UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN SITIOS WEB CONTRA ATAQUES INFORMÁTICOS

CALERO ORDOÑEZ CRISTINA LISSETTE
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN SITIOS WEB CONTRA ATAQUES INFORMÁTICOS

CALERO ORDOÑEZ CRISTINA LISSETTE
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN SITIOS WEB CONTRA ATAQUES INFORMÁTICOS

CALERO ORDOÑEZ CRISTINA LISSETTE
INGENIERA DE SISTEMAS

CÁRDENAS VILLAVICENCIO OSCAR EFRÉN

MACHALA, 04 DE FEBRERO DE 2019

MACHALA
04 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Implementación de controles de seguridad en sitios web contra ataques informáticos, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

CÁRDENAS VILLAVICENCIO OSCAR EFRÉN
0703935312
TUTOR - ESPECIALISTA 1

LOJÁN CUEVA EDISON LUIS
0703249698
ESPECIALISTA 2

JUMBO CASTILLO FREDDY ANIBAL
0704167949
ESPECIALISTA 3

Fecha de impresión: martes 05 de febrero de 2019 - 07:05

URKUND

Urkund Analysis Result

Analysed Document: CristinaCaleroComplexivo.pdf (D47114060)
Submitted: 1/22/2019 2:56:00 PM
Submitted By: oecardenas@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, CALERO ORDOÑEZ CRISTINA LISSETTE, en calidad de autora del siguiente trabajo escrito titulado Implementación de controles de seguridad en sitios web contra ataques informáticos, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

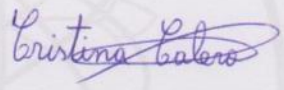
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 04 de febrero de 2019



CALERO ORDOÑEZ CRISTINA LISSETTE
0705473676

DEDICATORIA

El presente trabajo está dedicado a mis padres por brindarme su apoyo durante el lapso de mi preparación profesional.

A Diego Orellana Sánchez, por apoyarme en todo momento y estar pendiente de mí en cada meta alcanzada de mi vida.

Calero Ordoñez Cristina Lissette

AGRADECIMIENTO

En primer lugar, agradezco a Dios por brindarme salud y sabiduría para culminar este proyecto, a mis padres por apoyarme y darme las fuerzas necesarias para seguir adelante en cada momento de mi vida, al Ing. Oscar Cárdenas por su asesoramiento en este trabajo, finalmente a Diego Orellana Sánchez y Vanessa Piedra por su apoyo y motivación constante.

Calero Ordoñez Cristina Lissette

RESUMEN

IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN SITIOS WEBS CONTRA ATAQUES INFORMÁTICOS.

Calero Ordoñez Cristina Lissette,
0705473676

En la sociedad del conocimiento las potencialidades informáticas se prestan, en la gestación y desarrollo de profesiones, sociedad, cultura e integración de procesos virtuales en actividades cotidianas; destacando los sitios web que por ser sistemas online presentan vulnerabilidades y amenazas que podrían perjudicar a las organizaciones, debido a los constantes robos de información, extorsión, espionaje entre otros; a causa de esta problemática la documentación pertinente presenta la simulación de ataques y controles informáticos que mitiguen el impacto de estas amenazas, siguiendo las recomendaciones impuestas por la Open Web Application Security Project (OWASP), en la que se planteó escenarios de los ataques de entidades externas XML, pérdida de control de acceso y configuración de seguridad incorrecta, utilizando las herramientas de auditoría informática solventadas en Kali Linux como Nmap para el escaneo de puertos, Ettercap con respecto a las intercepciones de conexiones y Burp Suite para intermediar el tráfico de datos en la navegación. En los resultados se aprecia la interacción del sistema frente a la ejecución de los ataques, luego de implementar los controles a través del uso de librerías, tabla Address Resolution Protocol (ARP) y herramienta Fail2ban; mitigando las afectaciones al sitio web para mejorar la seguridad.

PALABRAS CLAVES: Sitio Web, OWASP, Entidades Externas XML, Pérdida de control de acceso, Configuración de seguridad incorrecta.

ABSTRACT

IMPLEMENTATION OF SECURITY CONTROLS ON WEBSITE AGAINST CYBER ATTACKS.

Calero Ordoñez Cristina Lissette, 0705473676

In the knowledge society, computer potentials are lent, in the gestation and development of professions, society, culture and integration of virtual processes in daily activities; highlighting the websites that, because they are online systems, present vulnerabilities and threats that could harm organizations, due to the constant theft of information, extortion, espionage, among others; because of this problem, the relevant documentation presents the simulation of attacks and computer controls that mitigate the impact of these threats, following the recommendations imposed by the Open Web Application Security Project (OWASP), in which scenarios of the attacks of entities were raised. External XML, loss of access control and incorrect security settings, using the computer audit tools solved in Kali Linux as Nmap for port scanning, Ettercap with respect to connection interceptions and Burpsuite to intermediate data traffic in navigation. The results show the interaction between the system and the execution of the attacks, after implementing the controls through the use of libraries, the Address Resolution Protocol (ARP) table and the Fail2ban tool; Affecting the website to improve security.

KEYWORDS: Website, OWASP, XML External Entities, Loss of access control, Incorrect security settings.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

1. INTRODUCCIÓN

En el ámbito social contemporáneo los sitios web son clave en la prestación de servicios tanto, para entidades públicas y privadas que cuentan con páginas web e inclusive realizan operaciones en línea a través de servidores, que interactúan en tiempo real con los usuarios. [1]

La versatilidad de los sitios web junto a sus principales potencialidades, derivan en vulnerabilidades y amenazas aprovechadas por personas inescrupulosas que buscan beneficio propio o persiguen fines lucrativos mediante el *hackeo* de sistemas informáticos, trayendo consecuencias como pérdida de información, suplantación de identidad, robo de contraseñas, transacciones bancarias, entre otras. [2]

La Open Web Application Security Project (OWASP) es una normativa abierta de carácter internacional que vela por la seguridad de las aplicaciones web, de los cuales se destacan los ataques de entidades externas XML que consiste en aprovechar la configuración inadecuada del lenguaje, para obtener la información del sistema o consumir los recursos del mismo, también se encuentra los ataques de pérdida de control de acceso que por medio de la fuerza bruta, se puede desencriptar los datos obteniendo las contraseñas de acceso de los sitios web y los ataques de configuración de seguridad incorrecta, que ocurren cuando se encuentra habilitada de manera inadecuada los servicios desprotegiendo de esta manera las cuentas de los usuarios.

La problemática abordada es escenificar los ataques informáticos citados en el párrafo anterior, delineando las indicaciones de la OWASP mediante simulaciones aplicando las medidas correspondientes, a través de las herramientas Kali Linux, Hydra, y Burp Suite que permitirán reducir las afectaciones a los sitios web. El proyecto se estructura como caso de estudio, cuyo objetivo es implementar controles de seguridad en sitios web mediante un análisis sustentado en los criterios de auditoría informática para disminuir las vulnerabilidades frente a los ataques informáticos, analizando el desempeño de los controles en relación a la respuesta del sistema. La documentación se compone de:

Capítulo I: Abarca información preliminar, de carácter investigativo como introducción, problemática, objetivos e inducción de la temática al lector.

Capítulo II: Compete el estado del arte, caracterización de las concepciones teóricas desde la perspectiva del autor, también contiene el desarrollo de los ataques con los controles informáticos correspondientes para garantizar la seguridad del sitio web.

Capítulo III: Comprende la culminación del caso de estudio, a través de las conclusiones y

recomendaciones argumentadas en los resultados apreciados en el desarrollo del proyecto.

