doi: 10.47460/minerva.v2i6.39

Vulnerabilidad de ciberseguridad en el comercio electrónico, caso del protocolo http

Moreno Almanza Olmedo
olmedo.moreno@up.ac.pa
https://orcid.org/0000-0003-1944-8684
Universidad de Panamá,
Centro Regional Universitario de Panamá Oeste
La Chorrera-Panamá

Recibido (03/09/2021), Aceptado (04/010/2021)

Resumen: Este trabajo fue diseñado con la intención de analizar la vulnerabilidad de los sitios web de comercio electrónico. Vamos a describir la transmisión de datos en texto claro sin encriptación mediante el protocolo de transferencia de hipertexto (HTTP), por lo que argumentamos que mediante una técnica de sniffer se puede capturar esta información y así violar la información de privacidad del cliente.

Palabras Clave: Seguridad, Vulnerabilidad, Sniffing, http

E-commerce cybersecurity vulnerability, http protocol case

Abstract: This paper was designed with the intention of analyzing the vulnerability of e-commerce web sites. We are going to describe the transmission of data in clear text without encryption by hypertext transfer protocol (HTTP), reason why we argue that by means of a sniffer technique this information can be captured and this way violating customer privacy information.

Keywords: Security, Vulnerability, Sniffing, http

I.INTRODUCCIÓN

En esta época de conectividad electrónica universal en la que el mundo se está convirtiendo en una aldea global, diferentes amenazas como los virus y los hackers, las escuchas y el fraude, es innegable que no hay momento en el que la seguridad no importe [1]. [1]

Internet es una enorme red formada por una combinación de millones de redes conectadas desde todo el mundo. Cuando se envían datos por Internet de una red a otra, los datos en tránsito y los almacenados en servidores, ordenadores, bases de datos, son vulnerables, en el sentido de que pueden ser fácilmente accesibles por personas no autorizadas tanto en tránsito como en almacenamiento. Debido a la cantidad de redes que atraviesan los datos antes de llegar a su destino final, no es fácil proporcionar una seguridad total de los datos en tránsito, incluso cuando han sido encriptados. Todos los sitios web a los que se accede en Internet son lanzados por servidores web. Las cuentas financieras, los correos electrónicos, etc., se guardan en bases de datos en servidores web y si un atacante vulnera el sistema de seguridad y es capaz de entrar en un servidor web, dicha información correría el riesgo de ser robada o manipulada. Hoy en día, los gobiernos y las organizaciones criminales apoyan y financian equipos altamente capacitados que planifican y ejecutan ciberataques. El objetivo de estos ataques es robar información confidencial que pueda ser vendida o utilizada en beneficio del atacante. Los datos guardados en bases de datos, servidores web, etc., pueden ser accedidos por personas no autorizadas en cualquier momento, por lo que es posible que esto provoque la pérdida de información sensible y confidencial de personas, empresas, etc. y, en consecuencia, la pérdida de millones, en términos monetarios, para la víctima. Las personas no autorizadas que acceden a dicha información pueden ser usuarios legítimos de la red[2]

Cada vez más en nuestra vida cotidiana se utilizan las aplicaciones web. Las aplicaciones web se utilizan a menudo para funcionalidades empresariales críticas y para almacenar información financiera y personal sensible. Los atacantes están buscando nuevas vulnerabilidades de los sistemas todo el tiempo y también creando exploits para abusar de estos hallazgos. Es fundamental que las empresas se protejan contra estos exploits. Si un atacante es capaz de exponer datos sensibles u obtener acceso sin restricciones al sistema, puede tener un grave impacto en el negocio y la reputación de la empresa [3].

La seguridad de las aplicaciones web ha recibido mucha atención en los últimos años. Grupos como Anonymous y LulSec han atacado a numerosas organizaciones privadas y públicas y han extraído información de ellas y la han filtrado al público. También el incidente de LinkedIn, donde se filtraron las contraseñas de millones de sus usuarios, son sólo algunos ejemplos de la importancia de identificar cómo se atacan las vulnerabilidades de las aplicaciones web y cómo las organizaciones pueden protegerse contra ellas [3].

