Prototipo MITM evil twin attack

*

1st Freddy Tacuri
Maestría en Software.
Universidad Politécnica Salesiana.
Quito, Ecuador
ftacurip@est.ups.edu.ec

2nd Fausto Amaguaña
Maestría en Software.
Universidad Politécnica Salesiana.
Quito, Ecuador
famaguana@est.ups.edu.ec

***Abstract*—Un tipo de ataque informático conocido como Evil Twin, el cual consiste en crear un punto de acceso Wi-Fi no autorizado que se asemeje a uno legítimo, con el objetivo de interceptar las comunicaciones inalámbricas. Este tipo de ataque puede utilizarse para obtener contraseñas de usuarios desprevenidos a través de un portal cautivo que muestra una página web falsa y engaña a los usuarios para que ingresen sus contraseñas de acceso a la red Wi-Fi. El ataque se lleva a cabo clonando el punto de acceso legítimo, eliminando la contraseña y desautenticando a los usuarios para que se conecten automáticamente al punto de acceso falso. Cuando los usuarios abren el navegador e intentan navegar, son redirigidos a la página web fraudulenta, donde se les solicita su contraseña. Si la contraseña es correcta, el ataque finaliza.**

***Index Terms*—Palabras claves— Gemelo malvado, ataque informático, denegación de servicio, fraude, PSK.**

I. Introducción

Un ataque de Evil Twin consiste en crear un punto de acceso no autorizado Wi-Fi que parece ser legítimo, creado para escuchar las comunicaciones inalámbricas. Este tipo de ataque puede ser utilizado para conseguir las contraseñas de los usuarios desprevenidos, mediante un portal cautivo que muestra una página web fraudulenta y logra atraer a los usuarios a ese sitio para que ingrese sus contraseñas de acceso a la red WiFi (PSK). La forma de trabajo de Evil Twin Attack (MITM Fake/Rouge AP) clona el punto de acceso dejándolo sin contraseña, se des-autenticara a los usuarios conectados al punto de acceso legítimo para que se contacten automáticamente al nuestro, cuando abran el navegador e intenten navegar, irán a la página web fraudulenta, una vez ponga la contraseña esta es verificada y si es la correcta finalizará el ataque.

II. Desarrollo de contenidos

Para este Prototipo MITM evil twin attack vamos a usar como referencia ejemplos de tipo académico. [3] que nos permita experimentar en un ambiente controlado. también usaremos trabajos de investigación. [7]

Antes de empezar con el desarrollo es necesario identificar cuáles son los pasos previos y requisitos mínimos para poder realizar el prototipo y posteriormente resaltar los resultados de este.

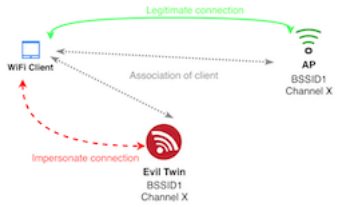

Fig. 1. Evil Twin. "Duplicate association of client." [7]

A. Procedimiento previo requerido.

Se necesitó ciertas configuraciones mínimas y preparar el ambiente para la ejecución del laboratorio, entre esos pasos están los que a continuación se mencionan:

- Descargar la máquina virtual de Kali Linux para el virtualizador de preferencia de la página oficial, en este caso se usará para VirtualBox. [8]

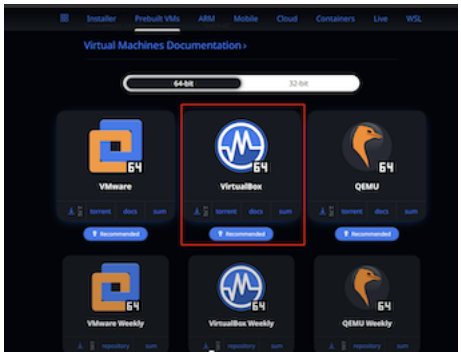

Fig. 2. Máquina Virtual VirtualBox

- Se procede a descomprimir en un directorio específico.
- Levantamos la VDI desde el VirtualBox.
- Configuramos el adaptador USB Wifi para que pueda ser utilizado dentro de la máquina virtual.
- Levantar el equipo físico.
- Configuración del equipo a realizar las pruebas con las credenciales solicitadas.

