ISSN 2529-9824

Artículo de Investigación

Modificación de la red de área local del hogar para aumentar la seguridad

Modification of home LAN to enhance security

Antonio Porras Pérez: Universidad de Granada, España.
aporras@ugr.es

Fecha de Recepción: 21/05/2024

Fecha de Aceptación: 09/09/2024

Fecha de Publicación: 04/02/2025

Cómo citar el artículo:

Porras Pérez, A. (2025). Modificación de la red de área local del hogar para aumentar la seguridad [Modification of home LAN to enhance security]. *European Public & Social Innovation Review*, 10, 1-19. https://doi.org/10.31637/epsir-2025-1424

Resumen:
Introducción: Las actuales redes de fibra óptica instaladas en los hogares proporcionan una seguridad relativamente avanzada con múltiples opciones de configuración. Sin embargo, no se encuentra exento de posibles fallos o de que los usuarios se vean expuestos a múltiples amenazas que pueden comprometer su seguridad y su privacidad. **Metodología**: Basándose en un estudio y selección de las distintas amenazas y técnicas existentes para suprimir o mitigar las vulnerabilidades, se pretende crear un esquema más seguro. Se proponen dos modelos de routing Linux: *router* como punto de acceso, y *router* como intermediario. **Resultados:** El uso de dispositivos autorizados por dirección MAC y usuarios y contraseña con un acceso limitado por un cortafuegos reduce el riesgo de los atacantes a cometer una intrusión en nuestras redes locales. **Discusión**: La instalación y configuración de ambos modelos implica una serie de conocimientos y un mayor coste para aquellos usuarios que desean ampliar las especificaciones de seguridad de sus redes. **Conclusiones**: Aunque se consigue una mejor seguridad y la privacidad con los modelos propuestos, se ha de tener en cuenta la evolución de las amenazas y su evolución, por lo que los usuarios deben seguir siempre las recomendaciones de protección.

Palabras clave: cortafuegos; linux; seguridad perimetral; *router*; VPN; autenticación; WLAN; privacidad.

Abstract:
Introduction: Today's fiber optic networks installed in homes provide relatively advanced security with multiple configuration options. However, it is not exempt from possible failures or users being exposed to multiple threats that can compromise their security and privacy. **Methodology**: Based on a study and selection of the different security threats and the existing techniques to suppress or mitigate vulnerabilities, the aim is to create a more secure scheme. Two Linux routing models are proposed: router as an access point, and Linux router as an intermediary. **Results:** The use of devices authorized by MAC address and users and password with access limited by a firewall reduces the risk of attackers intruding into our local networks. **Discussions:** The installation and configuration of both models implies a series of knowledge on the part of users who wish to extend the security specifications of their networks, just as their application implies an increase in cost. **Conclusions**: Although better security and privacy is achieved with the proposed models, the evolution of threats and their evolution must be taken into account, so users should always follow the protection recommendations.

Keywords: firewall; linux; perimeter security; router; VPN; authentication; WLAN; privacy.

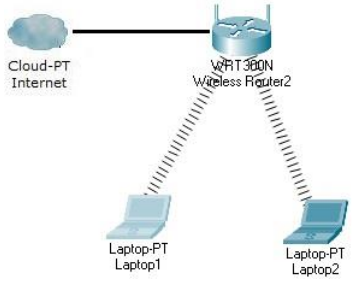
1. Introducción

Actualmente las empresas de telefonía e Internet que proporcionan a sus clientes una conexión de fibra óptica proveen, por defecto en la mayoría de las ocasiones, un *router* wifi específico que suele incluir un conector ONT del proveedor; en otras ocasiones, el dispositivo ONT está separado del *router*. Por defecto, los *router* wifi instalados cuentan con el protocolo de cifrado WPA2-PSK con una contraseña de entre 8 y 63 caracteres para ofrecer una seguridad relativamente avanzada para un entorno doméstico.

Las conexiones al *router* se llevan a cabo de dos posibles formas: a través de cableado mediante un conector RJ-45 aprovechando los puertos disponibles o mediante una conexión inalámbrica con un dispositivo wifi, la cual permite una cantidad significativa de dispositivos (véase Figura 1). Dado el limitado número de conexiones cableadas, sería necesaria una intrusión física. Respecto a las conexiones inalámbricas, el número de dispositivos y equipos a conectar está condicionado al número de clientes soportado en el servidor DHCP. Para este caso, existen otros tipos de intrusiones que un atacante puede aprovechar, estando principalmente muy relacionada con la captación de la red wifi de la víctima para usos maliciosos (Nikolov, 2020; Cloudflare, 2020).

Figura 1.

Modelo actual de una red de área local



Fuente: Elaboración propia (2024).

En los últimos años el Instituto Nacional de Ciberseguridad (INCIBE) ha percibido e informado de un aumento significativo de incidencia en la seguridad informática. Solo en 2023

se incrementó un 24% el número de incidentes respecto a 2022, además de la identificación de más de 180000 sistemas vulnerables. Algunas de estas vulnerabilidades que afectan a la ciudadanía pueden deberse, entre otros casos, a una falta de actualizaciones de seguridad o incluso a técnicas de cifrado débiles, obsoletas o cuya fortaleza ha sido rota como sugiere Ochoa (2024). Estos datos evidencian la necesidad de tomar una formación, así como en la identificación y prevención de potenciales amenazas externas (malware, phishing) que algunas aplicaciones pueden detectar.

Desde el año 2018, existe el estándar WPA3 anunciado por la wifi Alliance con motivo de reemplazar WPA2, puesto que existe una vulnerabilidad crítica denominada KRACK (Cloudflare, 2020; INCIBE, 2019) por el cual un hacker puede obtener la contraseña en el momento que el que host autentica con el dispositivo cliente. No obstante, al ser un protocolo muy reciente todavía existe un número significativo de dispositivos que todavía no lo soportan, ya que requiere una tecnología de soporte de wifi 6, por lo que todavía no es muy frecuente su uso en redes, además de que muchos usuarios todavía emplean a diario dispositivos adquiridos con anterioridad a 2019, lo que implicaría que para que la mayoría de los clientes pudieran usar este nuevo protocolo sería necesario una renovación de los dispositivos inalámbricos.

La formación en seguridad informática es una de las materias que presentan una gran importancia en el ámbito de la administración de redes, siendo que estos conceptos se imparten a partir de los cursos de técnico de sistemas microinformáticos y redes y técnico superior de administración de sistemas informáticos en red. Las ideas impartidas sirven al alumnado como una muestra ampliable de conocimientos mediante el refuerzo de los conceptos y la continua búsqueda de nuevas vulnerabilidades que afecten a un sistema, lo cual en este artículo se va a realizar a través de una investigación sobre vulnerabilidades y posibles contramedidas, con la idea de diseñar modelos de referencia que tengan en cuenta estos elementos.

