Enfoque UTE
ISSN: 1390-9363
ISSN: 1390-6542
Universidad Tecnológica Equinoccial

Cueva Hurtado, Mario E.; Alvarado Sarango, Diego Javier
Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación.
Enfoque UTE, vol. 8, núm. 1, Suppl, 2017, pp. 273-286
Universidad Tecnológica Equinoccial

DOI: https://doi.org/10.29019/enfoqueute.v8n1.128

Disponible en: https://www.redalyc.org/articulo.oa?id=572262176020

Enfoque UTE, V.7-Sup.1, Feb.2017, pp.273 - 286
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9363
Recibido (Received): 2017/01/09
Aceptado (Accepted): 2017/02/24

Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación.

(Analysis of free SSL/TLS Certificates and their implementation as Security Mechanism in Application Servers.)

Mario E. Cueva Hurtado [1], Diego Javier Alvarado Sarango[2]

Resumen:
La seguridad en la capa de aplicación (SSL), proporciona la confidencialidad, integridad y autenticidad de los datos, entre dos aplicaciones que se comunican entre sí. El presente artículo es el resultado de haber implementado certificados SSL / TLS gratuitos en servidores de aplicación, determinando las características relevantes que debe tener un certificado SSL/TLS, la Autoridad certificadora que lo emita. Se realiza un análisis de las vulnerabilidades en los servidores web y se establece un canal cifrado de comunicaciones con el fin de proteger de ataques como hombre en el medio, phising y mantener la integridad de la información que es trasmitida entre el cliente y servidor.

Palabras clave: Seguridad; Certificados SSL/TLS; Autoridad Certificadora; Vulnerabilidades; X.509; Kali Linux.

Abstract:
Security in the application layer (SSL), provides the confidentiality, integrity, and authenticity of the data, between two applications that communicate with each other. This article is the result of having implemented Free SSL / TLS Certificates in application servers, determining the relevant characteristics that must have a SSL/TLS certificate, the Certifying Authority generate it. A vulnerability analysis is developed in application servers and encrypted communications channel is established to protect against attacks such as man in the middle, phishing and maintaining the integrity of information that is transmitted between the client and server

Keywords: Security; Certificates SSL/TLS; Certifying Authority; Vulnerabilities; X.509; Kali Linux.

1. Introducción

Hoy en día, Internet es la herramienta más utilizada a nivel mundial debido al auge de los servicios y transacciones virtuales; se han desarrollado e incorporado una serie de elementos que contribuyen directamente al control de la seguridad, destacándose en ella los mecanismos seguros que son implementados para proveer confidencialidad, integridad y disponibilidad, brindando confianza a los clientes que se benefician de estos servicios. No obstante, las amenazas son cada vez más frecuentes y complejas, en este sentido los distintos protocolos establecidos para las transacciones web están basados en tecnología antigua, a pesar de haberse

[1] Universidad Nacional de Loja, Loja – Ecuador (mecueva@unl.edu.ec)
[2] Universidad Nacional de Loja, Loja – Ecuador (djalvarados@unl.edu.ec)

actualizado con mejoras, es posible que, estas no aporten el resultado esperado en toda la dimensión requerida de seguridad y sea necesario estudiar nuevos mecanismos de seguridad para las transacciones web.

Para este nivel de necesidades, el protocolo de seguridad TLS (Transport Layer Security) y SSL (Secure Socket Layer) son protocolos criptográficos que operan por debajo de la capa de aplicación y proporcionan cifrado de extremo a extremo a la seguridad de un gran número de protocolos, incluidos HTTPS, IMAPS, SMTP (Ordean & Giurgiu, 2010)(Durumeric & Kasten, 2013). SSL creada por la empresa Netscape Communication, famosa por la creación del navegador web Netscape Navigator, logró con SSL estandarizar un procedimiento para proporcionar comunicaciones seguras en la red (Clark & Van Oorschot, 2013)(Mu, Zhang, Du, & Lin, 2011).

Actualmente no existen estudios previos registrados en bases de datos científicas sobre el uso de certificados digitales gratuitos, por lo que el aporte del presente artículo es de gran importancia. Se plantea la siguiente pregunta investigativa ¿Se puede asegurar la trasmisión de datos con los certificados digitales SSL/TLS gratuitos en los servidores de aplicación?, para dar respuesta a esta pregunta se realiza las siguientes fases: Una fase de **análisis** en el que se determina las amenazas más comunes en los servidores de aplicación utilizando la herramienta Kali Linux v2.0; se determina las características técnicas que debe cumplir un certificado digital para que sea seguro, en base a una revisión sistemática basada en la metodología propuesta por Bárbara Kitchenham; y una fase de **implementación** en el que se selecciona e implementa el certificado digital basado en una comparativa de las Autoridades Certificadoras (AC) gratuitas con los parámetros obtenidos en la fase de análisis. Se comprueba las vulnerabilidades contrarrestadas. El escenario de prueba son los servidores de aplicación de la Universidad Nacional de Loja.