1.1 Marco Contextual

A nivel global se evidencian estudios referentes sobre los controles para salvaguardar sitios y aplicaciones web, en especial de ataques de inyección en lenguaje de consulta estructurados, configuración incorrecta y falsificación de solicitud como los más destacados, en base a una nueva modalidad que automatiza la evaluación de los sitios a través de herramientas que ejecuta diversos ataques en niveles como código fuente para identificar vulnerabilidades midiendo la capacidad de respuesta de los controles.

A nivel nacional se enfatiza en la implementación de las bondades de transferencia tecnológica en sistemas informáticos, orientados a mejorar las prestaciones de las instituciones, en especial de las entidades bancarias/financieras que buscan reducir los ataques por suplantación de identidad; en lo referente a nivel micro en la Universidad Técnica de Machala, particularmente en la carrera de Ingeniería de Sistemas, se profundiza en la cátedra de auditoría informática gestando el análisis de controles lógicos por medio de emular ataques que diagnostiquen falencias en los sistemas digitales, con la finalidad de aplicar las medidas adecuadas en el diseño optimizado de sitios web.

1.2 Problema

Los sitios web son desarrollados por personas por lo tanto contienen errores ya sea por la incomprensión de los controles de seguridad, carencia de recursos o equipamiento inadecuado al momento de proteger la seguridad informática de las vulnerabilidades que perjudican la integridad, confiabilidad y disponibilidad de los medios de la organización por lo que se pretende implementar medidas de seguridad que reduzca o evite los ataques informáticos. Por lo tanto, se plantea la siguiente pregunta ¿Cómo implementar controles de seguridad en sitios web para reducir el impacto de los ataques informáticos de entidades externas XML, pérdida de control de acceso y configuración de seguridad incorrecta?

1.3 Objetivo General

Implementar controles de seguridad en sitios web mediante herramientas de auditoría para la disminución de vulnerabilidades en ataques informáticos.

2. DESARROLLO

2.1 Marco teórico

2.1.1 Ataque informático

Es una acción enfocada a dañar la integridad, confiabilidad y disponibilidad de sistemas computacionales, aprovechándose de las vulnerabilidades del hardware o software con el propósito de perjudicar la seguridad del entorno obteniendo como personales. [3]

2.1.1 Amenaza

Es todo agente externo que represente un riesgo, al aprovechar las debilidades de un sistema informático con la finalidad de efectuar un ataque, sin importar la causa que vulnere la seguridad del hardware o software. [4]

2.1.2 Vulnerabilidad

Es toda falencia interna en un sistema informático, se constituye en base a factores e indicadores que representan una debilidad en la parte lógico o física, dejando en riesgo la integridad y seguridad de la información. [5]

2.1.3 Auditoría informática

Es una ciencia pragmática de carácter interdisciplinario que mediante un análisis multiobjetivo evalúa las vulnerabilidades y amenazas de sistemas computacionales, para emitir un juicio crítico sobre las medidas correspondientes al garantizar la calidad de la información. [6]

2.1.4 Seguridad web

Es garantizar la integridad de datos en un entorno web, proteger y salvaguardar las cualidades del servidor, mantener una configuración adecuada del sistema lógico y certificar una respuesta oportuna frente a un ataque informático. [7]

2.1.5 Controles Informáticos

Son el conjunto de medidas de prevención, monitoreo y reacción del sistema para garantizar la seguridad y calidad de la información, así como las conjeturas necesarias en el desempeño lógico del entorno, a través de una implementación tecnológica acorde a las vulnerabilidades-amenazas o necesidades del sistema. [8]

2.1.6 OWASP

Es un conjunto de normativas técnicas orientadas a dinamizar la seguridad en sitios web, aplicaciones o entornos virtuales de forma abierta en beneficio y desarrollo de la comunidad cibernauta, se caracteriza por promover una retroalimentación tecnología en la infraestructura lógica. [9]

2.1.7 Entidades Externas XML

Este ataque consiste en la configuración incorrecta del intérprete XML, que se lo ejecuta mediante una aplicación web que lee el código en sus indicadores desde una máquina externa. [10]

Las posibles consecuencias van desde la obtención de información confidencial, alteración de solicitud del servidor y análisis de puertos hasta denegación de servicios. [11]

2.1.8 Pérdida de Control de Acceso

Es un ataque que incapacita al sistema para gestionar los privilegios y accesibilidad de usuarios a las configuraciones de la página web, facilitando la manipulación, robo o daño en los datos del sitio web. [12]

2.1.9 Configuración de Seguridad Incorrecta

Es cuando se descuida la infraestructura del sistema, dejando libre acceso a puertos, falencias en líneas de código, carencia de certificaciones contra amenazas y toda debilidad del entorno web. [13]

2.1.10 Man in the middle

Es un ataque que consiste en breves rasgos situarse en medio de dos partes que requieran comunicación (usuario/transacciones, login/páginas web) mediante un agente que pasa desapercibido, en este caso un virus, correo electrónico, puerto externo; cualquier amenaza que intercepte datos del sistema sin autorización ni el debido proceso. [14]

2.1.11 Fuerza Bruta

Es un ataque caracterizado por emplear la potencia computacional de cálculo, para

desencriptar la contraseña de un sitio web o claves, probando todas las combinaciones posibles hasta dar con el password correcto. [15]

2.1.12 HYDRA

Es un método para crackear contraseñas, mediante la utilización de un script o automatización del proceso a través de líneas de código, es un complemento presente en Kali Linux. [16]

2.1.13 Burpsuite

Es un gestor de auditoría informática, sustentado en Kali Linux que sirve como plataforma en la implementación de pruebas de seguridad a entornos web, faculta combinar ataques, controles o ejecutar secuencias de análisis en el sitio web; su versatilidad y utilidad radica en la facilidad con la cual gestiona las herramientas y configuraciones en la simulación de respuesta de un sistema informático en forma retroalimentaria. [17]

2.1.14 Fail2ban

Es una herramienta de seguridad informática que permite bloquear ataques de fuerza bruta, al momento de detectar una serie de intentos de accesos al servidor esta herramienta bloqueará la dirección IP automáticamente por medio de la configuración de filtros de acuerdo a las necesidades del sistema. [18]

2.2 Solución del problema

Es este apartado, se escenifican los ataques informáticos a través de simulaciones virtuales en herramientas de Kali Linux, GNS3 y Virtual Box para ejecutar una auditoría a la red, midiendo su vulnerabilidad e infiriendo su respuesta al implementar los respectivos controles.

2.2.1 Ataque 1: Entidades Externas XML (XXE)

Para realizar este ataque, se requieren las herramientas e implementos descritos en la *tabla 1.*

Tabla 1: Direccionamiento IP del Ataque de Entidades Externas XML

Infraestructura	Dirección IP	Máscara de Subred
Servidor – Debian	192.168.10.6	255.255.255.240

Cliente – Kali Linux	192.168.10.3	255.255.255.240
Router – Cisco 3640	192.168.10.1	255.255.255.240

Fuente: Elaboración propia

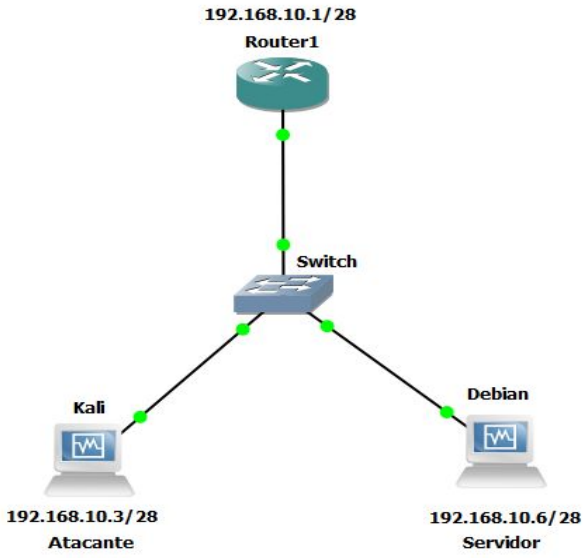


Figura 1: Topología de red usada en el ataque entidades externas XML
Fuente: Elaboración Propia