1.1. Objetivos

En el presente artículo se tratará de buscar mediante una serie de vulnerabilidades conocidas que pueden comprometer la seguridad de las redes locales del hogar, qué contramedidas existen, con las cuales se ideará al menos un modelo de referencia que pueda significar una mejora respecto a la idea inicial de una red local aplicando los elementos encontrados. Posteriormente, con una serie de pruebas se expondrán unos resultados para entender las capacidades de los modelos diseñados abordando las posibles limitaciones y mejoras existentes en los casos expuestos.

Adicionalmente, se pretende hacer uso de métodos o técnicas adicionales de refuerzo con el fin de incrementar el nivel de seguridad y privacidad que suelen integrar nuestras conexiones mediante protocolos de autenticación y cifrado para evitar que terceros sustraigan la información que es manejada o mediante software antivirus y cortafuegos para detectar y prevenir amenazas externas. Estos elementos van a ser explorados en los siguientes apartados los diferentes métodos adicionales que permitan cumplir los objetivos establecidos.

2. Metodología

A través de la búsqueda y lectura de artículos, tanto de investigación como de páginas web o blogs de conocidos portales web, se la logrado seleccionar un conjunto de vulnerabilidades conocidas. En el proceso de búsqueda mediante el portal Google Scholar, así como en el propio motor de Google se han empleado términos clave tales como “vpn ubuntu”, “radius”,

"freeradius ubuntu", "krack attack", "wifi vulnerabilidades", "wpa2 psk vulnerabilidades", "arp vulnerabilities", entre otros. Respecto a la búsqueda de fuentes de páginas web, el método de búsqueda ha sido similar, encontrando un total de 28 fuentes que contuvieran las ideas y conceptos principales para el trabajo. Entre dichas fuentes se destaca artículos de ACADEMIA, Alhambra, Avast, Cloudflare, IEEE Xplore, IJARCCE, INCIBE, IONOS, Kaspersky, Kinsta, Redestelecom, RedesZone, ResearchGate, SmallStep, Springer, STUME Journals, Universidad Católica de Oriente, Universidad Politécnica de Valencia, Xataka, Zenodo, entre otras fuentes. Finalmente, entre el total de fuentes recolectadas se han mantenido 20 por la relevancia en su contenido y la puesta en práctica para la corrección de fallos de seguridad.

Tras la recopilación de artículos y fuentes, se ha procedido a la búsqueda de los diferentes tipos de vulnerabilidades más comunes o conocidas, así como específicas, que afecten a la seguridad y privacidad de las redes de área local en el ámbito del hogar. Entre las vulnerabilidades encontradas se ha analizado su funcionamiento y algunas de las variantes que posee. De estas vulnerabilidades se ha seleccionado un conjunto de ellas y, posteriormente, se ha realizado una búsqueda de las posibles técnicas que pueden solucionar o mitigar las vulnerabilidades seleccionadas. En este apartado se ha procedido a la visualización de los distintos tipos de vulnerabilidades y posibles fallos que afectan a las redes de área local que se aplican en los hogares y las posibles técnicas que pueden minimizar estos fallos de seguridad.

Para el diseño del nuevo tipo de red se parte del proceso inicial que compone una red local en el hogar, siendo principalmente la conexión de fibra óptica que instala el proveedor de servicios de Internet, la cual se compone de una conexión a un ONT, también conocido como Terminal de Red Óptica y un *router* wifi que ya incluye al menos el estándar de wifi 5. En muchas ocasiones, el ONT ya viene integrado en el *router*.

En los siguientes subapartados se explican las vulnerabilidades de las redes seleccionadas, las técnicas de mitigación propuestas para cada una de dichas vulnerabilidades. A continuación, se seleccionan unas soluciones compatibles con un sistema Linux como intermediario, para poder identificar dos modelos de prueba.

2.1. Listado de vulnerabilidades

2.1.1. Ataques de denegación de servicio

Los ataques de denegación de servicio tienen como objetivo privar o anular uno o más servicios o aplicaciones a un cliente o grupo de clientes pudiendo verse afectada tanto el origen que proporciona el servicio como una red en sí. Normalmente este tipo de ataques se encuentran dirigidos hacia servidores Web, aumentando en un espacio de tiempo muy corto el número de solicitudes hasta sobrepasar las que puede soportar llegando a bloquearse el servicio. Existen dos tipos de ataques (Jiménez, 2024): Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS).

Este tipo de ataques generan una cantidad masiva de peticiones hacia el servicio objetivo desde un mismo ordenador o una dirección IP sobrecargando los recursos del sistema al que va dirigido hasta que empiece a rechazar cualquier petición. En el caso de la denegación de servicio distribuida, se lleva a cabo mediante un gran número de equipos coordinados para generar un alto número de peticiones al mismo tiempo; generalmente esto se consigue con una red "botnet" mediante la cual los equipos que realizan este ataque han sido infectados previamente con un malware que permite a los atacantes tener un control de las máquinas de las víctimas y realizar peticiones o enviar instrucciones.

2.1.2. Infección por malware

Las infecciones por malware suponen un riesgo para las redes debido a los efectos dañinos que provoca en los equipos, así como por su propagación. Algunos tipos de virus están especializados en la captura de credenciales de sesión de los navegadores que emplean cookies para autorizar o mantener abiertas las sesiones o recoger las contraseñas, pues hay casos de que se guardan en archivos de texto plano sin cifrar, lo que supone un grave agujero de seguridad. Otros permiten tener el control del equipo de la víctima, este tipo de malware son troyanos RAT (Remote Administration Tool), llegando a tener la capacidad de crear botnets que lleven a cabo ataques coordinados DDoS.

2.1.3. Modificación de direcciones MAC

La dirección MAC de un equipo puede ser modificada de forma fácil añadiendo una dirección MAC con un formato válido en las propiedades de la tarjeta de red dependiendo del sistema operativo. Esto permite que los atacantes puedan suplantar la identidad de las víctimas y acceder a determinados recursos, evitar rastreos y llevar a cabo acciones maliciosas.

2.1.4. Man in the Middle

En este tipo de vulnerabilidad, un atacante puede interceptar la información transmitida entre dos dispositivos, de modo que la víctima continúe creyendo que la comunicación es directa y segura (Jiménez, 2024). De forma general, este ataque implica que el atacante se encuentre dentro de la red objetivo y configure sus dispositivos como una parte intermediaria de modo que el tráfico pase a través de su equipo e interceptar la información que desee. Uno de estos ataques a nivel inalámbrico se denomina "Evil twin" (Ghimiray, 2023) donde el atacante genera un punto de acceso con el mismo SSID por el que el equipo de la víctima se conecte y pueda obtener contraseñas e información que no se encuentre cifrada o las propias credenciales del verdadero SSID al que se conecta la víctima para posteriormente, obtener un acceso a la red.