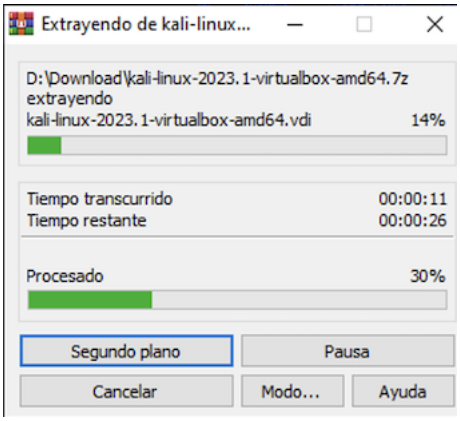

Fig. 3. Descomprimir archivo: kali-linux-2023-.1-virtualbox-amd64.7z.

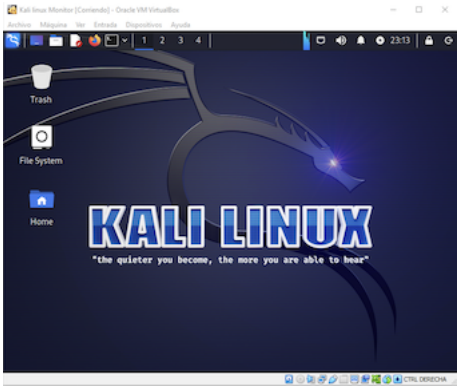

Fig. 4. KaliLinux.

III. Ejecución de ataque MiTM

- Descargar el repositorio de airgeddon que es un proyecto de código abierto con fines educativos.
- Ingresamos al directorio y ejecutamos el código bash con permisos SUDO.
- Ejecutamos Airgeddon.
- Se instalará las librerías faltantes.
- Poner antena en modo monitor Wifislax.
- Configuración de Airgeddon.
- Seleccionamos ATAQUE EVIL TWIN.
- Seleccionamos CON PORTAL CAUTIVO.
- Buscas todas las redes disponibles.

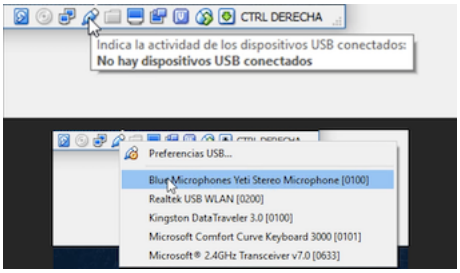

Fig. 5. Adaptador USB Wifi.

Fig. 6. Equipo TP-LINK TL-WR740N

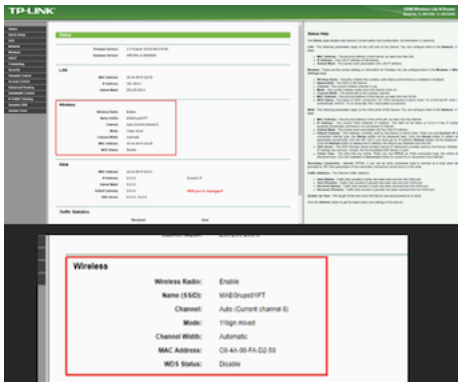

Fig. 7. Administración TP-LINK.