La distribución de este trabajo es la siguiente, en la sección II se refiere al protocolo de comunicación Protocolo de transferencia de hipertexto (HTTP), en la sección III se describe la mitología de sniffing, en la sección IV se describen los resultados, en la V algunos aspectos referentes a la mitigación, en la sección VI las conclusiones.

II.DESARROLLO

A.Visión general de HTTP

El protocolo de transferencia de hipertexto (HTTP) es un protocolo sin estado y utiliza un modelo basado en mensajes. Básicamente, un cliente envía un mensaje de solicitud y el servidor devuelve un mensaje de respuesta. El RFC 2616 define numerosas cabeceras diferentes para los mensajes de solicitud y respuesta, que se discutirán más adelante en este documento. Cuando se ataca una aplicación web, la carga útil se envía en el mensaje de solicitud. Existen diferentes posibilidades para hacerlo: utilizar métodos HTTP peligrosos, modificar los parámetros de la solicitud o enviar otro tipo de tráfico malicioso[4].

Los métodos HTTP son funciones que un servidor web proporciona para procesar una solicitud. GET es el más utilizado para recuperar un recurso de un servidor web. Enviará los parámetros directamente en la cadena de consulta de la URL. El método POST se utiliza para realizar acciones y permite enviar los datos también en el cuerpo del mensaje. Ambos métodos son interesantes para un atacante cuando se trata de inyectar contenido malicioso[5]

El GET y el POST se utilizan para solicitar una página web y son los dos más comunes que se utilizan en HTTP. HEAD funciona exactamente igual que GET, pero el servidor sólo devuelve las cabeceras en la respuesta [6] . La desventaja de GET es que pasa cualquier parámetro a través de la URL y es fácil de manipular. Se recomienda utilizar POST para las peticiones porque los parámetros se envían en la carga útil de HTTP. De esta manera es más difícil manipular los parámetros, pero con el intercambio de métodos o el proxy de interceptación esto lo convierte en un

esfuerzo trivial [7].

B.Identificar el sitio web del entorno peligroso del comercio electrónico

En 2013, el gigante minorista Target vio comprometida la información de contacto y de las tarjetas de crédito de más de 110 millones de sus clientes. Esta filtración provocó la dimisión de su director general (CEO) y de su director de información al año siguiente. [8]

En otro incidente de violación de datos, Adobe informó de que los atacantes accedieron a las identificaciones y contraseñas cifradas de 38 millones de sus usuarios activos. Una investigación también descubrió que los hackers robaron el código fuente de varios de sus productos, incluido Photoshop. [8]

Y en otro incidente de violación de datos, Verizon tuvo 53.000 incidentes y 2.216 violaciones de datos confirmadas que resultaron en más de 43.000 accesos exitosos a través de credenciales robadas en 2018.[8]

El indicador del navegador se refiere a un icono opcional junto a la URL que es controlado por el navegador para indicar un estado de seguridad o inseguridad con respecto a la conexión actual y a veces el estado de la lista negra. Al hacer clic en los indicadores se obtiene más información y ajustes específicos del sitio o de la conexión. Las advertencias del navegador suelen aparecer en el área de contenido del navegador o surgen de un icono en la barra de URL, según el contexto. Ambas se utilizan actualmente en los navegadores convencionales para advertir al usuario de amenazas o darle confianza en sus actividades. Las advertencias de los navegadores han cambiado a lo largo de los años.

Actualmente los navegadores como mozilla firefox, Google Chrome e Internet Explorer tienen el análisis de los sitios web para este caso que utilizamos jugando con la versión 81 indica que el sitio web visitado potencialmente tiene problemas con la privacidad de los datos y podría ser obtenido por un tercero información como la contraseña del usuario información de la tarjeta de crédito. [9]

