Análisis de Vulnerabilidades en Sistemas de Automatización del Hogar

Geovanny Manuel García Villafuerte

Guía: Roque Hernández

Presentado como parte de los requisitos para el Título de Magíster en Ciberseguridad.

CES: RPC-SE-01-N°.014-2020. Cohort2 2022 - 2023.

Correo electrónico del autor: geovanny.garcia@casagrande.edu.ec Guayaquil,

4/Marzo/23.

Introducción

Las casas inteligentes

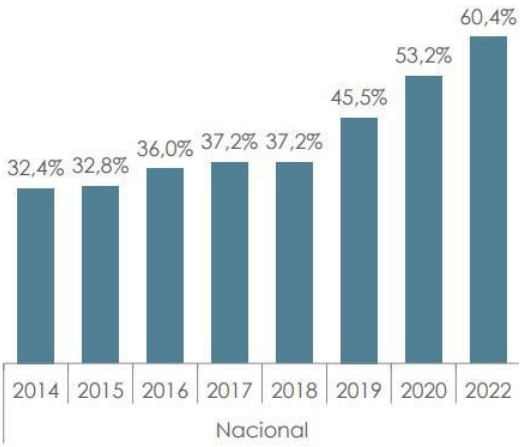
Las casas inteligentes (también conocidas como hogares o viviendas inteligentes) son hogares equipados con dispositivos tecnológicos que les permite automatizar y controlar varios sistemas, equipos y electrodomésticos. Estos sistemas pueden ser controlados desde una aplicación móvil o un panel de control centralizado, y pueden incluir:

- Sistemas de iluminación inteligente que se pueden ajustar en función de las preferencias de los residentes, el tiempo y la actividad que se realiza en la habitación.
- Termostatos inteligentes que ajustan la temperatura automáticamente para mejorar la eficiencia energética y el confort de los habitantes.
- Sistemas de seguridad inteligentes que incluyen cámaras de vigilancia, sensores de movimiento y puertas de entrada inteligentes para mantener a los habitantes seguros.
- Electrodomésticos inteligentes que se pueden controlar desde una aplicación móvil, como lavadoras, secadoras, refrigeradores y cocinas.

El uso de la tecnología en los hogares ha crecido exponencialmente como consecuencia de la pandemia y la transformación digital, de acuerdo con el informe de "Tecnologías de la Información y comunicación" publicado por el INEC en el 2022 el uso del equipamiento tecnológico en los hogares se ubicó en 40.4% comparado con el 37.5 % en el 2014, así como el acceso a internet en los hogares se ubicó en 60.4% de la población a nivel nacional.

En la siguiente gráfica se refleja el creciente uso del acceso a internet en los hogares.

Ilustración 1
Hogares con acceso a internet



Estos datos nos demuestran que el uso de la tecnología en los hogares y el acceso a internet son cada vez más comunes, sin embargo, existe un gran desconocimiento de los riesgos que existen en la red y cómo establecer una conexión segura para evitar el robo de información, estafas, extorsión o incluso se podría ver afectada nuestra integridad física al compartir información sensible como nuestra ubicación o rutina diaria.

El objetivo de este documento es demostrar cómo se puede vulnerar la seguridad de la red en el hogar y cuáles podrían ser las medidas que se pueden implementar para proteger la integridad de la información y los dispositivos conectados.

Todas las materias ofrecidas en la maestría de Ciberseguridad contribuyeron con conocimientos para el desarrollo de este proyecto, sin embargo, las siguientes materias otorgaron herramientas específicas para su implementación.

Ciberseguridad Ubicua la cual permitió conocer cómo los dispositivos se comunican entre sí y cómo esa comunicación puede ser vulnerada.

Las materias **Hacking Ético y Análisis del Ciberataque** y **Ciberseguridad en Entornos Industriales** presentaron las herramientas y conocimientos necesarios para analizar y comprender cómo la explotación de vulnerabilidades puede afectar el entorno. Por último, la materia de **Estrategias y Políticas Multilaterales** fue necesaria para comprender cómo enfocar las estrategias que permitan prevenir los diferentes tipos de ciberataques y cómo las políticas y las normas que existen en nuestro país pueden ser aplicadas.

