XV Jornadas de Ingeniería Telemática.
JITEL 2021.
Universidad de A Coruña.

Actas de las XV Jornadas de Ingeniería Telemática (JITEL 2021), A Coruña (España), 27-29 de octubre de 2021.

Auditoría Wi-Fi basada en placas de bajo coste

Anxo Otero, Carlos Dafonte, Diego Fernandez, Fidel Cacheda, Manuel López-Vizcaíno, Francisco J. Novoa
Centro de Investigación en Tecnologías de la Información y las Comunicaciones (CITIC)
Facultad de Informática
Departamento de Ciencias de la Computación y Tecnologías de la Información
Universidade da Coruña

anxo.oterod@udc.es, carlos.dafonte@udc.es, diego.fernandez@udc.es, fidel.cacheda@udc.es, manuel.fernandezl@udc.es, francisco.javier.novoa@udc.es

En la actualidad, el uso de redes inalámbricas crece exponencialmente en entornos empresariales de todo tipo. Si bien es cierto que existen una gran cantidad de soluciones en el ámbito de auditoría de redes inalámbricas para grandes organizaciones, las soluciones que existen para las pequeñas empresas son escasas, y esto junto a la falta de conocimientos y experiencia en Tecnologías de la Información (TI) del personal de dichas organizaciones, provoca que este tipo de empresas se encuentren habitualmente en un nivel de riesgo en ciberseguridad alto.

En este contexto desarrollamos una herramienta que tiene como objetivo la auditoría de redes inalámbricas en entornos empresariales, basada en *hardware* de bajo coste y que requiera, únicamente, un nivel básico de conocimientos de TI y ciberseguridad por parte del usuario.

El diseño arquitectónico de la herramienta se basa en un sistema distribuido de dispositivos de bajo coste que permite monitorizar y auditar el entorno inalámbrico y mostrar la información obtenida al usuario de forma inteligible.

En la implementación actual utilizamos Raspberry Pi 3B+ como placas de bajo coste, a las que conectamos antenas Wi-Fi externas, que facilitan la captura de tráfico de red. Posteriormente, procesamos dicho tráfico y los resultados obtenidos se muestran al usuario mediante una interfaz web.

Tras la finalización del desarrollo de la herramienta, hemos realizado pruebas, tanto en un entorno real como en un entorno simulado, lo que nos ha permitido obtener interesantes conclusiones acerca del trabajo realizado.

***Palabras Clave*- Wi-Fi, auditoría, placas de bajo coste**

I. Introducción

En la actualidad, el uso de las redes inalámbricas crece exponencialmente en entornos empresariales de todo tipo, fundamentalmente en las empresas de pequeño tamaño (menos de 10 trabajadores), denominadas microPYMEs. Las características que proporciona esta tecnología (movilidad, facilidad de despliegue y ahorro de coste frente a las redes cableadas) provocan que sean la opción de conectividad preferida en este tipo de organizaciones.

Sin embargo, en este tipo de entidades rara vez se realiza una auditoría o evaluación de seguridad y es habitual que sus miembros no sean conscientes de los riesgos que implica el uso de las redes inalámbricas [1].

Tal y como se describe en "*Survey on WiFi intrastructure attack*" [2], los ataques *"Rogue AP"* o *"Evil Twin"*, *"ARP spoofing"* y *"WiFi MiTM"* son cada vez más habituales. Además, es necesario tener en cuenta las amenazas *DoS* que se implementan a través de ataques de deautenticación, desasociación, falsa autenticación o *"beacon flood"*, son difícilmente evitables.

Los grandes proveedores de infraestructura LAN inalámbrica (WLAN) como Cisco Aironet, HPE-Aruba, Huawei o Fortinet proporcionan soluciones de seguridad avanzadas que ayudan a mitigar estas amenazas y que facilitan la realización de auditorías detalladas. Existen también productos orientados a empresas de tamaño intermedio como Cisco Meraki o Unify de Ubiquiti que también proporcionan productos de monitorización y evaluación de seguridad. Sin embargo, estas soluciones no son habituales en las microPYMEs debido a su coste y al desconocimiento acerca de los riesgos que entraña el uso de WLAN. En España, el 94,8% de las empresas son de este tipo [2] lo que implica que existe una gran cantidad de organizaciones que utilizan tecnologías Wi-Fi en situación de riesgo de seguridad.