2. Metodología

En todo proceso investigativo es necesario seguir una secuencia de fases que conforman una metodología con el fin de ejecutar ordenadamente los procesos, la cual se compone de tres fases: análisis, diseño e implementación.

Análisis.- Se utiliza la herramienta Kali Linux v2.0 con el fin de analizar, explotar y comprobar las amenazas existentes dentro del servidor de aplicaciones, también se realiza una revisión sistemática de literatura aplicando la metodología propuesta de acuerdo el artículo de Bárbara Kitchenham (Kitchenham, 2004), con el fin de obtener las características relevantes que debe cumplir un certificado digital para que sea seguro.

Diseño.- Se selecciona la Autoridad Certificadora (AC) a utilizar, esta debe cumplir con aspectos claves como las características relevantes que debe cumplir un certificado digital para que sea seguro y cubrir las vulnerabilidades encontradas.

Implementación. - Se realiza la implementación de la seguridad con los certificados emitidos por la AC propuesta en la fase de diseño, realizando las pruebas respectivas de las mismas.

3. Resultados

Se presenta el proceso para determinar las vulnerabilidades, características y selección de la AC con el fin de implementar los certificados digitales SSL/TLS gratuitos.

3.1. Análisis de Vulnerabilidades

En esta sección se determina las debilidades contra los servidores de aplicación, analizando sobre un servidor web público de pruebas brindado por la Universidad Nacional de Loja, cumpliendo la estructura mostrada en la *Figura 1*.

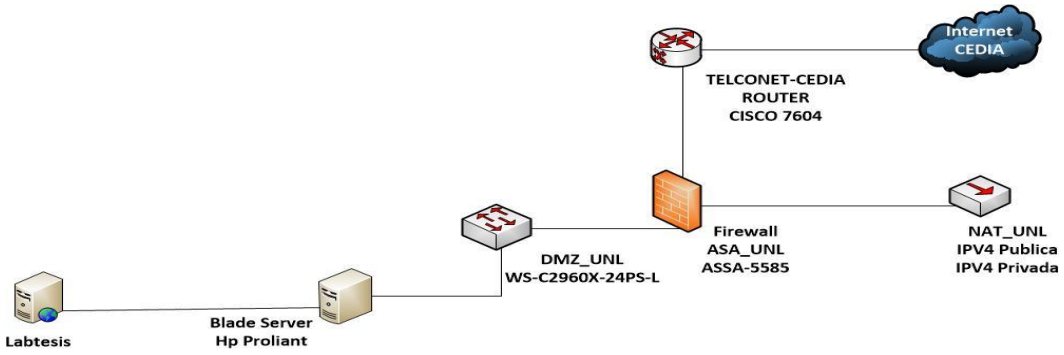

Figura 1. Infraestructura de Red

3.1.1. Selección de Herramienta

Para poder realizar la explotación de amenazas, es necesario tomar las herramientas adecuadas, como se muestra en la *Tabla 1*, la cual se realiza una comparativa especificando criterios como la fácil instalación de la herramienta, el tipo de licencia, el tipo de función que cumple y el consumo de recursos que realiza.

Tabla 1. Comparación de Herramientas para la Explotación de las amenazas

Caracteristicas	Nmap	Nessus	OpenVas	MetasPloit	Kali Linux 2.0	WireShark
Fácil instalación	✓	✓		✓	✓	✓
Interfaz gráfica amigable		✓	✓		✓	✓
Licencia	Libre	Pagada	Libre	Libre	Libre	Libre
Multiplaforma		✓	✓			✓
Detecta vulnerabilidades		✓	✓	✓	✓	

Explota vulnerabilidades	✓			✓	✓	✓
Fácil Configuración	✓	✓	✓	✓	✓	✓
Permite incorporar herramientas extras					✓	
Consumo de recursos	Medio	Medio	Alto	Medio	Medio	Medio

Se selecciona Kali Linux v2.0, como una de las mejoras herramientas para la fase de explotación, debido a sus principales características en la que permite incorporar herramientas extras para detectar y explotar las amenazas.