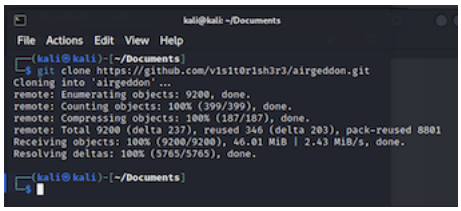

Fig. 8. Proyecto airgeddon

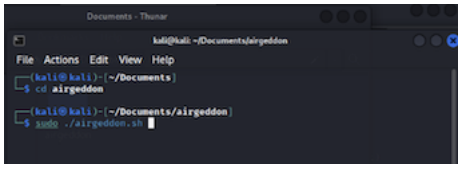

Fig. 9. Comandos de ejecución airgeddon.

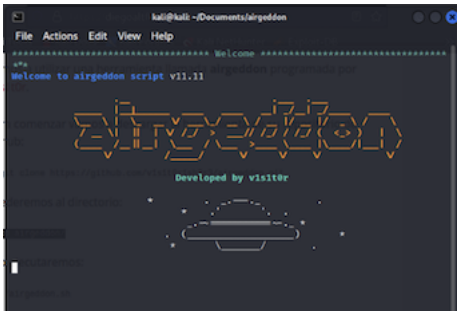

Fig. 10. Ejecución airgeddon.

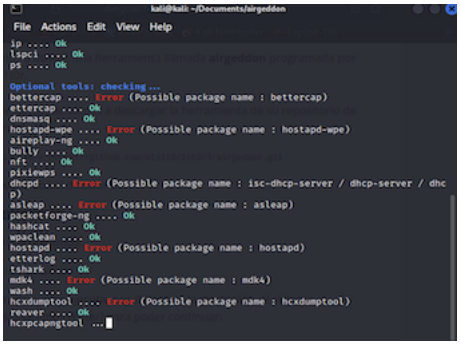

Fig. 11. Paquetes adicionales de airgeddona.

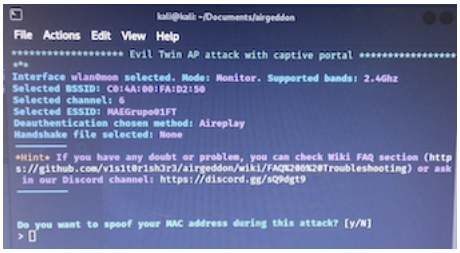

Fig. 12. Configuración Router modo Monitor.

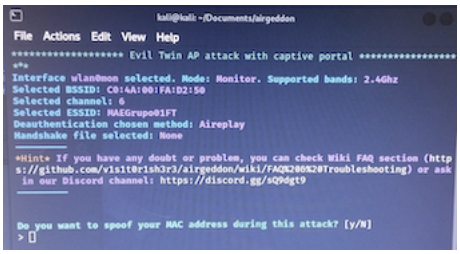

Fig. 13. Selecionamos Router modo Monitor.

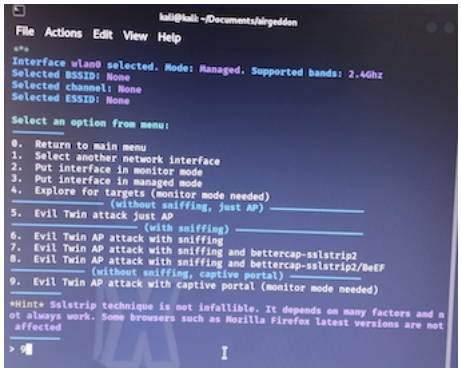

Fig. 14. Ataque evil twin.

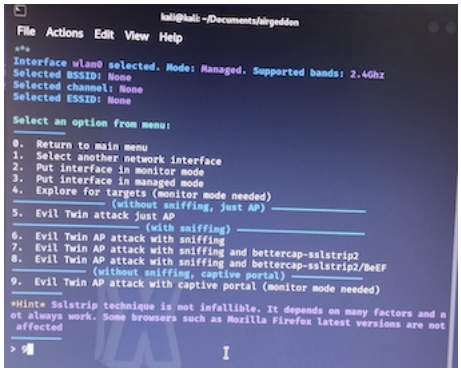

Fig. 15. Usamos portal cautivo.