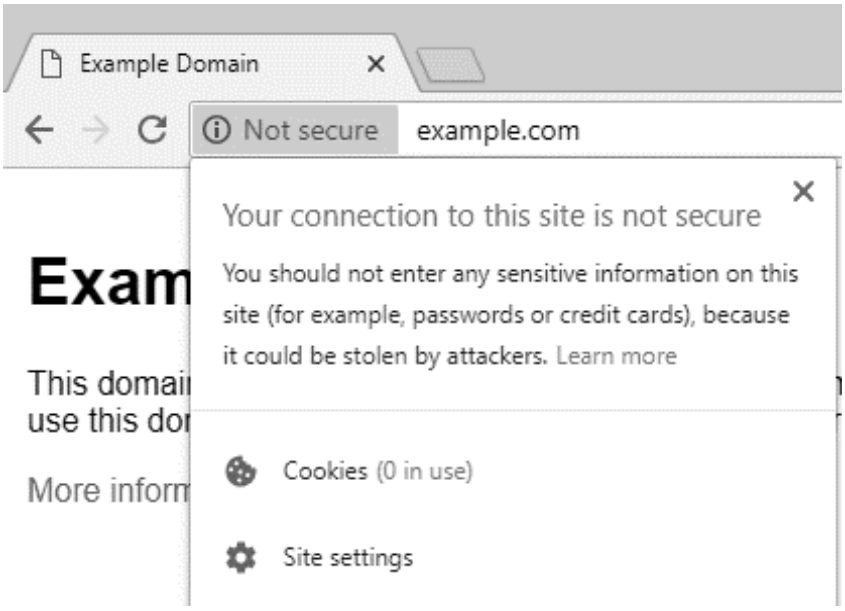

Fig 1: A partir de Chrome 68, Google Chrome etiqueta todos los sitios web que no son HTTPS como "No seguros" [10].

III.METODOLOGÍA

A.Metodología Sniffing

La tecnología de la información se está convirtiendo en una parte integral y básica de la infraestructura de las industrias y organizaciones. Con el enorme crecimiento y desarrollo de las redes informáticas y de Internet, la administración y la auditoría del tráfico de datos son importantes para aumentar la seguridad y la eficacia de un sistema de red global. El packet sniffing es el proceso de recogida de paquetes de datos de la red como datos binarios, convierte esos datos

binarios en un formato legible y los analiza mostrando los protocolos utilizados, las contraseñas en texto plano, etc., lo que ayuda a los administradores de la red a supervisar y controlar la red informática para superar el abuso de los activos informáticos y disminuir el riesgo de ataques externos y el mal funcionamiento de los ordenadores. Así como simplificar la resolución de problemas de la red mediante la detección y el reconocimiento de los errores y el mal uso de los datos por parte de empleados descontentos y/o atacantes. [11]

Hay varios objetivos para habilitar las herramientas de sniffing de paquetes, algunos de ellos en los siguientes puntos:

•Los administradores de la red los utilizan para analizar, supervisar y auditar el tráfico de la red para investigar el abuso de los empleados de los activos de TI que conducen a prevenir la violación de las políticas, normas y procedimientos de una industria u organización.

•Los rastreadores de paquetes se utilizan como prueba de detección de intrusos y de penetración por parte de los desarrolladores de aplicaciones de red, programadores, ingenieros de redes y de seguridad, especialmente para alarmar sobre el mal funcionamiento de la red o el ataque cuando el rendimiento de la red es lento o no funciona.

•Ayudar a los administradores de red a detectar los puntos débiles, las amenazas y las vulnerabilidades de la red para mejorar la seguridad general de las redes.

•Comprender las diferentes aplicaciones de red que utilizan el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagramas de Usuario (UDP), sus parámetros, tipo de carga útil, IP, direcciones de Control de Acceso al Medio (MAC), etc. [12]