2.1.5. Vulnerabilidades inalámbricas

Debido a que los protocolos de cifrado WEP y WPA ya no son considerados seguros para la conexión de dispositivos a un punto de acceso o un *router* wifi, hoy en día se emplea por defecto en la mayoría de las ocasiones el protocolo WPA2, el cual es la evolución de WPA. No obstante, pueden presentar ciertas debilidades, entre ellas, las que se mencionan a continuación (Nikolov, 2018):

- Contraseñas débiles o cortas: la fortaleza de la red inalámbrica se encuentra relacionada con la fortaleza de la contraseña, las cuales si no presentan una longitud y una complejidad de caracteres alfanuméricos mínimos puede dar lugar a su acceso por ataques de fuerza bruta por diccionario. Una de las herramientas de fuerza bruta más conocidas es “John the ripper” o con suites de auditoría como Kali Linux.
- KRACK: este ataque aprovecha una vulnerabilidad en el protocolo WPA2 para interceptar la información transmitida a través de la red (Cloudflare, 2020). WPA2 cuenta con 4 vías en su protocolo de enlace, aunque solo utiliza 3 para obtener una mayor velocidad, de modo que un usuario que se ha conectado previamente a una red wifi conocida utiliza esta tercera vía de forma seguida para volver a intentar conectarse a la red, la cual es la vulnerabilidad. El atacante puede crear una copia de la red wifi a la que la víctima intente volver a conectar, dicha red puede contar con una conexión real a Internet para dar una mayor verosimilitud con la original, con lo que si la víctima quiere intentar volver a conectarse el hacker solo tiene que reenviar la tercera parte del

protocolo de enlace y que esta sea aceptada.

- WPS: Esta alternativa para las conexiones de equipos se encuentra muy relacionada para una fácil conexión de dispositivos IoT (Internet of Things) haciendo uso de un PIN de 8 dígitos o un botón que incluye físicamente el *router* (Véase Figura 2). Cuando esta característica es activada permite a los atacantes descifrar el PIN que es su vulnerabilidad para realizar la conexión con el *router*.

Figura 2.

Router wifi con botón WPS

Fuente: Elaboración propia (2024).

2.1.6. DHCP starvation

Este ataque hacia el servidor DHCP tiene como objetivo agotar todas las direcciones IP disponibles presentes en el servidor DHCP al inundar de solicitudes DHCPDISCOVER un atacante, normalmente haciendo uso de diferentes direcciones MAC falseadas con el propósito de parecer diferentes clientes pudiendo resultar en una posible denegación de los usuarios autorizados. Una herramienta conocida para provocar ataques de DHCP starvation es Yersinia.

2.1.7. Vulnerabilidades del protocolo ARP

Uno de los ataques que afectan el protocolo ARP es ARP Spoofing/ARP Poisoning (Jiménez, 2024), un tipo de suplantación que altera la información almacenada en las tablas ARP del sistema con el objetivo de asociar la dirección MAC del atacante con una dirección IP de la víctima o de un servidor enviando mensajes ARP falsos a través de una red local, por lo cual el tráfico que debería llegar a la víctima llega al atacante, lo cual implica la sustracción de información sensible en una red. Dada su naturaleza, este tipo de ataque también puede considerarse un tipo de ataque Man in the Middle.

2.2. Técnicas de mitigación

2.2.1. Ocultación de SSID

Las técnicas de ocultación de SSID eliminan de las emisiones los Beacon Frames, lo que permite al propietario de una red inalámbrica la posibilidad de que esta no sea visible para otros dispositivos ajenos al de los usuarios finales. Un usuario que desee conectarse a una red que no emplea Beacon Frame debe configurar de forma manual la seguridad y las opciones que conformaría la red, sin embargo, esta es una técnica que se puede burlar con relativa facilidad.

2.2.1. Listas negras

Es un método de control de acceso para utilizar y/o acceder a recursos de un sistema e identificar y bloquear direcciones IP, sitios web, software o correos electrónicos considerados como amenaza entre otros. Mediante esta técnica todos los elementos de una red están permitidos a excepción de aquellos indicados explícitamente en una lista considerados por los administradores como inseguros o con un riesgo elevado.

2.2.2. Listas blancas

Al igual que con las listas negras, este método es también un método de control de acceso con la diferencia de que, en estas listas, por defecto, todo acceso se encuentra bloqueado para todos y solo se le permite los accesos y la utilización de recursos a aquellos usuarios o dispositivos que son nombrados explícitamente en la lista. Este método ofrece una mayor protección al limitar el acceso solo a usuarios específicos, por lo que es una solución muy recomendada.

2.2.3. Mitigación de DHCP starvation

El ataque de DHCP starvation se puede mitigar implementando la técnica "Port security", suele estar configurada e implementada en conmutadores de red pudiendo limitar el número de direcciones MAC que aprende por puerto. De forma adicional, se puede implementar como medida que el propio servidor DHCP asigna una configuración IP por medio de una dirección MAC especificada previamente de entre las autorizadas.

2.2.4. Software antivirus

Considerando que una gran cuota del mercado se relaciona con sistemas operativos Windows, el uso de programas antivirus está presente. Por defecto, este sistema operativo trae incorporado Microsoft Defender, el cual es desactivado automáticamente al instalar otro antivirus. En sistemas Linux es opcional con el motivo de que la mayoría del malware existe en plataformas de Microsoft.

2.2.5. VPN

Una VPN es una red privada formada entre dos puntos a través de una red pública, que por lo general es Internet (Albarrán, 2024; Bourdoucen, 2009). Las VPN permiten a los usuarios un alto nivel de seguridad debido a los protocolos de cifrado y de autenticación con los que cuentan, siendo los tipos más comunes los que emplean IPsec y SSL, cada una de estas implementaciones tiene sus fortalezas y debilidades y están mejor orientadas en función de su aplicación.

