generada específicamente para su uso en esta arquitectura.

VPN over LAN o VPN sobre LAN

Este es el caso menos conocido de uso de las VPN.

Diagrama de acuerdo al tipo de VPN que realizaría en este ejercicio[xl]*, donde una red Wifi o directamente Internet externo queda fuera del alcance de otras redes*

a través de un servidor VPN en formato PUNTO - PUNTO:

2) De acuerdo a la solución mencionada en la pregunta anterior explique qué beneficios traerá el uso del protocolo IPsec.

IPsec realiza los procesos de autenticando y/o cifrando cada paquete IP sobre la red de datos. Además, incluye protocolos para la incorporación de claves de cifrado (Laurel.datsi.fi.upm.es, 2012).

Los protocolos de IPsec trabajan sobre la capa 3 del modelo OSI, a diferencia de otros protocolos tales como SSL, TLS y SSH, los que operan de la capa de transporte (capas OSI 4 a 7) en adelante.

Intercambio de Claves de Internet (IKE)

IKE es un protocolo que tiene como objetivo el intercambio de claves de internet. Según Pérez (2001), el Internet Key Exchange (IKE) "permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH (Cabecera de autenticación) y ESP (Carga de Seguridad Encapsulada)".

Modos de funcionamiento protocolo IKE:

- Transporte: Solo el contenido de los paquetes es encriptado, la cabecera IP no es encriptada, pero se inserta una cabecera IPSec luego de la cabecera IP y antes de los datos.
- Túnel: Todo el paquete de datos es encriptado incluyendo su cabecera (Autentificado y cifrado). Posteriormente se le agrega la cabecera AH o ESP y se re encapsula luego con otra cabecera IP para viajar por la red.

Protocolos IPSec

Descripción general de IPSec

IPSec tiene tres grandes componentes, dos protocolos de seguridad e intercambio de llaves:

- Autenticación de cabecera IP (AH).
- Carga de seguridad de encapsulado (ESP).
- Intercambio de llaves de Internet (IKE).

Dentro de las topologías que comenzare a nombrar, creo yo que la opción mas optima es HOST-HOST, ya que en este caso se cifra todo para una mayor confidencialidad.

Topologías VPN:

- HOST-HOST: La implementación más sencilla de una VPN es de un host a otro. Esta topología aparece como solución al problema de que dos hosts estén conectados directamente para realizar intercambio de información sobre una línea dedicada o módems. Esta clase de conexión no ofrece seguridad, por lo cual en la implementación de una VPN la conexión se autentifica y los datos se cifran para que la confidencialidad no sea vulnerada entre las comunicaciones de los Hosts.
- HOST-RED: Esta es la solución más sencilla que los usuarios móviles tienen a disposición para conectar con la red de la empresa. En esta configuración, cada host se conecta independientemente con una LAN mediante una puerta de enlace VPN. Se autentica cada host y los túneles VPN se inician para cada uno de ellos.
- RED-RED: En esta opción cada puerta de enlace se ubica en el borde de cada red la cual está, por ejemplo, conectada a internet y proporciona un canal de comunicación seguro entre las 2 o más redes. Esta es la solución que las empresas de comunicaciones entregan a sus clientes cuando deben enlazar sucursales alejadas geográficamente. Lo interesante de esta implementación es que para los usuarios esta solución es transparente.

IKE es un protocolo que tiene como objetivo el intercambio de claves de internet. Según Pérez (2001), el Internet Key Exchange (IKE) "permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH (Cabecera de autenticación) y ESP (Carga de Seguridad Encapsulada)".

Modos de funcionamiento protocolo IKE:

- Transporte: Solo el contenido de los paquetes es encriptado, la cabecera IP no es encriptada, pero se inserta una cabecera IPSec luego de la cabecera IP y antes de los datos.
- Túnel: Todo el paquete de datos es encriptado incluyendo su cabecera (Autentificado y cifrado). Posteriormente se le agrega la cabecera AH o ESP y se re encapsula luego con otra cabecera IP para viajar por la red.

[i] Owasp.org. (s. f.). Modelado de amenazas. Recuperado de: https://bit.ly/2U6ttNu

[ii] Robledo Sosa, C. (2002). Redes de computadoras. México, Instituto Politécnico Nacional. Recuperado de https://elibro.net/es/ereader/iacc/101803?page=12 - page=398 - page=398

[iii] Análisis personal en riesgos de conexión a redes publicas, como en restaurantes y cafés.
[iv] Oficina de Seguridad del Internauta. https://www.osi.es/es/wifi-publica

[ix] Oficina de Seguridad del Internauta. https://www.osi.es/es/wifi-publica
[x] Escrivá Gascó, G. (2013). Seguridad informática. Madrid, Spain: Macmillan Iberia, S.A. Recuperado de https://elibro.net/es/ereader/iacc/43260?page=188.
[xi] Instituto Nacional de Normalización (INN). (2013). Nch-ISO27002: Tecnologías de la información – Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información. Santiago, Chile.