Desarrollo

En el siguiente capítulo se describe de manera detallada las materias de la maestría que contribuyeron al desarrollo de este proyecto.

La materia de Ciberseguridad Ubicua describe cómo los dispositivos interactúan entre sí y como es necesario implementar mecanismos de seguridad, que permitan proteger los sistemas y los dispositivos de información de amenazas cibernéticas en cualquier lugar y momento (Ortega Candel, 2021).

La ciberseguridad ubicua implica el monitoreo y la detección constante de amenazas de seguridad, incluyendo virus informáticos, malware, y ataques. Para el desarrollo de este proyecto, se utilizaron diversas técnicas y herramientas de seguridad aprendidas en la materia, como el reconocimiento de tráfico a través de herramientas de software como wireshark. Además, se revisaron herramientas de cifrado, y autenticación de usuarios, se aprendió sobre la gestión de identidades y accesos, la detección de intrusiones y la respuesta a incidentes de seguridad.

Otra de las materias dictadas en la maestría de Ciberseguridad fue la de Hacking Ético y Análisis del Ciberataque, la cual nos permitió obtener habilidades y conocimientos en seguridad informática para identificar y solucionar vulnerabilidades en sistemas y redes de manera legal y ética. El objetivo principal del hacking ético es mejorar la seguridad informática de una organización o empresa al descubrir y remediar vulnerabilidades antes de que sean explotadas por hackers malintencionados.

El hacking ético se define esencialmente como el proceso de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar que estas vulnerabilidades sean explotadas por atacantes malintencionados (Vallejo, 2017).

Gran parte de lo aprendido en esta materia fue necesario para la ejecución del proyecto, los conocimientos adquiridos sobre Kali Linux y sus programas permitieron vulnerar la seguridad de la red wifi previamente configurada para el proyecto, además otorgó los conocimientos para monitorear y capturar paquetes en la red.

En la materia de Ciberseguridad en entornos Industriales aprendimos acciones específicas para la protección de usuarios y entidades que forman parte de un entorno industrial. El concepto se aplica para pequeñas redes domésticas (SOHO) que integren un sistema domótico simple, basado en sensores y actuadores IoT aplicado desde el punto de vista de la norma IEC62443-4-1 la cual garantiza el desarrollo de un producto seguro a través de un ciclo de vida que incluye su diseño, desarrollo y posterior mantenimiento. A través de esto, los fabricantes aseguran sus productos y brindan la confianza necesaria a los integradores de sistemas (Leander, 2019, August) (Diaz Cacho, 2021).

La Ciberseguridad Industrial es la disciplina de la ciberseguridad que contiene acciones específicas para la protección de usuarios y entidades que forman parte de un entorno industrial. Básicamente se centra en la seguridad de los ICS (Industrial Control System) y los sistemas SCADA (Supervisory Control and Data Acquisition) de una red industrial (Diaz Cacho, 2021).

La materia nos otorgó los conocimientos necesarios para poder configurar dispositivos MQTT y entender cómo estos se comunican entre sí, estas bases ayudaron en el desarrollo del proyecto ya que permitieron entender los estándares que actualmente usan los dispositivos IoT y sus posibles vulnerabilidades.

Una de las materias que nos ayudó a identificar y prevenir diferentes tipos de ciberataques fue la de Estrategias y Políticas Multilaterales ya que analiza la seguridad social y organizacional de la actualidad, la materia nos otorgó los conocimientos necesarios para establecer planes de continuidad de negocio y cómo hacer cumplir las políticas establecidas las cuales se pueden aplicar a grandes o pequeñas empresas.

Analizar y entender la política nacional de ciberseguridad fue necesario para el desarrollo de este proyecto, ya que se realizó en un ambiente controlado y no se afectó la integridad ni se vulneró la seguridad de ninguna red no autorizada.