- Seleccionamos la red a Clonar.
- Realizamos un ataque de desautenticación con aireplay.
- Configuración del ataque aireplay para varios dispositivo, falsificación de la dirección MAC y configuración del tiempo de ataque a 10 segundos, en este lapso de tiempo se expulsará a los clientes.
- Realizada la configuración capturará el handshake expulsando a los clientes. Ya ha expulsado del teléfono de pruebas, se conecto y ya tiene el handshake. Ahora preguntará dónde queremos que guarde la información, lo dejamos por defecto.
- Configuramos el idioma en el que va a aparecer el portal cautivo, seleccionamos español.
- Realizado esto ya está el ataque listo y en ejecución.

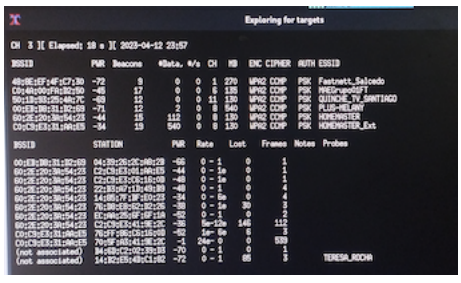

Fig. 16. Redes disponibles.

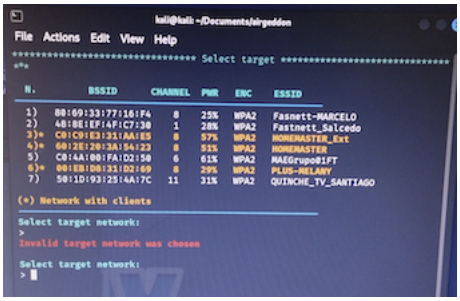

Fig. 17. Red a Clonar.

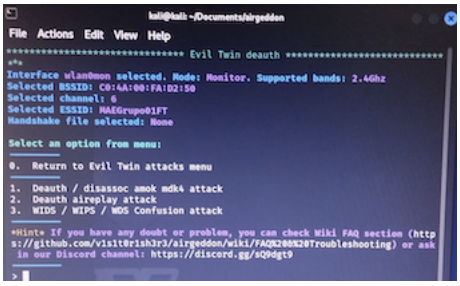

Fig. 18. Desautenticación con aireplay.

La red esta disponible pero no permite conexión. Se visualiza otra red con la señal al máximo, seleccionamos y conectamos. Escogemos que inicie sesión para navegar, y solicitará la contraseña de la red.

- Con el portal esperando capturar la contraseña, si ingresamos mal la contraseña no pasa nada, le dirá que la contraseña es incorrecta y que la vuelva a escribir.Error Evil Twin. En el caso que escriba bien la contraseña entonces le dirá que la contraseña es correcta, se guardará en un documento y la desconectará del AP que se ha

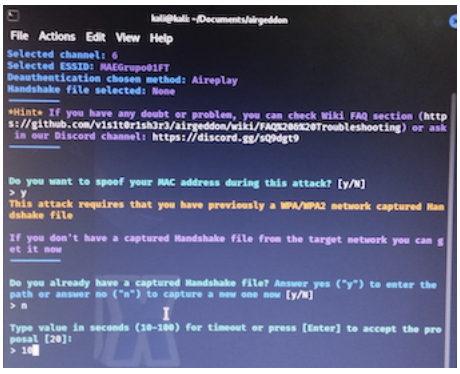

Fig. 19. Configuración para aireplay.

Fig. 20. Configuración de almacenamiento de información.

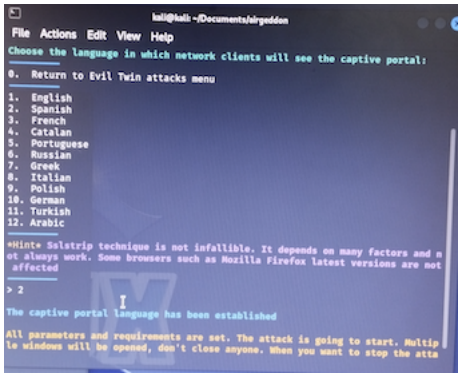

Fig. 21. Configuración del Idioma para el portal cautivo.