2.2.6. Cortafuegos

Son programas que inspeccionan y controlan el tráfico de una red en función de un conjunto de reglas de seguridad (Duò, 2020). En sistemas Linux, las herramientas que permiten la gestión de reglas para cortafuegos son: iptables, nftables y firewalld. Dado que firewalld es muy básico, un administrador puede optar entre iptables y nftables, para cortafuegos más complejos y de un rendimiento crítico se suele utilizar la utilidad nftables. Existen varios tipos de cortafuegos, algunos de ellos específicos que se comercializan para unas necesidades muy específicas, entre ellas:

- Basados en proxy: hace uso de proxies que se encuentran entre los usuarios y los servidores, con lo cual, los paquetes salientes de un usuario son inspeccionados por el firewall que se conecta.
- Cortafuegos de estado: Su función es la inspección completa del paquete de datos y los elementos que los compone.
- Cortafuegos sin estado: Este tipo de firewall solo considera el origen, destino y otros parámetros del paquete para determinar el nivel de amenaza y bloquear o no el paquete en función de sus parámetros.
- Firewall de nueva generación (NGFW): El apartado "Firewall de nueva generación (NGFW)" detalla más detenidamente este tipo de cortafuegos.
- Firewall de aplicaciones web (WAF): Cortafuegos orientados a la protección de aplicaciones web.

2.2.7. Firewall de nueva generación (NGFW)

Son dispositivos de seguridad que procesan el tráfico de la red y aplican reglas de seguridad para bloquear el tráfico potencialmente peligroso (Duò, 2020). Los datos son inspeccionados a un nivel más profundo para identificar las amenazas, entre sus funciones se encuentran las siguientes:

- Filtrado de paquetes: Inspecciona cada paquete individual de datos y bloquea los paquetes peligrosos o inesperados.
- Inspección profunda de paquetes: Examina los paquetes en su contexto para asegurarse de que forman parte de una conexión de red legítima.
- Identificación de tráfico VPN: Capacidad para la identificación del tráfico de VPN encriptado y la autorización de su paso.

2.2.8. DMZ

Zona Desmilitarizada o Demilitarized Zone, es una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo. Normalmente se utiliza para separar los servicios con acceso externo de la red local, por lo cual, si un intruso logra romper las barreras y acceder a la DMZ, aún no tendrá acceso a la red interna, ya que las conexiones procedentes de la DMZ se encuentran bloqueadas.

Actualmente, los *router*s que proporcionan las compañías de telefonía e Internet también incluyen la opción de cortafuegos DMZ, aunque no es la opción más aconsejable ya que toda la carga del tráfico recaería sobre el propio *router*.

2.2.9. Servicio RADIUS

Este protocolo permite la autenticación y autorización permitiendo el uso de credenciales a los clientes como puede ser el uso de usuarios y contraseñas (De Luz, 2024). Actualmente, el software FreeRADIUS es uno de los servicios de autenticación más populares en Linux para la implementación de autenticación en redes wifi y puntos de acceso comerciales.

2.2.10. 802.1X

Esta norma del IEEE se basa en puertos para el control de acceso a la red, encargándose de bloquear las conexiones a equipos y dispositivos no autorizados. Este estándar suele estar disponible para algunos tipos de conmutadores de red y configurarlo para autenticar nodos que están equipados con software suplicante.

2.2.11. Prácticas para evitar el malware

No existe per se una práctica para evitar por completo las infecciones por malware en un dispositivo, no obstante, sí para minimizar las posibilidades de infección cumpliendo una serie de pautas o recomendaciones por parte de los usuarios. Entre estas prácticas se encuentran las siguientes:

- Actualizar los sistemas operativos relacionados con aspectos de la seguridad. Se recomienda emplear sistemas operativos que tengan soporte para actualizaciones.
- Evitar la descarga de archivos provenientes de redes o entornos poco fiables o seguros.
- Configurar y usar navegadores y complementos catalogados como más seguros que eviten abrir páginas emergentes u otros archivos.
- Uso de antivirus y cortafuegos actualizados y escaneo periódico del sistema en busca de amenazas.
- Eliminar las cookies del navegador y evitar que recuerde las contraseñas en inicios de sesión.
- Planificar una estrategia de copias de seguridad de los archivos en caso de posible pérdida por malware de tipo ransomware o similares.

2.3. Técnicas seleccionadas

Una vez vistos algunos de los ataques que suelen que afectan a las redes locales y las técnicas empleadas para resolver o mitigar estos fallos, se procede a la selección de aquellas soluciones compatibles con un sistema Linux como intermediario para filtrar el tráfico y minimizar los efectos de las vulnerabilidades de las redes que serán propuestas en los siguientes experimentos. Algunos de los elementos seleccionados coinciden con los propuestos por Marín (2020), tales como la implementación de cortafuegos y VPN, aunque para este caso no se ha propuesto el uso de Sistemas de Detección de Intrusos (IDS):

- Asignación de direcciones IP a direcciones MAC autorizadas
- Servicio Radius
- Cortafuegos con iptables
- Uso de listas blancas y negras
- Servicio VPN
- Uso de buenas prácticas del uso de Internet

2.4. Casos de prueba

Dadas las técnicas mencionadas en los apartados anteriores, se identifican dos posibles modelos de pruebas que incluyan las características mencionadas. Para ello se ha hecho uso de equipos con procesadores x64 y sus correspondientes adaptadores de red Ethernet e inalámbricos configurados, cuyo hardware corresponde al de un i5-2500 de 4 núcleos y 4 hilos a 3.3 GHz con 8 GB de memoria RAM DDR3 y dos adaptadores Ethernet a 1Gbps que será empleado como *router* Linux e intermediario entre el *router* de la compañía y el punto de acceso. Respecto al punto de acceso inalámbrico se presentan como características un procesador i3-2328M de 2 núcleos y 4 hilos a 2.2 GHz con 6 GB de RAM DDR3 con un

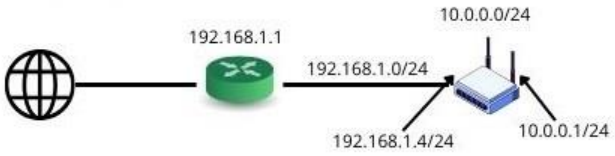
adaptador Ethernet a 1Gbps y un adaptador wifi b/g/n Broadcom, ambas máquinas harán uso de un sistema operativo Linux para la modificación del esquema actual de una red local.

2.4.1. Modelo 1: Punto de acceso inalámbrico LinuxPrácticas para evitar el malware

Este caso presenta el uso de un punto de acceso inalámbrico haciendo de *router* al mismo tiempo, cuyo hardware para las pruebas corresponde al de un ordenador portátil con interfaces Ethernet y wifi con un sistema Ubuntu, el cual se conecta al *router* (véase Figura 3). Emplea los servicios hostapd para la creación de un punto de acceso, DHCP para la provisión de direcciones IP de los usuarios y el servicio FreeRADIUS para la autenticación.

Figura 3.

Arquitectura de red con punto de acceso wifi Linux



Fuente: Elaboración propia (2024).