Implementación

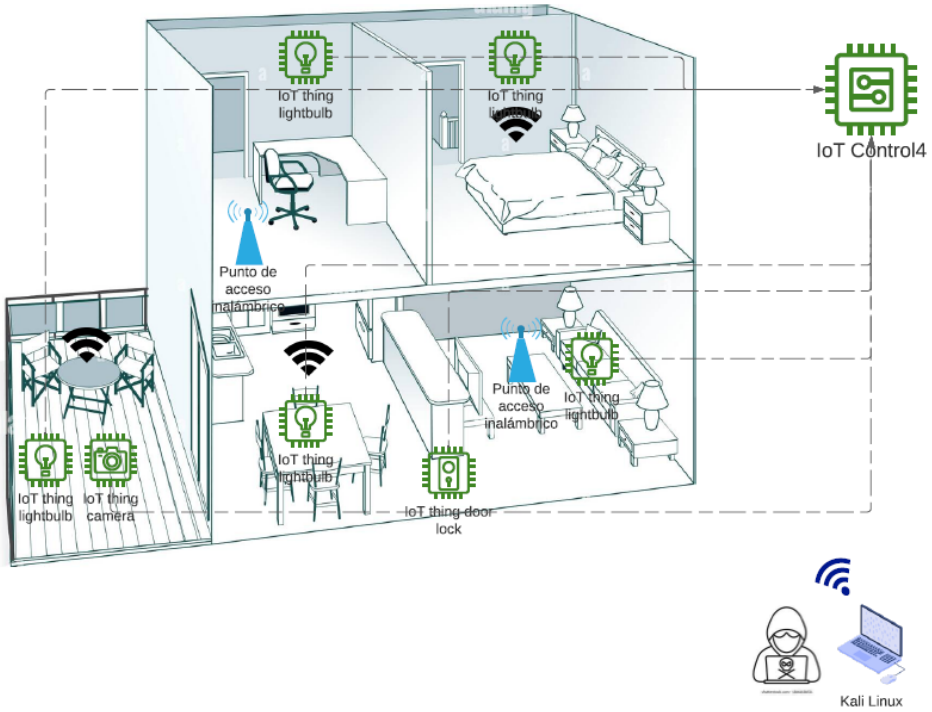
En esta sección se describen los pasos que se realizaron para vulnerar la seguridad de la red, escaneo de los dispositivos conectados, monitoreo de la comunicación e intersección de tráfico.

El método que se utilizó para romper la seguridad de la red es el conocido como “handshake” el cual establece monitorear la red hasta que algún dispositivo se

conecte en ella. Luego de capturar registros WPA handshake y a través de herramientas que se encuentran disponibles en Kali Linux como Aircrack-ng y el diccionario rockyou se analiza hasta obtener la clave de la red en un formato entendible.

Una vez que se obtenga el acceso a la red se realiza el escaneo y análisis de los dispositivos conectados con el fin de identificar posibles vulnerabilidades que nos permitan obtener información.

Ilustración 2
Diagrama de red



Breve descripción de los pasos realizados para vulnerar la red

1. Configuración de la tarjeta wifi monitor.

A través de la herramienta airmon-ng disponible en Kali Linux cambiamos la interfaz wlan0 a modo "Monitor". *"airmon-ng start wlan0"*