3.1.2. Explotación de vulnerabilidades

Se procede a determinar las vulnerabilidades en los servidores de aplicación mediante la herramienta Kali Linux v2.0.

3.1.2.1. Hombre en el medio (Main he Middle)

Según el autor M. Markovi en su artículo de investigación define “Main the middle como su nombre indica, un ataque de hombre en el medio ocurre cuando alguien entre dos usuarios intercepta la comunicación supervisando, capturando y controlando la comunicación sin el conocimiento de los usuarios. Por ejemplo, un agresor puede negociar claves de cifrado con ambos usuarios y cada usuario envía datos cifrados al atacante, que puede descifrar los datos con las claves públicas y privadas” (Markovi, 2007). La mayoría de los protocolos criptográficos incluyen alguna forma de autentificación de extremos específicamente para prevenir los ataques Hombre en el medio (siglas en ingles MITM), un ejemplo sería SSL que autentica al servidor web mediante una autoridad de certificación de confianza.

Para la ejecución del ataque y comprobar la existencia de la amenaza en la capa de transporte, se la realiza mediante las herramientas como SslStrip, que permite filtrar todo acceso por HTTPS a HTTP y Ettercap en la que se intercepta los paquetes seleccionando la tarjeta de red, ambas vienen integradas en Kali Linux v2.0.

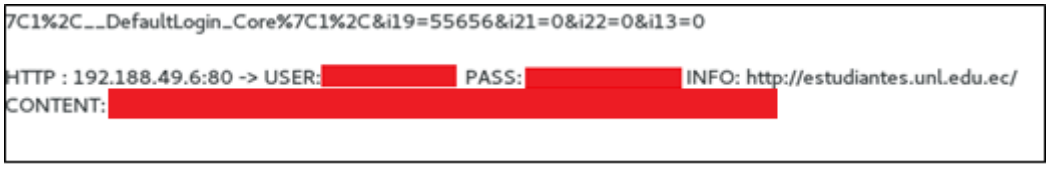

Figura 2. Captura de Credenciales

Como se puede notar en la *Figura 2*, se captura el usuario y clave del sitio “estudiantes.unl.edu.ec”, mostrando una gran deficiencia en el cifrado de datos al inicio de sesión de usuarios.

3.1.2.2. Denegación de Servicios (DoS)

De acuerdo al autor M. Markovi en su artículo de investigación define “A diferencia de muchos otros ataques, la denegación de servicio proviene de enviar datos no validos a aplicaciones o redes, haciendo que las aplicaciones y los servicios cierren o funcionen de manera anormal”(Markovi, 2007). Enviar una inundación de paquetes se lo realiza hasta que se apague un servicio o una red entera bloqueando el tráfico, lo que resulta en una pérdida de accesos a los recursos de red por parte de los usuarios.

Mediante la utilización de la herramienta Slowloris que permite implementar en Kali Linux 2.0, se comprueba que existen servidores públicos que son vulnerables a este tipo de ataques. Es necesario simular el ataque con múltiples peticiones hacia un servicio, para ello utilizamos la herramienta Slowloris el mismo que permite enviar múltiples peticiones por milisegundo, simulando a varias peticiones en diferentes maquinas; el tiempo que colapsa el servidor dependerá del hardware computacional del servidor. La *Figura 3* muestra el sitio web colapsado.

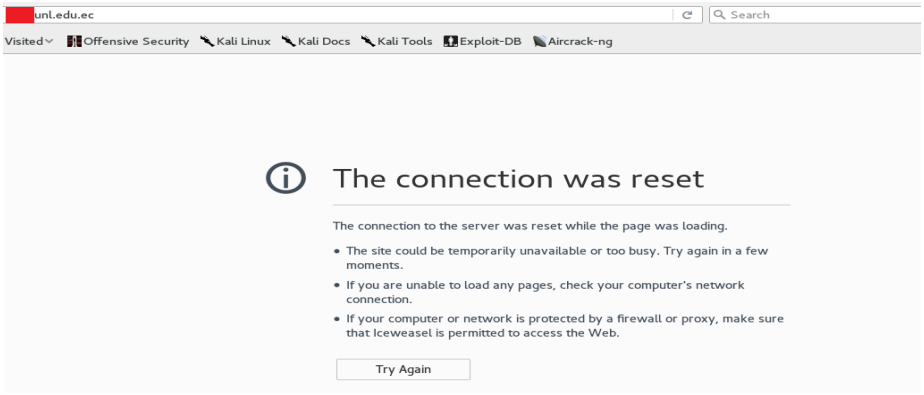

Figura 3. Resultado del Ataque DoS

3.1.2.3. Suplantación de Identidad (Phishing)

En su artículo el autor M. P. Subías define “El Phishing es el término utilizado para un fraude en Internet, consistente en falsificar una página web y lanzar un e-mail masivo para ver si el receptor de ese correo “pica” y entra en la página falsa creyendo que es la original y suministra sus credenciales de acceso, las cuales caen inmediatamente en manos del defraudador” (Subías, n.d.).