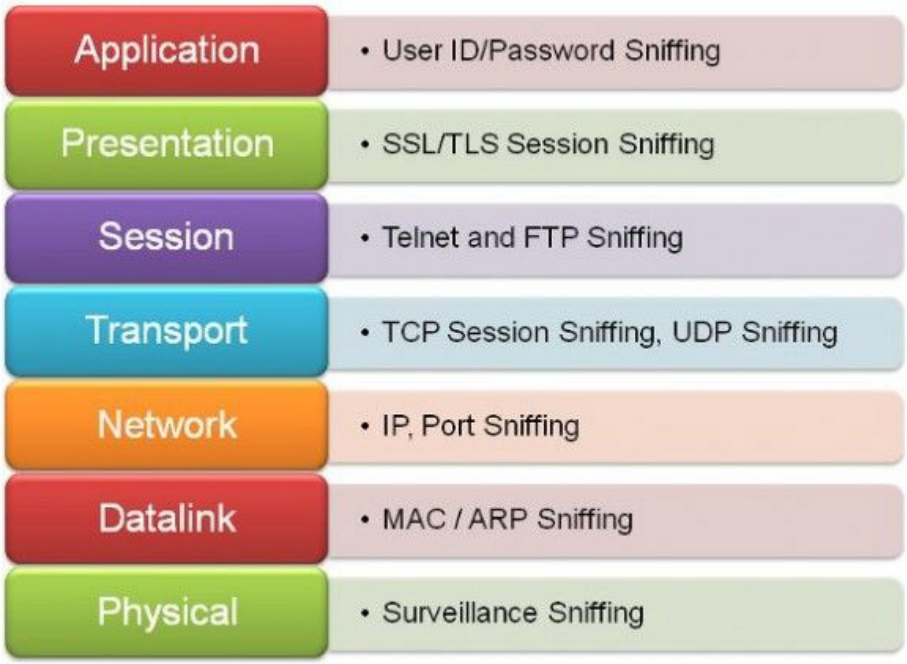

Fig 2: muestra las capas OSI y la información que un pirata informático puede robar en cada capa si consigue husmear en una red[13].

Es importante recordar que el sniffing puede abarcar desde la Capa 1 hasta la Capa 7. Hablando de conectividad física, una persona (que puede ser un empleado de la empresa) que ya esté conectada a la LAN interna puede ejecutar herramientas para capturar directamente el tráfico de la red. Utilizando técnicas de suplantación de identidad, un pirata informático ajeno a la red objetivo puede interceptar los paquetes a nivel del cortafuegos y robar la información. En la forma más reciente de esnifar paquetes, el uso generalizado de las redes inalámbricas ha facilitado la posibilidad de situarse cerca de la red y penetrar en ella para obtener información[13].

Independientemente de dónde se encuentren los hackers en la red que se está husmeando, utilizan software de

captura de paquetes o packet sniffer. Se supone que los rastreadores de paquetes modernos se utilizan para solucionar problemas de la red, pero también pueden utilizarse para piratear. Consulte la siguiente tabla, que muestra el lado ético y no ético del software sniffer[13].

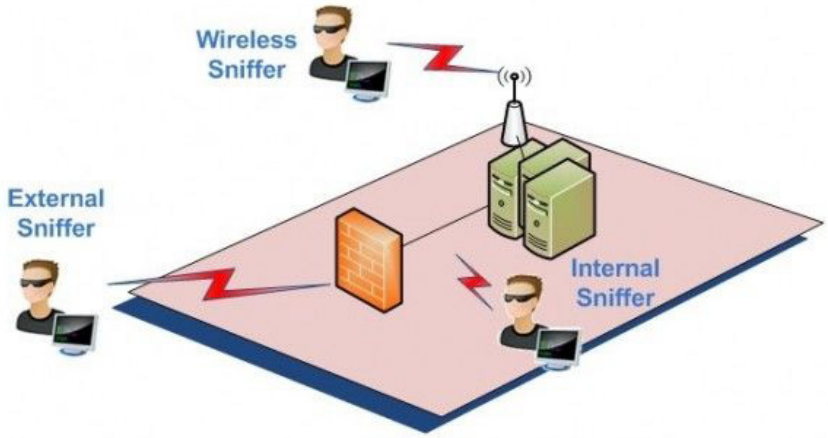

Fig 7: Mostrar como El rastreo de la red utiliza software de rastreo, ya sea de código abierto o comercial. A grandes rasgos, hay tres formas de rastrear una red[13].

Como su nombre indica, las sesiones HTTP son robadas y analizadas para robar el ID de usuario y la contraseña. Aunque se han incorporado las capas de sockets seguros (SSL) para asegurar las sesiones HTTP en la red, hay numerosos sitios web internos que siguen utilizando un cifrado estándar pero menos seguro. Es fácil capturar paquetes Base64 o Base128 y ejecutar un agente descifrador contra ellos para descifrar la contraseña. En los sniffers modernos, las sesiones SSL también pueden ser capturadas y analizadas para obtener información, aunque este método no es muy fácil [13].

