UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

Propuesta de estudio de la vulnerabilidad o riesgo de dispositivos móviles o tarjetas de red inalámbricas

Proyecto de Investigación

Sebastián Andrés Ramos Regalado

Ingeniería en Sistemas

Trabajo de integración curricular presentado como requisito
para la obtención del título de
Ingeniero en Sistemas

Quito, 30 de abril de 2020

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

COLEGIO CIENCIAS E INGENIERIAS

HOJA DE CALIFICACIÓN
DE TRABAJO DE TITULACIÓN

Propuesta de estudio de la vulnerabilidad o riesgo de dispositivos móviles o tarjetas de red inalámbricas

Sebastián Andrés Ramos Regalado

Calificación: _____

Nombre del profesor, Título académico Fausto Pasmay, Master of Science

Firma del profesor _____

Quito, 30 de abril de 2020

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante: _____

Nombres y apellidos: Sebastián Andrés Ramos Regalado

Código: 00116305

Cédula de identidad: 1715825533

Lugar y fecha: Quito, mayo de 2020

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

RESUMEN

La presente tesis pretende ser una propuesta de estudio de las vulnerabilidades y riesgos en el área de la ciberseguridad personal a los que están expuestos los estudiantes e individuos en un campus universitario u otro tipo de área similar, para ello se pretende estudiar varios tipos de ataques que podrán ser llevados a cabo y el diseño de como implementarlos.

Este estudio sirve como guía para un trabajo de campo, puede ser este en un campus universitario o cualquier tipo de estudio técnico en campo que se desee llevar a cabo con esta propuesta de estudio de ciberseguridad.

El tema central es la ciberseguridad personal, donde se propone un tutorial para implementar pruebas, se revisan además temas sobre la privacidad y la ética de los datos, para concienciar a la comunidad a cuidar sus datos e información que a diario se ven expuestos en redes públicas inalámbricas y en las distintas aplicaciones y servicios populares de los que se dispone actualmente, proponiendo una secuencia de pasos que se podrán llevar a cabo.

Palabras clave: vulnerabilidad, ciberseguridad, inalámbrica, ética.

ABSTRACT

This dissertation intends to be a proposal for studying the vulnerabilities and risks in the area of personal cybersecurity to which students and individuals are exposed on a university campus or another type of similar area, It is intended to study different types of attacks that can be carried out and the design that will follow each one of them.

This Investigation serves as a guideline for fieldwork as it can be applied on a university campus or any type of technical study in the field you want to carry out the research.

The main idea is personal cybersecurity, where a tutorial is proposed to implement tests, and topics on data privacy and ethics are also reviewed, to raise awareness in the community to take care of their data and information that are exposed daily on networks by proposing a sequence of steps that can be carried out so you can be protected.

Key words: vulnerabilities, cybersecurity, networks, ethics

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El análisis de información se ha vuelto un tema de debate a nivel mundial, la seguridad de la información no solo se basa en cuidar la información ya existente, sino también en resguardarla que se va generando día a día, segundo a segundo, esta explosión en la generación de datos ha creado un nuevo interés sobre la seguridad de su información llegando a niveles sociales, es decir en cómo tratar este nuevo tipo de datos de los cuales muchos de ellos son capturas de nuestro comportamiento social.

La ética y privacidad de los datos se han ido poniendo sobre la mesa de discusión a nivel mundial, tanto dentro de la industria como a nivel de usuarios. En la actualidad se ha monetizado la información para realizar mercadeo con grandes datos, llevando incluso a que empresas encargadas de nuestra seguridad vendan nuestra información para obtener ganancia, un caso reciente "El antivirus Avast recoge los datos de navegación de sus más de 400 millones de usuarios para vendérselos a terceros" (Europa Press, 2020).

Casos en los que se vulneran datos e información de usuarios existen cientos, dentro de nuestras aplicaciones como redes sociales, mensajería instantánea, geolocalización se nos muestran como juegos con la ilusión de estar mejor comunicados y conectados; además de las tecnologías como Big Data que son parte del Internet de las cosas (IoT) son actualmente un fenómeno socio tecnológico, haciendo que la frontera entre los espacios público y privado sea muy difusa. Como dice Castells entendemos las sociedades no como "comunidades que comparten valores e intereses", sino como "estructuras sociales contradictorias surgidas de conflictos y negociaciones entre diversos actores sociales, en muchos casos opuestos" (Castells & Hernández, 2014).

La privacidad de los datos e información es otro tema que requiere atención ya que la monetización de los datos además ha hecho que sea rentable el mercado de datos.

CAPÍTULO 1: MARCO TEÓRICO

1.1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN Y A LA CIBERSEGURIDAD

La información se ha vuelto el activo mas importante para los individuos y las organizaciones a nivel mundial, la cual requiere ser resguardada. Con el auge de las aplicaciones en línea, redes sociales, y temas como la minería de datos, etc,. La explosión de datos e información a aumentado vertiginosamente en la última década, aumentando no solo la información sino también el riesgo y las vulnerabilidades de ser víctima de la ciberdelincuencia.

Según dice Sumeet Dua and Xian Du: "la divulgación de datos financieros comerciales o privados a ciberdelincuentes puede conducir a pérdidas financieras a través de la banca por Internet y recursos en línea relacionados… Las personas también deben estar atentas contra los delitos cibernéticos y el uso malicioso de la tecnología de Internet" (Dua & Du, 2016).

Esto obliga a que los individuos deban estar mejor informados y protegidos de la delincuencia organizada cibernética, de acuerdo a Homeland Security Council "Muchos de los servicios esenciales y de emergencia del país, así como nuestra infraestructura crítica, dependen del uso ininterrumpido de Internet y los sistemas de comunicaciones, datos, monitoreo y sistemas de control que comprenden nuestra infraestructura cibernética. Un ataque cibernético podría ser debilitante para nuestra Infraestructura Crítica y Recursos Clave (CIKR) altamente interdependientes y, en última instancia, para nuestra economía y seguridad nacional" (Dua & Du, 2016).

1.1.1 **PIRÁMIDE D-I-K-W**

Lo anteriormente expuesto lleva a ordenar y definir conceptos sobre lo que son y significan los datos, para una compresión de la seguridad de la información, para conocer que proteger:

La figura 1.1, Se conoce como pirámide D-I-C-S (dato, información, conocimiento y sabiduria) “de modo que la información se define a partir de los datos disponibles, el conocimiento se extrae de dicha información y la sabiduría es entendida como la habilidad para aplicar dicho conocimiento en beneficio propio o común” (Jifa & Lingling, 2014).

Figura 1. 1: Pirámide D-I-K-W (Minguillon, 2018).

Un dato es una recopilación de valores asignados a medidas de base, medidas derivadas y / o indicadores. Informaciòn conocimiento necesario para gestionar objetivos, metas, riesgos y problemas ("ISO/IEC 27000:2018," n.d.).

A partir de estos se puede según el giro de negocio o el área de investigación definir el conocimiento y generalizarlo a sabiduría.

1.1.2 **ESTANDARES ISO DE SEGURIDAD DE LA INFORMACIÓN**

La Familia de estándares ISO/IEC 27000 esta integrada por varios documentos en materia de seguridad de la información, que orientan y dan una base conceptual sobre la ciberseguridad, entre ellas se encuentran.

La Norma ISO/IEC 27000:2014 proporciona una visión general de las normas de la Familia 27000, que permite entender los conceptos aceptados a nivel mundial ("ISO/IEC 27000:2018," n.d.). La ISO/IEC 27032:2012 define al ciberespacio como un entorno complejo resultado de la interacción de personas, con la tecnología tanto en software como en hardware, que actualmente se encuentran distribuidos a nivel mundial y en formas bien complicadas, “Esto se debe a que los dispositivos y las redes conectadas que han admitido el ciberespacio tienen múltiples propietarios, cada uno con sus propias preocupaciones comerciales, operativas y normativas” ("ISO/IEC 27032:2012," n.d.).