[xii] Bogotá (Colombia), Colombia: Universidad Militar Nueva Granada. Recuperado de https://elibro.net/es/ereader/iacc/6558?page=3.
[xiii] Acedo Arias, M. A. (2009). Análisis de los secretos compartidos para la autenticación de nodos en las wireless sensor networks mediante el algoritmo de Shamir.
[xiv] Castaño Ribes, R. J. (2013). Redes locales. Madrid, Spain: Macmillan Iberia, S.A. Recuperado de https://elibro.net/es/ereader/iacc/43257?page=252.
[xv] Molina Robles, F. J. y Polo Ortega, E. (2015). Servicios en red. Madrid, Spain: RAMA Editorial. Recuperado de https://elibro.net/es/ereader/iacc/62455?page=512.

[xvi] Ariganello E. (2016). REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. Cuarta edición. Madrid: Editorial: Rama.
[xvii] Cisco (s. f.). What Is a Firewall?. Recuperado de: http://bit.ly/2KVP0Vc.
[xviii] Colomés, P. (2015). ¿Qué es la DMZ?. Redescisco.net. Recuperado de: http://bit.ly/2XFFAid.
[xix] Geovanny, D. (2016). Firewalls de nueva generación: la seguridad informática vanguardista. Recuperado de: http://bit.ly/2W11Dz8.
[xx] Hernández, T. y Salazar, P. (2017). Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones.
[xxi] Revista de Simulación Computacional, vol.1 (2), pp. 24-31. Recuperado de: http://bit.ly/2W3vPtC.

[xxii] Innovando-me (2014). Firewall y usos en redes. Recuperado de: http://bit.ly/2viNpOE.
[xxiii] Mendoza, M. (2014). ¿Por qué es necesario el firewall en entornos corporativos?. Welivesecurity.com. Recuperado de: http://bit.ly/2KWks5z.
[xxiv] Symantec (2018). Cómo el firewall usa la inspección de estado. Recuperado de: https://symc.ly/2XGyUQX.
[xxv] Escrivá Gascó, G. (2013). Seguridad informática. Madrid, Spain: Macmillan Iberia, S.A. Recuperado de https://elibro.net/es/ereader/iacc/43260?page=104.
[xxvi] IPS: Sistema de Prevención de Intrusos - infotecs.mx - https://bit.ly/3d4A7M6

[xxviii] Rediris.es (2002). Criptología. Recuperado de: http://bit.ly/2LJ7OHt.
[xxix] Adslzone.net (2017). Qué es el MD5, y por qué es tan importante en las descargas. Recuperado de: http://bit.ly/2WhGocK.
[xxx] Kaspersky.com (2014). ¿Qué es un Hash y cómo funciona?. Recuperado de: http://bit.ly/2XTYz8L.
[xxxi] Ecured.cu (s. f.). Criptografía asimétrica. Recuperado de: http://bit.ly/2vZbs5z.
[xxxii] IBM.com (s. f. 1). Función Resumen/Hash. Recuperado de: https://ibm.co/2WIAscN.
Isaca (2017). Fundamentos de Ciberseguridad. 2.ª edición. Schaumburg, USA: Isaca.org

Larevistainformatica.com (2015). Que es la encriptación de la informática. Recuperado de: http://bit.ly/2YxGMnU.
Laurel.datsi.fi.upm.es (2012). Protocolo IPsec. Recuperado de: http://bit.ly/2JmFngx.
Maddox, N. (s. f.). ¿Cuál es la diferencia entre SSL y TLS? Techlandia.com. Recuperado de: http://bit.ly/2W4yzKE
Ocad, G. (2015). Algoritmo HMAC. Recuperado de: http://bit.ly/2W8c3jT.

Upm.es (s. f.). Introducción a la criptografía. Recuperado de: http://bit.ly/2W5Z56f.
Winrar.es (s. f.). Codificación. Recuperado de: http://bit.ly/2HuztXp.

[xxxiii] ¿Cómo roban contraseñas en Windows? Importancia de una autenticación robusta - welivesecurity.com - https://bit.ly/3wxhN6j
[xxxiv] Protocolos Ventajas de un Sistema Distribuidos - buap.mx - http://mtovar.cs.buap.mx/doc/cap4Red.pdf
[xxxv] Seguridad en redes telemáticas - rediris.es - https://bit.ly/3dEH45B
[xxxvi] https://elibro.net/es/ereader/iacc/54964?page=116.
[xxxvii] Ortega Triguero, J. y López Guerrero, M. Á. (2006). Introducción a la criptografía: historia y actualidad. Cuenca, Spain: Ediciones de la Universidad de Castilla-La Mancha.
[xxxviii] Alan Turin @ Wikipedia https://bit.ly/39MuKiF
[xxxix] Criptografía y criptoanálisis: la dialéctica de la seguridad - unam.mx - https://bit.ly/3mlQtmJ
[xl] *Las redes virtuales privadas o VPN. Extensiones de una red pública. - https://bit.ly/3s7ai2s*