B.Pasos para la captura de datos

Recogida: El Packet sniffer cambia la interfaz de red seleccionada al modo de promoción. En este modo, la tarjeta de red puede escuchar todo el tráfico de red en su segmento de red particular para capturar los datos binarios en bruto del cable.

Conversión: Los datos binarios capturados se convierten en una forma legible. Aquí es donde se detienen la mayoría de los rastreadores de paquetes avanzados basados en la línea de comandos. En este punto, los datos de la red están en una forma que puede ser interpretada sólo en un nivel muy básico, dejando la mayor parte del análisis al usuario final.

Análisis: El sniffer de paquetes toma los datos de red capturados, verifica su protocolo en base a la información extraída, y comienza su análisis de las características específicas del protocolo. Wireshark es uno de los analizadores de paquetes de código abierto más populares. Originalmente se llamaba Ethereal, pero en mayo de 2006 el proyecto pasó a llamarse Wireshark por cuestiones de marca[14].

C.Ciberataque

El ciberataque incluye cualquier tipo de maniobra ofensiva empleada por individuos o mientras organizaciones que tienen como objetivo el sistema de información informática, las infraestructuras, la red informática y/o los dispositivos informáticos personales por diversos medios de actos maliciosos, normalmente originados por una fuente anónima que roba, altera o destruye un objetivo específico mediante la piratería o el craking en un sistema susceptible. [15]

Ataque exterior

Un ataque externo es aquel que se origina desde fuera de la red de la víctima. Estos ataques son organizados por personas que no poseen autorización de acceso a la red objetivo. El atacante puede atacar una red mediante el reenvío de correos electrónicos no deseados (e-mails), que pueden llevar software malicioso como troyanos, como se ha explicado. El motivo de este tipo de ataque varía de un atacante a otro. Puede incluir la codicia y, por lo general, lleva a

acceder a los nombres de usuario y contraseñas de las víctimas de forma ilegal para acceder a sus fondos [15]

Ataque de información privilegiada

Es un ataque que se origina en la red de la víctima. Este tipo de ataque lo llevan a cabo personas que tienen autorización de acceso para utilizar una red determinada. Estas personas pueden ser empleados descontentos o antiguos empleados que deciden organizar este tipo de ataques como venganza contra sus superiores o como medio de malversación de fondos. El ataque podría ser llevado a cabo por individuos o grupos de personas con diferentes motivos. La red puede pertenecer a una organización como una escuela, un banco, un hospital, etc. La mayoría de estos ataques son llevados a cabo por personas que conocen a fondo el sistema de seguridad de la red de la organización. Esto permite a estas personas organizar con éxito ciberataques eficaces y eficientes contra la red de la organización. Las estadísticas han demostrado que este tipo de ataques tienen una tasa de ocurrencia del 80% en comparación con los ataques externos [15].