1.1.3 **LA CIBERSEGURIDAD**

Según lo define Wayne Patterson Cynthia E. la ciberseguridad es una ciencia diseñada para proteger la computadora y todo lo relacionado con ella, “La seguridad cibernética no solo está diseñada para proteger contra intrusos externos, sino también contra personas maliciosas y benignas” (Patterson & Winston-Proctor, 2019).

1.1.3.1 **Amenazas en la CIBERSEGURIDAD**

Hay 3 términos en los que se pueden definir las amenazas en un entorno informático (Patterson & Winston-Proctor, 2019):

Vulnerabilidad es la debilidad de un sistema que pone en riesgo la información, es decir, es un punto donde un sistema es susceptible a ataques. D-I-K-W Amenaza es un posible peligro para el sistema que aprovecha una vulnerabilidad en un contexto negativo hacia la información. Contramedida es una opción, idea o técnica para aplacar el peligro, denominados también controles.

En este punto podemos ver que la Ciberseguridad es una parte de un todo, este todo es la Seguridad de la Información considerada en los estándares ISO.

1.1.4 **METODOLOGÍAS DE ATAQUE INFORMÁTICO**

Para obtener los datos e información se utilizan métodos y técnicas de ataques para una red inalambrica, entre estos ataques se encuentran.

1.1.4.1 **Metodología MITM WPA**

Este ataque es uno de los más conocidos y utilizados, se resume como funciona este ataque en la figura 1.2 y la figura 1.3. Consiste en que el atacante se encuentra en medio de la transmisión de la información entre la fuente y el destino, capturando así todos los datos e información que el atacante esté interesado.

Como se puede observar en la figura 1.3 el ataque MITM puede realizarselo en cualquier tipo de enlace inalàmbrico incluido la tecnologìa celular, un ejemplo en GSM. La mejor opción que tenemos para protegernos de este ataque es la “comunicación asegurada con TLS” (Waschke, 2017)

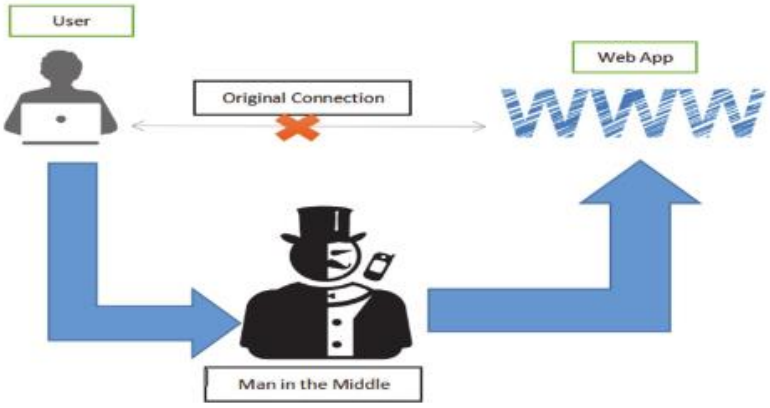

Figura 1. 2: Ilustración del A man in the middle (MITM) attack (Mallik, 2019).

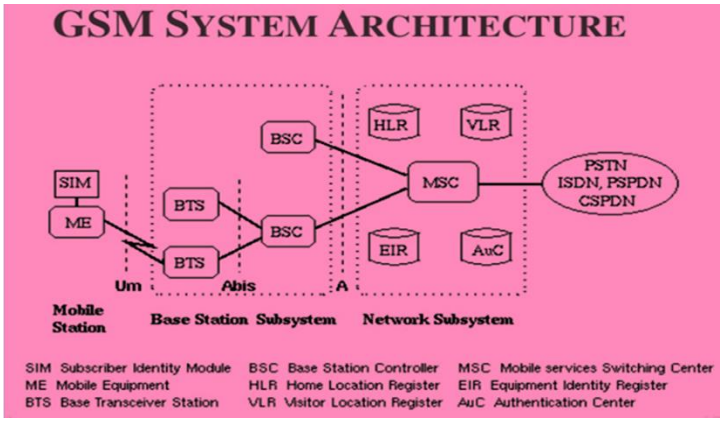

Figura 1. 3: MITM en GSM: una amenaza para la seguridad de la comunicación telefónica (Mallik, 2019).

El resultado es la captura de datos e información, es decir que el atacante en medio de la transmisión captura la información y envía una copia de esta información a su destino real para que el usuario o el destino no se percate del ataque.

1.1.4.2 **Metodología *Evil Twin***

Denominado *Evil Twin Attack* ETA, es un punto de acceso inalámbrico fraudulento disfrazado de un punto de acceso a red legítimo, suele ser un ataque común en entornos domésticos inteligentes donde los atacantes pueden comprometer la seguridad de los dispositivos conectado, “Al configurar un punto de acceso no autorizado, engañando a los usuarios para que establezcan la conexión de red con el mismo SSID que el legítimo, el atacante puede lanzar el ataque *man-in-the-middle* y robar información privada” (Kuo et al., 2018).

Los pasos comunes para este tipo de ataque suelen ser los siguientes:

Paso 1: el atacante realiza una búsqueda en el aire en busca de la información del punto de acceso objetivo. Información como nombre SSID, número de canal, dirección. Luego usa esa información para crear un punto de acceso con las mismas características, por lo tanto, Evil Twin Attack. Paso 2: Los clientes en el AP legítimo se desconectan repetidamente, lo que los obliga a conectarse al punto de acceso fraudulento. Paso 3: Tan pronto como el cliente esté conectado al punto de acceso falso, puede comenzar a navegar por Internet. Paso 4: el cliente abre una ventana del navegador y ve una advertencia de administrador web que dice "Ingrese la contraseña WPA para descargar y actualizar el firmware del router". Paso 5: En el momento en que el cliente ingrese la contraseña, será redirigido a una página de carga y la contraseña se almacenará en la base de datos MySQL de la máquina atacante. El almacenamiento persistente y la autenticación activa hacen que el ataque Evil Twin sea automatizado.

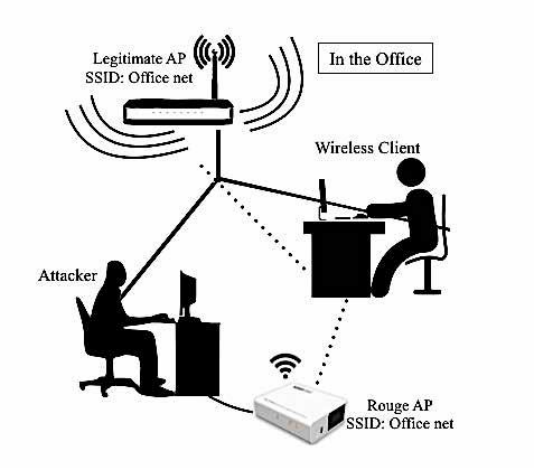

Figura 1. 4: Ilustración del Ataque Evil Twin (Mallik, 2019).

1.1.4.3 **Phishing**

Forma de ingeniería social donde el atacante conocido como *phisher*, intenta recuperar de manera fraudulenta las credenciales confidenciales de los usuarios del servicio imitando las comunicaciones electrónicas y los comportamientos de una organización pública o confiable en línea de manera automatizada.

Tipos de ataques Phishing ("(PDF) Analysis of phishing attacks and countermeasures," 2006).:

1. Ataque de phishing por fraude, donde el usuario es engañado por correos electrónicos fraudulentos para revelar información personal o confidencial.
2. Ataque de phishing por software infeccioso, donde el atacante logra ejecutar software peligroso en la computadora del usuario.
3. Ataque de phishing por falsificación de DNS, donde el atacante compromete el proceso de búsqueda del dominio para que el clic del usuario lo lleve a un sitio web falso.
4. Ataque de phishing mediante la inserción de contenido dañino, donde el atacante coloca contenido malicioso en un sitio web normal.