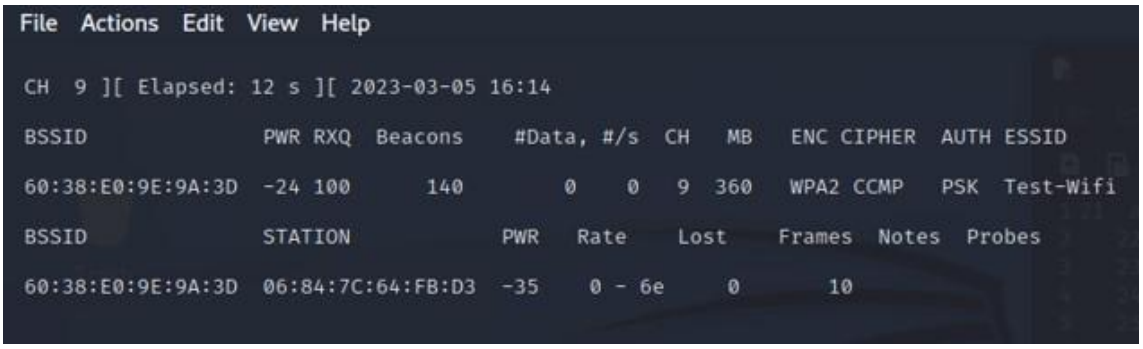
2. Escaneo de redes disponibles.

Procedemos con el escaneo de las redes disponibles con el comando *"airodump-ng wlan0mon"*

3. Monitoreo de la red escogida.

El monitoreo se lo realiza con el comando *"airodump-ng wlan0mon -d 60:38:E0:9E:9A:3D"* el ID corresponde al BSSID el cual es el nombre público de la red escogida.

Ilustración 3
Monitoreo de la red

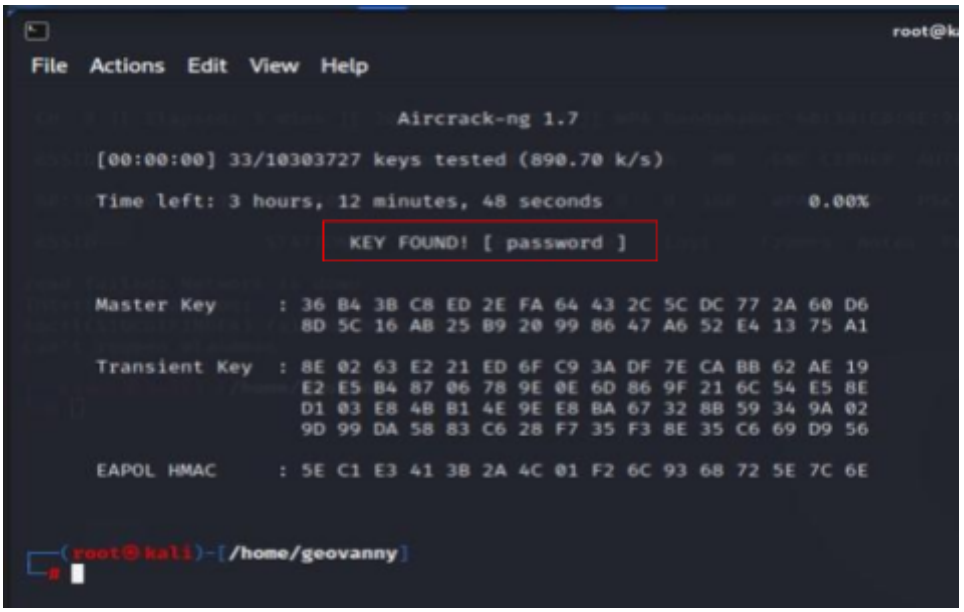


4. Análisis del tráfico capturado

Se realiza el análisis del registro con el fin de obtener la clave de la red con el comando

"ircrack-ng hack1-02.cap -w /usr/share/wordlists/rockyou.txt"