IV.RESULTADOS

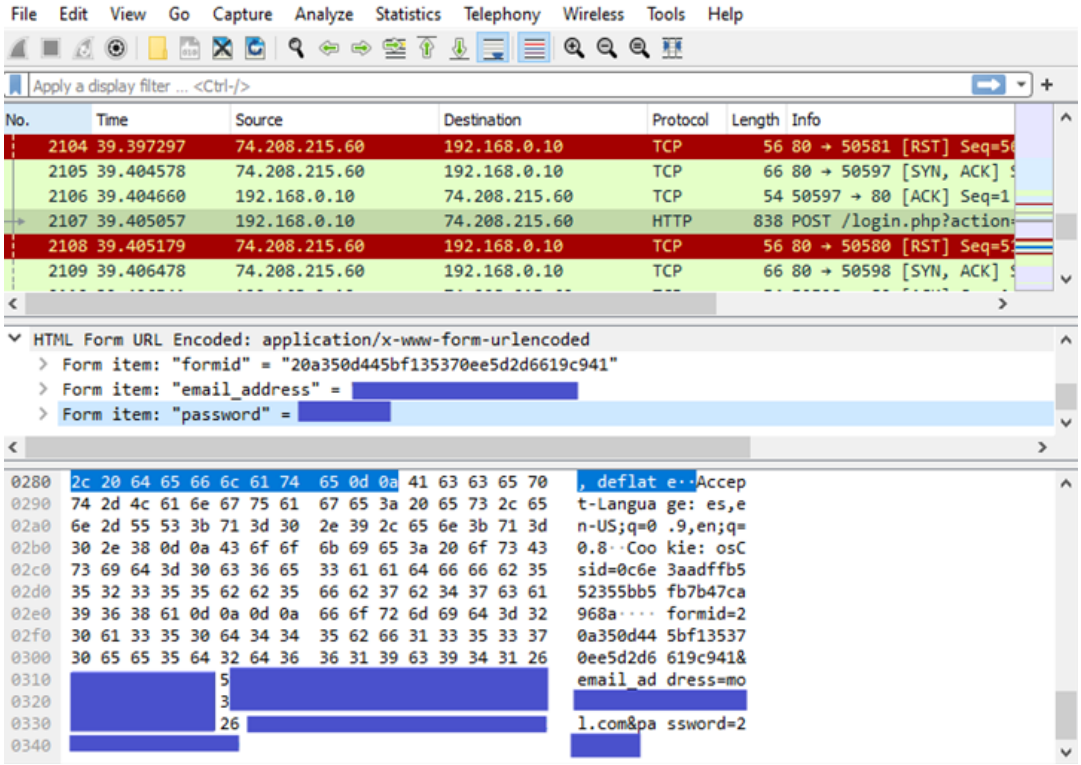

Fig 3: De acuerdo a la imagen para el sitio de comercio electrónico 1 podemos observar un claro ejemplo de extracción de usuario y contraseña a través de Wireshark, además podemos notar la captura de paquetes de red filtrando la información en texto plano en el protocolo HTPP, concretamente en la línea 2107 POST /login.php?action