5. Enfoque de phishing por MITM, donde el atacante se interpone entre el usuario y el sitio legítimo y toca información confidencial.

6. Indexación de ataque de phishing por motor de búsqueda, donde las páginas web falsas con ofertas atractivas creadas por el atacante son indexadas por un motor de búsqueda, de modo que un usuario pueda tropezar con él.

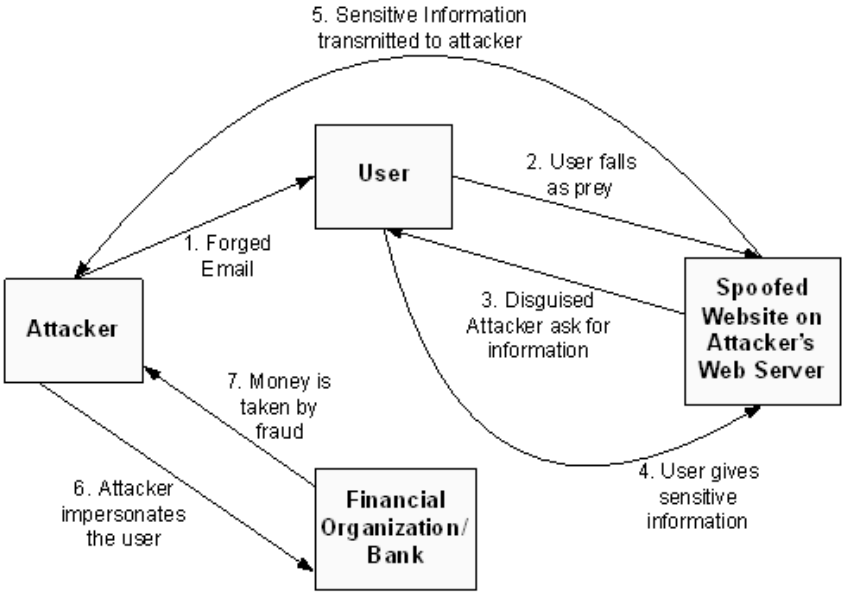

Figura 1. 5: Flujo de Información para el phishing ("(PDF) Analysis of phishing attacks and countermeasures," 2006)..

El ataque de *phishing* completo implica tres roles de *phishers*. Inciando se encuentran los *mailers* los cuales envían una gran cantidad de correos electrónicos fraudulentos (generalmente a través de *botnets*), estos los redirigen a sitios web fraudulentos, continúan con los coleccionadores que configuran sitios web fraudulentos (generalmente alojados en máquinas comprometidas), lo que induce a los usuarios a proporcionar información confidencial. Finalmente, los cobradores usan la información confidencial para conseguir un pago por la información o servicio

comprometido. Los intercambios monetarios a menudo ocurren entre esos *phishers* ("(PDF) Analysis of phishing attacks and countermeasures," 2006).

1.1.4.4 **Ingeniería Social**

La ingeniería social tiene sus raíces en el área de la ciencia política a inicios del siglo XX, donde pretendía representar métodos inteligentes que resuelven los problemas sociales. Por las connotaciones positivas de la palabra ingeniería, fue apropiada para varios problemas sociales de la época. “Karl Popper, en su libro, respaldó la idea como un sentido de cambio social basado en un conocimiento instrumental bien establecido (Hansson, 2006)” (Kuo et al., 2018).

Existen una infinidad de ataques de Ingeniería Social y la variedad y el alcance de tales ataques solo se limitan a la imaginación y creatividad del atacante. Suele dividirse en dos categorías (1) Ingeniería social basada en el ser humano que es el que mediante la psicología manipulan emociones o estados de ánimo para extraer información y (2) Ingeniería social basada en la tecnología es en la que se utilizan sitios web o mensajería que proviene de lugares fraudulentos los cuales están diseñados para extraer información (Kuo et al., 2018).

1.1.5 **ÉTICA Y PRIVACIDAD DE LA INFORMACIÓN**

En la era de la explosión de la información, se presentan nuevos paradigmas en el área de las tecnologías actuales, esto lleva a preocuparse por nuevos temas que en la década pasada no eran relevantes, el Internet de las Cosas (IoT), el Big Data, la Minería de Datos, el Análisis de la Información en tiempo real y para toda la población, es decir que ya no solo se trabaja con muestras como tradicionalmente se venía haciendo, la tecnología brinda la posibilidad de trabajar con la

población entera de un determinado estudio o mercado. Esto hace que nuevos temas se pongan sobre la mesa tales como la Ética en el manejo y gestión de la información, la privacidad de la información personal o corporativa.

1.1.5.1 **Ética**

Durante el siglo XX quedó en evidencia la necesidad urgente de desarrollar una ética adaptada a los cambios que provocarían los avances tecnológicos sobre la calidad y las formas de vida. Debido al cambio constante a la dinámica de los datos digitales y el comportamiento humano actuales lo cuales se motivan por la eclosión de información que el uso masivo de tecnología genera al minuto (Cabanillas, n.d.,).

Muchos aspectos sociales se consideran aquí, por ejemplo, ¿Quién es el dueño o a quién pertenecen los datos, al que los genera, al que los almacena, o al que las compran?, ¿Quién está autorizado a vender esos datos?, ¿Qué hacer, lo bueno, lo justo o lo correcto?

Estos debates que se están presentando a nivel mundial no solo son en el área tecnológica, también es en el área jurídica, comercio, negocio, política, robótica, social y filosófica. Por ejemplo, la ética aplicada a la IoT puede decirse como una ética en el ámbito profesional en el ámbito público y privado los cuales desarrollan una determinada cultura ética y permiten tomar decisiones orientadas hacia el interés general de la sociedad o bien común (Cabanillas, n.d.,).

1.1.5.2 **Privacidad**

Las personas valoramos nuestra privacidad y la protección de nuestra información y la de nuestros seres queridos o personas que consideremos muy próximas a nosotros. Pretendemos mantener cierto control sobre quién sabe qué sobre nosotros mismos. “No deseamos que nuestra información personal sea accesible a cualquier persona en cualquier momento. Así de modo que entendemos que tanto *big data* como la tecnología en general están modificando el sentido y el significado de lo que llamamos identidad”, (Cabanillas, n.d.,)..

Los avances en la tecnología de la información amenazan la privacidad y han reducido el control sobre los datos personales, incrementando el riesgo de efectos negativos sobre la privacidad. El siglo XXI es el siglo de *big data*, y la tecnología de la información avanzada permite el almacenamiento y procesamiento de exabytes de datos. Las revelaciones de Edward Snowden demostraron que estas preocupaciones son reales y que las capacidades técnicas para recolectar, almacenar y buscar grandes cantidades de datos sobre conversaciones telefónicas, búsquedas en internet y pagos electrónicos ya están en vigor y son usadas rutinariamente por los gobiernos y las corporaciones para sus fines mercantiles y comerciales. Para las empresas, los datos personales sobre clientes fieles o potenciales también son ahora un activo clave. Al mismo tiempo, el significado y el valor de la privacidad sigue siendo objeto de considerable controversia.

Se puede establecer las siguientes razones morales para la protección de datos personales y para proporcionar el control directo o indirecto sobre el acceso a esos datos por otros (Cabanillas, n.d.,).:

1) Prevención del daño: garantizar que las contraseñas de acceso a los sitios son seguras y que la geolocalización no es activada por los dispositivos sin el consentimiento del usuario son dos formas inexcusables de evitar daños.

