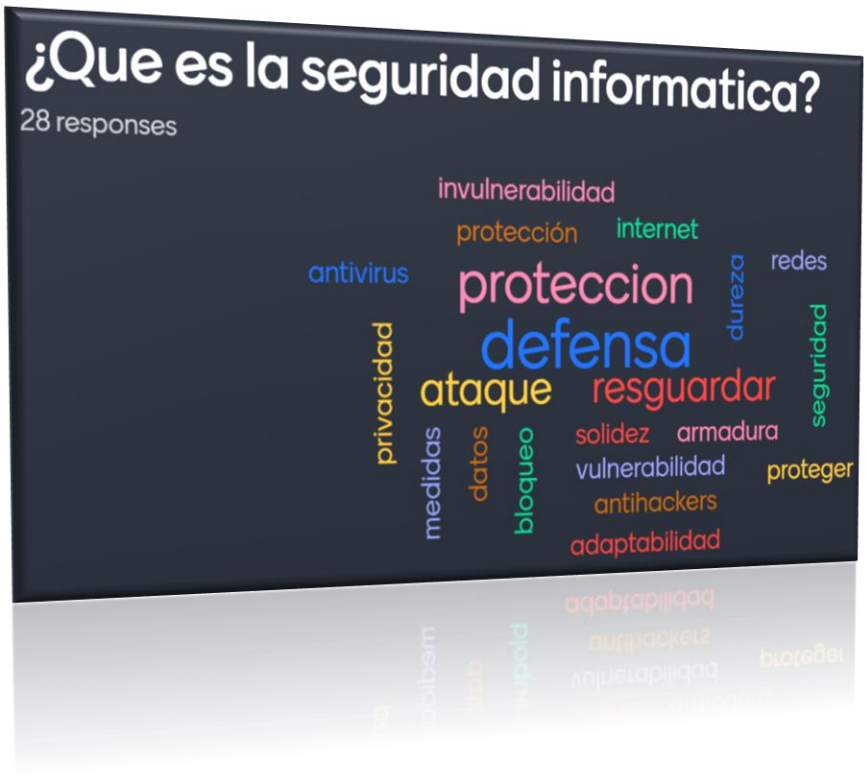
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

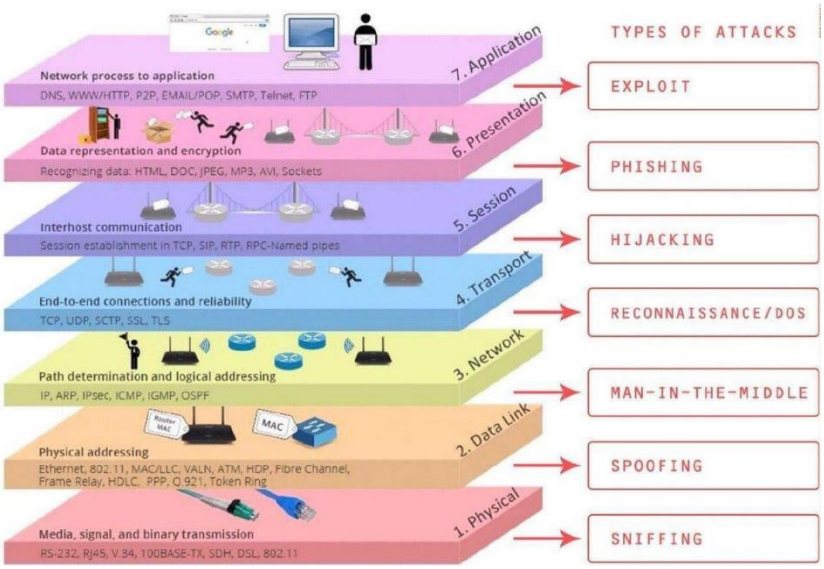
Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Fundamentos de Seguridad en Redes

Vulnerabilidades de los servicios de red

Hoy en día, el uso de las telecomunicaciones permite que una persona pueda jugar en red con otra que se encuentra al otro lado del mundo, utilizar su teléfono móvil para navegar por Internet o incluso gestionar su vivienda desde el trabajo mediante aplicaciones domóticas. Todo esto es posible gracias a las comunicaciones en red.