Para la ejecución y validación de la amenaza, se utiliza la herramienta Setoolkit y Ettercap que vienen integradas en Kali Linux 2.0 y provee mayor eficacia en la intercepción de las peticiones DNS.

Figura 4. Menú de Setoolkit

Para la ejecución del ataque Phishing, se inicia presentando algunas opciones de diferentes métodos con los que cuenta la herramienta Setoolkit, como se muestra en la *Figura 4*, seleccionando la opción de Ataques de Ingeniería Social, que es el grupo al cual pertenece el ataque denominado Phishing. Luego seleccionamos la opcion 2 (Website Attack Vectors), y opción 3 (Credential Harvester Attack Method), con ello obtenemos el siguiente resultado mostrado en la figura 5.

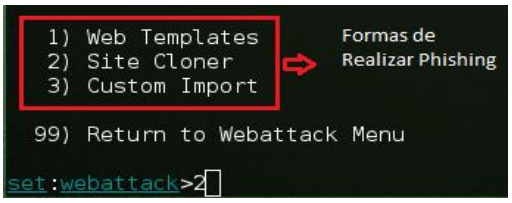

Figura 5. Tipo de ataque de Ingeniería Social

Seleccionamos “Site Cloner” e ingresamos la dirección IP de la maquina atacante y el dominio al cual se va a clonar, como se muestra en la *Figura 6*.

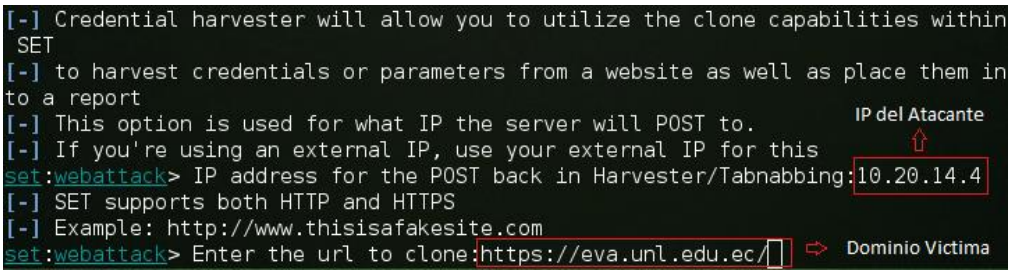

Figura 6. Clonación de Pagina Web

Para poder apreciar la web clonada, se introduce en el navegador la dirección IP de la maquina atacante, esta página clonada es idéntica a la real, por lo que es más sencillo engañar a los usuarios que desconozcan de este tipo de ataques, como se muestra en la *Figura 7*.

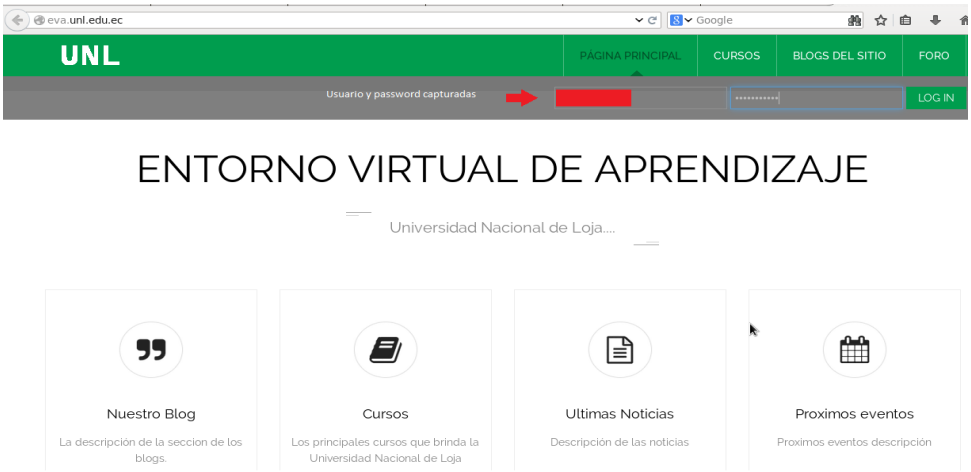

Figura 7. Resultado del Ataque Phishing

Después de haber clonado el sitio web, para hacerlo más efectivo, con la herramienta Ettercap se atrapa las solicitudes DNS de la víctima y así cuando se realice la conexión al dominio, se redirigirá la petición a la página falsa que es similar a la real.