Fig. 22. Portal para captura de contraseña en teléfono móvil.

clonado y la conectará a la red real o valida.

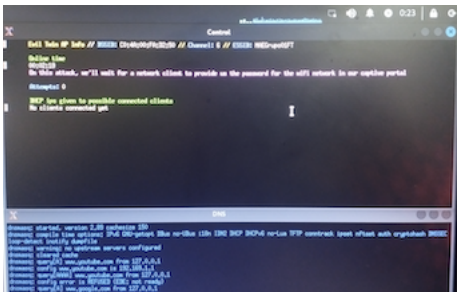

Fig. 23. Captura contraseña, conexión a red real con navegación.

IV. RESULTADOS Y ANÁLISIS

Actualmente el usar Wi-Fi ya sea en entornos públicos y privados se lo hace de forma natural, para revisar mensajes, navegar, comprar o trabajar, sin tener el conocimiento que puede ser víctima del ataque de gemelos malvados. Este ataque parte de encontrar una ubicación correcta para realizar un ataque, buscan lugares concurridos con Wifi gratuitos, siendo este escenario el ideal para clonar la red legítima y configurarla como una nueva cuenta con el mismos SSID, para que el usuario o cliente no dude en colocar sus credenciales en un portal cautivo y así el atacante obtener sus datos personales.
La capa MAC del protocolo 802.11 posee una debilidad inherente que la hace vulnerable a varios ataques de seguridad como denegación de servicio, ataque de desautenticación, ataques de inundación, punto de acceso no autorizado (RAP). [5]
Una solución para la detección y mitigación de gemelos malvados es ”EvilScout”, un marco de detección y mitigación que utiliza la información de la distribución de prefijos de IP por parte del LAP. EvilScout explota el potencial de SDN para la detección de un gemelo malvado sin necesidad de hardware adicional o modificaciones en el punto de acceso o el cliente. Además, la información que está disponible en el controlador SDN permite una detección de gemelos malvados simplificada y más precisa. [7]
Existen casos de estudios para la detección de ataques de gemelos malvados Wi-Fi del lado del usuario mediante monitoreo de canales inalámbricos aleatorios, el cliente inalámbrico puede probar los 11 canales Wi-Fi completos de la red 802.11 b/g para ETA con aproximadamente medio minuto. [10] Son soluciones sustentadas en procesos matemáticos que proponen reducir la complejidad del proceso de recopilación de huellas dactilares, utilizando el mecanismo de sabiduría colectiva y proponen un modelo de ubicación basado en puntos de referencia. [4], incluso hay casos de estudio donde se propone un novedoso mecanismo de reflexión TCP SYN bidireccional contra ETA multimodelo. El BiRe propuesto se puede realizar en el lado del cliente, no requiere ningún dispositivo de detección dedicado, no depende de ninguna característica de transmisión volátil como RTT , IAT, etc., y funciona tanto en redes abiertas como encriptadas para proporcionar a los usuarios detección en tiempo real. [2] WiFi o redes inalámbricas IEEE 802.11 es probablemente el tipo de red más popular para redes domésticas inalámbricas, así como para compartir redes públicas o de invitados, 802.11 deja espacio para implementaciones personalizadas con respecto a la fase de asociación WiFi, los proveedores de sistemas operativos tienden a priorizar las funciones de usabilidad en lugar de la seguridad. [1]
Todavía es posible realizar un ataque MiTM utilizando una técnica Evil Twin en muchas redes Wi-Fi en todo el mundo, con protocolo 802.11v. que es posible usarlo de manera malintencionada para realizar un ataque Evil Twin MiTM. Usando pruebas y simulaciones, se ha demostrado que, en comparación con el ataque de desautenticación, el método propuesto tiene las siguientes ventajas: (a) realiza silenciosamente el ataque MiTM al enfocarse en el objetivo sin molestar a otros usuarios, (b) amplía el alcance del ataque que ya no está relacionado con las intensidades de la señal recibida de la competencia, (c) no es fácil de detectar por los sistemas inalámbricos de detección de intrusos (WIDS), ya que puede enmascararse como un proceso legítimo, (d) puede ser efectivo desde largas distancias mediante el uso de antenas direccionales siempre que se mantenga el umbral RSS de -70 dBm. Los defensores pueden intentar mitigar el ataque utilizando Management Frame Protection como se describe en (IEEE 2009), en caso de que sea compatible con el AP. [9]