En este último año, debido a la pandemia ocasionada por el SARS-CoV-2 (COVID-19), la mayor parte de la población mundial se ha visto obligada a confinarse en sus casas propiciando el uso de redes inalámbricas domésticas para llevar a cabo tareas de trabajo en remoto [3]. Normalmente, estas WLAN son proporcionadas por los proveedores de servicios de Internet y los usuarios desconocen cómo configurarlas o personalizarlas, así como el nivel de seguridad que ofrecen. De nuevo, esta realidad genera una situación de riesgo difícilmente mitigable con soluciones de bajo coste.

En este contexto surge la idea de desarrollar una herramienta de auditoría Wi-Fi, económica y de fácil uso.

II. OBJETIVOS

El objetivo principal del trabajo que estamos presentando es desarrollar un sistema basado en placas de bajo coste que realice auditorías de seguridad inalámbricas con una intervención mínima del usuario.

Para ello establecemos unos objetivos y funcionalidades básicas de la herramienta:

- Extracción de características de cada red detectada: para cada red inalámbrica se muestra una lista de características básicas, así como un estudio de la seguridad de la red y de la calidad y potencia de su señal.
- Inventario de dispositivos: generación de un listado de dispositivos en cada WLAN, previa autenticación, tratando de identificar sus características.
- Interfaz web: implementación de una interfaz web ligera y sencilla que muestre al usuario de forma inteligible el estado de su red desde el punto de vista de seguridad
- Envío de información a un servidor central: desarrollo de un mecanismo de envío de información a un servidor central por medio de una API REST que permita centralizar la información de las diferentes áreas del entorno.

III. DESARROLLO

En este apartado detallaremos el proceso de desarrollo de la herramienta. Inicialmente, presentaremos su arquitectura, las tecnologías utilizadas y, a continuación, explicaremos cada uno de los módulos que la conforman.

A. *Arquitectura*

El sistema está diseñado para ser escalable, es decir, para adaptarse a redes inalámbricas que dan cobertura a superficies de diferente tamaño. En el caso de entornos con una superficie limitada, es suficiente utilizar un dispositivo de auditoría, pero sin embargo si la superficie es extensa, es preciso analizar redes inalámbricas en diferentes localizaciones físicas (diferentes sucursales) o se trata de un edificio de varias plantas, es necesario desplegar varios dispositivos de monitorización o agentes.

Por lo tanto, la arquitectura consta de uno o más dispositivos, llamados agentes, cuya función es monitorizar el tráfico de red, extrayendo información relevante que se envía a un servidor central, tal y como se puede observar en la Figura 1.

Estos agentes envían la información clave recopilada y preprocesada a un servidor de almacenamiento central, utilizando una interfaz API REST. Este repositorio central permitirá, en un futuro, aplicar técnicas de Inteligencia Artificial para detectar anomalías o posibles intrusiones.

La ventaja que proporciona esta aproximación es que el sistema de auditoría se adapta a los cambios y el posible crecimiento de la red.

B. *Tecnologías utilizadas*

En este apartado enumeramos las tecnologías utilizadas para el desarrollo de esta herramienta.

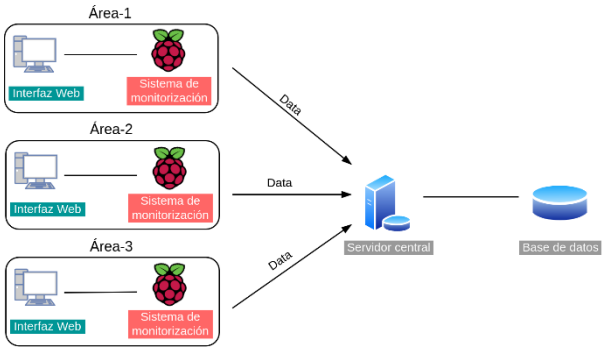

Figura 1. Arquitectura básica

El lenguaje de programación utilizado ha sido *Python*. Su elección se ha fundamentado en la existencia de librerías que han facilitado enormemente el desarrollo, así como por su versatilidad y facilidad para programar de forma ágil y rápida.