Ilustración 4
Clave de acceso



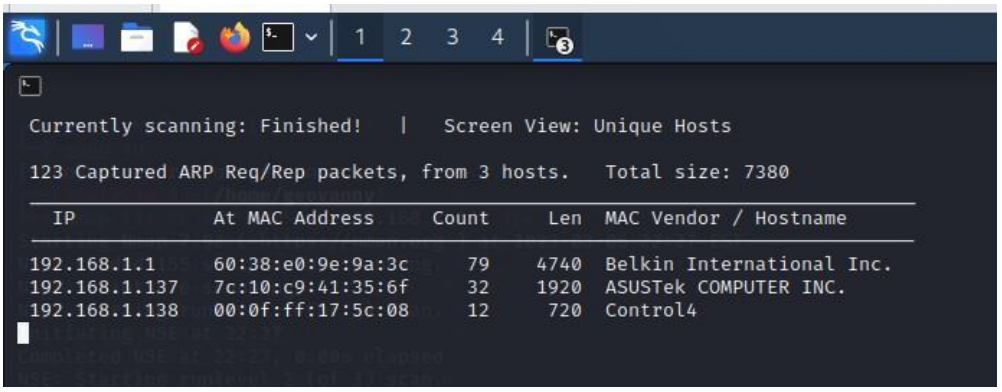
Como podemos observar la clave “password” es la misma que está configurada en el router.

Ilustración 5
Clave configurada en el router

Una vez registrado nuestro equipo en la red podemos realizar el reconocimiento de los dispositivos conectados y empezar a capturar y filtrar el tráfico que consideremos importante.

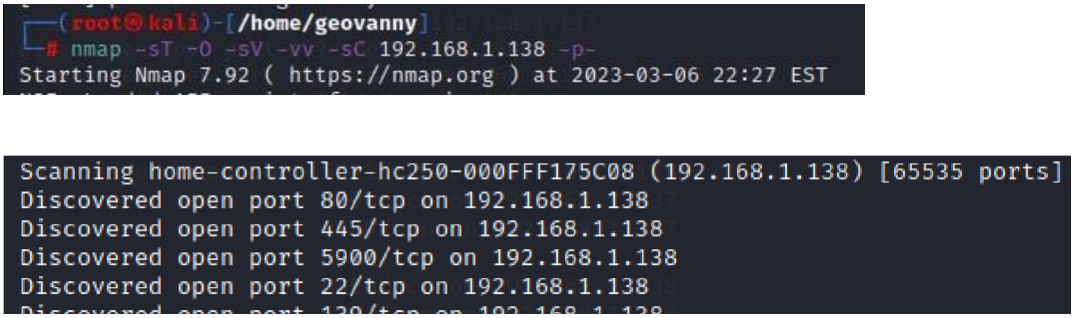
Utilizando el comando netdiscover en Kali realizamos la identificación de los dispositivos en la red. Entre los dispositivos encontrados verificamos que existe un controlador de domótica de marca Control4 el cual es un equipo que permite centralizar y gestionar los dispositivos inteligentes y nos permitiría el acceso y control a otros dispositivos del hogar.

Ilustración 6
Reconocimiento de los dispositivos



Con ayuda del comando nmap, se realiza un escaneo de puertos sobre el dispositivo Control4 para identificar los puertos abiertos del equipo, se logra determinar que entre otros, el puerto 22 el cual permite una conexión ssh y el uso de comandos está abierto.