Todo intento de inicio de sesión será capturado por la maquina atacante. Es una manera sencilla de ejecutar esta vulnerabilidad ya que el usuario puede ser fácilmente engañado, capturando sus credenciales de acceso a los sitios web de la institución.

3.1.2.4. Descifrado de Contraseñas

El autor M. Markovi en su artículo de investigación define “El acceso a los recursos de una computadora y de la red se determina mediante un nombre de usuario y una contraseña. Las versiones anteriores de los componentes del sistema operativo no siempre protegían la información de identidad, ya que se pasaba a través de la red para su validación. Esto podría permitir que un espía determine un nombre de usuario y una contraseña válidos y los use para obtener acceso a la red haciéndose pasar por un usuario válido”(Markovi, 2007). Los ataques de descifrado de contraseñas por lo general se realizan bajo protocolos como SSH, HTTP, FTP o sobre todo acceso que tenga un sistema de login de usuarios que no se ha controlado en base al número de intentos por acceder a su sistema web.

Para la ejecución de esta técnica, se requiere de un diccionario de datos teniendo en cuenta las combinaciones de letras, números y signos, con el fin de efectuar las combinaciones necesarias, hasta descubrir usuarios y contraseñas correctas.

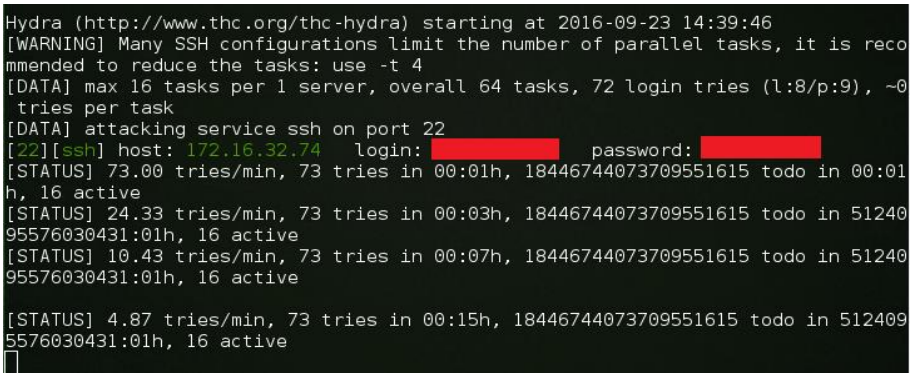

Figura 8. Ataque con Hydra

Como se puede observar en la *Figura 8* el ataque fue efectivo capturando claves con nombre de usuario de un servidor como se muestra en la línea de color verde, también se puede visualizar varios intentos fallidos obtenidos al momento que la herramienta Hydra comienza a ejecutar múltiples combinaciones como se muestra en las líneas de color Gris. Se recalca que el tiempo de duración del ataque puede tomar varias horas o días.

3.2. Selección del Certificado Digital

Se realiza la comparativa de las autoridades certificadoras gratuitas como Let's Encrypt, Start SSL y GoDaddy, las características técnicas tomadas en cuenta para la comparativa se obtuvo de dos partes, la primera se basó en una revisión sistemática de literatura SRL (Enrique et al., n.d.) y la segunda se basó en proformas realizadas a las autoridades certificadoras de paga como: Symantec, GeoTrust y Thawte.

Tabla 2. Comparativa de Autoridades Certificadoras Gratuitas

AUTORIDADES CERTIFICADORAS **CARACTERÍSTICAS TECNICAS**	**Let's Encrypt**	**Start SSL**	**GoDaddy**
Utilizan el algoritmo Sha-2	✓	✓	✓
Robustez del cifrado de 2048 bits	✓	✓	✓
Usa el certificado estándar X.509	✓	✓	✓
Utiliza los certificados SSL/TLS V1.2	✓	✓	✓
Confianza del 99% (Son reconocidos como certificados validos en la mayoría de los navegadores web como Chrome, Firefox, Opera, Safari, entre otros)	✓	✓	✓
Tipo de Validación	DV (Validación de Dominio)	DV (Validación de Dominio)	DV (Validación de Dominio)
Tiempo de emisión	5 – 15 minutos	5 – 15 minutos	1 – 2 Días

			laborales
Reemisión	Ilimitada	Limitada	Limitada
Soporte para dispositivos móviles	✓		
Multiplicidad	✓		
Tiempo de valides de licencia	3 meses	1 año	1 año
Se puede actualizar constantemente	✓		
Precio por año	$ 0	$ 0	$ 0

Como se puede observar en la *Tabla 2*, de acuerdo a las características analizadas se deduce que la autoridad certificadora idónea para la utilización de los certificados digitales gratuitos es con la AC de Let's Encrypt ya que permite actualizar constantemente sus certificados a diferencia de las otras dos AC que solo ofrecen sus certificados gratuitos por un año, además la multiplicidad que ofrece nos provee la facilidad de generar un certificado multi-dominio y por último es soportada por dispositivos móviles.