Merece una especial mención la librería *Scapy* [5], que permite la manipulación completa de paquetes de red. Es capaz de crear y decodificar paquetes de una gran cantidad de protocolos, transmitirlos, capturarlos o emparejar solicitudes y respuestas.

Proporciona funcionalidades para implementar la mayoría de las tareas clásicas de reconocimiento como *scanning*, *tracerouting*, *probing*, *network discovery*, entre otras.

Para la interfaz web se ha elegido Django [6] y se ha seguido el patrón de diseño *Model-View-Controller*. Para la ejecución de tareas en *background* durante largos periodos de tiempo, sin bloquear la comunicación con el usuario, se ha utilizado Celery [7], que es una librería de código abierto que permite la implementación de colas de tareas de forma asíncrona y facilita la ejecución de operaciones en tiempo real.

En la implementación de la interfaz web se ha utilizado también HTML, CSS, Javascript, JQuery y las librerías Javascript Vis.js [8], para la visualización dinámica de las redes y sus componentes, y Chart.js [9], para la visualización de datos de forma gráfica.

Para el almacenamiento de los datos de la aplicación web se ha elegido PostgreSQL, dada su alto nivel de integración con Django y para el almacenamiento de la información del tráfico recopilado se ha elegido un sistema de gestión de base de datos no relacional como MongoDB, que facilita la lectura y escritura de datos en formato JSON.

Para facilitar el despliegue de la herramienta en múltiples dispositivos hemos empaquetado la aplicación en *docker*. En la implementación actual del sistema utilizamos como plataforma hardware para los agentes una placa *Raspberry Pi 3B+* con un adaptador de red inalámbrico *CSL-AC1200-USB 3.0 Dual Band WLAN Stick"*, que contiene un chip *Realtek8812AU.*

C. *Agentes o dispositivos de captura*

Cada agente se compone de cuatro elementos: un sistema de escucha, un procesador de información, una base de datos y una aplicación web.

El sistema de escucha permite al dispositivo capturar todo el tráfico de red del área en la que se encuentra, de forma pasiva, mediante un adaptador de red externo. Existe

una gran cantidad de tráfico que es irrelevante para propósitos de auditoría y monitorización, por lo que el agente dispone de una funcionalidad de procesado que se encarga de analizar las tramas útiles y extraer la información más importante de cada una de ellas.

Además, cada dispositivo dispone de una base de datos en la que se almacena la información extraída en la escucha, una vez que ha sido procesada.

Cada agente dispone también de una interfaz web, que muestra la información recopilada, procesada y almacenada al usuario mediante un *dashboard* ligero y amigable.

Por último, periódicamente, el agente hace un volcado de la información recopilada al servidor central.

En resumen, cada dispositivo de captura tiene como función procesar y transformar toda la información recibida, guardarla en una base de datos y mostrarla mediante una interfaz web. Además, se encarga de enviar los datos almacenados cada cierto tiempo a un servidor central, de manera que podremos tener toda la información de diferentes áreas de una organización en un sistema centralizado. Este comportamiento permite tener una visión global de todo el entorno.

A continuación, ofrecemos los detalles de implementación de cada uno de estos cuatro módulos funcionales que incluye cada agente.

D. *Módulo de captura de tráfico*

Como hemos comentado previamente, cada agente implementa un sistema de captura de tráfico de red mediante un adaptador de red externo, que proporciona las capacidades físicas para recibir el tráfico inalámbrico. Hemos utilizado la función *sniff()* de la librería *Scapy*, para capturar, de forma pasiva, todo el tráfico de red que está a nuestro alcance y la función *channel_hooper()* nos permite hacer un barrido por un conjunto de frecuencias predeterminadas, de modo que aplicación podrá recibir paquetes de señales inalámbricas de cualquier frecuencia predefinida.