En la *figura 1*, se ilustra la red empleada en el ataque de entidades externas XML; en primer paso se obtiene la URL del sitio web, con la cual se accede al servidor; luego con la herramienta Burp Suite de Kali Linux atrapa el tráfico de datos, tal como se aprecia en la *figura 2.*

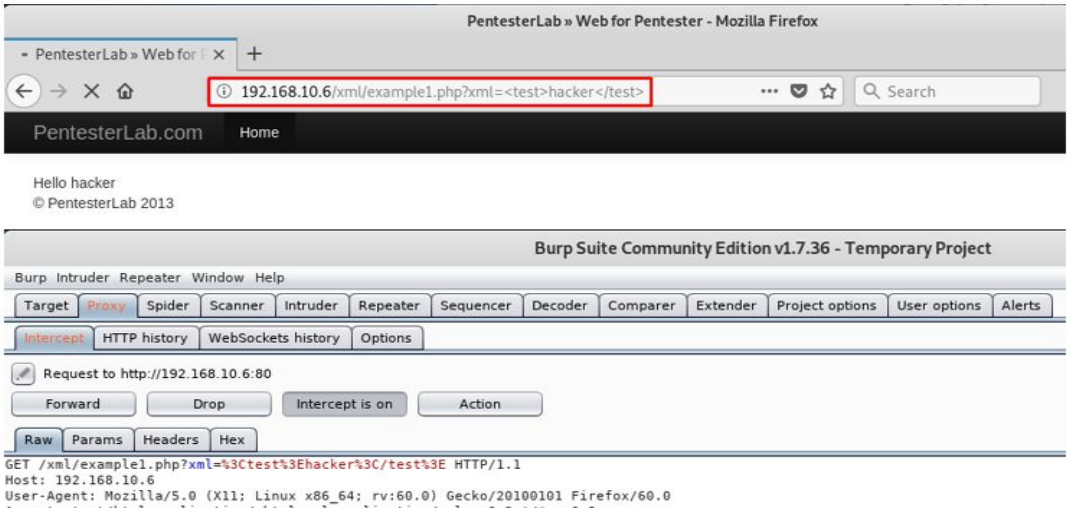


Figura 2: Ingreso de la URL del servidor para atacar
Fuente: Elaboración Propia

Continuando con el ataque, se reescribe una línea de código suplantando la configuración nominal del sitio web (ver *figura 3)*, forzando a que muestre todos los usuarios y contraseñas registradas en el servidor, lo cual se aprecia en la pestaña Response en la *figura 4.*

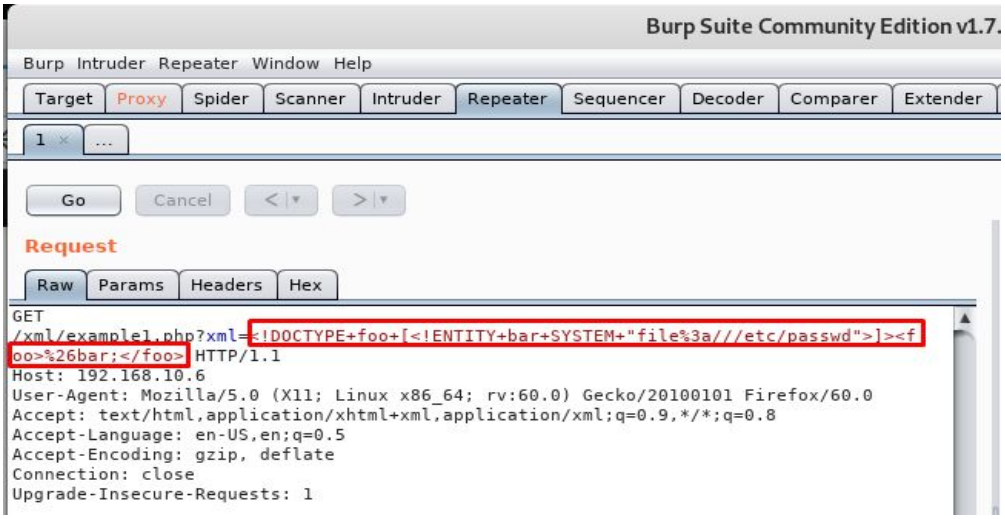


Figura 3: Línea de código que permite robar las contraseñas de la máquina del servidor
Fuente: Elaboración Propia

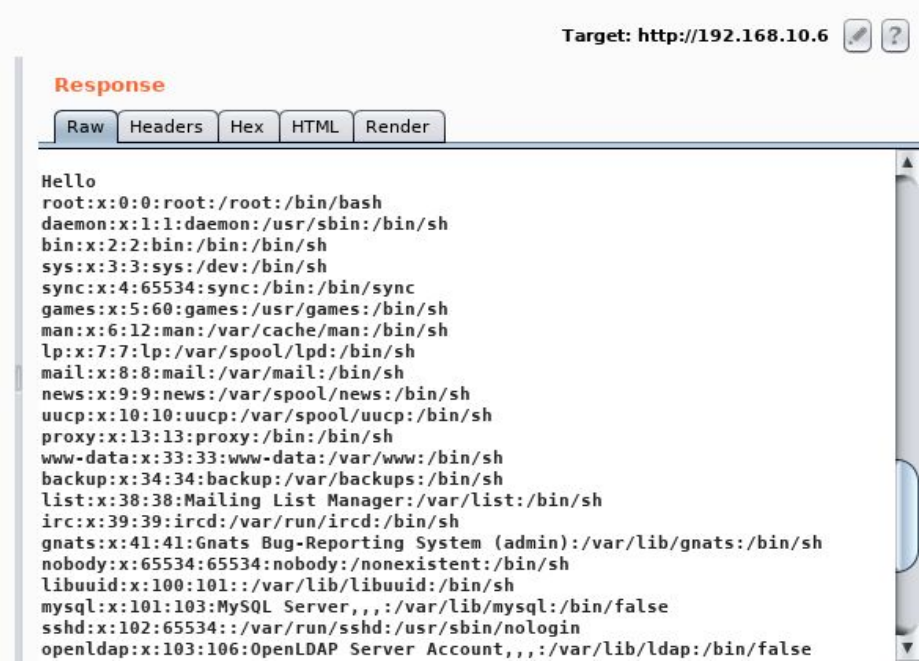


Figura 4: Robo de contraseñas del servidor vulnerado
Fuente: Elaboración Propia

Una vez efectuado el ataque, se puede adquirir privilegios en el manejo de datos, suplantar identidad o secuestrar sesión de usuarios; además puede derivar en otros ataques

conjugados a partir de esta vulneración al sistema, debido a que no se detecta de manera lógica, a menos que el administrador audite a la página.