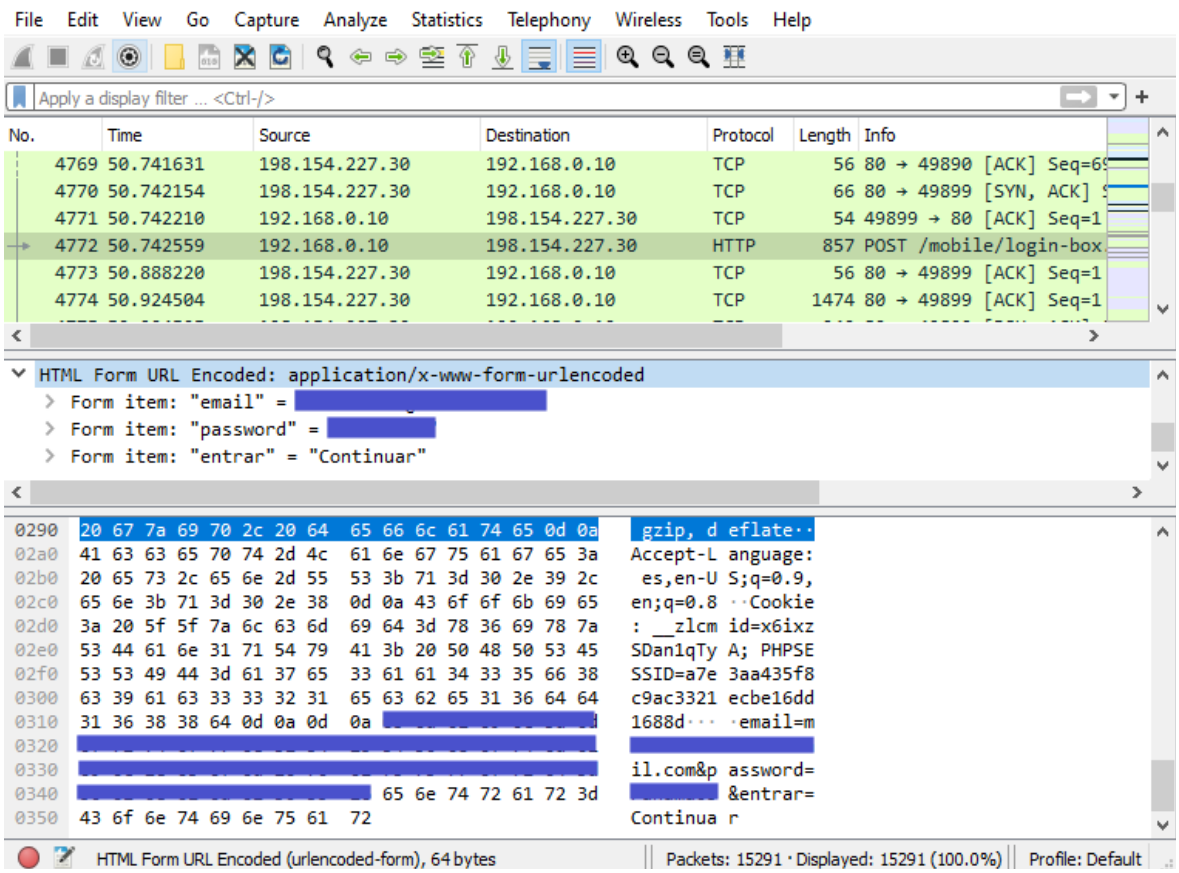

Fig 4: De acuerdo a la imagen para el sitio de comercio electrónico 2 podemos observar un claro ejemplo de extracción de usuario y contraseña a través de Wireshark, además podemos notar la captura de paquetes de red filtrando la información en texto plano en el protocolo HTPP, concretamente en la línea 4772 POST /mobile/login box.php?

V.MITIGACIÓN

A.Protección contra sniffers

Aunque el primer paso debería ser diseñar un sistema de defensa perimetral estricto mientras se crea la arquitectura de la red, hay algunos métodos que se pueden implementar para que la infraestructura sea menos propensa a los sniffer. Los siguientes trucos ayudan a conseguirlo en gran medida.

Desactivar el modo promiscuo en las interfaces de red tiene como resultado el cierre de la mayoría del software de sniffer. Esto se puede hacer ejecutando un script de administración como trabajo diario en la red, o desplegando una política de red a nivel de host para controlar el acceso a los ajustes de configuración de la tarjeta de red.

El uso de redes conmutadas puede reducir la posibilidad de que un sniffer se ejecute en la red. A diferencia de lo que ocurre en un concentrador de red, en una red conmutada los paquetes se entregan al destino y no son visibles para todos los nodos, lo que reduce las posibilidades de que alguien los husmee por el camino. Además, para los administradores de la red resulta fácil detectar a los sniffers centrándose en los segmentos de la red conmutada, de uno en uno.

Las herramientas antisniffing pueden utilizarse para detectar el modo de interfaz de red, así como diversos procesos y software presentes en los servidores o hosts de red. Los sistemas modernos de detección de intrusos tienen esta función integrada.

El cifrado IPSec puede utilizarse para la seguridad de los paquetes en la infraestructura de red, si los datos son de carácter confidencial. IPSec proporciona encapsulación y encriptación de datos de alto nivel, y está disponible en routers

modernos, cortafuegos y otros componentes de red. Casi todos los sistemas operativos son compatibles con IPSec, y se utiliza ampliamente en infraestructuras informáticas serias. Para la protección de la capa de sesión, se pueden utilizar SSL y TLS para cifrar el tráfico[13].

B.Cifrado

El cifrado es uno de los aspectos importantes al momento de mitigar el riesgo por perdida de información, bajo este esquema se puede preservar la privacidad de los usuarios tomando como dinámica el transporte de los datos tanto al momento de abrir la comunicación con el servidor como también al momento de que el servidor se encuentre en un estado de reposo, además también el cifrado nos ayuda con la transmisión de información en tiempo real bajo esquemas de seguridad aceptable[16].

VI.CONCLUSIONES

Los resultados encontrados en esta investigación muestran que es posible obtener la información de la cuenta del cliente, utilizar la herramienta correcta, la metodología, y seguir pasos simples. Muchos sitios web de comercio electrónico se encuentran bajo esta peligrosa práctica, utilizan el protocolo de transferencia de información sin encriptar porque solo compran el dominio y el alojamiento web pero no entienden que la seguridad es un pilar importante en este negocio. En otra ocasión al integrar la tecnología web no se toman los procedimientos de seguridad necesarios para evitar la pérdida de datos de los clientes en ocasiones cuando este riesgo se materializa los datos quedan expuestos y pueden ser obtenidos por personas malintencionadas.