Como medidas de seguridad de este modelo, se incluye el protocolo WPA2 con FreeRADIUS para proveer una autenticación de usuarios, los cuales son permitidos mediante una lista de direcciones MAC autorizadas que son incluidas por el administrador o dueño de la red. El filtrado de paquetes se procede con un script bash de iptables para filtrar los puertos y accesos de los usuarios de modo que tienen autorización para usar protocolos como HTTP y HTTPS y evitar entrar en las capacidades de los *router*s.

2.4.2. Punto de acceso hostapd

Mediante el uso del servicio hostapd se modifica la interfaz inalámbrica del ordenador portátil para crear un punto de acceso wifi con protocolo WPA2 en conjunto con un servidor DHCP que provee las direcciones IP dinámicas a los clientes. Se ha asignado a la interfaz del punto de acceso la dirección privada de red 10.0.0.0/24. El propio servicio incluye una directiva por la que se puede especificar un fichero de texto plano donde incluyen las direcciones MAC autorizadas que se podrán conectar a la red. Otra de las directivas de hostapd permite el uso de un servidor RADIUS para la autenticación por el protocolo WPA2-Enterprise en lugar de WPA2-PSK (Personal) mediante el uso de usuarios y contraseña registradas previamente en el servidor RADIUS.

2.4.3. FreeRADIUS

FreeRADIUS es el servicio de autenticación RADIUS libre con licencia GNU, siendo una de las soluciones open source más populares para aplicar este tipo de servicio (De Luz, 2024). Cuenta con un soporte para la autenticación por PAP, CHAP, EAP, EAP-TTLS, EAP-TLS entre otros protocolos que permite, además, el almacenamiento de usuarios en bases de datos como MySQL, PostgreSQL y LDAP. Los ficheros de configuración de FreeRADIUS se modifican mediante editores de texto; sin embargo, una configurado puede usar un cliente web como DaloRADIUS para la gestión de los usuarios que hacen uso del servicio para la autenticación.

2.4.4. Cortafuegos del modelo 1

De forma inicial, la interfaz Ethernet se ha configurado en modo NAT con el propósito de que los usuarios autorizados por la interfaz inalámbrica obtengan un acceso a través de la red. El cortafuegos compuesto por comandos iptables (IONOS, 2023) realiza inicialmente una política de conexiones abiertas; en primera instancia todo se acepta, posteriormente se declara una serie de restricciones por las cuales la propia interfaz localhost del *router* tiene intactos los accesos, e otra instancia el tráfico de los usuarios que pase a través de la interfaz Ethernet del punto de acceso tiene permitido las peticiones HTTP y HTTPS, DNS, los distintos puertos de correo y FTP. El resto se deniega y se procura bloquear el escaneo de puertos de la red, como se puede ver a continuación en la Figura 4, el contenido del scrip.

Figura 4.

Script bash del cortafuegos

```
#!/bin/bash

iptables -F
iptables -X
iptables -Z

iptables -t nat -F

#Cortafuegos abierto. Política de todo aceptado
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

iptables -t nat -A POSTROUTING -o enp2s0f0 -j MASQUERADE

# El localhost se deja
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 587 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -p tcp --dport 20 -j ACCEPT

# Cerramos el rango de todos los demas puertos
iptables -A INPUT -s 192.168.1.1/24 -p tcp --dport 1:65535 -j DROP
iptables -A INPUT -s 192.168.1.1/24 -p udp --dport 1:65535 -j DROP

#El resto de paquetes de la red inalámbrica se deniegan
iptables -A FORWARD -s 192.168.1.0/24 -i enp2s0f0 -j DROP

# Bloquear acceso a protocolos específicos
iptables -A INPUT -p tcp --syn -j DROP  # Bloquear escaneo de puertos
```

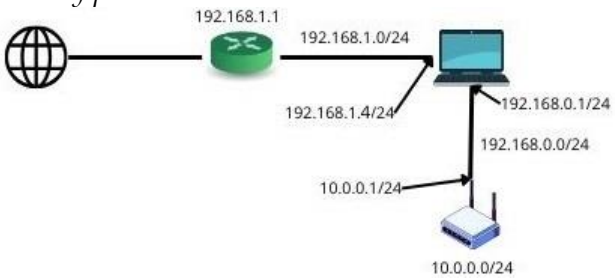
Fuente: Elaboración propia (2024).

2.4.5. Modelo 2: Router Linux como intermediario

Este modelo hace uso de un ordenador que ejecuta un sistema Linux con dos adaptadores Ethernet, por el cual hace de intermediario entre la red pública de Internet y el punto de acceso al que se conectan los usuarios. En este caso, el *router* Linux destaca más como elemento de filtrado al separarse el esquema en diferentes módulos (véase Figura 5), empleando también un script bash basado en iptables muy similar al del primer modelo para realizar las operaciones de filtrado de tráfico en la red. Cuenta con dos interfaces: la primera emplea la red 192.168.1.0, mientras que para la interfaz para la conexión del punto de acceso se ha creado la red 192.168.0.0 mediante un servidor DHCP que incluye únicamente la dirección IP del punto de acceso, la cual es la puerta de enlace de la red.

Figura 5.

Arquitectura de red con router y punto de acceso Linux



Fuente: Elaboración propia (2024).

Así mismo, el *router* Linux incluye el servicio FreeRADIUS para la autenticación, cuya dirección de red es incluida en la configuración del punto de acceso.

2.4.6. Cortafuegos del modelo 2

El cortafuegos del segundo modelo de red local comparte características similares a las del primer modelo: la interfaz Ethernet conectada al *router* de telefónica está configurado en NAT y de forma inicial permite conexiones permisivas otorgando acceso HTTP y HTTPS, DNS, los distintos puertos de correo y FTP. Al igual que con el cortafuegos del primer modelo, este cortafuegos deniega el acceso al resto.

2.2.11. VPN

Se ha empleado el servicio de código libre OpenVPN para la integración del servidor VPN con el fin de crear una comunicación cifrada de los usuarios entre el punto de acceso y el propio *router* Linux, de tal modo que un usuario conectado a la red que se encuentre escuchando no pueda entender nuestro tráfico si los usuarios se comunican a través de un túnel cifrado y el atacante no es consciente de ello. Por defecto, emplea la red 10.8.0.0 (véase Figura 6).

Figura 6.