2.2.2 *Medida de control para evitar ataque de Entidades Externas XML*

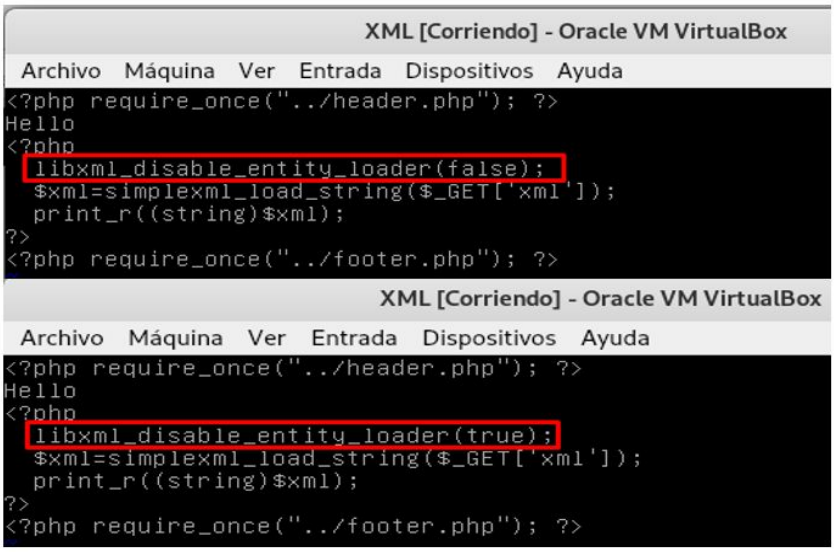


Figura 5: Control para bloquear/acceder a cargar entidades XML
Fuente: Elaboración Propia

Es necesario implementar manualmente el control, ya sea mediante interfaz gráfica del sitio web o a través de la consola del servidor; consiste en emplear una librería llamada libxml que impide la carga de entidades externas XML. Esta medida es de fácil aplicación, cuyo proceso se observa en la *figura 5;* una vez asegurada la página al reintentar el ataque, el sistema responde con un mensaje de advertencia, que notifica tanto al administrador como potencial infractor que no puede vulnerar al sitio web (ver *figura 6).*

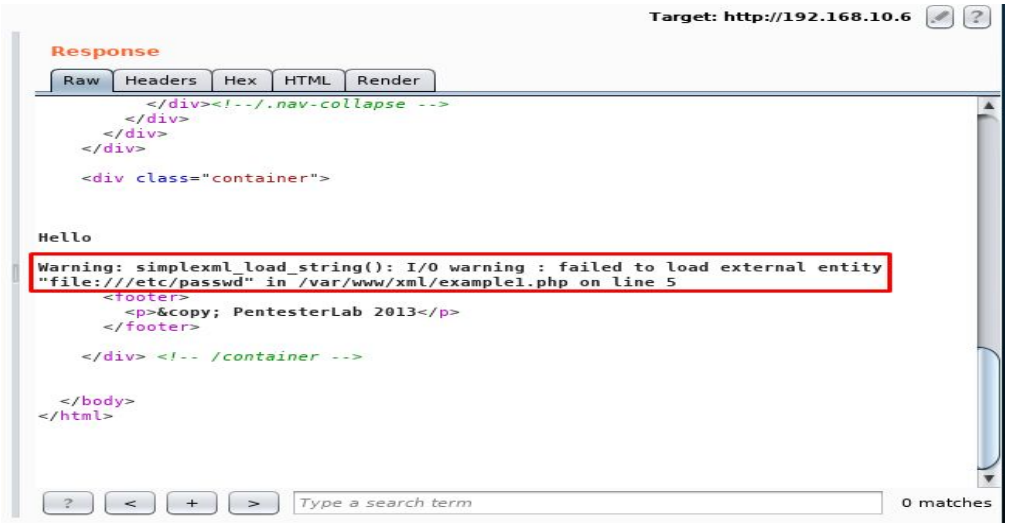


Figura 6: Advertencia como negación del ataque
Fuente: Elaboración Propia

2.2.3 Ataque 2: Pérdida de Control de Acceso (Hombre en el Medio)

Para realizar este ataque, se requieren las herramientas e implementos descritos en la *tabla 2.*

Tabla 2: Direccionamiento IP del Ataque de Pérdida de Control de Acceso

Infraestructura	Dirección IP	Máscara de Subred
Servidor – Ubuntu	192.168.10.2	255.255.255.240
Cliente – Kali Linux	192.168.10.3	255.255.255.240
Cliente – Windows 7	192.168.10.4	255.255.255.240
Router – Cisco 3640	192.168.10.1	255.255.255.240

Fuente: Elaboración propia

Se empieza desde la tipología de red apreciada en la *figura 7,* las direcciones IP de todos los equipos se especifican en la *tabla 2.* El ataque a efectuar es "Hombre en el Medio" para ejemplificar la pérdida de control de acceso que consiste en perder la capacidad de autentificar a los usuarios.

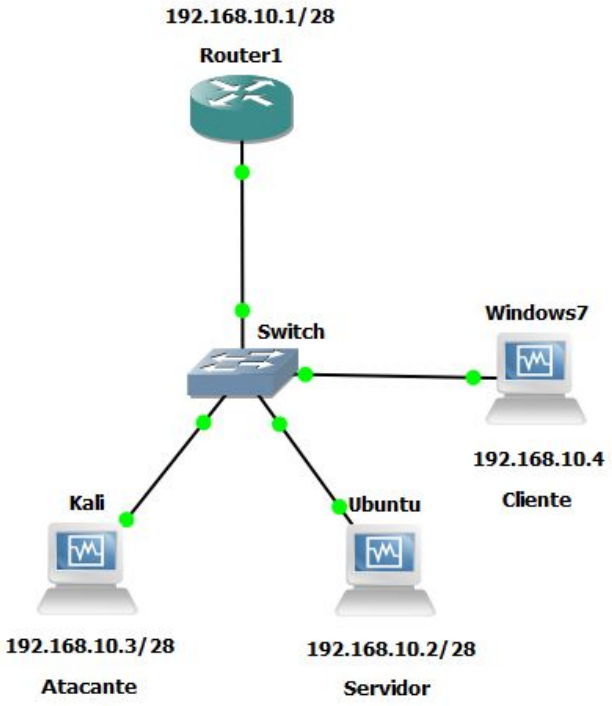


Figura 7: Topología de red empleada en el ataque de Pérdida de Control de Acceso
Fuente: Elaboración Propia

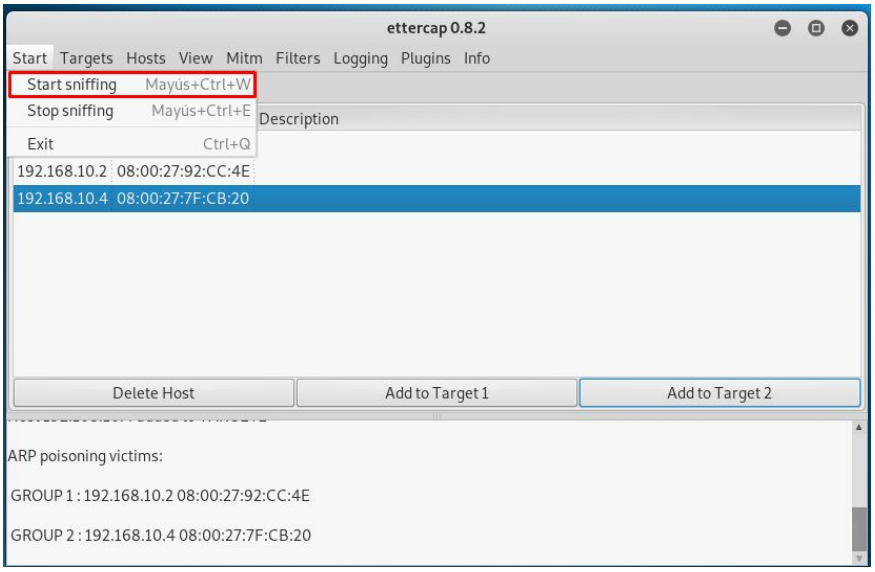


Figura 8: Herramienta Ettercap usada para ejecutar el ataque
Fuente: Elaboración Propia

Se requiere la herramienta Ettercap, que permite analizar la red para conocer las direcciones de las máquinas, luego se realiza un envenenamiento ARP que engaña al servidor haciendo creer que la dirección de cliente, se encuentra alojada en la MAC de Kali Linux, para así interceptar el tráfico siendo mediadores entre la comunicación del sistema vulnerado.