3.3. Implementación de seguridad con los certificados digitales

3.3.1. Proceso para la implementación de los certificados SSL/TLS en los servidores web

Se especifica los pasos para la implementación de los certificados digitales en servidores de aplicación apache y nginx.

3.3.1.1. Proceso de implementación de certificados SSL/TLS en Apache

Para implementar los certificados digitales en servidor web sobre apache, se realiza los siguientes pasos:

1. Actualizar el sistema operativo existen con el fin de evitar conflictos de incompatibilidad por desactualización de paquetes por parte del servidor.
2. Instalar la extensión Git con el fin de clonar desde un repositorio web el proyecto Let's Encrypt hacia el servidor web local.
3. Clonar desde el repositorio web, el cliente de Let's Encrypt con la extensión Git
4. Generar los certificados digitales con el nombre del dominio y correo del administrador del sitio web.
5. Generar un grupo Diffie-Hellman seguro para el intercambio de claves.
6. Configurar el servidor web para implementar los certificados digitales SSL/TLS.
7. Comprobar la validez del certificado digital SSL/TLS

3.3.1.2. Proceso de implementación de certificados SSL/TLS en Nginx

Para implementar los certificados digitales en servidor web sobre nginx, se realiza los siguientes pasos:

1. Actualizar el sistema operativo existen con el fin de evitar conflictos de incompatibilidad por desactualización de paquetes por parte del servidor.
2. Instalar la extensión Git con el fin de clonar desde un repositorio web el proyecto Let's Encrypt hacia el servidor web local.
3. Implementar el cliente certbot para la implementación de los certificados digitales con Let's Encrypt.
4. Generar los certificados digitales con el nombre del dominio y correo del administrador del sitio web con el cliente certbot.
5. Configurar el servidor web para implementar los certificados digitales SSL/TLS.
6. Configurar la seguridad adicional para robustecer el servidor web
7. Comprobar la validez del certificado digital SSL/TLS

Después de haber implementado los certificados digitales SSL/TLS, se obtiene el candado verde de navegación por HTTPS, como se muestra en la siguiente *Figura 9*.