V. CONCLUSIONES

- Este ataque tiene un alto porcentaje de efectividad, es así que las empresas como Kaspersky expone a sus clientes soluciones. Una VPN o red privada virtual lo protege de los ataques de gemelos malvados al cifrar sus datos en Internet sin importar la red que esté utilizando. Una VPN confiable como Kaspersky Secure Connection encripta o codifica su actividad en línea antes de enviarla a la red, lo que hace que sea imposible que un pirata informático la lea o la entienda. También puede asegurarse de tener instalado un producto de seguridad integral. Kaspersky Internet Security protege su dispositivo de una amplia gama de ciberamenazas. Kaspersky Internet Security recibió dos premios AV-TEST por el mejor rendimiento y protección para un producto de seguridad de Internet en 2021 . En todas las pruebas, Kaspersky Internet Security mostró un rendimiento y una protección sobresalientes contra las ciberamenazas. [6]
- Evitar los puntos de acceso Wi-Fi no seguros, evitar conectarse a una red pública, evitar los puntos de acceso marcados como ’No seguros’.
- Utilizar su propio punto de acceso en lugar de Wi-Fi público especialmente en entornos laborales, lo protegerá de los ataques gemelos malvados.
- Verifique las notificaciones de advertencias al intentar conectarte a una red.
- Evitar las conexión automática en los dispositivos, Esto puede ser peligroso en lugares públicos. En su lugar,

deshabilite la función de conexión automática cuando esté fuera de una red segura ya sea doméstica o de trabajo.

- Evite iniciar sesión en cuentas privadas en Wi-Fi público:
- Evite realizar transacciones financieras o personales en Wi-Fi público.
- Utilizar la autenticación multifactor.
- Usar una VPN especialmente en ambientes laborales.

REFERENCES

[1] Association Attacks in IEEE 802.11: Exploiting WiFi Usability Features, shorttitle = Association Attacks in IEEE 802.11, url = https://bibliotecas.ups.edu.ec:3401/chapter/10.1007/978-3-030-55958-$8_6, doi = 10.1007/978-3-030-55958-8_6, abstract = , language = en, urldate = 2023-04-23, booktitle = Socio-TechnicalAspectsinSecurityandTrust, publisher = Springer, Cham,$
$author = Chatzisofroniou, GeorgeandKotzanikolaou, Panayiotis, year = 2021, pages = 107--123, file = 2021-AssociationAttacksinIEEE802.11, .$

[2] BiRe: A client-side Bi-directional SYN Reflection mechanism against multi-model evil twin attacks, volume = 88, issn = 0167-4048, shorttitle = BiRe, url = https://www.sciencedirect.com/science/article/pii/S0167404819301658, doi = 10.1016/j.cose.2019.101618, abstract = , language = en, urldate = 2023-04-23, journal = Computers & Security, author = Lu, Qian and Jiang, Ruobing and Ouyang, Yuzhan and Qu, Haipeng and Zhang, Jiahui, month = jan, year = 2020, keywords = Evil twin attack, Man-in-the-middle attack, Rogue access point detection, Wi-Fi security, WLAN Security, pages = 101618, file = ScienceDirect Snapshot:files/144/S0167404819301658.html:text/html,.