En la *figura 9* se aprecia que el sitio atacado no es seguro, y se pueden ingresar libremente los datos, además la *figura 10* evidencia la obtención del login/password gracias al tráfico de datos, que a su vez permite espiar o acceder a la página vulnerada ocasionado afectaciones, en función de las intenciones del hacker.

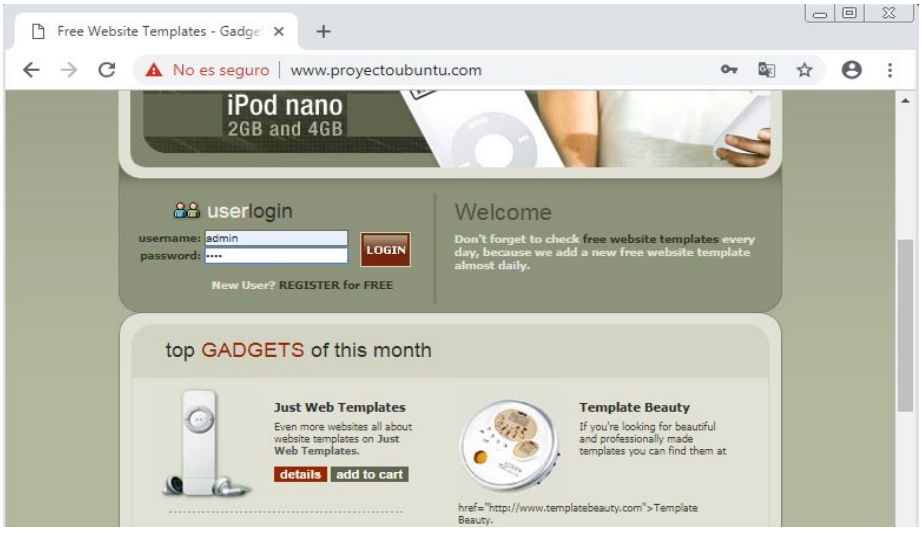


Figura 9: Vulneración de la página e ingreso con datos capturados
Fuente: Elaboración Propia

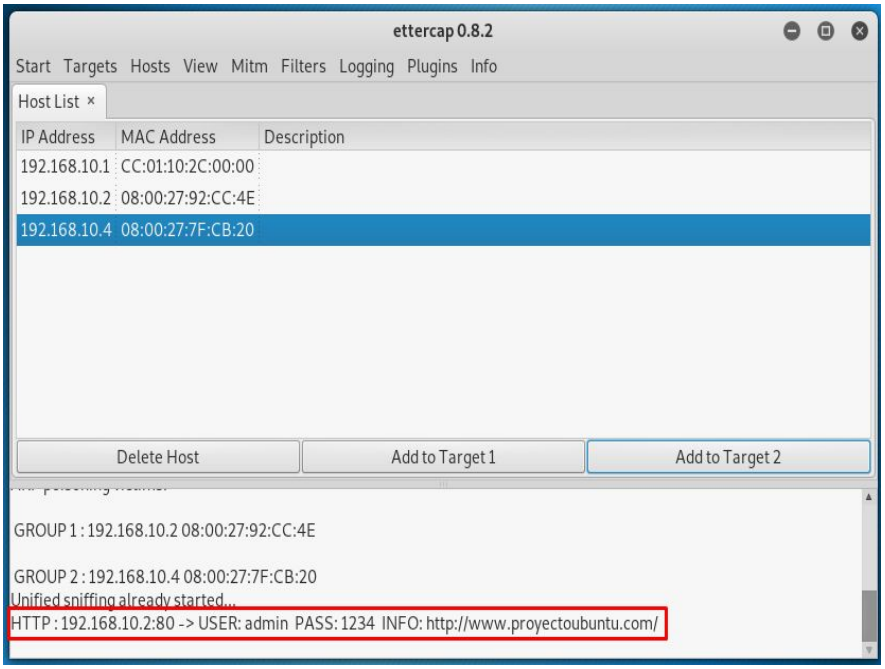


Figura 10: Usuario y contraseña capturados
Fuente: Elaboración Propia

2.2.4 *Medida de control para evitar ataque de pérdida de control de acceso*

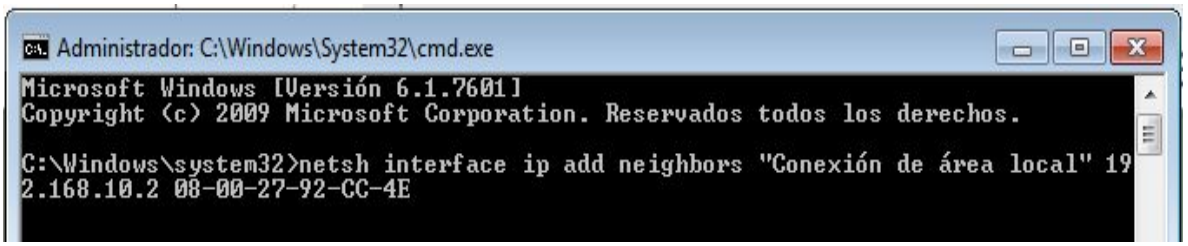


Figura 11: Control que comanda la identidad del cliente evitar ataque
Fuente: Elaboración Propia

Esta medida fija la dirección MAC e IP del cliente en la tabla ARP del servidor (ver *figura 11)*, señalando el camino por el cual circulan los datos, de forma estática impidiendo, que la dirección sea suplantada desde otra máquina; cabe recalcar que este ataque no es percibido por la víctima, debido a que la información viaja con normalidad siendo husmeada, desde el ordenador del atacante.

2.2.5 *Ataque 3:* Configuración *de Seguridad Incorrecto*

Para realizar este ataque, se requieren las herramientas e implementos descritos en la *tabla 3.*

Tabla 3: Direccionamiento IP del Ataque de Configuración de Seguridad Incorrecto

Infraestructura	Dirección IP	Máscara de Subred
Servidor – Ubuntu	192.168.10.2	255.255.255.240
Cliente – Kali Linux	192.168.10.3	255.255.255.240
Router – Cisco 3640	192.168.10.1	255.255.255.240

Fuente: Elaboración propia

En la *tabla 3*, se detalla las direcciones de los hosts empleados en esta prueba, la tipología de red utilizada se observa en la *figura 12.*

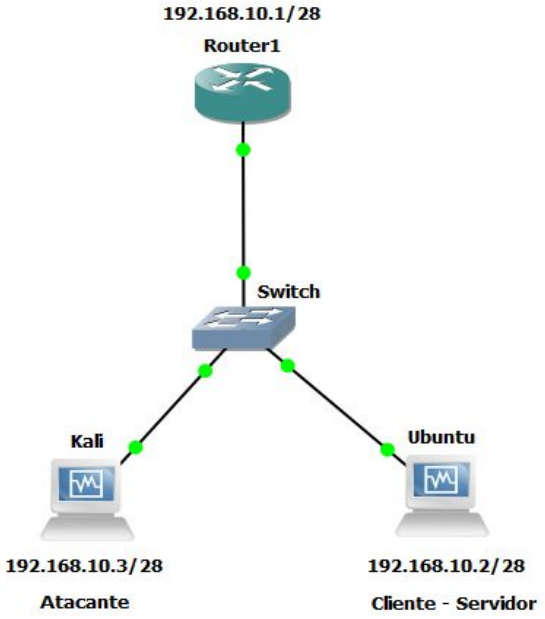


Figura 12: Topología de red usada en ataque de Configuración de Seguridad Incorrecto
Fuente: Elaboración Propia