2) Desigualdad informativa: los datos personales se han convertido en mercancías. Las personas suelen estar en posición de desventaja para negociar contratos sobre el uso de sus datos y no tienen los medios para verificar si el proveedor cumple con los términos del contrato. Las leyes, la reglamentación y la gobernanza de la protección de datos tienen por objeto establecer condiciones equitativas para la redacción de contratos relativos a la transmisión y al intercambio de datos personales, así como para la provisión de controles y garantías de reparación. Esto conlleva garantizar la redacción de contratos inteligibles para el usuario que velen por su seguridad y no solo por la del proveedor del servicio.

3) Injusticia informativa y discriminación: la información personal proporcionada en un determinado contexto (por ejemplo, en atención médica) puede cambiar su significado cuando se utiliza en otro contexto (como las transacciones comerciales) y puede conducir a discriminación y desventajas para el usuario.

4) Intrusión en la autonomía moral: la falta de privacidad expome a los individuos a fuerzas externas que influyen en sus elecciones. Pudiendo crearse algoritmos para identificar comportamientos sociales y tendencias a nivel regional y mundial. “Por ejemplo, Lazer y Bakshy y otros advirtieron, en sus respectivos artículos publicados por la revista *Science* en junio de 2015, de aquello que denominaron el advenimiento del algoritmo social y de las consecuencias que estaba teniendo su implantación en las redes sociales más populares, como Facebook y Twitter”.

Con estos y muchos actos de vulneración de la privacidad, muchos analistas han denunciado que este modo de gestionar las noticias, permitiendo que tanto las verdaderas como las falsas sean consideradas por el algoritmo en igualdad de condiciones, ha servido por ejemplo para que Donald Trump llegue a ser presidente. “Un fenómeno que ha llevado a establecer el potencial de lo que ya se conoce como la post-verdad, que ampara lo que podríamos llamar la certeza de las mentiras, y que ha ganado la posición de palabra del año 2016 otorgada por el *Oxford Dictionary*” (Cabanillas, n.d.,)..

4) Intrusión e interferencia en la toma de decisiones son las dos principales formas de vulneración de la privacidad. El segundo de ellos es quizá el más difícil de comprender, aunque aquí ya hemos visto varios ejemplos relacionados con el rol que asumen los algoritmos en las redes sociales o en los buscadores, y la limitación en el ejercicio de la autonomía personal que ello implica.

CAPÍTULO 2: DISEÑO E INFRAESTRUCTURA

2.1. DISEÑO DE LA INFRAESTRUCTURA

Esta guia de implementación revisa mediante una infraestrutura típica los ataques que comunmente se realizan an ambientes de redes inalámbricas, donde los datos e información fluyen con escasa seguridad, vamos a tomar como ejemplo una red inalambrica en un Campus universitario y detallar la infraestructura necesaria para varios tipos de ataque. Pueden utilizarse varias herramientas o software de código abierto o de pago que realizan todo este análisis, en este caso se utilizará la herramienta Kali Linux definiendo los ataques a realizar y los pasos.

En la figura 2.1 se muestra un bosquejo del área donde se propone realizar la infraestructura para el análisis y estudio dentro de un Campus Universitario y la cobertura de acción que será limitada por el alcance de la señal inalámbrica del equipo de red.

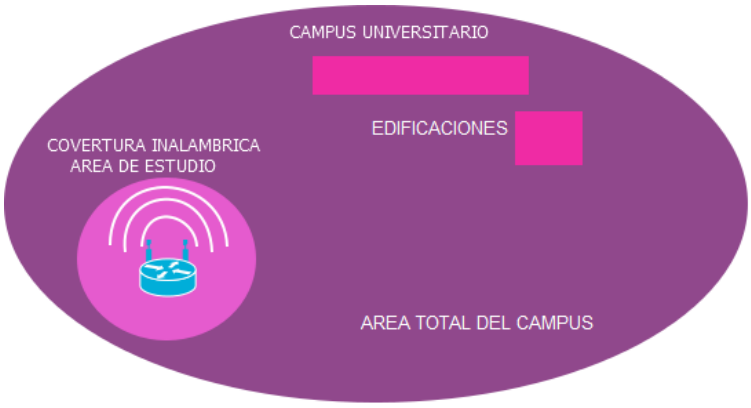

Figura 2. 1: Diseño a nivel físico bosquejo de ubicación dentro del campus universitario.

En la figura 2.2 se propone un diseño de infraestructura tecnológica es decir el hardware necesario para la implementación y estudio de los ataques a ralizarse.

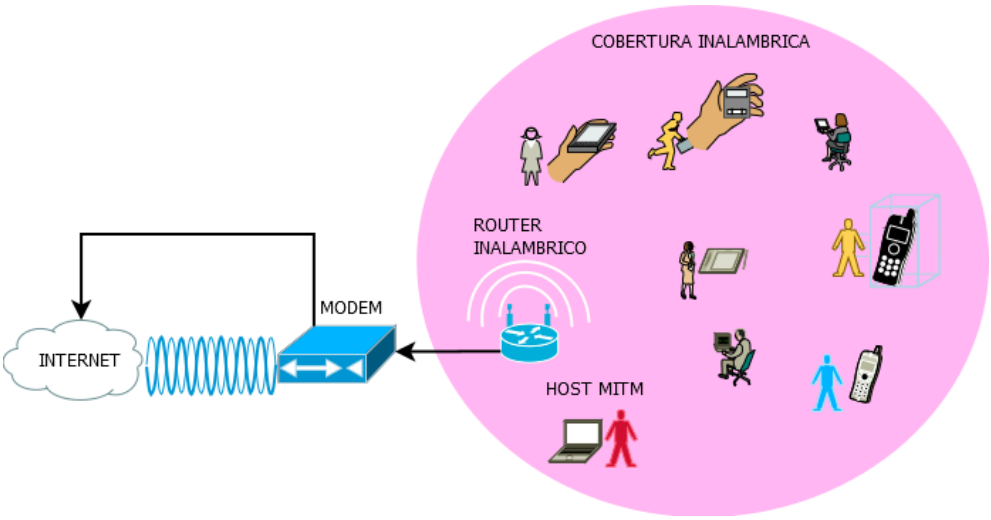

Figura 2. 2: Propuesta de diseño de la infraestructura tecnológica necesaria.

Las caracteristicas básicas recomendadas del hardware para el HOST MITM son:

- CPU: Intel Core i5
- RAM: 4GB
- 1 Interfaz Gb LAN
- 1 Intrefaz Wi-Fi

La caracteristica del sistema operativo del HOST MITM es Kali Linux 2019 rolling.

En a figura 2.3 se muestran los tipos de ataque que se utilizarán dentro del sistema operativo, con esto se tiene lo necesario para empezar la implementación propuesta.

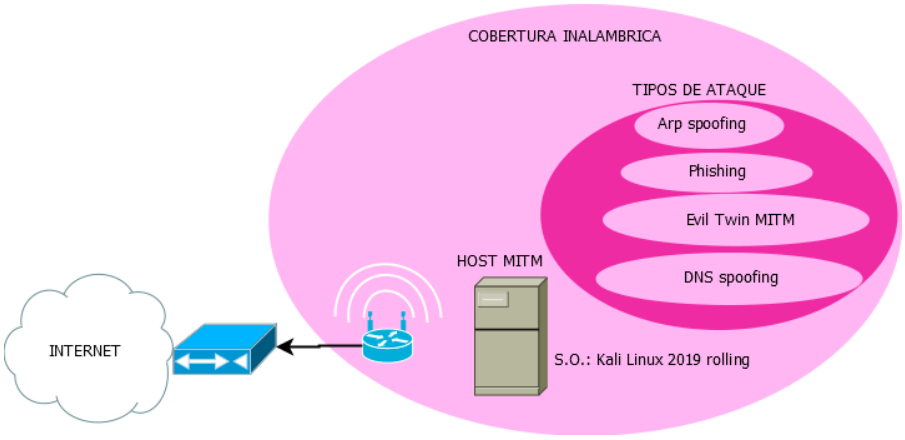

Figura 2. 3: Diseño a nivel de ataques propuestos.