Uso del servicio VPN del router Linux

```
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.2/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fddd:1194:1194:1194::1000/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::3104:87b:c0cd:24c/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Fuente: Elaboración propia (2024).

3. Resultados

El primer modelo, compuesto por un punto de acceso Linux con hostapd y FreeRadius, muestra un comportamiento por el cual solo aquellos usuarios con una dirección MAC registrada pueden conectarse mediante la autenticación por RADIUS, por el cual se le asigna la configuración de red en función de la propia MAC. En la figura 7 se pueden apreciar las diferencias entre un usuario con un dispositivo no autorizado y otro usuario con un dispositivo autorizado.

Figura 7.

Conexión a la red por RADIUS

Fuente: Elaboración propia (2024).
Nota: A la izquierda, la conexión. En el centro, el resultado de un acceso no permitido. A la derecha, la conexión permitida.

Al autorizar en la lista de direcciones MAC del servicio hostapd y asignar después una dirección IP, la conexión en la red se realiza con éxito y se le asigna la dirección IP. En las pruebas del cortafuegos se ha comprobado que los equipos conectados por el punto de acceso hostapd no pueden acceder a la puerta de enlace del *router* instalado por la empresa telefónica, así como algunos servicios como SSH (Véase Figura 8).

Figura 8.

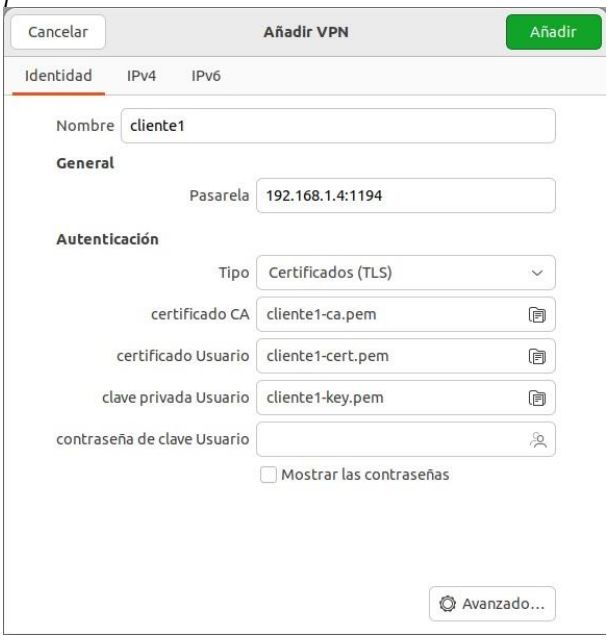
Denegación al servidor SSH de pruebas

Fuente: Elaboración propia (2024).

Con el segundo modelo de arquitectura de red propuesto, se consigue el mismo comportamiento que en el caso anterior: los usuarios que se autentican mediante RADIUS con una dirección MAC registrada pueden conectarse a la red. En este caso, el *router* Linux actúa además como servidor VPN que encripta la información de los usuarios conectados desde el punto de acceso, lo cual favorece una mayor privacidad. Dicho servidor permite generar un archivo ovpn que contiene los certificados para la conexión al servidor OpenVPN. Su importación en Linux es relativamente simple desde el gestor de redes (véase Figura 9), mientras que otros sistemas como Windows, MacOS o Android necesitan del programa de OpenVPN para importar el archivo de certificados.

Figura 9.

Importación de ficheros OpenVPN en Linux



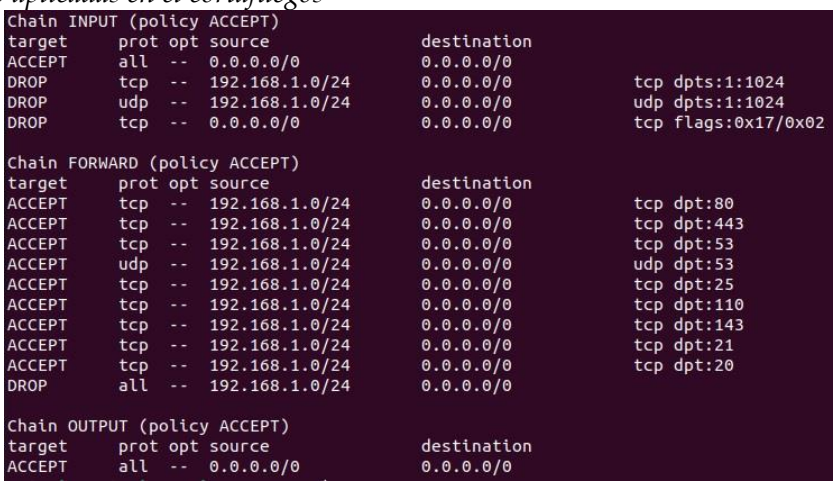
Fuente: Elaboración propia (2024).

De forma general, en el apartado inalámbrico un usuario solo podrá conectarse de forma inalámbrica si se da la condición de que la dirección MAC de su equipo esté registrada en el sistema del punto de acceso y del mismo modo este cuente con un usuario y contraseña válidos que se encuentren en el servidor RADIUS para autenticar el dispositivo. Esta combinación, en un principio, puede dificultar significativamente la tarea de un atacante de intentar entrar en la red del propietario, puesto que el atacante debería conocer de primera instancia alguna dirección MAC que se utilice y un usuario y contraseña.

En el caso de que el atacante pueda burlar la seguridad del servidor RADIUS, este solamente tendría acceso a los servicios básicos HTTP, HTTPS y uso de protocolos de correo para la configuración de un cliente local como puede ser Outlook o Thunderbird. El resto de recursos como SSH, telnet, u otros puertos son denegados, así como el acceso a los recursos del servidor RADIUS y del *router* principal de la compañía de teléfono por medio del cortafuegos situado en el punto de acceso Linux que se ha creado. La Figura 10 presenta las políticas desde el punto de acceso Linux que funciona tanto para el primer como el segundo modelo.

Figura 10.

Reglas de acceso aplicadas en el cortafuegos



```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
DROP       tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpts:1:1024
DROP       udp  --  192.168.1.0/24       0.0.0.0/0           udp dpts:1:1024
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  192.168.1.0/24       0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:25
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:110
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:143
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:21
ACCEPT     tcp  --  192.168.1.0/24       0.0.0.0/0           tcp dpt:20
DROP       all  --  192.168.1.0/24       0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

Fuente: Elaboración propia (2024).

Durante las pruebas de las conexiones del cortafuegos se ha comprobado que los usuarios autorizados previamente conectados a la red, no tienen acceso a los recursos del *router* de telefónica, así como a otros recursos del *router* Linux y el punto de acceso instalado.

4. Discusión

En los siguientes párrafos, se van a discutir los resultados de la aplicación de estos modelos con el objeto de responder a las cuestiones sobre la seguridad aportada respecto a las dadas por defecto en las redes locales del hogar.