E. *Módulo de análisis de tráfico*

Una vez capturado el tráfico, es necesario analizarlo para clasificarlo y utilizarlo para alguna de las funcionalidades que se especifican a continuación:

- Detección de WLAN y extracción de su información básica: en este caso es necesario procesar las tramas baliza (*beacon frames*) capturadas. Su contenido se transmite en texto claro y contienen información básica acerca de ellas. La función de Scapy *beacon_packet()* permite extraer las características de este tipo de tramas. Entre otros, los datos que se pueden obtener son: SSID, BSSID, fabricante y ratios de transferencia soportados. Además, podemos obtener las características de la señal física que emite un punto de acceso concreto. Para ello, hacemos uso de la cabecera *Radiotap,* que contiene toda la información relacionada con la señal emitida. Entre otros permite obtener los siguientes datos: RSSI, canal utilizado, canal central, frecuencia, ancho de banda utilizado (20 o 40 MHz.), espectro o atenuación de la señal (FSPL, *Free Space Path Loss*). Finalmente, podemos obtener también las características de seguridad de las redes detectadas, por ejemplo: protocolo de seguridad, sistema de autenticación y algoritmo de cifrado.
- Detección de dispositivos conectados a la red (sin autenticación previa): analizando las tramas de datos y control capturadas previamente podemos generar el inventario de dispositivos conectados, a partir de las direcciones MAC origen y destino.
- Detección de tráfico potencialmente peligroso: clasificamos en este caso las tramas de deautenticación debido a que se utilizan en múltiples ataques de DoS. Almacenamos información sobre el punto de acceso al que se han enviado las tramas y cuál es la razón indicada para la deautenticación. Esta información nos ayuda a determinar si las tramas son legítimas o forman parte de un ataque.

F. *Módulo de inventario tras autenticación*

Si bien anteriormente hemos indicado que es posible realizar un inventario de dispositivos sin completar la asociación con un punto de acceso, la información que podemos obtener de estos dispositivos es muy limitada. Además, en ese contexto (no asociados a un punto de acceso) se puede producir un escenario de "nodo oculto", ampliamente referenciado en la literatura, y habría dispositivos que no serían detectados.

Dado que esta herramienta está diseñada como un elemento de auditoría que se instalará en entornos controlados, existe la posibilidad de que el agente se asocie al punto de acceso, disponiendo entonces de conectividad a nivel de enlace en la WLAN a evaluar.

Las funcionalidades que proporciona este módulo son:

- Obtención del inventario de dispositivos, implementando una función que realiza peticiones *arp* a todas las IPs de la red asociada a la WLAN.
- Determinación del sistema operativo de cada dispositivo detectado, mediante las funciones proporcionadas por la librería "nmap3" para Python.

II. Resultados

Debido a que este trabajo está todavía en desarrollo, los resultados obtenidos son bastante limitados. Hemos probado una implementación de la herramienta en la que utilizamos un único agente que hemos probado en dos entornos: un entorno simulado y un laboratorio de investigación de la Facultad de Informática de la Universidade da Coruña (UDC).

A continuación, se detallan los datos más relevantes de ambas auditorías.

A. Entorno simulado

El objetivo de esta prueba es validar la capacidad de la herramienta para realizar todas las funcionalidades indicadas previamente, en especial, la detección de posibles amenazas. Para ello, simulamos un entorno de red inalámbrica de una microPYME, basada en una WLAN proporcionada por un ISP, y lanzamos diferentes simulaciones de ataque.

Los resultados obtenidos son los siguientes:

- Detección de redes inalámbricas: realizamos un escaneo durante 1 hora y detectamos 119 puntos de acceso.
- Simulamos un ataque de tipo *beacon flood* y la herramienta es capaz de detectarlo, al identificar posibles WLAN con SSID sumamente inusuales, sin ningún tipo de seguridad y con valores de señal emitidos completamente anómalos.
- En cuanto a la información referente a las redes inalámbricas asociadas a los puntos de acceso detectados, cabe destacar una gran variabilidad de las características físicas (e.g. RSSI), lo que se corresponde con las previsiones que teníamos. Dichos valores dependen, fundamentalmente, de la distancia a la que se encuentran los puntos de acceso. Los dispositivos finales detectados son, en su mayoría PCs y dispositivos móviles.
- Con respecto a la seguridad de las redes detectadas, aunque existe una cierta variabilidad, en la mayor parte de los casos se trata de redes que implementan el *framework* de seguridad WPA2, con autenticación basada en clave precompartida y un algoritmo de cifrado CCMP.
- En cuanto al análisis de la red inalámbrica propia, nos llama la atención la detección de 10.192 tramas de deautenticación recibidas en el espacio de una hora, lo que claramente indica que un elemento externo está lanzando un ataque DoS de deautenticación. Somos capaces de identificar la dirección MAC del agresor.