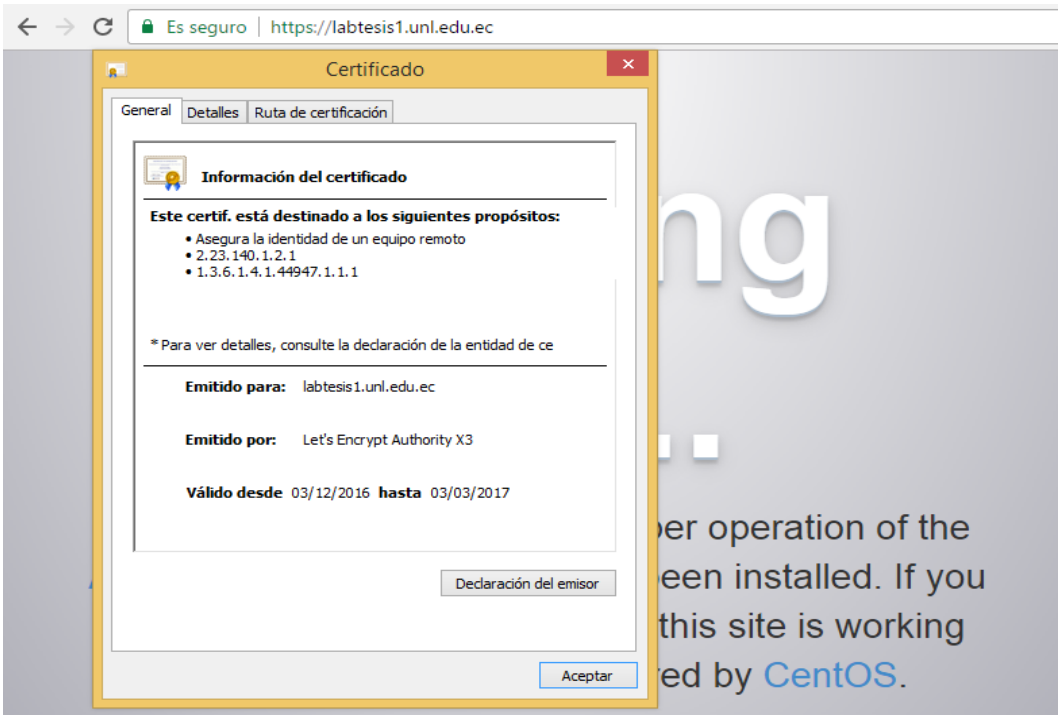

Figura 9. Sitio con Certificado digital SSL/TLS

Como se puede observar el certificado digital SSL/TLS del sitio muestra los siguientes aspectos como: el nombre del sitio web para el cual fue emitido, la AC que lo emite y por último la fecha de validez del certificado, que por lo general es de tres meses hasta su próxima actualización.

4. Discusión

Los resultados obtenidos dan respuesta positiva a la pregunta principal de investigación demostrando que se puede brindar seguridad con la utilización de los certificados digitales gratuitos emitidos por Let's Encrypt. Si bien los límites del presente artículo investigativo abarcan hasta una pequeña parte en el ámbito de seguridad de la información en la web, con la configuración e implementación de los certificados digitales SSL/TLS, se comprueba que se puede dar comunicación segura con certificados gratuitos, contrarrestando ataques como hombre en el medio (main the middle), phishing.

Cabe indicar que el ataque DoS y de Fuerza bruta no fue contrarrestado, para esto se requiere certificados de paga como Symantec.

Como se mencionó en la sección de resultados los ataques que han sido explotados se contrastan con varios autores, donde definen los ataques más comunes que se realizan en los servidores de aplicación, como se muestra en la *Tabla 3*.

Tabla 3. Lista de Amenazas Vigentes en la Capa de Transporte

Autor	**Título de Trabajo**	**Amenazas Vigentes**
Marcelo Alejandro Riffo	"Vulnerabilidades de las Redes Tcp/Ip y principales mecanismos de seguridad" (Riffo, 2008)	• Lectura de paquetes enviados por el Cliente y Servidor • Suplantación de Servidor o Cliente • Alteración de paquetes
M. Markovi	"Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer Networks" (Markovi, 2007)	• Ataque de Denegación de Servicios (DOS) • Ataque por contraseñas (Fuerza Bruta) • Ataque de Hombre en el Medio (Man-in-the-Middle) • Ataque por análisis de tráfico (Sniffer)
Feiyan Mu Jiafen Zhang, Jing Du and Jie Lin	"Application of the Secure Transport SSL Protocol in Network Communication" (Mu et al., 2011)	• interceptación no autorizada de datos
David Wagner, Bruce Schneier	"Analysis of the SSL 3.0 protocol" (Wagner & Schneier, 1996)	• Espionaje • Análisis de Trafico

Las amenazas coinciden con las explotadas mostradas en las figuras 2, 3, 7 y 8 como las más comunes existentes dentro la comunicación cliente-servidor.

De los resultados obtenidos en esta investigación, se puede deducir que para la selección del certificado digital, como lo indica la tabla 2, debe tener las siguientes características: robustez de Cifrado no menos de 2048 bits, utilizar el estándar X.509; y los certificados

SSL/TLS V 1.2 mejorado. Aunque algunos sitios web públicos utilizan el algoritmo SHA-1, en la actualidad este algoritmo es obsoleto por sus bits de cifrado que son menores a 160 bits, mientras que el algoritmo SHA-2 ofrece sus bits de cifrado mayor a 160.

Otro aspecto a considerar en la selección del certificado digital es el tipo de validación y puede ser: tipo OV (validación de la Organización), DV (Validación de Dominio) y EV (Validación Extendida). Siendo los certificados SSL EV de mejor seguridad por su tipo de tipo de emisión y validación que va más allá del dominio sino también de la organización, brindado más confianza al usuario que visita el sitio web.

Para la utilización de los Certificados SSL/TLS y su correcto funcionamiento se deben considerar aspectos como: los servidores deben admitir las extensión SSL/TLS; validar la fecha de caducidad de los certificados digitales; ser emitido por una AC de confianza para ser reconocida por los navegadores web y evitar que se revoquen los certificados por un aviso de incompatibilidad de dominio.