[3] Cómo CLONAR REDES WIFI con EVIL TWIN Wifislax | Actualizado 2021, url = https://escuelanuevoshackers.com/curso-hacking-wifi/como-clonar-redes-wifi-con-evil-twin-wifislax/, abstract = Evil Twin, la herramienta que hará que tengas WIFI GRATIS, language = es, urldate = 2023-04-23, journal = Escuela Nuevos Hackers, month = jan, year = 2021, file = Snapshot:files/126/como-clonar-redes-wifi-con-evil-twin-wifislax.html:text/html,.

[4] Detecting Evil-Twin Attack with the Crowd Sensing of Landmark in Physical Layer, url = https://bibliotecas.ups.edu.ec:3401/chapter/10.1007/978-3-030-05063-$4_19, doi = 10.1007/978-3-030-05063-4_19, abstract = , language = en, urldate = 2023-04-23, booktitle = AlgorithmsandArchitecturesforParallelProcessing, publisher = Springer, Cham,$
$author = Wang, ChundongandZhu, LikunandGong, year = 2018, pages = 234--248, file = , .$

[5] An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks, volume = 25, copyright = 2018 Springer Science+Business Media, LLC, part of Springer Nature, issn = 1572-8129, url = https://bibliotecas.ups.edu.ec:3401/article/10.1007/s10776-018-0396-1, doi = 10.1007/s10776-018-0396-1, abstract = , language = en, number = 2, urldate = 2023-04-23, journal = Int J Wireless Inf Networks, author = Agarwal, Mayank and Biswas, Santosh and Nandi, Sukumar, month = jun, year = 2018, note = Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 2 Publisher: Springer US, pages = 130–145, file = Full Text PDF:files/136/Agarwal et al. - 2018 - An Efficient Scheme to Detect Evil Twin Rogue Acce.pdf:application/pdf,.

[6] Evil twin attacks and how to prevent them, url = https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks, abstract = An evil twin attack is a cyberattack that works by tricking users into connecting to a fake Wi-Fi access point. Learn about evil twin hacking & how to protect yourself., language = es, urldate = 2023-04-22, journal = www.kaspersky.com, month = apr, year = 2023, note = Section: Resource Center, file = Snapshot:files/124/evil-twin-attacks.html:text/html,.

[7] Evilscout: Detección y mitigación de evil twin attack en wifi habilitado para sdn, autor=Shrivastava, Pragati y Jamal, Mohd Saalim y Kataoka, Kotaro, journal=Transacciones IEEE sobre gestión de redes y servicios, año=2020, volumen=17, numero=1, páginas = 89-102, doi=10.1109/TNSM.2020.2972774.

[8] Get Kali, url = https://www.kali.org/get-kali/, abstract = Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments., language = English, urldate = 2023-04-17, journal = Kali Linux, file = Snapshot:files/122/get-kali.html:text/html,.

[9] A novel Evil Twin MiTM attack through 802.11v protocol exploitation, volume = 130, issn = 01674048, url = https://linkinghub.elsevier.com/retrieve/pii/S0167404823001712, doi = 10.1016/j.cose.2023.103261, language = en, urldate = 2023-04-23, journal = Computers & Security, author = Louca, Constantinos and Peratikou, Adamantini and Stavrou, Stavros, month = jul, year = 2023, pages = 103261, file = Louca et al. - 2023 - A novel Evil Twin MiTM attack through 802.11v prot.pdf:files/141/Louca et al. - 2023 - A novel Evil Twin MiTM attack through 802.11v prot.pdf:application/pdf,.

[10] User-side wi-fi evil twin attack detection using random wireless channel monitoring, author=Nakhila, Omar and Zou, Cliff, booktitle=MILCOM 2016 - 2016 IEEE Military Communications Conference, year=2016, volume=, number=, pages=1243-1248, doi=10.1109/MILCOM.2016.7795501.