No obstante, estas comunicaciones entre equipos a través de la red no están exentas de riesgos que debemos conocer. Para entender estos riesgos, conviene conocer cómo funcionan las redes de telecomunicación y estudiar sus vulnerabilidades. Las redes de telecomunicación basan su funcionamiento en el modelo OSI de interconexión de equipos informáticos, que define siete capas o niveles, de manera que cada nivel tiene una funcionalidad bien definida y se comunica mediante una interfaz que oculta los detalles de implementación al resto de niveles facilitando su uso por los niveles inmediatamente inferior o superior, que son los únicos que podrán acceder a él. Por ejemplo, el nivel 4 (nivel de transporte) solo puede enviar y recibir información de los niveles 3 (nivel de red) y 5 (nivel de sesión).

Cada nivel del modelo OSI presenta vulnerabilidades que pueden ser explotadas por un atacante, por lo que en los próximos apartados estudiaremos las vulnerabilidades de los niveles de este modelo.

Nivel físico

Este nivel es responsable de la conexión del equipo informático a la red y se encarga de la transmisión de información a través de ella. Las vulnerabilidades de este nivel están relacionadas con el acceso físico no autorizado a los dispositivos de red.

Algunos ejemplos de ataques sobre este nivel son: corte o desconexión de un cable de red o interferencias electromagnéticas ocasionadas por algún dispositivo que impidan el funcionamiento normal de la red.

Estos ataques pueden tener un gran impacto sobre el funcionamiento de los equipos informáticos, independientemente de si se han producido de forma accidental o intencionada, por lo que deberemos tenerlos en cuenta y controlar el acceso físico a los dispositivos de red.

Nivel de enlace de datos

Se encarga del direccionamiento físico, acceso al medio, la detección de errores, la distribución ordenada de tramas y del control de flujo. Aquí se dan vulnerabilidades asociadas al medio sobre el que se realiza la conexión, como el control de acceso y la confidencialidad. Algunos ataques son:

– **Escuchas de red**, tanto intrusivas en medios cableados (pinchar un cable), como no intrusivas en medios inalámbricos (ataques WEP).

– **Falsificación de direcciones MAC-** ***Medium Access Control*** para evitar restricciones de acceso basadas en el filtrado MAC.

– **Envenenamiento ARP-** ***Address Resolution Protocol***. El envenenamiento ARP o ARP Poisson, también conocido como ataque *Man In The Middle* (MITM), es un tipo de ataque donde el intruso intercepta el tráfico enviado a otra estación o al router, atendiendo a peticiones dirigidas a otras estaciones y suplantándolas.

Nivel de red

Este nivel proporciona conectividad entre equipos, permitiendo que la información llegue desde el origen al destino, aunque se encuentren en redes diferentes. Esto es posible gracias a la información de cabecera que contienen todos los paquetes IP y a la utilización de elementos que permiten la interconexión de redes como routers. Este nivel presenta vulnerabilidades asociadas a la integridad y confidencialidad de la información. Se pueden dar los siguientes ataques:

– ***Suplantación de mensajes*** (IP spoofing, en inglés). El atacante envía paquetes utilizando una dirección origen diferente, modificándola por una dirección IP falsa o de otro equipo legítimo de la red.

– ***Denegación de servicio*** (Denial of Service, en inglés o DoS). Los atacantes realizan ataques de inundación de la red (IP flooding o net flood, en inglés), que consisten en generar un elevado tráfico de red hacia una víctima con el objetivo de saturar su línea de comunicación. Existe una gran variedad de ataques de denegación de servicio y en la mayoría se trata de manipular los paquetes alterando algún campo o lanzando una gran cantidad de peticiones al resto de estaciones

Smurfing

Es una técnica de DoS muy utilizada que consiste en enviar una gran cantidad de paquetes ICMP (ping) a la dirección de broadcast, falsificando la dirección de origen por la de la víctima, que recibirá la respuesta de todas las estaciones de la red.

Denegación de servicio en televisores

Los ataques de denegación de servicio pueden atacar a cualquier dispositivo que utilice la red para enviar y recibir información, por lo que los teléfonos móviles, lectores de Blu-ray que se actualizan a través de la red o televisores que acceden a Internet pueden verse afectados.

Nivel de transporte

Este nivel proporciona un servicio de transporte desde la máquina origen a la de destino, independizándolo del hardware de red utilizado. Los protocolos más conocidos son TCP y UDP, que transmiten información sobre paquetes IP. Las vulnerabilidades de este nivel se asocian a la autenticación, integridad y confidencialidad de la información.