B. Entorno de laboratorio en la Facultad de Informática

En este entorno repetimos las tareas de auditoría realizadas anteriormente en el entorno simulado. Los resultados que hemos obtenido son:

- Detección de 42 puntos de acceso y 21 dispositivos finales. La mayor parte de los PAs detectados están vinculados a las redes inalámbricas oficiales de la UDC, como “eduroam”, “udcportal”, “udcodcencia” y “udceventos”.
- Con respecto a la seguridad, se observa que la mayor parte de las redes disponen de una configuración de seguridad fiable, puesto que implementan WPA2 y autenticación basada en usuario. Merece especial atención la red “udcportal”, puesto que podemos observar que se trata de una red abierta, que no implementa ningún tipo de configuración de seguridad, a nivel WLAN (sabemos que se trata de una red abierta que proporciona la UDC para permitir la conectividad a usuarios con problemas en las otras WLAN y que se trata de una solución basada en portal cautivo)

III. Conclusiones

En estos momentos podemos concluir que los objetivos establecidos cuando comenzamos este trabajo se han cumplido. Hemos desarrollado una herramienta con un coste muy contenido, que permite llevar a cabo auditorías de seguridad de redes inalámbricas en diferentes entornos. Somos capaces de detectar las redes inalámbricas que nos radian (tanto propias como ajenas) y determinar sus características, lo que puede ayudar a los usuarios a cambiar características físicas de su red (e.g. canales) y mejorar el rendimiento de su red.

Somos capaces también de detectar tráfico anómalo e inventariar, de forma detallada, los dispositivos de nuestra red inalámbrica.

En un futuro inmediato nuestro objetivo es continuar trabajando en la realización de pruebas y a medio plazo pretendemos integrar este trabajo con otros proyectos centrados en la detección temprana de ataques como [10].

Agradecimientos

Esta investigación ha sido financiada por el Ministerio de Economía y Competitividad de España y fondos FEDER de la UE (Proyecto PID2019-525 111388GB-I00) y por el Centro de Investigación de Galicia "CITIC", financiado por la Xunta de Galicia y la UE (Fondo de Desarrollo Regional Europeo - Programa Galicia 2014-2020), mediante la concesión de ED431G 2019/01.

Referencias

[1] C. Boletsis, R. Halvorsrud, J. B. Pickering, S. Phillips y M. Surridge, «Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assesment,» de *16th International Joint Conference on Computer Vision, Imaging and Computre Graphics Theory and Applications*, 2021.

[2] R. Guo, «Survey on WiFi infrastructure attacks,» *International Journal of Wireless and Mobile Computing,* vol. 16, nº 2, 2019.

[3] Organización para la Cooperación y el Desarrollo Económico (OCDE), «Entrepreneurship at a glance,» 2017.

[4] T. Weil y S. Murugesan, «IT Risk and Resilience—Cybersecurity Response to COVID-19,» *IT Professional,* vol. 22, nº 3, pp. 4-10, 2020.

[5] P. Biondi, «Scapy,» 2021. [En línea]. Available: https://www.scapy.net. [Último acceso: 01 06 2021].

[6] A. Makarudze, A. Basset, C. Kirby, W. Vincent, K. Nakamura, M. Eti-mfon y Z. Anderle, «Django Software Foundation,» 2021. [En línea]. Available: https://djangoproject.com. [Último acceso: 01 06 2021].

[7] A. Solem, «Celery - Distributed Task Queue,» 2018. [En línea]. Available: https://docs.celeryproject.org/. [Último acceso: 01 06 2021].

[8] Vis.js Community, «vis.js,» 2021. [En línea]. Available: https://visjs.org. [Último acceso: 01 06 2021].

[9] Chart.js Community, «Chart.js,» 2021. [En línea]. Available: https://chartjs.org. [Último acceso: 01 06 2021].

[10] M. López-Vizcaíno, F. J. Novoa, D. Fernández, V. Carneiro y F. Cacheda, «Early Intrusion Detection for OS Scan Attacks,» de *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, 2019.