2.2. DESCRIPCIÓN DE ATAQUES Y HERRAMIENTAS

Se describe los tres tipos de ataques MITM propuestos. “El 'ataque de hombre en el medio' también conocido / abreviado como MIM, MiM, MitM o MITMA es un tipo de ataque criptográfico sobre un canal de comunicación por parte de un tercero malicioso…” (Mallik, 2019). Este ataque puede (leer, modificar, interceptar, cambiar o reemplazar) el tráfico de comunicación entre las víctimas. El atacante no deja pista o rastro de la intercepción del tráfico entre el origen y destino, permaneciendo invisible para la víctima o víctimas.

En el capitulo 1 se ha resumido este tipo de ataque, a continuación se resumen los tipos de ataque a utilizar y las herramientas para lograr realizar dichos ataques.

2.2.1. MITM DNS Spoofing

“La falsificación de DNS, también conocida como envenenamiento del registro de DNS, implica infiltrarse en un servidor DNS y alterar el registro de dirección de un sitio” (Mallik, 2019).

Esto es los usuarios intentan llegar hasta el servicio legítimo son desviados a otro registro DNS indicado por el atacante.

Ejemplo de uso de una falsificación DNS realizado en Kali Linux (Messier, 2018):

root@kali:~# dnsspoof -i eth0 -f myhosts udp dst port 53

dnsspoof: listening on eth0 [udp dst port 53]

192.168.86.227.37972>192.168.86.1.53:10986+ A? www.bogusserver.com

192.168.86.227.49273>192.168.86.1.53:28879+ A? www.bogusserver.com

192.168.86.227.48253>192.168.86.1.53:53068+ A? www.bogusserver.com

192.168.86.227.49218>192.168.86.1.53:45265+ A? www.bogusserver.com

Ettercap es un Software alojado en el sistema operativo, versión 0.8.3-Bertillon. Tiene dos modos de funcionamiento, una interfaz estilo curses (se ejecuta en una consola o terminal pero no es estrictamente una línea de comando) es decir una GUI basada en caracteres, la segunda interfaz es una GUI completa basada en Windows. (Messier, 2018)

Setoolkit es un software alojado en el sistema operativo, versión 7.7.9. Herramientas de ingeniería social (setoolkit) automatiza ataques de ingeniería social. Puede crear correos electrónicos con archivos adjuntos o clonar un sitio web conocido agregando contenido infectado que proporciona acceso al sistema de un usuario objetivo. (Messier, 2018)

Sslstrip es un software alojado en el sistema operativo, versión 0.9.2. Esta herramienta puede ser utilizada para secuestrar el tráfico HTTP o monitorear el tráfico HTTPS. Es similar a un proxy haciendo que las conexiones HTTP no encriptadas tengan apariencia sesiones HTTPS encriptadas.

2.2.2. MITM ARP Spoofing

"La falsificación de ARP es la forma de vincular la dirección mac de un atacante con la dirección IP de un usuario legítimo en una red de área local utilizando mensajes arp falsos" (Mallik, 2019). En esta acción la información capturada del cliente a la entrega del host IP se transmite al atacante.

En la Figura 2.4 se puede observar una tabla ARP de varios segmentos dentro de una red LAN, todas las direcciones MAC pertenecen a la capa enlace de datos o *data link* del modelo OSI (Brooks et al., 2018). El ataque ARP Spoofing corrompe estas tablas para lograr el objetivo del atacante.

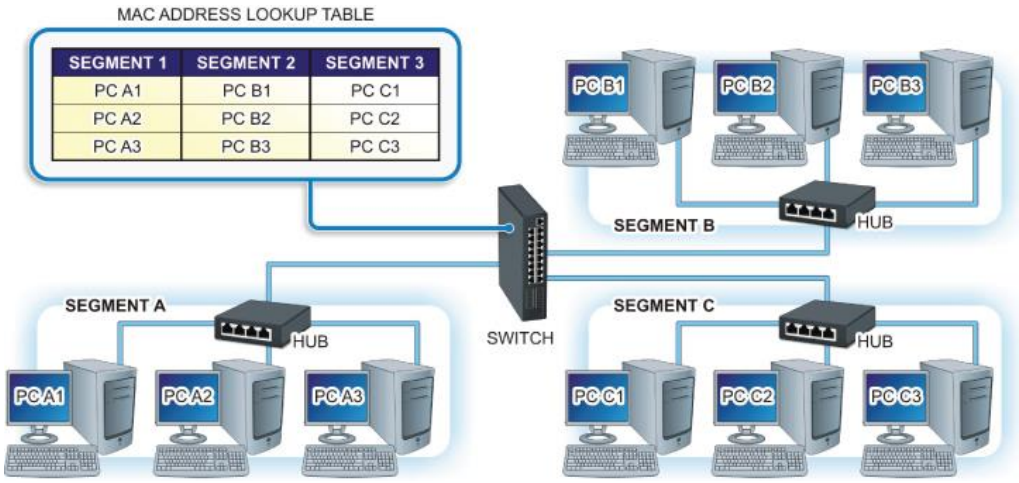

Figura 2. 4: Tabla ARP en una red ethernet LAN (Brooks et al., 2018).

Al alterar las Tablas ARP el atacante puede redirigir el tráfico desde la capa de enlace de datos, controlando la ruta de transferencia de información. Este ataque suele mantenerse oculto a un usuario común ya que tendría que revisar las tablas ARP de su equipo para notar que algo no está correcto.

Por ejemplo, si el HOST PC A1 quiere conectarse al HOST PC B1 el conmutador *switch* intermedio debe encaminar la información mediante su tabla ARP, si este es corrompido, se puede lograr que un HOST PC C1 obtenga esa información cambiando o manipulando la tabla ARP del conmutador, sin que el usuario se percate de los ocurrido.

Sslstrip Software alojado en el sistema operativo, versión 0.9.2.

Arpspoof es un software alojado en el sistema operativo, o denominado spoofa. Suplantación de ARP herramienta de un conjunto de herramientas conocido como dsniff desarrollado por Dug Song en la Universidad de Michigan.

Ettercap Software alojado en el sistema operativo, versión 0.8.3-Bertillon.

2.2.3. MITM Evil twin

Cuando lo usuarios de la red inalambrica en el área pública activen su Wi-Fi en el teléfono móvil, tableta o computadora personal portátil, elegirán el nombre de la red inalámbrica que corresponde con un nombre proporcionado por las áreas públicas de la universidad, el campus, la institución, etc., debido a que una red inalámbrica solo puede ser reconocida por el Identificador de conjunto de servicios (SSID) y la dirección de Control de acceso a medios (MAC), el atacante puede configurar un Punto de acceso no autorizado con el mismo SSID del Punto de acceso legítimo para atraer Clientes Wi-Fi que se conectan a él.

2.2.3.1. mitmAP

Software alojado en el sistema operativo a utilizar, versión 2.0.

2.3. PROCEDIMIENTO PROPUESTO

- Realizar una suplantación de identidad de una pagina web utilizando setoolkit que corre dentro del servidor web local se propone el servicio web de apache.
- Se propone usar ettercap para lanzar el ataque MITM utilizando la modalidad de dns spoofing.
- Primero se debe cambiar la configuración para que ettercap pueda redirijir el tráfico de las maquinas que se planea atacar.
- Dentro de ettercap se encuentra la opción de escanear la red y encontrar dispositivos conectados dentro de esta seleccionar tanto el router en un lado y por el otro seleccionar las maquinas que se pretende atacar.
- Para que ettercap nos muestre cuando el dns spoofing y entregue las credenciales que la otra máquina objetivo ingrese.