5. Conclusiones

- Al usar certificados SSL/TLS contrarresta ataques como: hombre en el medio (main in the middle), phishing, ataques con diccionario de datos, lo que proporciona a los servidores confidencialidad, integridad y autenticidad. SSL/TLS no ofrece seguridad en la disponibilidad del Servidor especialmente en ataques Negación de servicio (DoS) y otros ataques como XSS Cross-Site Scripting, backdoor.
- Para tener una conexión segura con los certificados digitales SSL/TLS se deben cumplir con ciertas características claves que son: primero utilizar el algoritmo SHA-2 e ignorar algoritmos de cifrado obsoletos, segundo la robustez del cifrado no tiene que ser menor a 2048 bits, como tercera característica se tiene que utilizar el certificado estándar X.509, como cuarta característica se debe utilizar las versiones más actuales de los certificados digitales que son SSL/TLS V 1.2.
- Al realizar la comparativa de ACs, se determina la utilización de los certificados SSL/TLS emitidos por Let’s Encrypt, los cuales cumplen con los requerimientos de seguridad como son: el SHA-2, 2048 bits de cifrado, certificado estándar X.509 y SSL/TLS V 1.2 y permite la actualización del certificado cada tres meses, siendo una de las mayores ventajas con respecto a otras Entidades certificadoras.
- Una desventaja de los certificados gratuitos con Let’s Encrypt es que solo emite un tipo de archivo con extensión DV mientras que otras ACs de paga como Thawte, emiten sus certificados con los tres tipos de extensiones como son OV, DV y EV, ofreciendo mejor seguridad al validar la organización(OV) y el dominio(DV).

- Para la implementación de los certificados digitales en el servidor Apache se utilizó el cliente de Let's Encrypt por defecto, mientras que para Nginx se utilizó el cliente certbot que permitió implementar estos certificados.

6. Recomendaciones

- Utilizar los certificados digitales SSL/TLS gratuitos emitidos por Let's Encrypt para plataformas que manejan informaciones educativas, PYMEs, y empresas que posean servidores en zonas DMZ y no cuenten con un presupuesto para la adquisición certificados digitales pagados.
- Se debe realizar un script en el servidor de aplicación para facilitar la actualización de los certificados digitales SSL/TLS gratuitos emitidos por Let's Encrypt.
- Ampliar el estudio con el fin de testear de manera más profunda a los certificados digitales SSL/TLS gratuitos, en ambientes de empresas bancarias.

Bibliografía

Clark, J., & Van Oorschot, P. C. (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. *Proceedings - IEEE Symposium on Security and Privacy*, 511–525. http://doi.org/10.1109/SP.2013.41

Durumeric, Z., & Kasten, J. (2013). Analysis of the HTTPS certificate ecosystem. *Proceedings of the 2013 …*, 291–304. http://doi.org/10.1145/2504730.2504755

Enrique, M., Hurtado, C., Javier, D., Sarango, A., Gustavo, R., Díaz, F., & Torres, H. (n.d.). Revisión Sistemática de Certificados SSL / TLS como Mecanismo de Seguridad en Servidores de Aplicación. http://doi.org/978-9978-389-32-4

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(TR/SE-0401), 28. http://doi.org/10.1.1.122.3308

Markovi, M. (2007). Data protection techniques, cryptographic protocols and PKI systems in modern computer networks. *2007 IWSSIP and EC-SIPMCS - Proc. 2007 14th Int. Workshop on Systems, Signals and Image Processing, and 6th EURASIP Conf. Focused on Speech and Image Processing, Multimedia Communications and Services*, 13–24. http://doi.org/10.1109/IWSSIP.2007.4381086

Mu, F., Zhang, J., Du, J., & Lin, J. (2011). Application of the Secure Transport SSL Protocol in Network Communication. http://doi.org/10.1109/ISCID.2011.25

Ordean, M., & Giurgiu, M. (2010). Implementation of a security layer for the SSL/TLS protocol.

2010 9th International Symposium on Electronics and Telecommunications, ISETC'10 - Conference Proceedings, 209–212. http://doi.org/10.1109/ISETC.2010.5679350

Riffo, M. A. (2008). Vulnerabilidades de las Redes TCP/IP y Principales Mecanismos de Seguridad. *In Vitro*, *3*(2), 1–23. Retrieved from http://www.ncbi.nlm.nih.gov.myaccess.library.utoronto.ca/pubmed/11720961

Subías, M. P. (n.d.). Desfalcos por "Phishing," 25–26. Retrieved from http://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-10678.pdf

Wagner, D., & Schneier, B. (1996). Analysis of the SSL 3.0 protocol. *Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2*, 4. http://doi.org/10.1.1.29.9990