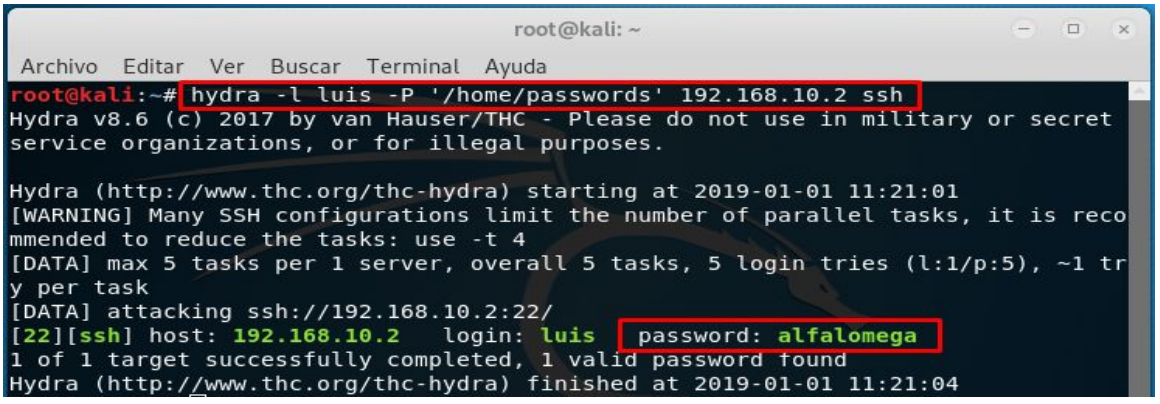


Figura 13: Herramienta Hydra para efectuar el ataque
Fuente: Elaboración Propia

Se inicia por medio de la herramienta NMAP, la cual escanea los puertos del servidor, identificando a los puertos vulnerables, en este caso el puerto SSH dirigiéndose al usuario LUIS, que se encuentra en el servidor. El ataque consiste en iterar las posibles combinaciones que conforman la clave correcta, a través de la herramienta Hydra la misma que realiza la prueba, con los datos almacenados en el diccionario de caracteres cargado en el ordenador del atacante (ver *figura 13)*. Luego de hallar la contraseña adecuada, se ingresa automáticamente permitiendo acceder a los archivos, modificarlos o realizar otra accionante ejecutada con fines malintencionados, dicho proceso es validado en la *figura 14.*

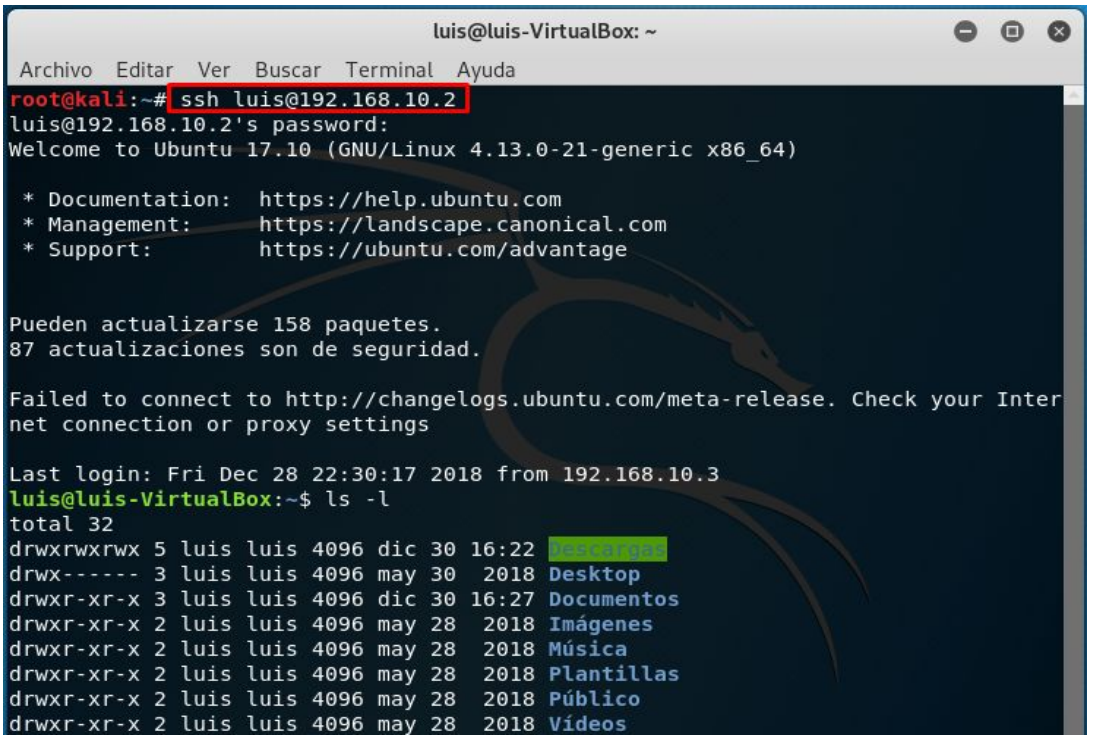


Figura 14: *Revisión y búsqueda de archivos en la máquina vulnerada*
Fuente: Elaboración Propia

2.2.6 Medida de control para el ataque configuración de seguridad incorrecto

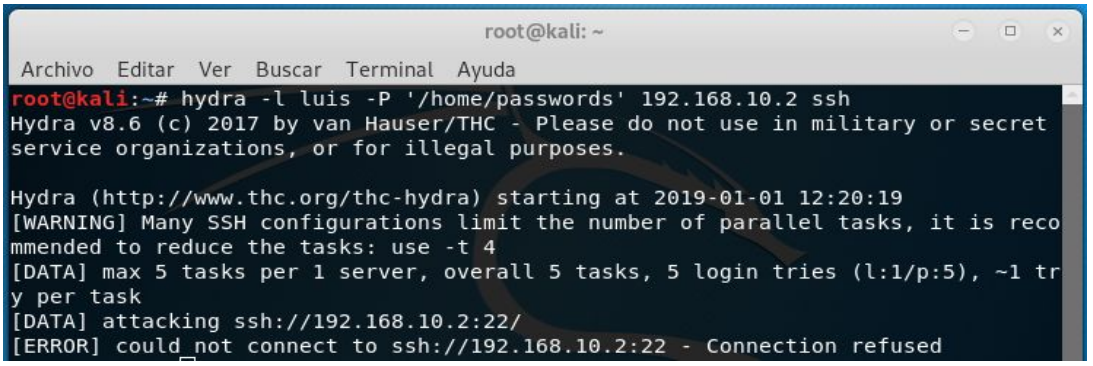


Figura 15: Respuesta de la máquina al detectar el ataque niega la conexión
Fuente: Elaboración Propia

El control se ejecuta, usando la herramienta fail2ban que permite habilitar o bloquear al puerto vulnerable, siendo el SSH el mayormente afectado, se protege cambiado el código a TRUE, para que al detectar el primer intento de forcejeo rechace la conexión, gracias al comando Maxretry=1. Esta medida se debe aplicar por prevención, debido a que es común mantener puertos abiertos por defecto, lo que da oportunidad a terceros de vulnerar al sistema.

2.1 Resultados

En la tabla 2 se sintetiza los resultados evidenciados en las pruebas conjugando los criterios técnicos y profesionales competentes a la auditoría informática en la seguridad de sitios web.

Tabla 4: Síntesis de resultados al analizar ataque/control

ATAQUE	CONTROL	RESPUESTA DEL SISTEMA
Entidades Externas XML	Utilización de la librería libxml en el servidor	Evita la carga de entidades externas visualizando una advertencia, a su vez notifica al administrador sobre el intento de ataque.
Pérdida de Control de acceso	Uso de la tabla ARP mediante el comando netsh interface ip add address	Fija la dirección ip para gestar una vía única flujo de datos, también denegando el acceso remoto del sitio web.
Configuración de Seguridad Incorrecto	Instalación y configuración de la herramienta fail2ban	Bloqueo de puerto ssh, emitiendo una alerta sobre el intento de ataque.