Una vez conocidos los ataques y cómo funcionan o trabajan, la herramienta propuesta en este caso Kali Linux no requieren mayor procedimiento para ser implementados, al igual que cualquier otra herramienta a utilizar en el campo de la ciberseguridad.

CAPÍTULO 3: ANÁLISIS Y ESTUDIOS DE ATAQUES MITM DESARROLLADOS

3.1 TRABAJO SOBRE EL ESTUDIO DE ATAQUE AUTOMÁTICO MITM CONTRA REDES WIFI

Este documento es una versión extendida de una versión original presentada en la novena Conferencia Internacional de EAI sobre Forense Digital y Delito Cibernético (Vondr a cek, Pluskal y Ry sav y, 2018) (Vondráček et al., 2018). Como dice el documento existen mejoras en la tecnología las cuales han pasado recientemente además de la introducción que estamos teniendo a tecnologías como 5G. Estas redes inalámbricas se vuelven más convenientes el acceso desde cualquier lugar y existen redes de mayor área de cobertura lo cual fortalece los beneficios de comunicación. La instalación y la configuración de redes inalámbricas cada vez se vuelve más fácil, pero esto también conlleva a la desinformación que tienen estas personas acerca de la seguridad que se debe tomar ya que un atacante potencial necesita estar dentro de la proximidad física de la red inalámbrica para ser una potencial amenaza hacia la red y los usuarios que ocupan dicha red.

Como ya se conoce el primer estándar web WEP era demasiado débil, por ello luego fue la introducción de WPA estándar más fuerte y más tarde WPA2 aún más fuerte. En 2017, Mathy Vanhoef anunció que descubrió una vulnerabilidad en los mecanismos de seguridad que utilizan el protocolo four-way *handdhake* (apretón de manos de cuatro vías. WPAy WPA2) y demostró la facilidad con que se puede explotar esta vulnerabilidad.

Se revisan datos estadísticos interesantes dentro de este trabajo, que se pueden observar en la Tabla 3.1, en esta tabla se observa que un número significativo de usuarios de la WLAN todavía

utiliza algoritmos de seguridad obsoletos, datos proporcionados por Wileaks.cz, estas medidas constan de 97’192.922 mediciones de 2’548.054 redes WLAN.

Tipo de Seguridad	Conteo	Porcentaje
WPA2	1’429.518	56%
WEP	393.579	15%
WPA	375.984	15%
open	67.388	3%
other	281.585	11%

Tabla 3. 1: Conecciones WLA de la República Checa 26 de mayo 2017(Vondráček et al., 2018)

En la Tabla 3.2, se centra en las vulnerabilidades de un ISP llamado UCP, con respecto a las contraseñas WPA2 PSK configuradas de manera predeterminada.

Brno, República Checa, 2016-02-10	Conteo	Porcentaje
Redes Total	17.516	
Redes UPC	2.868	16.37%
Redes UPC vulnerables	1.835	63.98 % UPC

Tabla 3. 2: Vulnerabilidades de contraseñas WPA2 PSK del ISP UPC(Vondráček et al., 2018)

El éxito de este experimento es realizar las conexiones de manera satisfactoria para que la comunicación con el internet sea constante y correcta para así utilizar las herramientas de los ataques siendo el que controla el tráfico de la red. Como una métrica observada dentro de este tipo de ataques existen un tiempo de ida y un tiempo de vuelta para él envió de paquetes lo que resultaría en un retaso que el usuario podría experimentar cuando estos ataques se estuvieran realizando

dentro de la red. Los casos evaluados dentro del documento revelaron que se hicieron estudios para ver si los usuarios dentro de la red podrían tener alguna sospecha sobre si estaban siendo parte de este ataque o si sintieron algún cambio dentro de su red y se pudo concluir que el usuario normal no tiene forma de saber si la reducción de velocidad dentro de una de sus redes es por causa de un ataque o por una causa normal de baja conexión como es nuevos usuarios conectándose a la misma red o un uso masivo de la misma.

Uno de los puntos de este documento es mostrar herramientas que ya están implementadas para automatizar los pasos que se tiene que seguir para realizar un ataque MITM incluyendo las limitaciones que te puedes encontrar utilizando estas herramientas y no realizar los pasos independientemente. Explotar vulnerabilidad del WPS es un estudio que se puede realizar en un futuro ya que las vulnerabilidades de las redes WLAN se están explotando mas ahora en día y existen muchas.

3.2 TRABAJO SOBRE INTERNET DE LAS COSAS Y LOS ATAQUES MITM - SEGURIDAD Y RIESGOS ECONÓMICOS

En este trabajo se presentan algunos aspectos de Internet de las cosas (IoT) y los ataques a los que IoT puede estar expuesto, sobre todo, el ataque del hombre en el medio (MITM) (Čekerevac et al., 2017).

En años anteriores los ataques MITM afectaban principalmente a las computadoras portátiles, pero ahora, debido a la gran cantidad de teléfonos celulares, un gran número de usuarios pueden estar bajo ataque. El problema podría ser aún peor porque un estudio reciente de Symantec mostró que alrededor del 50% de los encuestados ni siquiera pensaban en su protección de datos.

Este trabajo muestra estadísticos y apreciaciones más interesantes, como el de la figura 3.1 donde indica que según la investigación de McAfee (McAfee, 2016), los ataques más frecuentes son un ataque DoS y MITB, juntamente con el ataque SSL, constituyen el ataque MITM. Juntos realizan el 64% de todos los ataques.

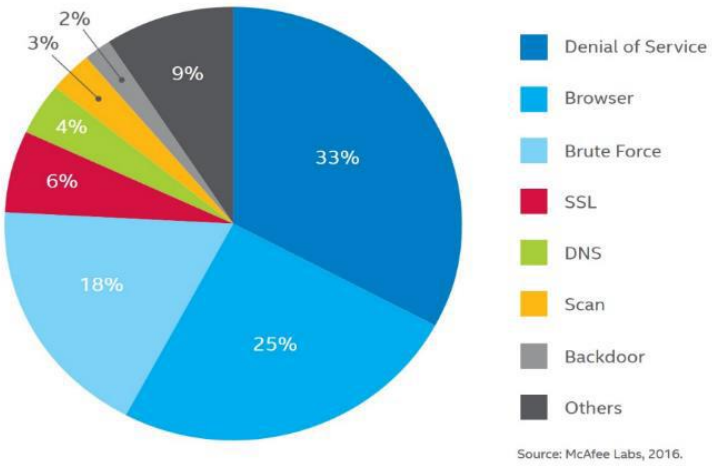

Figura 3. 1: Top de los ataques de red (Čekerevac et al., 2017)

En la actualidad hay millones de dispositivos de Internet de las cosas vulnerables, y su número sigue creciendo, la mayoría de ellos siempre están activados y residen en redes no supervisadas. El trabajo también entrega un dato económico como ejemplo de pérdida por los ataques del tipo MITM. El 2 de diciembre de 2013, la División del FBI de Seattle anunció que está al tanto de un fraude que victimiza a las empresas con sede en el estado de Washington, con la pérdida total experimentada por las tres compañías del área es de aproximadamente $ 1.65 millones (Čekerevac et al., 2017).

3.3 TRABAJO SOBRE UNA REVISIÓN DE LOS ATAQUES DEL HOMBRE EN EL MEDIO

Este trabajo muestra encuesta de ataques MITM en redes de comunicaciones ("review of man-in-the-Middle attacks," 2015) y se contrastará con otros datos más actualizados. Se menciona sobre el ataque SSL para dominios populares como google.com, yahoo.com, live.com y skype.com. Los certificados SSL falsos fueron emitidos por Comodo, la autoridad de certificación de confianza. El ataque fue descubierto y los certificados falsos fueron revocados.