Algunos ataques sobre este nivel son:

– **Denegación de servicio**, que como se ha comentado utiliza técnicas de IP flooding sobre datagramas UDP, TCP o ICMP. Una variante muy interesante es la inundación SYN (SYN flooding, en inglés), donde el atacante no completa el establecimiento de conexión TCP a propósito. Esto provoca que el servidor desperdicie recursos manteniendo conexiones que no serán utilizadas, por lo que se podría provocar el colapso en la máquina. Esta debilidad se debe a una pobre implementación del protocolo TCP, que fue aprovechada en las primeras implementaciones de la pila TCP. En la actualidad, los servidores suelen liberar las conexiones no utilizadas con rapidez, por lo que el problema debería estar solucionado.

– **Ataques contra el establecimiento de sesiones TCP**, que consisten en la interceptación de sesiones TCP establecidas para redirigirlas a otros equipos. Este tipo de ataques se aprovechan de la simplicidad del proceso de autenticación entre equipos, lo que puede ser aprovechado por un atacante a la escucha de los intercambios de información realizados en el inicio de la sesión.

– **Ataques de reconocimiento**, que consisten en realizar barridos de puertos TCP/UDP contra un equipo y de esta forma averiguar qué aplicaciones y puertos tiene en escucha para poder realizar un ataque posterior a un determinado servicio.

Niveles de sesión, presentación y aplicación

Los niveles superiores son los más cercanos al usuario y se suelen agrupar para facilitar su estudio. Estos niveles desconocen la forma en la que se comunican los equipos y la ruta establecida y se encargan de definir los protocolos de aplicación que utilizan las aplicaciones finales para intercambiar datos. No obstante, estos niveles presentan muchas vulnerabilidades que afectan a la confidencialidad, integridad, disponibilidad, no repudio o autenticación, que pueden ser aprovechadas por atacantes. Existe una gran variedad de ataques que aprovechan las vulnerabilidades de estos niveles:

– **Ataques sobre la confidencialidad**. Algunas aplicaciones presentan fallos importantes de seguridad y envían toda la información de la sesión sin cifrar (como telnet o FTP), por lo que un atacante podría obtener las claves de sesión usando programas de escucha de la red.

– **Suplantación del servicio de nombres de dominio** (pharming, en inglés). Cuando se solicita una petición sobre un servicio en un equipo remoto se debe conocer la dirección IP de ese equipo. Para ello se realiza una consulta sobre el servidor DNS enviándole un paquete UDP al servidor DNS que proporciona la dirección IP del destino. En este tipo de ataque se suplanta al servidor DNS, suministrando una dirección IP falsa que será utilizada por la víctima sin saberlo, accediendo a una página web falsa que imitará la página web legítima con la finalidad de obtener información importante de la víctima, como sus contraseñas.

– **Agotamiento de direcciones IP** (DHCP starvation, en inglés), que consiste en enviar una gran cantidad de peticiones al servidor DHCP con distintas direcciones físicas de origen para obtener una dirección IP diferente cada vez, con lo que se podría agotar las direcciones IP disponibles para el resto de los equipos legítimos.

Defensa contra el agotamiento de direcciones IP Una posible defensa sobre este tipo de ataque sería limitar la cantidad de peticiones DHCP que se puede realizar por cada puerto del switch o configurar la seguridad por puerto para que solo permita que determinadas direcciones físicas estén conectadas a un puerto y deniegue el resto

– **Inyección SQL** (SQL injection, en inglés), que aprovecha vulnerabilidades en el diseño de una aplicación web para ejecutar código SQL no esperado sobre una base de datos. Mediante este tipo de ataques se altera el funcionamiento normal de la consulta original y se consigue ejecutar operaciones de actualización o consultas no esperadas. Así, por ejemplo, una operación de consulta sobre una tabla modificada convenientemente puede dar como resultado la visualización de información de tablas para las que no se tiene acceso o a borrar su contenido.

– **Escalada de directorios**, que consiste en acceder a directorios para los que no se debería tener acceso. Existen muchas aplicaciones que permiten a usuarios acceder a directorios de un equipo remoto, lo que presenta problemas de seguridad si facilita el acceso a todos los directorios del equipo. Estas aplicaciones suelen proporcionar herramientas que permiten el "enjaulamiento" de los usuarios remotos para limitar el acceso solo a los directorios autorizados.

– **XSS (Cross Site Scripting, en inglés)**, que consiste básicamente en inyectar código malicioso en las páginas web visitadas.

– **Desbordamiento de búfer**, que consiste en aprovechar algún fallo de diseño de una aplicación con el objetivo de ejecutar código malicioso en el ordenador de la víctima.