Para una mejor práctica de seguridad, es necesario poder implementar una herramienta de monitoreo de vulnerabilidades o de análisis de riesgos, estas ayudarán a mitigar los riesgos al momento de lanzar nuestro proyecto de comercio electrónico, o también puede ayudar de manera positiva al momento de recuperarse de un evento desastroso.

El protocolo HTTP no se recomienda su uso en aplicaciones web o páginas de comercio electrónico, en este momento de investigación es de aceptación general el protocolo Hypertext Transfer Protocol Secure (HTTPS) que utiliza encriptación de texto y se transporta mediante Secure Socket Layer (SSL).

REFERENCIAS

[1]N. Ahmad y H. M. Kashif, "Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution", M.S. thesis Blekinge Institute of Technology, 2010.
[2]E. Nsambu y D. Aziz, "Computer Engineering The Defense Against the latest Cyber Espionage both insider and outsider attacks", M.S. thesis Mid Sweden University, 2012.
[3]N. Särökaari, "Identifying malicious HTTP Requests", B.S. thesis Haaga-Helia University, 2012.
[4]R. Fielding et al., "Hypertext Transfer Protocol -- HTTP/1.1", ACM Digit. Libr., pp. 13–176, jun. 1999, doi: 10.17487/rfc2616.
[5]D. Stuttard y M. Pinto, The web application hacker's handbook : finding and exploiting security flaws. Wiley, 2011.
[6]D. Gourley, B. Totty, S. Marjorie, A. Aggarwal, y S. Reddy, "HTTP Guide", Foreign Aff., vol. 91, núm. 5, p. 635, 2012, [En línea]. Disponible en: https://www.oreilly.com/library/view/http-the-definitive/1565925092/.
[7]SANS Institute, "Web Application Penetration Testing Training | SANS SEC542", 2010, [En línea]. Disponible en: https://www.sans.org/cyber-security-courses/web-app-penetration-testing-ethical-hacking/.
[8]Bigcommerce, "Ecommerce Data Breaches: Real Costs of Security Mismanagement", 2020. https://www.bigcommerce.com/articles/ecommerce/ecommerce-data-breaches/ (consultado abr. 21, 2021).
[9]M. W. Holt, D. Zappala, K. Seamons, y P. Egbert, "After HTTPS: Indicating Risk Instead of Security", M.S thesis Brigham Young University, 2019.
[10]C. Hoffman, "Why Does Google Chrome Say Websites Are 'Not Secure'?", howtogeek.com, 2018. https://www.howtogeek.com/359298/why-does-google-chrome-say-websites-are-"not-secure"/ (consultado abr. 16, 2021).
[11]Z. Wilson, "Global Information Assurance Certification Paper Hacking: The Basics", 2001. Consultado: abr. 15, 2021. [En línea]. Disponible en: http://www.giac.org/registration/gsec.
[12]I. A. Ibrahim Diyeb, A. Saif, y N. A. Al-Shaibany, "Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study", Int. J. Comput. Netw. Inf. Secur., vol. 10, núm. 7, pp. 12–22, jul. 2018, doi: 10.5815/ijcnis.2018.07.02.
[13]V. Network, "Cyber Security Attacks Network Sniffing". https://www.valencynetworks.com/articles/cyber-secu-

rity-attacks-network-sniffing.html (consultado abr. 15, 2021).
[14]O. N. Henry y M. A. Agana, "Intranet Security Using A LAN Packet Sniffer to Monitor Traffic", en 9th International Conference on Computer Science and Information Technology (CCSIT 2019), jun. 2019, pp. 57–68, doi: 10.5121/csit.2019.90806.
[15]K. Uchino, Global Crisis and Sustainability Technologies. WORLD SCIENTIFIC, 2017.
[16]F. M. S. Carreno, O. C. F. Unda, C. L. C. Naranjo, y L. D. Rosales, "Security For Applications With Multiple Users", en 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), jun. 2020, vol. 2020-June, núm. June, pp. 1–6, doi: 10.23919/CISTI49556.2020.9141157.

RESUMEN CURRICULAR

Mgtr. Olmedo Moren Almanza

Docente de la Universidad Tecnológica de Panamá, Docente de la Universidad de Panamá, estudiante de Doctorado en Tecnología de la Información y Negocios Electrónicos por la Universidad Popular Autónoma del Estado de Puebla.