Fuente: Elaboración Propia

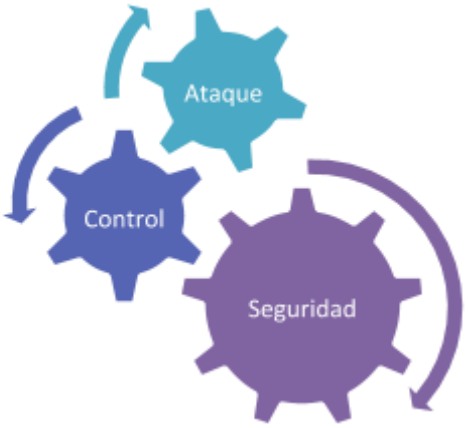


Figura 16: Esquema de implementación del caso de estudio
Fuente: Elaboración Propia

La auditoría informática, es un proceso de gestión iterativa, que exige una retroalimentación permanente en la seguridad del sistema, para garantizar una respuesta oportuna frente a posibles amenazas y minimizar daños en ataques potenciales; en la *figura 16* se aprecia una interacción entre control y ataque permitiendo un análisis capaz de armonizar las prestaciones, facilidades e inducir riesgos en ambientes digitales.

3. CONCLUSIONES

Se implementó en un escenario virtual los ataques de Entidades Externas XML, Pérdida de Acceso y Configuración de Seguridad Incorrecta con sus respectivos controles para mitigar el riesgo, preservando la confiabilidad, disponibilidad e integridad de la información.

La pérdida de control de acceso, utiliza el ataque de Hombre en Medio para interceptar la información y obtener contraseñas de diferentes sitios webs, lo que conlleva a un secuestro de sesión e induce al espionaje corporativo o expresa un medio de extorsión al titular de la cuenta.

El empleo de la herramienta Nmap facilita verificar vulnerabilidades, debido a que escanea los puertos lógicos de un computador, efectuando ataques de configuración de seguridad incorrecta, para medir el grado de protección del sitio permitiendo decidir si es necesaria la implementación del control e inferir qué medidas tomar al garantizar la integridad de la información.

BIBLIOGRAFÍA

[1] D. Gillman, Y. Lin, B. Maggs y R. K. Sitaraman, «Protecting Websites from Attack with Secure Delivery Networks,» *IEEE Computer Society ,* vol. 48, pp. 26 - 34, 2015.

[2] M. Liu y B. Wang, «A Web Second-Order Vulnerabilities Detection Method,» *IEEE Access,* vol. 6, pp. 70983 - 70988, 2018.

[3] K. E. Heckman, F. J. Stech, B. S. Schmoker y R. K. Thomas, «Denial and Deception in Cyber Defense,» *IEEE Computer Society ,* vol. 48, pp. 36 - 44, 2015.

[4] L. b. Othmanea, R. Ranchalb, R. Fernando, B. Bhargavab y E. Bodden, «Incorporating attacker capabilities in risk estimation and mitigation,» *Computers & Security,* vol. 51, pp. 41-61, 2015.

[5] G. Deepa y P. Santhi Thilagam, «Securing web applications from injection and logic vulnerabilities: Approaches and challenges,» *Information and Software Technology,* vol. 74, pp. 160-180, 2016.

[6] J. Thome, L. Khin Shar, D. Bianculli y L. Briand, «Security Slicing for Auditing Common Injection Vulnerabilities,» *The Journal of Systems & Software,* vol. 137, pp. 766-783, 2017.

[7] M. Salas y E. Martins, «Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security,» *Electronic Notes in Theoretical Computer Science,* vol. 302, pp. 133-154, 2015.

[8] V. Prokhorenko, K. K. Raymond Choo y H. Ashman, «Web application protection techniques: A taxonomy,» *Journal of Network and Computer Applications,* vol. 60, pp. 95-112, 2015.

[9] L. Sampaio y A. Garcia, «Exploring context-sensitive data flow analysis for early vulnerability detection,» *Journal of Systems and Software,* vol. 113, pp. 337-361, 2016.

[10] V. R. Mouli y K. P. Jevitha, «Web Services Attacks and Security- A Systematic Literature Review,» *Procedia Computer Science,* vol. 93, pp. 870-877, 2016.

[11] M. I. Palma Salas, P. L. De Geus y E. Martins, «Security Testing Methodology for Evaluation of Web Services Robustness - Case: XML Injection,» *IEEE World*

Congress on Services, 2015.

[12] O. M. Awoleyea, B. Ojulogeb y M. O. Ilori, «Web application vulnerability assessment and policy direction towards a secure smart government,» *Government Information Quarterly,* vol. 31, pp. 118-125, 2014.

[13] G. Steinkea, E. Tundrea y K. Kelly, «Towards an Understanding of Web Application Security Threats and Incidents,» *Journal of Information Privacy and Security,* vol. 7, pp. 54-69, 2014.

[14] N. Tuptuk y S. Hailes, «Security of smart manufacturing systems,» *Journal of Manufacturing Systems,* vol. 47, pp. 93-106, 2018.

[15] J.-S. Choa, Y.-S. Jeongb y S. O. Park, «Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol,» *Computers & Mathematics with Applications,* vol. 69, pp. 58-65, 2015.

[16] Y. Guo y Z. Zhang, «LPSE: lightweight password-strength estimation for password meters,» *Computers & Security,* vol. 73, pp. 507-518, 2017.

[17] N. Hoquea, M. H. Bhuyana, R. Baishyaa, D. Bhattacharyyaa y J. Kalita, «Network attacks: Taxonomy, tools and systems,» *Journal of Network and Computer Applications,* vol. 40, pp. 307-324, 2014.

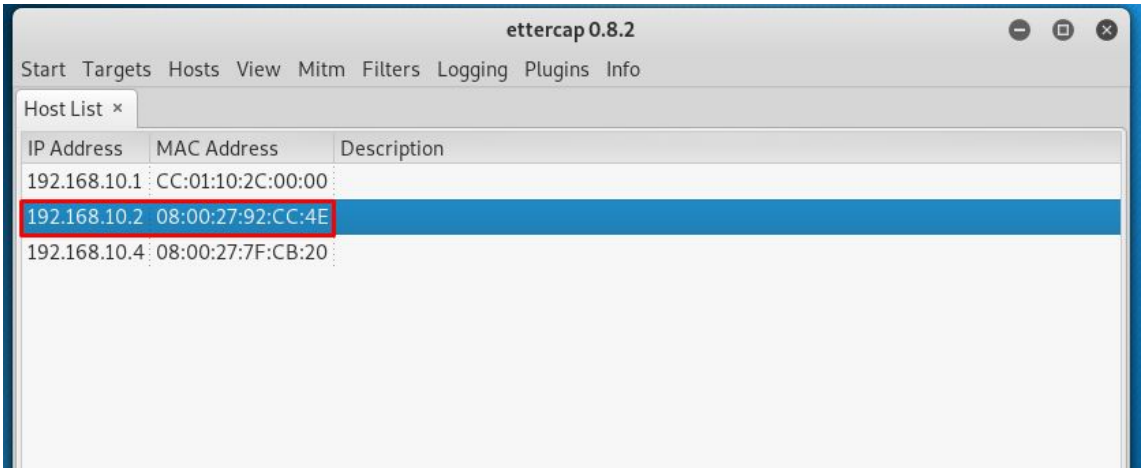
[18] H. Siew, S. Tan y C. Lee, «Summation And Division of Status Algorithm For Multiple Crosstalk Attacks Source Identification,» *Optik,* vol. 132, pp. 407-416, 2016.