Los servicios web se verían alterados debido a este certificado que facilita diferentes tipos de ataques, como los ataques de phishing. Para verificar la validez de los certificados TLS, los navegadores usan listas de revocación. Pero estas listas de revocación no están disponibles si Internet tiene una interrupción. Por lo tanto, se ha sugerido que los certificados no confiables deben codificarse permanentemente en los navegadores. La mayoría de los sistemas operativos disponibles ahora tienen un actualizador automático instalado para los certificados revocados. La actualización automática descargará automáticamente el certificado cancelado sin el conocimiento del usuario.

En la figura 3.2 se muestra una gráfica sobre la vulnerabilidad de los navegadores, son aplicaciones muy complicadas por lo tanto propenso a errores, “Entre 2013 y 2017, aproximadamente el 11% de las vulnerabilidades en total 40671 se encontraron en los 4 principales navegadores Chrome, Firefox, Internet Explorer y Edge”, A excepción de Chrome y Firefox, la mayoría de los exploits, se publican después de la vulnerabilidad ("Symantec attack patterns – IT security matters," n.d.).

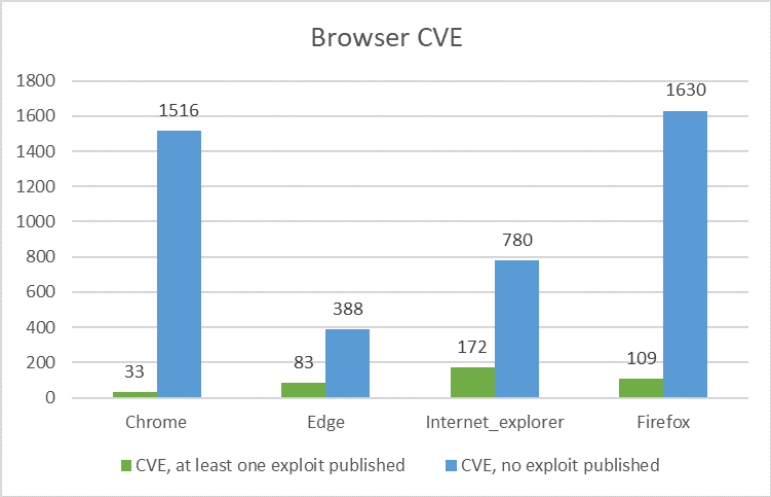

Figura 3.2: Publicación de explotación fecha de publicación de CVE 2013 – 2017 ("Symantec attack patterns – IT security matters," n.d.).

Se considera al ataque MITM una forma moderna de espionaje de manera anticuada, sin embargo no es simple, los ataques MITM también incluyen el uso de inyección o alteración de contenido, así como otras tácticas, la publicación del portal thesslstore.com ("80 eye-opening cyber security statistics for 2019," 2019) menciona que el 95% de los servidores son vulnerables a los ataques de MITM, además Los ataques MITM estuvieron involucrados en el 35% de las explotaciones Más de un tercio de la explotación de debilidades inadvertidas involucraron ataques MITM, según el Índice de Inteligencia de Amenazas X-Force 2018 de IBM. Otro dato interesante es que 10% de las empresas implementan HSTS. Solo el 10% de las empresas han implementado HTTP *Strict Transport Security* (HSTS) para sitios web, según una investigación de W3Techs ("80 eye-opening cyber security statistics for 2019," 2019).

3.4 ÀNALISIS DE UN CASO ACTUAL ZOOM VIDEO

Se analiza un caso particular en esta época de pandemia mundial ("Acceso," n.d.), es la aplicación ZOOM (Zoom Video, n.d.), es una empresa especializada en videoconferencia y audioconferencia en dispositivos móviles, computadoras de escritorio, fundada en 2011 que cotiza en bolsa en Nasdaq (ticker: ZM) y tiene su sede en San José, California.

Orientado a la seguridad (Video Conferencing, Web Conferencing, Webinars, Screen Sharing - Zoom, n.d.) la página oficial de ZOOM indica las tecnologías de cifrado que ayudan a la privacidad y seguridad del usuario todos sus datos e información transmitida mediante video *streaming* o flujo de video, se menciona las aplicaciones ZOOM clientes y cuando se usa en un explorador, según zoom se utilizan los siguientes métodos en sus aplicaciones, TLS 1.2, AES, SRTP. En este periodo de pandemia donde el trabajo desde casa aumento considerablemente, solo en marzo de 2020, se informó que el tráfico diario a la página de descarga de ZOOM un aumento del 535%, en el mismo mes hubo más de 200 millones de participantes diarios de la reunión de Zoom (Winder, 2020), Webroot experimento un aumento superior al 2000% en lo que respecta a archivos maliciosos con el nombre de ZOOM.

Según datos de BrandShield (Muncaster, 2020), en el último mes se han establecido más de 2000 nuevos dominios de phishing, y desde principios de año se habían registrado 3300 dominios nuevos con la palabra ZOOM en ellos, el 67% creados en marzo, además casi el 30% de estos nuevos dominios han activado un servidor de correo electrónico para facilitar los ataques de phishing. Se ha escuchado hablar de ZOOM como un malware en varias ocasiones, pero el engaño es otra práctica conocida en la ciberseguridad que quieren explotar su popularidad, no sorprende

ver esta tendencia, todos estos intentos incluyen descargar en forma encubierta malware a la máquina de la víctima, robar dinero de los usuarios de ZOOM, obtener detalles de la información y datos de los usuarios para comprometer cuentas y/o infiltrar llamadas confidenciales.

Una de las principales preocupaciones es la compartición de las identificaciones de en las reuniones pues, caso contrario pueden ser víctimas de ser 'Zoombombados', es decir tener invitados no deseados en la reunión, El FBI ha recibido múltiples informes de conferencias educativas interrumpidas por imágenes pornográficas y/o discursos de odio y lenguaje amenazante. La Cámara de Representantes de los EE. UU. Fue la víctima más reciente de un ciberataque de "bombardeo con zoom". La reunión fue interrumpida en al menos tres ocasiones por asistentes no invitados, como se informó recientemente en una carta interna a Carolyn Maloney, presidenta del Comité de Supervisión y Reforma de Nueva York, que es el principal comité de investigación de la Cámara de Representantes de los Estados Unidos ("Zoom-bombing" attacks during COVID-19: How can I protect myself?," 2020).

Se prohibió el uso a empleados del Ministerio de Defensa (MoD) del Reino Unido, aunque el Primer Ministro, Boris Johnson, todavía la usó para una reunión de gabinete (Muncaster, 2020). Debido a que ZOOM es un software complicado tiene sus errores, también se tienen varios reportes sobre otro tipo de vulnerabilidades a la seguridad y privacidad de los datos e información, por ejemplo ("latest Zoom security vulnerabilities: What you need to know," 2020), "El informe: Joe Cox, escribiendo para Vice Motherboard, informó el 26 de marzo de 2020 que la aplicación Zoom iOS envía datos a Facebook incluso si no tiene una cuenta de Facebook", Joe informó el problema a ZOOM por lo que eliminó el SDK de Facebook de su aplicación iOS para plataformas Apple al eliminar la función 'Iniciar sesión con Facebook'.

CONCLUSIONES

El presente trabajo trata de dar una vista resumida sobre la ciberseguridad orientada al estudio de los tipos de ataque MITM, desde un punto de vista teórico y de flujo de datos e información a través de Internet para un usuario de la red es importante entender sobre todos los riesgos que conlleva crear y mantener su información no solo social sino también financiera dentro de servidores que le proveen decenas de servicios algunos necesarios otros innecesarios para su cotidianidad.