Ataques de denegación de servicio en redes

Los ataques de denegación de servicio o DoS (Denial of Service, en inglés) en redes son tal vez el ejemplo más conocido de ataque sobre los niveles de red y transporte, también conocidos como ataques TCP/IP.

Existe una gran variedad de ataques de denegación de servicio: inundación IP, falsificación IP origen, inundación TCP/SYN, teardrop, snork, ping de la muerte, etc.

A continuación, describiremos los ataques de denegación de servicio más representativos, aunque algunos de ellos ya se han citado anteriormente:

– **Inundación IP** (IP flooding en inglés). Consiste en el envío de tráfico masivo para conseguir la degradación de los servicios de la red. El atacante consume un gran ancho de banda ralentizando las comunicaciones existentes en la red. Este ataque es efectivo en redes en las que no se rea liza ningún control de acceso al medio y cualquier equipo puede enviar y recibir paquetes sin ningún tipo de limitación del ancho de banda consumido.

– **Falsificación IP origen** (IP spoofing en inglés). Distinguimos dos tipos de ataque: broadcast y smurf.

• **Broadcast**. Variante del anterior ataque de denegación de servicio en el que se falsea la dirección IP origen del atacante, indicando la dirección de difusión (broadcast) de la red. En este caso, cada equipo responde a la dirección IP origen, que, al resultar la dirección de difusión, realiza un envío masivo al resto de equipos de la red.

• **Smurf**. Variante del ataque de inundación IP en la que el atacante falsea su dirección IP origen, enviando paquetes de difusión haciéndose pasar por la dirección IP de la víctima, quien recibirá las respuestas de todas las estaciones de la red.

Aunque en algunas ocasiones estos ataques pueden tener un único origen, es muy frecuente que el ataque se realice desde varias máquinas coordinadas, dando lugar a ataques DDoS (Distributed Denial of Service, Denegación de Servicio Distribuida) consiguiendo un mayor impacto sobre la víctima. En estos casos los atacantes pueden llegar a controlar centenares o miles de equipos formando una red de ordenadores "zombies" o botnet.

Tarea: Busca información sobre herramientas MITM (*Man In The Middle*)

Monitorización

Las redes informáticas constituyen un entorno dinámico con cambios continuos en el que los usuarios están continuamente navegando por Internet, descargando ficheros de otros equipos, enviando mensajes de correo electrónico, accediendo a otros equipos, etc.

Aunque una red funcione correctamente al principio, con el paso del tiempo su rendimiento puede ser menor y presentar riesgos de seguridad para los equipos. En ocasiones esta disminución del rendimiento puede ser debida a algún malware que genera tráfico en la red, a un aumento en el tráfico por el número de usuarios o la utilización de nuevas aplicaciones, a interferencias electromagnéticas o incluso al desgaste por la utilización de los dispositivos de la red como tarjetas estropeadas o cableado defectuoso. Por lo tanto, no basta con diseñar e implantar una red informática en una organización, es necesario monitorizar y evaluar el rendimiento de esta a lo largo de su vida mediante herramientas que permitan conocer cómo se comporta y si se está haciendo un uso indebido que ocasione un consumo excesivo del ancho de banda.

Para analizar el tráfico que circula por la red se suele enviar una copia de todo el tráfico que circula por la misma a una herramienta de monitorización.

Existen dos sistemas para enviar la copia del tráfico al analizador de redes:

– **Port mirroring**. Este sistema de monitorización se basa en configurar un dispositivo por el que pasa todo el tráfico de la red, como puede ser un switch, para que reenvíe una copia del tráfico que recibe a la herramienta de monitorización. El puerto que conecta el analizador de la red con el switch recibe el nombre de mirror port o monitor port. El funcionamiento de este sistema es simple: como todos los paquetes llegan al switch, se aprovecha esta circunstancia para reenviar una copia por el monitor port al equipo que analiza la red.

– **Network tap**. En esta forma de monitorización se utiliza un dispositivo hardware que permite acceder al tráfico de datos en un punto de la red donde no es posible usar port mirroring. El analizador de paquetes recibe todo el tráfico que le llega al dispositivo.