Entre los elementos más significativos que se introducen para modificar el actual esquema de red del hogar se encuentran la implementación de nuevas políticas en el servicio inalámbrico y el filtrado por cortafuegos de forma común en ambos modelos propuestos. Las mejoras del protocolo WPA2 han demostrado una mayor fortaleza en la seguridad de las redes wifi, no obstante, por medio de ataques de diccionario se ha conseguido obtener la contraseña durante los handshake con programas tales como la suite Aircrack, tal como muestra Kumkar (2012), en función de su longitud y su inclusión en diccionarios de ataque. Esto reflejaría la importancia de que una red wifi debería tener una contraseña personalizada con una longitud significativa y caracteres alfanuméricos.

A pesar de considerarse relativamente robusto, el protocolo WPA2-PSK todavía presenta el riesgo del ataque KRACK. En cambio, tal como indica INCIBE (2018, 2019), el protocolo WPA3, al tener los mecanismos del handshake actualizados en comparación de su contraparte, actualmente todavía sigue en uso. A largo plazo, los usuarios requerirán de una actualización de sus equipos o del hardware inalámbrico para funcionar bajo este protocolo. Sin embargo, la inclusión de una contraseña robusta no impide su interceptación en el caso de la vulnerabilidad KRACK o que se puedan interceptar las credenciales mediante la clonación de las características del punto de acceso con el ataque Evil twin.

El servicio FreeRADIUS da soporte a los protocolos PAP, CHAP, EAP, EAP-TTLS y EAP-TLS, entre otros, y permite que la autenticación sea por usuario y contraseña, y no, por el contrario, mediante la emisión de certificados, como indica "De Luz" (2024). Para este caso, por su facilidad de creación y mantenimiento, se ha optado por el método de usuarios y contraseñas

registradas, que en relación con su contraparte basada en autenticación por certificados, como indica Ikechukwu (2024) con el método EAP-TLS, considerado uno de los más seguros para una certificación.

En otra instancia, el segundo modelo de arquitectura de red presentaría un nivel de dificultad algo mayor al haber otro componente más que hace a su vez como *router* wifi, ya que este dispositivo supone un túnel VPN para cifrar las comunicaciones de aquellos usuarios que se conectan proporcionando la privacidad de los datos. Del mismo modo, se prevé un mayor coste en elementos hardware con este modelo.

Marin (2020) proponía en su arquitectura el uso de un IDS como herramienta complementaria con un cortafuegos y VPN. En el mercado, en el ámbito del software libre, existen diferentes tipos de herramientas IDS/NIDS, que ofrecen diferentes funcionalidades, para lo cual, en el artículo revisado, emplea Denyhosts (p. 8), cuyo uso está más orientado al bloqueo de accesos por SSH. Si bien es cierto que permite evitar accesos no autorizados, el cortafuegos ya permite la función de bloquear el puerto 22 al solo permitir los accesos más básicos. Sin embargo, la instalación y configuración de un IDS permitiría la notificación de comportamientos anómalos al administrador (p. 5).

Una observación relacionada con el diseño de redes con dispositivos adicionales se debe al consumo energético. En las pruebas realizadas el punto de acceso wifi configurado en un ordenador portátil se necesita una fuente de alimentación de 65 vatios, el *router* Linux del segundo modelo tiene instalado una fuente de alimentación de un máximo de 500 vatios donde el consumo varía en función de la configuración y uso de recursos del equipo, así como la eficiencia energética a nivel de hardware. Para un uso prolongado de los diseños de red propuestos sería un requisito adquirir equipos de tipo "mini-pc" por sus relativamente bajos precios, consumo y las múltiples conexiones que soportan.

Respecto al uso de servicios VPN, a pesar de que el primer modelo propuesto no provee de un servicio interno de VPN, se puede utilizar un servidor externo para la creación de un túnel cifrado. Debido a que la mayor parte de los dispositivos conectados a la red serán inalámbricos, el trabajo de Bourdoucen (2009) sugiere la probabilidad de una demora en el tiempo de los paquetes recibidos, lo cual puede afectar en la velocidad de la conexión de los clientes. Esto no sería muy significativo en el caso de una conexión cableada (Bourdoucen, 2009, p. 4).

Un inconveniente que se puede presentar en estos nuevos modelos se basa en la redundancia de las direcciones MAC introducidas en el sistema de los clientes autorizados que se conectarán. Esta redundancia se relaciona en los ficheros del servicio hostapd del punto de acceso que permitirá el acceso y del fichero de configuración del servidor DHCP que brinda una configuración IP a los hosts reservados. Para un administrador de redes es incómodo introducir la misma identificación a mano en más de un fichero, se puede elaborar un script que permita interactuar con dichos ficheros en la introducción, listado, modificación y borrado de las direcciones MAC de los usuarios, así como la recarga de los servicios de los que depende para hacer efectivos los cambios surgidos.

5. Conclusiones

Además de los modelos propuestos, otra posible arquitectura sencilla de llevar a cabo sería la implementación de un servidor RADIUS externo para la autenticación. Este servidor se encontraría conectado por cable al *router* instalado por la compañía de Internet y configurado siguiendo las pautas de equipos autorizados y el uso de cortafuegos para bloquear conexiones

sospechosas. Es necesario considerar que este tipo de arquitecturas se encuentran influenciadas por los conocimientos de seguridad que puedan tener los usuarios, por lo que un modelo más simple de instalar y configurar que incluya los elementos más significativos puede suponer igualmente un mayor nivel de seguridad.

En los supuestos del montaje de una infraestructura de un usuario propietario de una red no dispone de las tecnologías para la modificación del esquema de su red existe la posibilidad de llevar a cabo algunas modificaciones como el uso de claves de mayor longitud de tipo clave pública durante el handshake o que también utilice el método SHA-512 para la generación del hash, de modo que al ser interceptado este, se requiera un mayor coste en cálculos, como indica Najar (2021).

En el mercado actual de hardware, sería más adecuado emplear las técnicas vistas anteriormente usando el protocolo WPA3 en lugar de WPA2 que incluye mejoras respecto a los ataques de fuerza bruta y una mayor robustez en su cifrado (Díez, 2018; INCIBE, 2019). Los dispositivos deberán soportar el estándar wifi 6 (802.11 ax) o wifi 5 (802.11 ac), como mínimo, y las últimas actualizaciones de los sistemas operativos. Como aumento de la seguridad en el apartado wifi, se puede considerar en el futuro, según indica Ikechukwu (2024), una autenticación EAP-TLS mediante certificados con el protocolo WPA3-Enterprise, en adición del filtrado por direcciones MAC, para obtener una mayor robustez.

Un factor que todavía se ha de tener en cuenta es el ataque "Evil twin", ya que el atacante todavía podría crear un falso punto de acceso con el mismo SSID que su víctima y obtener sus credenciales de acceso y llevar a cabo acciones maliciosas. Si el rango efectivo de la señal del punto de acceso es relativamente corto, puede implicar que el atacante deba estar muy cerca para obtener acceso para que su punto de acceso falso pueda engañar a la víctima. No obstante, si se sospecha de este tipo de ataque se ha de limitar el acceso a la red y usar conexiones VPN.