En el primer capítulo se trata temas conceptuales sobre seguridad de la información, la pirámide de conocimiento, vulnerabilidades y contramedidas típicas dentro de la ciberseguridad, cual es la metodologías de ataque y definiciones sobre ética y privacidad, todas estas definiciones para dar una idea global a los usuarios que navegan y utilizan los servicios de la red sobre la enorme complejidad en el cual se están sumergiendo, los riesgos que conlleva utilizar los servicios en la red que cada vez utiliza nuevos protocolos, nuevas aplicaciones, nuevos servicios, etc.

Este universo de nuevas formas de comunicar la información a pesar de los múltiples beneficios traen consigo también multiplicidad de riesgos, ya que los diseñadores, desarrolladores, implementadores de aplicaciones y servicios en lo último que piensan es en la seguridad esto se planea realizar al final cuando la aplicación o servicio ya este implementado, eso se puede ver en los ejemplos de los trabajos analizados en el capítulo 3, con estudios estadísticos se analiza el enorme desafío de la ciberseguridad personal para que se pueda garantizar una navegación y utilización de los servicios de manera segura.

Los nuevos diseños y desarrollos del internet de las cosas y el *cloud computing* o computación en la nube también se transforman en nuevos retos para la ciberseguridad personal, un camino largo

por recorrer en un mundo digitalizado con cada vez mayor cantidad de datos e información transitando por ella, los esfuerzos también de crear nuevas taxonomías como se muestra en un ejemplo de trabajo en este capítulo para entender los diferentes tipos de ataques, riesgos o vulnerabilidades hacen que la ciberseguridad sea siempre un tema actual que trate de mantenerse a la par de la evolución de la tecnología.

No fue posible la realización de un trabajo de campo debido al tema emergencia sanitaria en estos instantes, el proyecto inicialmente fue diseñado para recolectar información y datos explotando algunas vulnerabilidades con herramientas y conceptos conocidos de la ciberseguridad, queda a libertad del lector llevar a cabo estas prácticas utilizando los conceptos y procedimientos explicados en este trabajo los cuales se han resumido de una manera que pueda comprenderse las potencialidades y riesgos de la ciberseguridad personal, dentro de una área inalámbrica de un campus, edificio o espacio abierto.

Las redes inalámbricas actualmente se han vuelto muy populares así también muy riesgosas debido a las vulnerabilidades conocidas y también a las nuevas vulnerabilidades que durante el tiempo se van conociendo, se trató de un proyecto de ejemplo de este tipo de vulnerabilidades en este capítulo, se pudo observar que los riesgos y vulnerabilidades existen en diferentes capas, estas capas se han estandarizado en el modelo OSI para una mejor comprensión y manejo, llevando a trabajar a la ciberseguridad personal por capas para su mejor comprensión.

REFERENCIAS BIBLIOGRÁFICAS

(PDF) Analysis of phishing attacks and countermeasures. (2006, January 1). ResearchGate. https://www.researchgate.net/publication/235947501_Analysis_of_Phishing_Attacks_and_Countermeasures

80 eye-opening cyber security statistics for 2019. (2019, June 28). Hashed Out by The SSL Store™. https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/

Acceso. (n.d.). WHO | World Health Organization. https://www.who.int/es

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. John Wiley & Sons.

Cabanillas, D. (n.d.). *SEGURIDAD Y PRIVACIDAD DE DATOS*. UOC Universidad Oberta de Cataluña.

Hwang, H., Jung, G., Sohn, K., & Park, S. (2008). A study on MITM (Man in the middle) vulnerability in wireless network using 802.1X and EAP. *2008 International Conference on Information Science and Security (ICISS 2008)*. https://doi.org/10.1109/iciss.2008.10

ISO/IEC 27000:2018. (n.d.). ISO. https://www.iso.org/standard/73906.html

ISO/IEC 27032:2012. (n.d.). ISO. https://www.iso.org/standard/44375.html

Jifa, G., & Lingling, Z. (2014). Data, DIKW, Big Data and data science. *Procedia Computer Science*, *31*, 814-821.

Kuo, E., Chang, M., & Kao, D. (2018). User-side evil twin attack detection using time-delay statistics of TCP connection termination. *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 211-216. https://doi.org/10.23919/icact.2018.8323699

The latest Zoom security vulnerabilities: What you need to know. (2020, April 22). Rapid7 Blog. https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109. https://doi.org/10.22373/cj.v2i2.3453

Messier, R. (2018). *Learning Kali Linux: Security testing, penetration testing and ethical hacking*. O'Reilly Media.

Minguillon, J. (2018). *Fundamentos de data science: Conceptos básicos*. UOC Universidad Oberta de Cataluña.

Muncaster, P. (2020, April 2). *Zoom Phishers register 2000 domains in a month*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/zoom-phishers-register-2000/

Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science*. CRC Press.

A review of man-in-the-Middle attacks. (2015, April 8). ResearchGate. https://www.researchgate.net/publication/274730018_A_Review_of_Man-in-the-Middle_Attacks

Stricot-Tarboton, S., Chaisiri, S., & Ko, R. K. (2016). Taxonomy of man-in-the-Middle attacks on HTTPS. *2016 IEEE Trustcom/BigDataSE/ISPA*. https://doi.org/10.1109/trustcom.2016.0106

Symantec attack patterns – IT security matters. (n.d.). IT Security Matters. https://klausjochem.me/tag/symantec-attack-patterns/

(n.d.). Video Conferencing, Web Conferencing, Webinars, Screen Sharing - Zoom. https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf

Vondráček, M., Pluskal, J., & Ryšavý, O. (2018). Automated man-in-the-Middle attack against Wi-Fi networks. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2018.1495

Waschke, M. (2017). *Personal cybersecurity: How to avoid and recover from cybercrime*. Apress.

Winder, D. (2020, April 12). *Zoom isn't malware but hackers are feeding that narrative, and how: Zoom-related threats up 2,000%*. Forbes. https://www.forbes.com/sites/daveywinder/2020/04/12/zoom-isnt-malware-

but-hackers-are-feeding-that-narrative-and-how-zoom-related-threats-up-2000/#46932fd41ae5

(n.d.). Zoom Video. https://zoom.us

Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017). Internet of things and the man-in-the-middle attacks – security and economic risks. *MEST Journal*, *5*(2), 15-5. https://doi.org/10.12709/mest.05.05.02.03

"Zoom-bombing" attacks during COVID-19: How can I protect myself? (2020, May 4). Hornetsecurity – Cloud Security Services for Businesses. https://www.hornetsecurity.com/en/security-information/zoom-bombing/

ANEXO 1 – GLOSARIO

- IoT: Internet of things
- D-I-K-W: Data-information-Knowledge-Wisdom
- MITM: Man in the middle
- WPA: Wi-Fi protected access
- GSM: Global system for mobile communication
- ETA: Evil Twin Attack
- SSID: Service Set Identifier
- MAC: Media access control
- AP: Access point
- MySQL: My Structured Query Language (Database management system)
- DNS: Domain Name Service
- HTTP: Hypertext transfer protocol
- HTTPS: Hypertext transfer protocol secure
- ARP: Address resolution protocol
- IP: Internet protocol
- LAN: Local area network
- OSI: Open system interconection
- SSID: Service Set Identifier
- 802.1X: Estándar IEEE para control de acceso a la red basado en puertos.
- EAP: Extensible Authentication Protocol
- WEP: Privacidad equivalente por cable.
- ISP: Proveedor de servicios de internet, Internet Service Provider

- UCP: La empresa UPC es un importante ISP en la República Checa
- PSK: Pre-Shared Key, Clave precompartida
- DoS: Denial of Service, Denegación de servicio
- SSL: Security Socket Layer
- TLS: Transport Layer Security
- Wileaks.cz: **https://www.wifileaks.cz/statistika.php**
- Exploits : Agujeros de Seguridad dentro de sistemas.