NOC – Network Operations Center

Es el responsable de diseñar, instalar, dar mantenimiento correctivo y preventivo a la operación (Gestión, Soporte y monitoreo) de redes de telecomunicaciones de datos. Así como el responsable de monitorizar las redes en función de alarmas o condiciones que requieran atención especial para evitar impacto en el rendimiento de las redes y el servicio a los clientes finales

SOC - Security Operations Center

Es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

SIEM - Security Information and Event Management

Es la principal herramienta del SOC ya que permite gestionar los eventos en toda la red

Debe existir la tecnología para recolectar datos a través de flujos de datos, mediciones, entrada de paquetes, syslog y otros métodos para que la actividad de datos pueda ser correlacionada y analizada por los equipos de OSC.

Herramientas de monitorización

Existen en el mercado muchas herramientas diseñadas para analizar y monitorizar una red, tanto comerciales como open source. Sus funciones son similares: generación de mapas de red automáticos, elaboración de informes con estadísticas, envío de alertas por email y/o sms, etc.

Estas son algunas herramientas muy utilizadas en el ámbito de la monitorización:

Redes	Seguridad
Wireshark	SolarWinds Security Event Manager
Ettercap	Micro Focus ArcSight Enterprise Security Manager (ESM)
Ntop	Splunk Enterprise Security
HP Openview	LogRhythm Security Intelligence Platform
MRTG	**AlienVault Unified Security Management**
Cacti	RSA NetWitness
Nagios	**FortiSIEM**
PandoraFMS	IBM QRadar
Ganglia	**McAfee Enterprise Security Manager**

Técnicas de protección

En unidades anteriores hemos estudiado la importancia de proteger los equipos contra atacantes y malware. En una red de ordenadores en la que varios equipos comparten información, se comunican entre sí y acceden a otras redes o a Internet, el impacto producido por un ataque sobre la red es más grave que el producido sobre un equipo, por lo que conviene establecer medidas específicas que protejan a los usuarios de la red. Entre las técnicas de protección más utilizadas en redes destacamos los cortafuegos, sistemas de detección de intrusos, proxies, sistemas de gestión unificada de amenazas, VPN, sistemas centralizados de autenticación y zonas desmilitarizadas. Algunas ya se han estudiado en unidades anteriores, como los firewalls, por lo que nos centraremos en cómo utilizarlas en redes, mientras que otras técnicas son nuevas y conviene conocerlas.

Firewall

Si en los equipos personales, el uso del firewall era una medida muy recomendable, en las redes de ordenadores es una técnica básica para evitar accesos no autorizados a equipos o servicios de la red.

En una red de ordenadores, el Firewall se ubica en el límite de la red para poder analizar todo el tráfico que entra o sale de la misma. En algunas redes, algunos dispositivos de red (routers) hacen las funciones de firewall, mientras que en otras existe un equipo que dispone de dos tarjetas de red y analiza todo el tráfico.

Un Firewall permite o deniega el tráfico en función de parámetros definidos en reglas. Si se cumplen las condiciones establecidas en una regla se aplicará la misma, aceptando o rechazando el paquete, y dejará de comprobarse el resto. Cuando no existe ninguna regla que coincida con las características del paquete recibido se aplicará la política por defecto para el paquete que entra al sistema o sale de él. Distinguimos dos tipos de políticas por defecto:

– Política restrictiva, donde se rechaza todo el tráfico por defecto y solo se permite el paso de los paquetes aceptados de forma explícita.

– Política permisiva, en la que se acepta todo el tráfico, excepto aquellos paquetes especificados en las reglas, que serán rechazados.

IPtables

IPtables es el cortafuegos por defecto de los sistemas Linux y permite filtrar paquetes, realizar tareas de encaminamiento, redirigir tráfico a equipos concretos, realizar traducción entre direcciones de red (NAT/PAT) y mantener registros de log.

Una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición. Sin embargo, también tienen usos adicionales, como, por ejemplo, distinguir tráfico prioritario.

Las listas de acceso de control pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un cortafuegos. Se pueden considerar como cada una de las reglas individuales que controlan y configuran un cortafuegos o firewall (COSTAS SANTOS, 2014).

Razones principales para crear las ACL:

- Limitar el tráfico de la red.
- Mejorar su rendimiento de la red.
- Controlar el flujo de tráfico, decidiendo qué tráfico se bloquea y cuál se
- permite, ya sea por direccionamiento o por servicios de red.
- Proporcionar un nivel básico de seguridad para el uso de la red.