ANEXOS

Anexo 1: Herramienta Ettercap

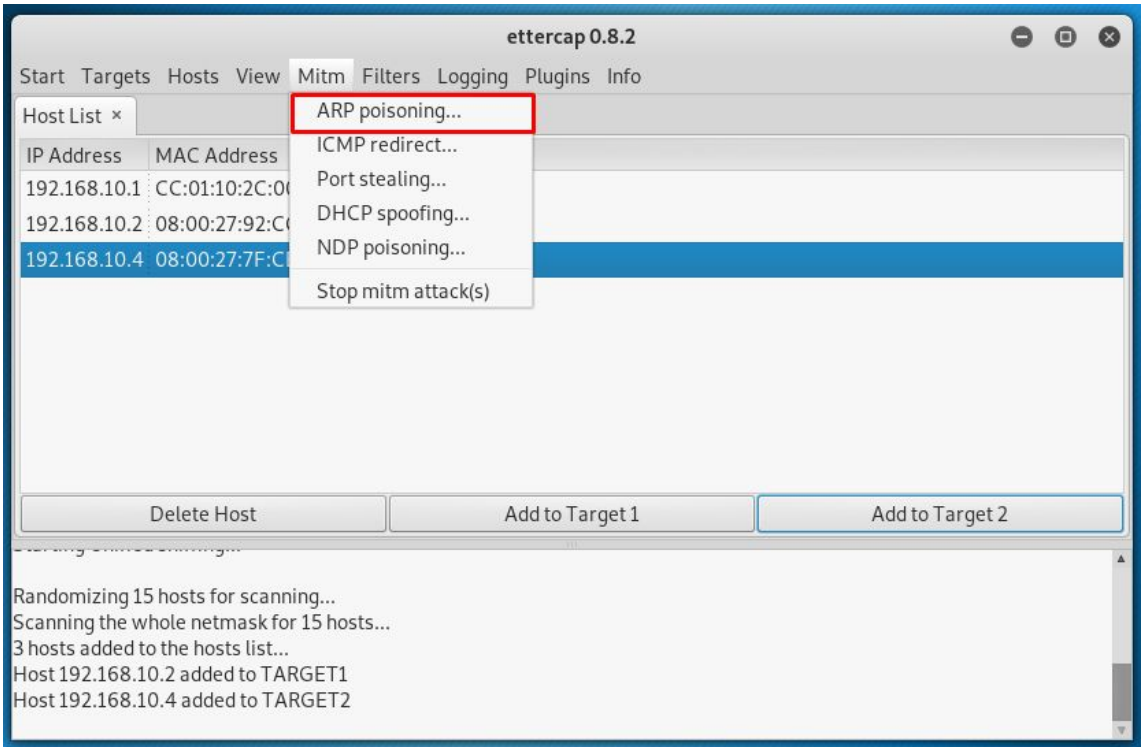
Fuente: Elaboración Propia

Anexo 2: Lista de hosts



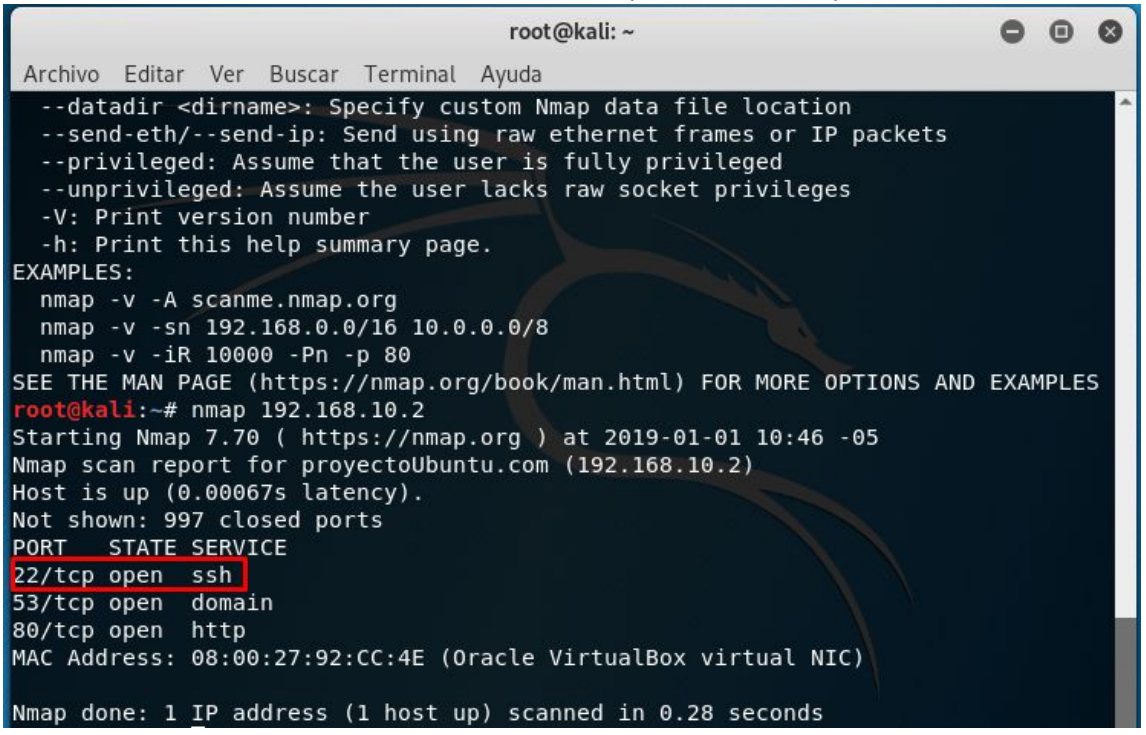
Fuente: Elaboración Propia

Anexo 3: Envenenamiento ARP



Fuente: Elaboración Propia

Anexo 4: Escaneo de puertos con Nmap



Fuente: Elaboración Propia

Anexo 5: Acceso a los archivos de la carpeta Descarga

```
luis@luis-VirtualBox:~$ cd Descargas
luis@luis-VirtualBox:~/Descargas$ ls -l
total 155976
-rw-rw-r-- 1 luis luis      3483 dic 29 08:59 2017-07-09.complete-user-registrat
ion-system-using-php-and-mysql-database.zip
drwxrwxr-x 2 luis luis      4096 dic 30 15:34 apache2
-rw-rw-r-- 1 luis luis   5010042 nov  2  2014 bWAPP_intro.pdf
-rw-rw-r-- 1 luis luis  15058349 dic 30 15:29 bWAPP_latest.zip
-rw-rw-r-- 1 luis luis       325 mar  8  2014 ClientAccessPolicy.xml
-rw-rw-r-- 1 luis luis       200 mar 11  2014 crossdomain.xml
drwxrwxr-x 2 luis luis      4096 dic 30 15:34 evil
-rw-rw-r-- 1 luis luis      2589 may 12  2014 INSTALL.txt
-rw-rw-r-- 1 luis luis      2491 nov  2  2014 README.txt
drwxrwxr-x 2 luis luis      4096 dic 29 09:01 registro
-rw-rw-r-- 1 luis luis      8271 nov  2  2014 release_notes.txt
-rwxrwxrwx 1 luis luis 139591999 dic 29 07:29 xampp-linux-x64-5.6.39-0-installer
.run
```

Fuente: Elaboración Propia

Anexo 6: Configuración de fail2ban

```
root@luis-VirtualBox: ~
Archivo  Editar  Pestañas  Ayuda
 GNU nano 2.8.6          Archivo: /etc/fail2ban/jail.conf

# JAILS
#


#
# SSH servers
#

[sshd]

# To use more aggressive sshd filter (inclusive sshd-ddos failregex):
#filter = sshd-aggressive
enabled = true
port    = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 1
backend = %(sshd_backend)s


[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois request
# in the body.
enabled = true
port    = ssh
filter = sshd
logpath = /var/log/auth.log
```

Fuente: Elaboración Propia