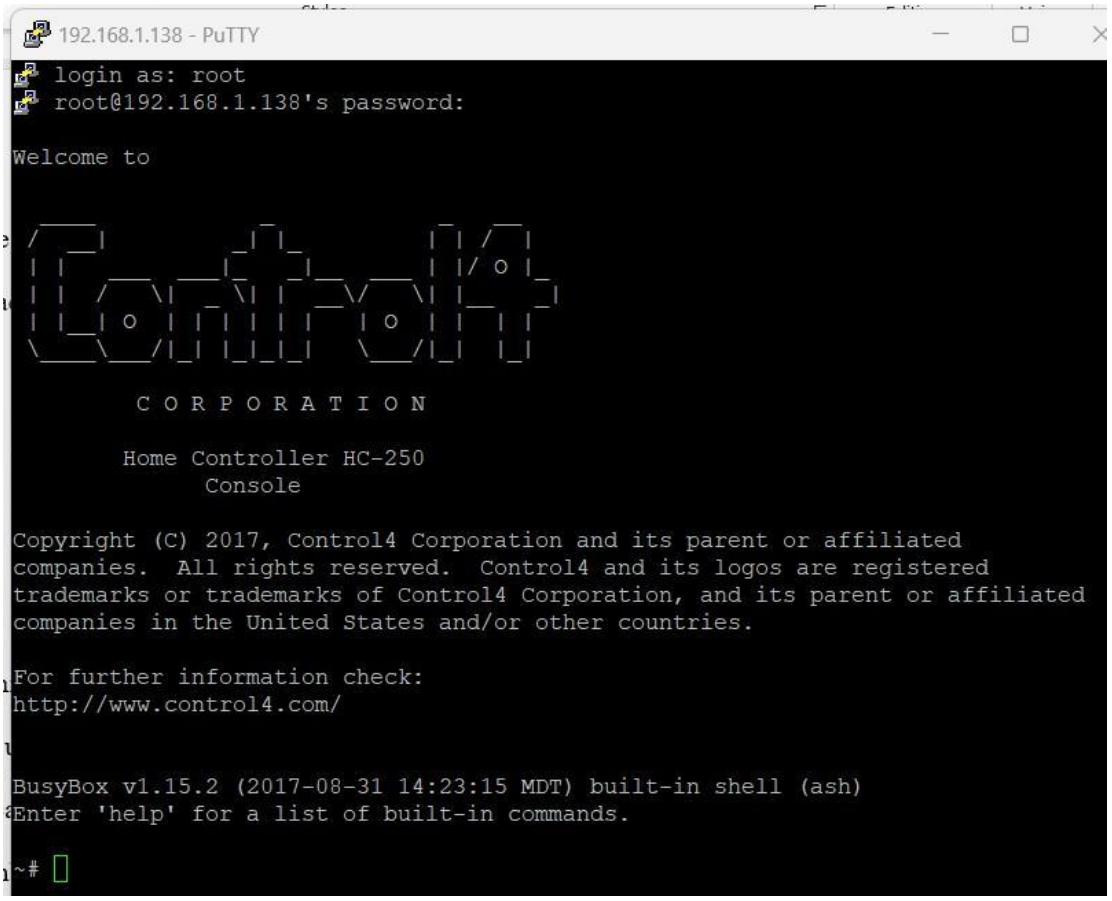
Ilustración 7
Reconocimiento de puertos



Como se revisó en la materia de Hacking Ético, la mayoría de los fabricantes establecen usuarios y claves predeterminadas en los equipos para su configuración, en su mayoría estos perfiles permanecen activos y sin modificación luego de su

instalación. Considerando lo anterior, se realizó una búsqueda en foros de internet y se logró identificar la clave del usuario root del dispositivo, la cual nos permitiría ingresar al controlador a través del puerto 22 previamente identificado.

Ilustración 8
Acceso SSH



Es importante recalcar que el acceso a la red, así como nos permitió obtener el control sobre este dispositivo, nos podría dar el acceso a monitorear y controlar otros como cámaras de seguridad, alarmas, puertas, control de iluminación y climatización.

Además, se evidencia que las claves predeterminadas de estos equipos se las puede encontrar con una búsqueda en internet dando lugar a los riesgos antes mencionados en este documento.

En la siguiente sección se establecen los controles y acciones que podemos realizar para prevenir estos ataques.

Métodos para asegurar la red

A continuación, se describen diversos métodos que podrían ayudar a mejorar la seguridad en la red.

1. Establecer contraseñas seguras y únicas para todos los dispositivos del hogar. Es necesario realizar el cambio de las contraseñas predeterminadas o fáciles de adivinar, como "123456" o "contraseña" como se evidenció en este proyecto, además, el uso de caracteres especiales en las contraseñas dificulta considerablemente el descifrado de éstas.
2. Actualizar el software y firmware de los dispositivos en la red. Este proceso ayuda en la protección de vulnerabilidades y errores de seguridad registrados en foros de internet, además es posible establecer búsquedas de actualizaciones frecuentes en los equipos.
3. Establezca el protocolo de cifrado WPA2 para su red inalámbrica, utilizar este nivel de cifrado más la contraseña robusta dificulta la obtención de la clave de su red.
4. Existen aplicaciones para equipos móviles que permiten realizar el escaneo de la red, con el fin de identificar y cerrar puertos abiertos que podrían poner en riesgo la seguridad.