Implementación de políticas de seguridad

Capacitación y concientización constante en todos los niveles

Protección en redes inalámbricas

Millones de personas utilizan el estándar 802.11 a diario, o lo que es lo mismo las redes inalámbricas o redes WiFi, que presentan muchas ventajas sobre las redes cableadas tradicionales, como la flexibilidad, movilidad y facilidad de conexión. Así, por ejemplo,

para poder comprobar el correo electrónico desde la calle, únicamente necesitamos que nuestro dispositivo inalámbrico (por ejemplo, una tablet o un smartphone) se encuentre dentro del alcance de la señal que proporciona un punto de acceso a Internet y que se establezca una conexión entre ellos.

Si bien es cierto que las redes inalámbricas presentan muchas ventajas para los usuarios, este tipo de redes no están exentas de vulnerabilidades que amenazan la disponibilidad, confidencialidad e integridad de la información, que debemos tener en cuenta y de las que deberemos protegernos adecuadamente.

Es un error muy común es pensar que solo los vecinos pueden acceder a una red inalámbrica, pues un intruso solo precisaría de estar dentro del alcance de la red, para lo cual puede utilizar equipos especiales que le permitan acceder a una red ubicada a cientos de metros de distancia, donde la señal original de la red no llegaría de forma normal.

Entre los tipos de ataques más comunes, distinguimos:

– **Ataques de denegación de servicio (DoS)** ocasionados por una fuente emisora de ondas que trabaja en la misma banda de frecuencias que la red inalámbrica, lo que provocaría que ningún equipo de la red pudiera comunicarse con el punto de acceso. Nos encontramos ante un ataque contra la disponibilidad de la red.

– **Escuchas del tráfico de la red (sniffing)**, donde cualquier equipo podría interceptar el intercambio de información enviada en la red, afectando a la confidencialidad de la comunicación.

– **Inyección de tráfico en la red**, donde un usuario no legítimo trata de inyectar paquetes sobre la red para generar tráfico entre las estaciones y obtener las claves de sesión si se está utilizando un protocolo de seguridad inseguro como WEP.

– **Conexiones no autorizadas a la red**, que podrían darle al atacante acceso sin restricciones a la red.

– **Ataques de acceso**, como la des-autenticación y la falsa autenticación. La desautenticación es un ataque diseñado para obtener un ESSID oculto de una red y capturar mensajes intercambiados para establecer una conexión, obligando a los clientes a re-autenticarse. También se utiliza para hacer denegación de servicio. La falsa autenticación (fake auth), se utiliza para registrar una dirección MAC de cliente falsa en un punto de acceso inalámbrico.

Acceso al tráfico en una red inalámbrica: en una red inalámbrica cualquier equipo que se encuentre dentro de su alcance puede acceder a la información transmitida en esa red, lo que puede ser aprovechado por usuarios ilegítimos para realizar ataques sobre ella.

Por lo tanto, debemos utilizar mecanismos que permitan establecer comunicaciones seguras en redes inalámbricas. Para ello debemos proteger tanto las redes inalámbricas, garantizando que solo equipos legítimos acceden a la red y que la información se encuentra protegida de forma conveniente, como a los clientes de la red inalámbrica frente a posibles ataques que puedan sufrir de otros equipos de la red.

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 cifrado (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 intermedio 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.

Rogue ap

En este tipo de ataque, un equipo se hace pasar por un falso punto de acceso al que se conecta el cliente, interceptando sus claves y toda la información que transmite por la red.

Para evitarlo es importante mantener actualizados el sistema operativo, las aplicaciones que hacen uso de Internet y los drivers del dispositivo, no conectarse a redes inseguras y mantener la lista de redes preferidas actualizada, eliminando redes no utilizadas y redes que no difunden su SSID de esta lista (ESCRIVA, 2013).

Bibliografía

BUENDIA, J. F. (2013). *Seguridad informática.* España: McGraw-Hill.

COSTAS SANTOS, J. (2014). Seguridad informática. *RA-MA, SA.*

ESCRIVA, G. R. (2013). *Seguridad Informática.* España: Macmillan Iberia SA .

GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad

INCIBE. (18 de 03 de 2021). *INCIBE - Taxonomia*. Obtenido de https://www.incibe-cert.es/taxonomia

INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Analisis de Riesgos: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Internautas. (07 de 04 de 2020). *Internautas*. Obtenido de https://www.internautas.org/w-scanonline.php

MITIC. (23 de 03 de 2021). Obtenido de CERT-PY: https://www.cert.gov.py/institucional

STEWART, J. M. (2013). *Network Security, Firewalls and VPNs.* Jones & Bartlett Publishers.

VIEITES, Á. G. (2014). *Gestión de Incidentes de Seguridad Informática.* . RA-MA Editorial.