Otro posible ataque a contemplar sería el ataque por fuerza bruta para encontrar la clave en un diccionario. Esta técnica de hacking sería más infructuosa para el atacante debido a que si la dirección MAC del equipo del atacante no se encuentra en la lista de direcciones permitidas en el sistema, este no autoriza la conexión y no se permite el uso de los recursos. No obstante, siempre se recomienda cambiar las contraseñas de forma periódica para dificultar accesos indebidos.

Un administrador de la red puede considerar la instalación de un IDS para monitorizar el tráfico de la red con el fin de reducir el número de ataques dentro de la misma, como sugiere Marín (2020). Entre los diferentes IDS se puede contemplar las opciones gratuitas mantenidas por la comunidad o las soluciones privativas. Del mismo modo, por su variedad, sería conveniente llevar a cabo un estudio de los posibles IDS empleados para determinar la herramienta.

Un inconveniente que se puede presentar en estos nuevos modelos se basa en la redundancia de las direcciones MAC introducidas en el sistema de los clientes autorizados que se conectarán. Esta redundancia se relaciona en los ficheros del servicio hostapd del punto de acceso que permitirá el acceso y del fichero de configuración del servidor DHCP que brinda una configuración IP a los hosts reservados. Para un administrador de redes es incómodo introducir la misma identificación a mano en más de un fichero, se puede elaborar un script que permita interactuar con dichos ficheros en la introducción, listado, modificación y borrado de las direcciones MAC de los usuarios, así como la recarga de los servicios de los que depende para hacer efectivos los cambios surgidos.

Finalmente, la decisión de modificar la arquitectura original de la red mediante el diseño y ejecución de un nuevo modelo recaerá sobre el propietario de la red, ya que deberá debatir acerca de si las opciones de seguridad en su red son o no suficientes y si existe la necesidad de ampliarla en el caso de considerarla insuficiente. En los últimos años, la cantidad de hogares conectados a Internet ha aumentado de modo que la gran mayoría de los usuarios cuentan con una conexión a Internet, lo cual implica que la probabilidad de que un atacante haga un intento de intrusión por vías inalámbricas es relativamente baja, sin embargo, persiste la posibilidad de una intrusión para enmascarar la localización del atacante y hacer uso de la red para fines maliciosos.

6. Referencias

Albarrán, C. (2024, 17 de mayo). *Qué es una VPN*. https://is.gd/EZPX5f

Bourdoucen, H., Al Naamany, A. y Al Kalbani, A. (2009). Impact of Implementing VPN to Secure Wireless LAN. *World Academy of Science, Engineering and Technology International. Journal of Electronics and Communication Engineering*, *3*(3). https://doi.org/10.5281/zenodo.1072349

Cloudflare. (2020). *¿Qué es un ataque KRACK? | Cómo protegerse contra los ataques KRACK*. https://www.cloudflare.com/es-es/learning/security/what-is-a-krack-attack/

De Luz, S. (13 de mayo de 2024). *Descubre para qué sirve un servidor RADIUS y su funcionamiento*. https://is.gd/HsjQtP

Díez Rodríguez, A. (30 de agosto de 2018). *WPA3, la mayor actualización de seguridad en redes Wi-Fi desde hace más de una década*. https://is.gd/eiYldX

Duò, M. (26 de junio de 2020). *¿Qué es un cortafuegos? La guía inicial de los diferentes tipos de cortafuegos y si necesitas uno*. https://is.gd/hAnUJI

Equipo editorial de IONOS. (1 de marzo de 2023). *iptables: cómo configurar las tablas de filtrado del núcleo de Linux*. https://is.gd/WB0ef2

Ghimiray, D. (5 de diciembre de 2023). *¿Qué es un ataque de gemelo malvado?* Avast. https://www.avast.com/es-es/c-evil-twin-attack

Ikechukwu, L. (5 de enero de 2024). Certificate Based Wifi Authentication With RADIUS and EAP-TLS. *Smallstep Blog*. https://smallstep.com/blog/eaptls-certificate-wifi

INCIBE. (10 de enero de 2019). *WPA3, la mayor actualización en redes Wi-Fi de la última década*. https://is.gd/li9PQ3

INCIBE. (14 de mayo de 2019). *Seguridad en redes wifi: una guía de aproximación para el empresario*. https://is.gd/l4YqgN

Jiménez, J. (3 de marzo de 2024). *Suplantación de ARP: qué es y cómo afecta a nuestra red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/ataques-arp-spoofing-evitar/

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A. y Shrawne, S. (2012). *Vulnerabilities of Wireless Security protocols (WEP and WPA2)*. https://is.gd/NjYoXd

Marín Valencia, J. J., Patiño Valencia, A. y Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. *Revista Universidad Católica de Oriente*, *31*(45), 84-99. https://revistas.uco.edu.co/index.php/uco/article/view/284

Mushtaq, A. (2010). Vulnerabilidades y preocupaciones de la seguridad en redes inalámbricas. *Security Technology, Disaster Recovery and Business Continuity*, *122*(1), 207-219. https://doi.org/10.1007/978-3-642-17610-4_23

Najar, Z. y Mir, R. (2021). Wi-Fi: WPA2 Security Vulnerability and Solutions. *Wireless Engineering and Technology*, 12, 15-22. https://doi.org/10.4236/wet.2021.122002

Nikolov, L. G. (2018). Wireless network vulnerabilities estimation. *Security & Future*, *2*(2), 80-82. https://stumejournals.com/journals/confsec/2018/2/80

Ochoa, J. M. (6 de mayo de 2024). *Tipos de vulnerabilidades en el ámbito corporativo*. https://is.gd/xpAIDJ

Ramírez, I. (2 de julio de 2024). *¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene?* https://is.gd/TwAW9C

Zihadul, I., Rahman, K. M. A., Ibrahim, H. y Rabbi, H. (2021). Analysis the importance of VPN for Creating a Safe Connection Over the World of Internet. *International Journal of Advanced Research in Computer and Communication Engineering*, *10*(10), 2319-5940. https://dx.doi.org/10.17148/IJARCCE.2021.101017

AUTOR:

Antonio Porras Pérez:
Universidad de Granada.

Ingeniero informático especializado en Ingeniería del Software por la Universidad de Córdoba con experiencia en el desarrollo de programas y gestión de dispositivos para la conexión de redes. Actualmente desempeño mis funciones como técnico especialista en aulas de informática en la Universidad de Granada y cursando el doctorado en Tecnologías de la Información y la Comunicación.

aporras@ugr.es