5. Desactive la opción de administración remota de los dispositivos a través de internet si no lo necesita.
6. Verifique que no están exponiendo información personal o confidencial a Internet, desactive las características de "escucha" o "vigilancia" que no sean necesarias en los asistentes del hogar Alexa, Siri o Google, estas características por lo general están activadas de forma predeterminada en los dispositivos.
7. La mayoría de los routers en la actualidad permiten crear una red específica para los invitados en el hogar. Activar esta característica permite mantener la privacidad y evita un riesgo innecesario.
8. Considere que existen equipos que ayudan a proteger la red como firewalls, los cuales permiten un mayor control al filtrar el tráfico de la red. Existen diferentes tipos de firewall dependiendo del modelo y la red que necesita asegurar varía el precio.

Conclusiones

Limitaciones

Para el alcance de este proyecto se creó una red wifi independiente, y se configuró el protocolo de seguridad WPA y una contraseña fácil de descifrar por las herramientas utilizadas en Kali Linux, ya que una clave más robusta tomaría días poderla descifrar. En la red wifi se enlazaron dispositivos como Control4 el cual permite la gestión de otros dispositivos inteligentes, y un teléfono celular para realizar las pruebas de acceso. Para realizar el ataque a la red se instaló Kali Linux sobre una

laptop con el fin de utilizar la tarjeta wifi como monitor ya que no se contaba con dispositivos de escaneo usb para enlazar a máquinas virtuales.

Recomendaciones

Considerando lo valiosa que es la información para cada usuario, es importante implementar las medidas de seguridad descritas en este documento para evitar ataques, robo de información, extorsión y demás delitos que puedan poner en riesgo la integridad de los datos y de cada persona.

Una red wifi no protegida puede incurrir en afectaciones físicas de las personas al exponerse información sensible, su ubicación o rutinas diarias, es importante considerar implementar las recomendaciones dadas en éste documento con el fin de mantener la integridad de los datos y las personas.

Glosario de términos

Virus informático: Se define como software malicioso diseñado para propagarse de una computadora a otra, causando daño a los archivos, programas y sistemas en los que se ejecuta. Los virus pueden ser diseñados para una variedad de propósitos maliciosos, incluyendo la destrucción de datos, la toma de control de sistemas, el robo de información, el espionaje y la extorsión.

Malware: El Malware es un término genérico que se refiere a cualquier software malicioso diseñado para dañar, interferir con el funcionamiento normal o robar información de un sistema informático sin el conocimiento o consentimiento del usuario.

El malware puede tomar muchas formas diferentes, como virus, gusanos, troyanos, spyware, adware y ransomware, cada uno con sus propios métodos de propagación y objetivos maliciosos.

Wireshark: Wireshark es un software de análisis de red de código abierto que permite capturar y analizar el tráfico de red en tiempo real.

Firmware: El firmware es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Protocolo: En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier medio físico o inalámbrico.

Referencias

Bibliography

Diaz Cacho, M. (2021). *Cybersecurity analysis in SOHO environments.*

Leander, B. Č. (2019, August). *Applicability of the IEC 62443 standard in Industry 4.0/IIoT.* In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).

Ortega Candel, J. M. (2021). *Ciberseguridad. Manual práctico.*

Vallejo, M. R. (2017). *Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas.* Revista Publicando, 4(10 (1)), 31-51.

Anexos

Anexo1

https://booming-burrito-81e.notion.site/Evidencias-de-Aprendizaje-c6c67caaf4cf4882a6ff16bd102d6e22

Anexo2

https://www.canva.com/design/DAFdw2VwXBI/ZTk6qeezIyrGe6HG67YIPA/view?utm_content=DAFdw2VwXBI&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton