CLAVE: 13DIT0001E

Titulación Integral

Tesis

"Pentesting a Base de Datos en Sistemas Operativos de Distribución Gratuita o de Paga"

Para obtener el Título de

Ingeniería en Sistemas de Computación

Integrante(s)
Christopher Romero Hernández
Everardo Salinas Salvador

Director
M. en C. Ing. Leodegario Redondo Martínez

Codirector
Ing. José Manuel Romero Orta

Fecha: Noviembre 2020

PRELIMINARES
AGRADECIMIENTOS

El presente trabajo de investigación se lo dedico principalmente a Dios, por ser el inspirador y darme fuerza para continuar en éste proceso de obtener uno de los anhelos más deseados.

A mis Padres: por su amor, trabajo, por los valores y principios que me inculcaron, por apoyarme y alentarme a superarme, por ser la fuente de inspiración y motivación para superarme cada día más.

A mis Hermanos: por ser parte de mi vida, por el apoyo que siempre me brindaron, por apoyarme día con día.

A mis docentes: por haberme compartido de sus conocimientos a lo largo y preparación de mi profesión, al Ingeniero Egleyde Gómez Nochebuena, al Ingeniero Leodegario Redondo Martínez, al Ingeniero Delfino Olivares Sagahón.

De Manera Especial: al Maestro David Gómez Montiel y a la Sra. Gilberta Nochebuena Hernández.

A mi Pareja: quien me apoyo en todo momento, quien estuvo conmigo en los momentos difíciles de este proceso de formación, por su paciencia por su amor y comprensión.

Todos y cada uno de ustedes fueron una parte clave en el proceso de mi educación.

Christopher Romero Hernández

A Dios:

Por permitirme llegar a esta etapa de mi vida, por darme salud, paciencia y la fortaleza para no desfallecer en los momentos más difíciles.

A mis padres:

Taurino Salinas Reynosa e Ignacia Salvador Ángeles

Por darme la vida, por creer en mí, por todos sus buenos consejos y por todo su amor, por enseñarme las cosas buenas de la vida, por su gran valor y sabiduría para llevarme por el buen camino.

A mi esposa:

Natalia Santos Ramírez

Por ser paciente durante todo este largo trayecto, por soportar los días en que debería estar en casa y no lo estaba, gracias por todo el amor y confianza en que podría lograrlo.

A mi hijo:

Eber Abimael Salinas Santos

Por ser el motor que siempre me ha impulsado a ser una mejor persona, principalmente por que fue quien me motivó a tomar este gran desafío y con esto demuestro que nunca es tarde para soñar y hacer realidad esos sueños.

A mi asesor:

El M. en C. Leodegario Redondo Martínez

Quien fungió como asesor para que el presente proyecto se llevara a cabo, gracias por todo el apoyo a lo largo de la carrera, siempre ha sido un docente entregado a su trabajo y ansias de aprender y enseñar y por esa razón estoy profundamente agradecido.

A mi Jefe del Departamento de Sistemas y Computación:

M. en C. Rosi Areli Hernández Cruz:

Por los buenos consejos grupales y su manera de enseñar, por el apoyo brindado a lo largo de mi formación y por la autorización del presente proyecto.

A mis compañeros de carrera:

Estoy muy agradecido por compartir esta gran aventura durante casi cuatro años. Compartiendo sueños, conocimientos, por el apoyo mutuo porque siempre trataron que ninguno perdiera el camino, gracias los voy a extrañar.

Al Instituto Tecnológico de Huejutla

Por ser una casa de estudios enfocada y dedicada a formar profesionistas capaces, de ella me llevo muy buenos recuerdos, sus docentes muy entregados a sus alumnos.

Everardo Salinas Salvador

RESUMEN

En el presente proyecto se presentan las diferentes fases para realizar un Pentesting a un servidor remoto dentro o fuera de la misma red con el fin de penetrar su seguridad y poder acceder a la base de datos alojada en él, se abordan temas como el reconocimiento pasivo y activo del host objetivo, la recopilación de información utilizando herramientas especializadas para este fin como Nmap para el escaneo de puertos abiertos y los servicios activos en ellos así como sus versiones, la detección del sistema operativo anfitrión y sus versiones, la detección de vulnerabilidades, también se realizan algunas pruebas de penetración con ataques de fuerza bruta por diccionarios de palabras utilizando herramientas avanzadas desarrolladas en lenguajes de programación python y/o Ruby que se pueden encontrar en la web o con ayuda de algunos módulos de Metasploit Framework para este fin y dependiendo los resultados de las pruebas se hacen breves recomendaciones que hay que tomar en cuenta para reforzar la seguridad en los servidores de bases de datos tanto a nivel humano como a nivel físico o de hardware y a nivel de software.

Para poder realizar todo lo antes mencionado se crea un laboratorio de pruebas con todo lo necesario para ejecutar las actividades que se plantean en el presente proyecto, se instalaron los sistemas operativos objetivos (Windows 7 y Linux, distribución Ubuntu) y posteriormente se instaló en ellos el Sistema Gestor de Bases de Datos (SGBD) para crear el servidor de bases de datos, también se instaló el sistema operativo Linux, distribución kali, desde el cual se realizaron todas las pruebas de seguridad lanzando escaneos y ataques a los objetivos para romper su seguridad.

El presente proyecto no pretende otra cosa más que hacer ver la importancia de mantener segura e integra la información almacenada en las bases de datos.

ÍNDICE

ÍNDICE DE IMÁGENES

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

Las bases de datos son un elemento fundamental en el entorno informático hoy en día y tienen aplicación en la prácticamente la totalidad de campos. Concebidas con un propósito general, son de utilidad para toda disciplina o área de aplicación en la que exista una necesidad de gestionar datos, tanto más cuanto más voluminosos sean estos.

Sin embargo el masivo incremento en el uso de las computadoras y el desarrollo de aplicaciones cada vez más sofisticadas han creado la necesidad de aplicar técnicas de seguridad a las bases de datos para poder hacer frente a estos cambios y priorizar un enfoque preventivo e intentando actuar antes o durante el hecho, asegurando que los activos de las compañías o instituciones permanezcan protegidos y que se han establecido los controles internos adecuados para salvaguardar los recursos informáticos apropiadamente.

“La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.” (*Cesar H. Tarazona, 2007*).

Si bien es cierto que los sistemas de gestión de bases de datos proveen mecanismos que garantizan la seguridad, consistencia y reglas de integridad no está de más controlar y reforzar estos mecanismos con otras capas de seguridad por ejemplo el SO del servidor anfitrión donde se alojen estas estructuras debe cumplir con ciertos estándares asegurando que la información almacenada se mantenga segura e integra ante cualquier intento de extracción de datos por entidades externas, otro ejemplo es validar que tipo de usuarios están autorizados para el uso, es por ello que se realizaron pruebas de penetración a diferentes

sistemas operativos, para poder dar un informe detallado de las vulnerabilidades que se pueden presentar.

.

DESCRIPCIÓN DE LA ORGANIZACIÓN

TECNOLÓGICO NACIONAL DE MÉXICO CAMPUS HUEJUTLA

Dirección: **Carretera Huejutla-Chalahuiyapa, Km 5.5**
Teléfono: **(01- 789) 89-6-06-48**
Email: **dir_huejutla@tecnm.mx**

INFORMACIÓN SOBRE LA EMPRESA, ORGANISMO O DEPENDENCIA PARA LA QUE SE DESARROLLARA EL PROYECTO

VISIÓN

Ser una Institución líder en la Educación Superior Tecnológica, de alto desempeño y comprometida en la práctica de valores, contribuyendo así a la formación de una sociedad a la altura de las exigencias del entorno.

MISIÓN

Formar profesionales competitivos emprendedores y humanistas con un enfoque de desarrollo sustentable, capaz de transformar el entorno social, preservar y rescatar la identidad cultural.

Valores

- Honestidad
- Respeto
- Tolerancia
- Humildad
- Ética
- Trabajo en Equipo
- Solidaridad

OBJETIVOS

OBJETIVO GENERAL

- Realizar pruebas de penetración a diferentes sistemas operativos, para poder dar un informe detallado de las vulnerabilidades que se pueden presentar.

OBJETIVO ESPECÍFICO

- Identificar huecos de seguridad en los sistemas operativos de paga o gratuitos.
- Solventar las vulnerabilidades encontradas en los sistemas operativos y bases de datos.
- Otorgar informes al TecNM Huejutla sobre las pruebas realizadas.
- Fortalecer el servidor que alojará la base de datos en el TecNM Huejutla.
- Determinar si existe alguna restricción legal que pueda impedir el desarrollo del proyecto en el TecNM Huejutla.

JUSTIFICACIÓN

Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad.

Las pruebas de Pentest se han convertido en un paso importante para poder evaluar la efectividad de los procesos y mecanismos de ciberseguridad en las organizaciones, así como el identificar la fragilidad de sus sistemas de Seguridad e incluso justificar la adopción de nuevas herramientas y procesos en el área.

Este tipo de pruebas tienen como objetivo principal el identificar vulnerabilidades potenciales en los sistemas y estructuras de red de las organizaciones, y por medio de herramientas especializadas intentar lograr una intrusión desde el punto de vista de un atacante, midiendo el impacto y alcance que se tendría al recibir un ataque dirigido hacia la empresa. De esta manera se conocerían sus debilidades y huecos de seguridad, permitiendo al departamento de seguridad blindar y robustecer las capas de seguridad implementadas en su infraestructura.

De ahí surge la necesidad y el interés por realizar pruebas con diferentes sistemas operativos, para informar cuál es el sistema operativo con menos vulnerabilidades para así, desarrollar una base de datos que sea lo suficientemente segura como para mantener la información del alumnado y de la misma escuela integra, por lo cual nos daremos a la tarea de realizar dicha investigación y de realizar pruebas de penetración a dichos sistemas operativos.

MARCO TEÓRICO

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de las tecnologías de la información como una herramienta esencial para lograr sus objetivos sin embargo todos están expuestos a ciertos riesgos que pueden llevar a la pérdida parcial o total de la información, estos riesgos están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

Las instituciones educativas, aunque no lo parezca, siempre han sido un blanco fácil por entidades malintencionadas para sustraer información almacenada en sus bases de datos ya sea con fines de corromper los datos para beneficio propio entre otros propósitos personales.

¿Qué es una base de datos?

Entendemos como base de datos a un conjunto de datos estructurado y almacenado de forma sistemática con objeto de facilitar su posterior utilización (*Olaya, 2020*). Los

elementos clave de la base de datos son esa estructuración y sistematicidad, pues ambas son las responsables de las características que hacen de la base de datos un enfoque superior a la hora de gestionar datos.
Algunas ventajas que afectan directamente a los datos son las siguientes:

Mayor independencia. Los datos son independientes de las aplicaciones que los usan, así como de los usuarios.

Mayor disponibilidad. Se facilita el acceso a los datos desde contextos, aplicaciones y medios distintos, haciéndolos útiles para un mayor número de usuarios.

Mayor seguridad (protección de los datos). Por ejemplo, resulta más fácil replicar una base de datos para mantener una copia de seguridad que hacerlo con un conjunto de ficheros almacenados de forma no estructurada. Además, al estar centralizado el acceso a los datos, existe una verdadera sincronización de todo el trabajo que se haya podido hacer sobre estos (modificaciones), con lo que esa copia de seguridad servirá a todos los usuarios.

Menor redundancia. Un mismo dato no se encuentra almacenado en múltiples ficheros o con múltiples esquemas distintos, sino en una única instancia en la base de datos. Esto redunda en menor volumen de datos y mayor rapidez de acceso.

Mayor eficiencia en la captura, codificación y entrada de datos.

¿Qué es un sistema gestor de bases de datos?

Un sistema gestos de bases de datos (SGDB o DBMS, del inglés *DataBase Management System*) es una colección de programas o software que permiten a los usuarios crear y mantener una base de datos (*Bertino & Martino, 1995*), dedicado a servir de interfaz entre las bases de datos, el usuario y las aplicaciones que la utilizan. Tienen como objetivo la abstracción de la información, la consistencia, la seguridad o el tiempo de respuesta a las peticiones que se le hagan.

¿Qué es un servidor?

Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente *("¿Qué es un servidor?", 2020)*. Los servidores funcionan basándose en el modelo “cliente-servidor”. El cliente puede ser tanto un ordenador como una aplicación que requiere información del servidor para funcionar. Por tanto, un servidor ofrecerá la información demandada por el cliente siempre y cuando el cliente esté autorizado.

Un Servidor de Base de Datos es aquel que provee servicios de base de datos a otros programas o equipos cliente.

¿Qué es un sistema operativo?

Para el manejo de la información almacenada en una base de datos es importante que exista un intermediario que nos permita leer el medio de almacenamiento en donde se encuentran alojados los datos

Un sistema operativo (SO). Es el programa o conjunto de programas que efectúan la gestión de los procesos básicos de un Sistema informático y permite la normal ejecución del resto de las operaciones *("Sistema operativo - EcuRed", 2020)*. Por tanto un SO administra los recursos conectados a un equipo de cómputo para que estos puedan funcionar correctamente y dar servicio al usuario.

Entre los SO más importantes o conocidos se encuentran los de paga como Windows y MacOS y los de uso libre como lo es Linux.

¿Cómo podemos mantener segura e integra la información almacenada en una base de datos?

Sencillamente poniendo todo tipo de candados para evitar que cualquier entidad externa pueda corromper la integridad de los datos. Tener bien identificados los miembros o entidades que pueden tener acceso a los datos.

¿Qué es el Pentesting?

Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas *("Qué es el Pentesting", 2020*). Derivado de muchos casos de filtraciones y ataque a empresas es que ha surgió esta rama de estudio la cual es relativamente nueva y en auge.

Vulnerabilidad

Las vulnerabilidades son debilidades internas de un Sistema de Información las cuales, si son explotadas, podrían causar un daño significativo. La existencia de una vulnerabilidad no causa por sí misma un daño, es necesario que se presente una amenaza para detonarla.

De esta manera, la vulnerabilidad es una deficiencia en el diseño, implementación, operación o los controles internos en un proceso, que podría utilizarse para violar la seguridad de un sistema. Ahora bien, una vulnerabilidad que no tiene su correspondiente amenaza, puede que no requiera la implantación de un control, pero aun así debe ser reconocida y monitoreada para cambiarla.

Todos los Sistemas de Información tienen vulnerabilidades. Debemos considerar que éstos son desarrollados, implementados y operados por personas, por lo tanto, el error está presente intrínsecamente en todos ellos. Sin duda, existen casos en los cuales el administrador o programador instalan maliciosamente una falla en un sistema para ser detonados posteriormente. Asimismo, la mayoría de las vulnerabilidades surgen de factores tales como la complejidad, la ignorancia o el costo de los controles financieros.

El punto para la gestión de riesgos y las auditorías es la identificación y corrección de las vulnerabilidades antes de que puedan ser utilizadas, o por lo menos, para

limitar el rango de aplicación de las amenazas que puedan valerse de ellas, hasta el punto de que ya no sean creíbles.

Riesgo Asociado con las Aplicaciones Web

La seguridad de la web debe ser prioritaria para aquellas organizaciones que usan internet como elemento primordial de comunicación con sus clientes. Asegurarse de una adecuada protección contra aquellos accesos no autorizados a los recursos de información, es esencial para la viabilidad de cada organización.

Lo anterior debe ser incluido en la parte más alta de la lista de riesgos a los que hay que hacer frente, lo cual puede requerir de capacitación especializada para los auditores, profesionales de la seguridad y equipo de desarrollo. Lo más importante, es que estos grupos sean conscientes de todas las vulnerabilidades de las aplicaciones web, que incluyen la conocida y recientemente descubierta debilidad que puede ser explotada por los atacantes de internet.

Vulnerabilidades Web más Comunes

Para entender mejor las vulnerabilidades de las aplicaciones Web, exponemos los siguientes ejemplos de conocidos casos de seguridad, la cual continúa siendo quebrantada por atacantes desde la Internet ya sea para su propia diversión o beneficio ilícito.

Cross-site scripting: Esto ocurre cuando la aplicación web toma los datos suministrados por el usuario y los envía al browser sin una validación o codificación previa del contenido. En consecuencia, las vulnerabilidades XSS* permiten a los atacantes ejecutar un programa script en el browser de la víctima. Además, este riesgo es considerado como TOP TEN dentro de las debilidades de las aplicaciones web.

Inyección SQL: Esta vulnerabilidad, ocurre al nivel de la base de datos de una aplicación. Es un ataque vía web, que aprovecha errores en la filtración de datos

introducidos por el usuario y que permiten a un atacante tener el control de cierta aplicación.

Insecure Direct Object Reference: Una referencia directa a un objeto ocurre cuando un desarrollador expone una reseña a un objeto de implementación interno como un archivo, directorio, registro de una base de datos, clave como una URL o un parámetro formal. Los atacantes pueden manipular estas referencias para acceder a otros objetos sin autorización.

Cross-site request forgery (Falsificación en sitios cruzados): CSRF o también conocido como XSRF es una clase de ataque que afecta a las aplicaciones web con una estructura de invocación predecible.

Existen aplicaciones que usan cookies, autentificación de navegador o certificados de cliente. La idea básica de XSRF es un simple atacante que engaña de alguna manera al usuario para que realice una acción determinada en la aplicación objetivo / vulnerable sin que el usuario tenga conocimiento de los hechos que están ocurriendo realmente.

Manejo incorrecto de errores: Algunas aplicaciones pueden filtrar involuntariamente información sobre su configuración y funcionamiento. De esta manera, las aplicaciones web a menudo otorgan datos acerca de su estado interno por medio de mensajes de error detallados o de depuración. Muchas veces esta información puede ser aprovechada para poner en marcha o incluso automatizar los ataques más poderosos.

Error para restringir un acceso URL: El método de ataque para explotar una vulnerabilidad puede ser muy simplista. Este incluye enlaces y el uso de técnicas de fuerza bruta para encontrar páginas desprotegidas. Vulnerabilidades específicas incluyen acceso y explotación de la información sensible, Urls ocultos y especiales, artículos y códigos de seguridad que evalúan los privilegios en el cliente. Como resultado, los atacantes pueden obtener acceso a información confidencial, de control de seguridad en el cliente para que el navegador y las aplicaciones eludan los controles integrados en el código que se envía a browser.

DESARROLLO

DESCRIPCIÓN DETALLADA DE LAS ACTIVIDADES

Para la realización de este proyecto y de las pruebas no se siguió una metodología como tal sin embargo se realizaron las siguientes actividades para lograr los objetivos:

Actividad 1 – Análisis de Sistemas Operativos
Actividad 2 – Análisis de Gestores de Base de Datos
Actividad 3 – Análisis de Servidores
Actividad 4 – Herramientas de Hackeo
Pruebas de Penetración – Identificando a Nuestro Objetivo
Prueba 1 – Reconocimiento Pasivo
Prueba 2 – Reconocimiento IP
Prueba 3 – Escaneo de DNS
Prueba 4 – Mapeo de Ruta
Prueba 5 – Reconocimiento Activo, Escaneo de Red
Prueba 6 – Escaneo de Puertos e Identificación de BD
Prueba 7 – Identificación de Base de Datos
Prueba 8 – Identificación de BD con Metasploit
Prueba 9 – Ataque de Fuerza Bruta a BD
Prueba 10 – Explotando Base de Datos
Prueba 11 – Escaneo de Vulnerabilidades Script 1
Prueba 12 – Escaneo de Vulnerabilidades Script 2
Prueba 13 – Escaneo de Vulnerabilidades Script 3

Todas las anteriores se describen a continuación.

ACTIVIDAD 1 ANALIS DE SISTEMAS OPERATIVOS

Definición de sistema Operativo

“Según la Real Academia de la Lengua Española un sistema operativo es un conjunto de programas que realizan funciones básicas y permiten el desarrollo y ejecución de otros programas sobre un equipo de cómputo.”

Un sistema operativo es el software base sobre el cual se pueden ejecutar el resto de programas de usuario, establecen una interfaz que permite la comunicación entre el usuario y la computadora, su tarea principal es administrar el uso de los recursos disponibles en el equipo de cómputo como la memoria, el disco interno, los medios de almacenamiento y los recursos periféricos como el teclado, el mouse, las impresoras, la placa de red, etc. esto en función de prioridades requeridas por los programas que sobre él corren, es decir si un programa tiene mayor prioridad sobre otro entonces asigna mayor tiempo y recursos al de mayor prioridad.

Funciones que desempeña un Sistema Operativo

Dentro de las funciones que desempeña un sistema operativo podemos encontrar las siguientes:

Administración del procesador

Administra la distribución del procesador entre los programas mediante un algoritmo de programación.

Gestión de memoria de acceso aleatorio (memoria RAM)

Gestiona el espacio de asignación de memoria para cada programa que se desee ejecutar, si la memoria no es suficiente, el sistema operativo crea un espacio de memoria en el disco duro denominado memoria virtual aunque este es más lento.

Gestión de entradas y salidas

Un sistema operativo permite unificar y controlar el acceso de los programas al hardware mediante los drivers.

Gestión de ejecución de aplicaciones

Gestiona los recursos necesarios para que un programa o aplicación pueda ejecutarse sin ningún problema.

Administración de autorizaciones

Vigila que los recursos disponibles sean utilizados por programas o usuarios autorizados para su uso.

Gestión de archivos

Gestiona la lectura y escritura de ficheros existentes en el sistema de archivos así como el acceso de las aplicaciones y usuarios autorizados.

Gestión de la información

Proporciona indicadores para diagnosticar el correcto funcionamiento del equipo de cómputo.

Características de un Sistema Operativo

- Conveniencia
- Eficiencia
- Habilidad para evolucionar
- Administración de hardware
- Comunicación de dispositivos
- Organización de datos
- Manejar la comunicación en red
- Facilitar las entradas y salidas
- Recuperación de errores
- Interferencia de usuarios
- Generación de estadísticas
- Acceso compartido

Historia de los Sistemas Operativos

En el inicio de la computación el programador debía tener íntimo contacto con el hardware de una computadora ya que si algún proceso fallaba debía examinar detalladamente los registros arrojados para determinar la raíz del fallo y corregir el programa. Estas tareas eran muy tediosas y se invertía demasiado tiempo y recursos para ejecutarlas, para la ejecución de estas tareas se hacían siempre los mismos procedimientos se hizo evidente que se podían optimizar notoriamente de ahí la idea de crear un programa base encargado de administrar y llevar a cabo estas responsabilidades.

Históricamente los sistemas operativos tienen sus orígenes en la década de los 50's y de acuerdo a los grandes cambios sufridos por los mismos podemos dividir su evolución en 5 grandes generaciones.

- Generación cero (década de los 40´s) ○ Sencillamente los sistemas operativos no existían ○ la codificación se realizaba en lenguaje maquina ○ los programas se introducían bit a bit
- Primera generación (finales de los 50´s) ○ Aparecen los sistemas de procesamientos por lotes, cada tarea que se ejecutaba obtenía el control total de los recursos de la computadora y era devuelto al sistema operativo al concluirse dicha tarea.
  ○ Máquinas de gran tamaño ○ Se utilizaban bulbos y conexiones ○ Codificación en lenguaje maquina ○ Se utilizaban las tarjetas perforadas
- Segunda generación (mitad de los 60´s) ○ Aparecen los sistemas compartidos con multiprogramación, en estos se utilizan varios procesadores en un

solo sistema con el fin de incrementar
el poder de procesamiento.

- Tercera generación ○ Surgen la familia de computadoras IBM/360 para uso general, aquí es donde aparecen los sistemas de modos múltiples los cuales soportaban al mismo tiempo procesos por lotes, tiempo compartido, procesamiento en tiempo real y multiprocesamiento.

Arquitectura interna de un Sistema Operativo

Un sistema operativo se compone de un conjunto de paquetes de software que gestionan la interacción con el hardware. Entre los componentes fundamentales de un Sistema Operativo se encuentran:

- Núcleo (kernell)

Representa el corazón del sistema operativo que siempre está presente en la memoria real del ordenador y administra todo el sistema, se encarga de la gestión de la memoria, los procesos, los archivos, las entradas y salidas y la comunicación. API del núcleo

Se entiende como API (Interfaz de Programación de Aplicaciones) al conjunto de servicios que ofrece un sistema a las aplicaciones y procesos que usan a este mismo sistema, las aplicaciones invocan estos servicios mediante llamadas a procedimientos. Los nombres de estos procedimientos, sus argumentos y el significado de cada uno definen la API.

Al conjunto de servicios que ofrece el Núcleo a los procesos se le llama API del núcleo y pueden ser llamados desde un proceso cualquiera y la invocación a estos procedimientos se le conoce como “llamada al sistema”.

- Drivers

La operación de los dispositivos es altamente dependiente de su implementación y para independizar el código del núcleo de los variados mecanismos de

interacción con los dispositivos el núcleo define clases de dispositivos y para cada clase se define una interfaz estándar para interactuar con cualquier dispositivo que pertenezca a la clase. Esta interfaz corresponde a las declaraciones de un conjunto de procedimientos no implementados.

Un driver es entonces el código que implementa una interfaz estándar para interactuar con un dispositivo en específico.

- Interprete de comandos

Posibilita la comunicación con el sistema operativo mediante un lenguaje de control para que el usuario pueda controlar los periféricos disponibles.

- Sistema de archivos

Registra los archivos y ficheros dentro de una estructura, generalmente de árbol.

Clasificación de los Sistemas Operativos

Podemos clasificar a los sistemas operativos en función de la diferencia entre sus componentes.

Sistemas operativos por lotes.

Los trabajos se procesas en orden de admisión según el modelo “primero en llegar primero en ser atendido”, requieren que la información se reúna en bloques (el programa, los datos y las instrucciones).

Estos sistemas operativos dividen la memoria en dos zonas, la que es ocupada por el mismo sistema operativo y la que se utiliza para cargar y ejecutar los programas que se encuentran en transición.

Sistemas operativos multiprogramación.

Estos son capaces de cargar en memoria más de un proceso de manera simultánea y estos deben competir por los recursos disponibles para su ejecución, según sea

su prioridad de ejecución el sistema operativo asigna recursos y tiempo necesario para cada proceso.

Sistemas operativos multiusuario.

Permiten el acceso simultáneo a un sistema de computadoras a través de más de una terminal son básicamente utilizados en el manejo de redes de computadoras.

Sistemas operativos de tiempo compartido.

Reparten los recursos de manera equitativa dando la impresión de que cada usuario posee una computadora independiente.

Sistemas operativos de tiempo real.

Tratan de proporcionar respuesta en un menor tiempo posible, muchos procesos residen de manera permanente en memoria haciendo que el administrador de memoria sea menos solicitado.

Tipos de Sistemas operativos

Generalmente un equipo de computadora viene con un sistema opresivo precargado.
Existen una gran variedad de sistemas operativos, según su capacidad para administrar simultáneamente la información.

Microsoft Windows

Este sistema operativo es el más común del mercado, fue desarrollado durante la década de los ochenta.

Dentro de esta familia podemos encontrar sus diferentes versiones.

- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000
- Windows 2000 Server
- Windows XP
- Windows Server 2003
- Windows CE
- Windows Mobile
- Windows XP 64 bits
- Windows Vista (Longhorn)
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

Ventajas

- Gran cantidad de software para cualquier necesidad del usuario, ofimática, diseño gráfico, contabilidad, antivirus, etc. es casi imposible no encontrar el software que el usuario necesita.
- La facilidad para manejarlo gracias a su amigable entorno grafico que ha evolucionado con los años.
- La gran mayoría de hardware en el mercado viene con los controladores y drivers compatibles con este sistema operativo

Desventajas

- Al ser el sistema operativo más popular es el más atacado por virus, ransomware o malware

Mac OS

Este sistema operativo es propiedad de Apple Inc. Y viene preinstalado todas las computadoras Macintosh desarrolladas por la misma empresa.
Pertenecen a esta familia:

- Mac OS 7
- Mac OS 8
- Mac OS 9
- Mac OS X

Ventajas

- Fluidez en la realización de tareas muy específicas y que requieren gran cantidad de recursos.
- Actualizaciones constantes
- La disponibilidad de software para este sistema operativo ha ido en aumento en los últimos años.
- Ausencia nula o casi nula de virus informáticos

Desventajas

- Poco software disponible para entornos empresariales o profesionales
- Costos elevados de hardware y software

GNU/Linux

Este sistema operativo de código abierto es uno de los más utilizados por las grandes empresas ya que además de ser gratuito puede hacerse las modificaciones necesaria para adaptarlo a las necesidades de cada organización. Generalmente son utilizados para servidores, además de que es uno de los sistemas operativos más seguros del mundo de las computadoras.

Ventajas

- Software de código abierto
- Robusto y eficaz para uso empresarial

Desventajas

- Manejo confuso para usuarios comunes
- Poco software disponible para uso general

Los Sistemas operativos y la Seguridad informática

Los sistemas de archivos administrados por el sistema operativo generalmente contienen información valiosa para sus usuarios razón por la cual deben estar protegidos contra la lectura o escritura por usuarios o programas no autorizados. Si un sistema operativo no está preparado para resguardar y proteger la integridad de la información que administra esta puede ser leída por intrusos e incluso pude ser modificada o destruida.

Por lo cual se llegó a la conclusión de tomar los sistemas operativos más conocidos tanto de paga como libres para realizar las pruebas de seguridad, Windows 7 y Ubuntu.

ACTIVIDAD 2 ANALISIS DE GESTORES DE BASES DE DATOS

En esta etapa al igual que en el análisis de sistemas operativos se encontró infinidad de información relacionada a las bases de datos, las siguientes páginas veremos una pequeña parte de la información más importante.

BASES DE DATOS

Las bases de datos son un elemento fundamental en el ámbito de la informática, nacidas con un propósito general han adquirido gran relevancia y son de gran utilidad para cualquier disciplina o área de aplicación en donde exista la necesidad de gestionar datos

Definición de Base de Datos

Una base de datos es un conjunto estructurado de datos que representa entidades y sus interrelaciones (*Camps Paré et al., 2007*). Estos datos son almacenados de manera sistemática con la finalidad de ser utilizador en un futuro.

Historia y Evolución de las Bases de Datos

A lo largo de la historia la administración y almacenamiento de los datos ha sufrido una serie de cambios que han permitido hacer el fácil manejo de los mismos.

Ventajas de las bases de Datos

Algunas de las ventajas que afectan directamente a los datos son:

- Mayor independencia: los datos son independientes de las aplicaciones que lo usan, así como de los usuarios.

- Mayor disponibilidad: existe una mayor facilidad para el accesos a los datos desde diferentes contextos, aplicaciones y medios haciéndolos útiles para un mayor números de usuarios.
- Mayor seguridad: al estar organizados sistemáticamente es más fácil mantener una copia de seguridad para proteger los datos que hacerlo con un conjunto de ficheros almacenados de manera no estructurada.
- Menor redundancia: existe una única instancia de los datos sin entrar en redundancias ahorrando espacio en memoria y aumentando la rapidez para el acceso.
- Mayor eficiencia en la captura, codificación y entradas de datos: esta ventaja tiene consecuencia directa sobre los resultados obtenidos de la explotación de la base de datos
    - ✓ Mayor coherencia:
    - ✓ Mayor eficiencia: facilita el acceso a los datos y hace sencilla su explotación.
    - ✓ Mayor valor informativo
- Mayor facilidad y sencillez de acceso: el usuario solo se preocupa de usar los datos con el apoyo de las herramientas adecuadas.
- Facilidad para reutilización de datos: esto refiere a la facilidad para compartir los datos.

Desventajas de las Bases de Datos

- Instalación costosa: el control y administración de la base de datos requiere software y hardware potentes
- Personal calificado: esto debido a la dificultad de manejo de este tipo de sistemas
- Implantación larga y difícil: la adaptación del personal es complicada y lleva tiempo.

Clasificación de las Bases de datos

En función a su estructura existen diferentes modelos de bases de datos, entre los más comunes podemos encontrar a:

Bases de datos jerárquicas

Los datos se recogen mediante unas estructuras llamadas nodos los cuales están interconectados unos con otros. Cada nodo puede tener un único padre y cero o varios hijos, de esta manera se crea una estructura en forma de árbol invertido. Algunas de las desventajas de esta estructura es que existe escasa independencia de sus registros ya que para acceder a un datos debe pasarse por sus padres, mala gestión de la redundancia de los datos ya que si un registro tiene relación con más de uno debe almacenarse varias veces, aumentando el volumen de almacenamiento y reduciendo la integridad y coherencia de los datos.

Bases de datos en red

Este modelo resuelve los problemas del modelo jerárquico haciendo posible que un registro pueda relacionarse con varios registros pero la desventaja es que son muy complejas dificultando la administración de las bases de datos.

Bases de datos relacionales

Este modelo es el más común entre las bases de datos utilizados en la actualidad ya que son muy sencillos de comprender y de utilizar, sus esquemas están basados en tablas las cuales contiene un numero dado de registros los cuales constituyen a las filas (tuplas) y un número dado de campos, los cuales forman a las columnas.

Bases de datos orientadas a objetos

Es uno de los modelos más actuales y se deriva del paradigma de la programación orientada a objetos

Según la variabilidad de las bases de datos

Según la forma en la en la que están estructurados los datos dentro de las bases de datos podemos clasificarlas en:

- Bases de datos Estáticas: diseñadas especialmente para la lectura de datos se implementan especialmente para almacenar y registrar hechos históricos, los datos en ellas no pueden modificarse.
- Bases de datos Dinámicas: por el contrario de las bases de datos estáticas, los datos son modificables permitiendo funciones de actualización, edición y eliminación de datos.

Fases para el Diseño de Una Base de Datos

Para el desarrollo de una base de datos debe tomarse en cuenta las siguientes fases en el proceso.

- Diseño lógico

Pretende modelizar el contenido de la base de datos, implica el análisis de los datos que se van a recoger

- Diseño físico

Adapta el diseño lógico a las particularidades del SGBD

- Implementación

Se introducen los datos a la base de datos

- Mantenimiento

Monitorear la actividad sobre la base de datos

Los Manejadores de Bases de datos (SGBD)

¿Qué es un SGBD?

Es una aplicación que permite a los usuarios definir, crear y mantener la base de datos, además de proporcionar un acceso controlado a la misma (*Marqués, 2011*), al conjunto formado por la bases de datos y el SGBD se le denomina sistema de bases de datos.

Los servicios que proporciona un SGBD son:

La definición de la base de datos

Esto lo hace mediante un lenguaje de definición de datos (DDL, data Description Language). Este lenguaje permite especificar la estructura y el tipo de datos que contendrá la base de datos así como las restricciones sobre los mismos.

La inserción, actualización, eliminación y consulta de datos

Esto lo realiza mediante el lenguaje de manejo o manipulación de datos (DML, Data Manipulation Language)

Acceso controlado a la base de datos

- Sistema de seguridad: de esta manera se controla el acceso a usuarios autorizados por medio de un lenguaje de control de datos (DCL, Data Control Language).
- Sistema de integridad: mantienes la integridad y la consistencia de los datos almacenados.
- Sistema de control de recuperación: reestablece la base de datos después de un fallo en el hardware o en el software.
- Diccionario de datos o catalogo: contiene la descripción de los datos de la base de datos y es accesible por el usuario.

La principal herramienta con la que cuenta un SGBD es la interfaz de programación con el usuario el cual consiste en un lenguaje muy sencillo para la comunicación entre el usuario y el servidor al que se denomina SQL, Structure Query Language.

Este lenguaje esta estandarizado por la ISO 1.

Objetivos de un SGBD

- Acceso transparente a los datos: los datos deben ser accesibles por los usuarios sin que estos se preocupen por la estructura y la forma en que estos están almacenados.
- Protección de datos: un SGBD debe controlar el acceso a la base de datos para mantener la integridad de los datos, restringiendo los accesos cuando corresponda, esto se consigue estableciendo distintos privilegios a los usuarios según su rango.
- Eficiencia: un sistema gestor de bases de datos debe ser capaz de gestionar de manera fluida los datos y las operaciones.
- Gestión de transacciones: los SGBD deben ser capaz de permitir que las consultas de los usuarios se realicen de manera correcta evitando que estas queden en un estado intermedio de esta manera se garantiza la integridad de la información y permiten, en caso de que una consulta ejecutada no se concluya, volver a un estado inicial.

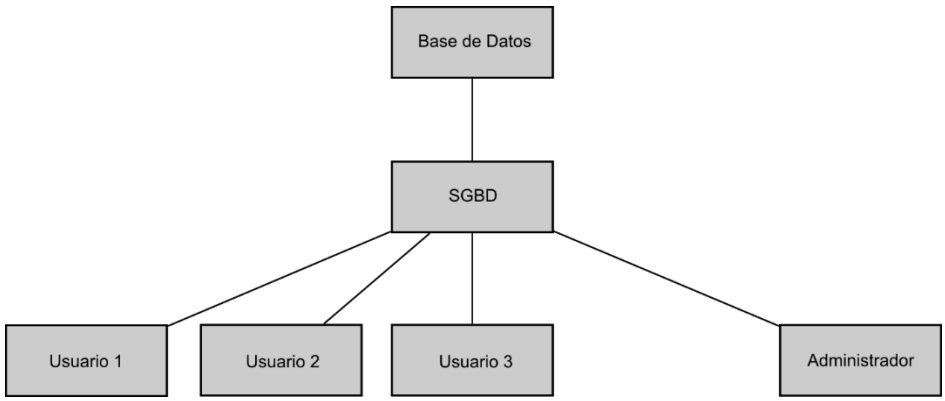

Ilustración 1 - Diagrama de un SGBD

Tipo de SGBD

Los gestores de bases de datos se pueden clasificar según la capacidad y potencia del gestor.

- SGBD ofimáticos: manipulan bases de datos relativamente pequeñas orientadas al uso doméstico o de pequeñas empresas, por ejemplo Microsoft Access y LibreOffice Base
- SGBD corporativos: orientados a gestionar bases de datos enormes con una carga de datos y transacciones que requieren de un servidor de grandes capacidades, por ejemplo ORACLE.

Ventajas de los SGBD

- Control de redundancia de datos
- Control de restricciones de acceso
- Almacenamiento persistente de estructuras y objetos de base de datos
- Múltiples interfaces de usuario
- Integridad referencial
- Seguridad y recuperación

Los SGBD más utilizados en la actualidad

Desde el surgimiento del modelo de bases de datos relacionales en los años 70 ha venido sufriendo una serie de cambios hasta convertirse en el más utilizado hoy en día y al mismo tiempo también han venido surgiendo diferentes tipos de SGBD, entre los más importantes podemos mencionar a:

MySQL

Es un SGBD relacional por excelencia, multihilo y multiusuario, actualmente utilizado en gran parte por páginas web y en aplicaciones creadas como software libre.
Se ofrece bajo la GNU GPL pero también puede adquirirse una licencia para uso empresarial.

Las ventajas de este sistema gestor de bases de datos son.

- Facilidad de uso y gran rendimiento
- Facilidad para instalar y configurar
- Soporte multiplataforma
- Soporte SSL

Las desventajas

- La escalabilidad, no trabaja de manera eficiente con bases de datos de gran tamaño

MariaDB

Este SGBD derivado de MySQL cuanta con la mayoría de características de este e incluye varias extensiones.
Nació a partir de la adquisición de MySQL por parte de ORACLE con el fin de continuar con la filosofía de OpenSource.

Entre las ventajas de este SGBD podemos mencionar que:

- Es totalmente compatible con MySQL
- Aumento de motores de almacenamiento
- Gran escalabilidad
- Seguridad y rapidez de transacciones

Las Bases de Datos y la seguridad

Los datos guardados en una base de datos deben estar protegidos contra accesos no autorizados, la destrucción o alteración de los datos.

Algunos de los riesgos que puede sufrir una base de datos son:

- La lectura no autorizada
- La modificación no autorizada
- La destrucción no autorizada

Para proteger los datos contenidos en una base de datos es necesario adoptar medidas de seguridad en diferentes niveles:

- Sistemas de Bases de datos o SGBD
- Sistemas Operativos
- Red
- Físico
- Humano

Ahora que sabemos que son los gestores y las bases de datos elegimos al mejor y más eficiente de todos MySQL y Xampp

ACTIVIDAD 3 ANALISIS DE SERVIDORES

En esta etapa del proyecto se realiza la búsqueda de información acerca de servidores el cual nos ayuda a entender la función de cada uno, a comparación de los gestores y bases de datos, la información adquirida sobre servidores fue muy limitada, a continuación lo más relevante:

Definición de Servidor

Definición Servidor (hardware): un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software *("¿Qué es un servidor? Un concepto, dos definiciones", 2020*).

Definición Servidor (software): un servidor basado en software es un programa que ofrece un servicio especial que otros programas denominados clientes (clients) pueden usar a nivel local o a través de una red *("¿Qué es un servidor? Un concepto, dos definiciones", 2020*).

Clasificación de Los Servidores

Los servidores se clasifican, según su función, en:

- Servidor dedicado. Este pone a disposición todos sus recursos para atender las peticiones que realice un equipo cliente.
- Servidor compartido. No dedica todos sus recursos a atender peticiones de los equipos cliente sino que también puede ser utilizado por un usuario para trabajar de manera local sobre él.

Tipos de Servidores

Según el tipo de peticiones que pueden atender, existen varios tipos de servidores

 Servidor de archivos

Como sus nombre lo indica, su función es servir de almacén de ficheros y tenerlos disponibles para las solicitudes de los clientes

- Servidor de directorios/dominio

Almacena información de los usuarios equipos o grupos de la red.

- Servidor de impresión

Sirve y administra trabajos de impresión a los clientes en una red

- Servidor de correo

Administra, gestiona y almacena correos de los usuarios de la organización

- Servidor de fax

Gestiona él envió, recepción y almacenamiento de faxes.

- Servidor proxy

La función principal es almacena en memoria cache las páginas web visitadas por los usuarios de la red para que en su próxima visita la respuesta sea más rápida.

- Servidor web

Almacena contenido web y sirve a los usuarios que hacen peticiones

- Servidor de bases de datos

Provee de servicios de bases de datos a los clientes

- Servidor DNS

Permite establecer la relación entre los nombres de dominio y las direcciones IP de los equipos de una red.

- Servidor DHCP

Este dispone de un rango de direcciones con el cual, asigna automáticamente los parámetros de configuración de red IP a las maquinas cliente cuando estas realizan una solicitud.

- Servidor FTP

Su función es permitir el intercambio de ficheros entre equipos, normalmente su aplicación va muy ligada a los servidores Web.

- Servidores IRC

El Internet Relay Chat por sus siglas en inglés, es actualmente uno de los servicios de chat más utilizados, el cual consiste básicamente en que varios servidores están conectados a una red, de modo que cualquier persona alrededor del mundo puede unirse a uno de éstos y chatear con cualquier otro usuario conectado a Internet.

- Servidor VPN (Virtual Private Network)

Este servidor se utiliza para realizar conexiones seguras a una red privada de una o varias computadoras sin que se encuentren físicamente en el mismo lugar. Ayuda a proteger nuestra información, los datos enviados o solicitados se encuentran cifrados hasta que salen de la VPN.

ACTIVIDAD 4 Herramientas de Hackeo

Metasploit

Metasploit es una herramienta de pentest para el desarrollo y ejecución de exploits destinada a auditar vulnerabilidades, fue desarrollada por HdMoore en el verano del año 2003 (*Muños Mogrobejo, 2012*).

Metasploit es un proyecto de código abierto destinado a la seguridad informática, además de proporcionar información acerca de vulnerabilidades de seguridad y ayuda al desarrollo de firmas para sistemas de detección de intrusos.

Metasploit Framework es un subproyecto de Metasploit destinado al desarrollo y ejecución de exploits contra una máquina remota. Inicialmente fue creado utilizando el lenguaje de programación Perl para más adelante ser transcrito al lenguaje de programación Ruby.

Metasploit puede ser ejecutado es sistemas basados en Unix (Linuc y MacOSX) y también en Windows.

Para la elección de un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, por ejemplo la versión del sistema operativo y los servicios de red instalados sobre él. Esta información puede obtenerse con la ayuda de herramientas de escaneo de puerto como Nmap, NeXpose o Nessus, estos programas pueden detectar vulnerabilidades del sistema de objetivo. Metasploit también puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas.

Sqlmap

Sqlmap es una poderosa herramienta la cual permite automatizar la vulnerabilidad de Inyección SQL (*Academy, 2020*). Esta herramienta cuenta con un potente motor de detección, muchas funciones de nicho para el pentester definitivo y una amplia gama de interruptores que van desde la toma de fingerprint de la base de datos, la obtención de datos, hasta el acceso al sistema de archivos subyacente y la ejecución de comandos en el sistema operativo a través de conexiones out-of-band (Ilustración 2).

Ilustración 2 - Interfaz Sqlmap

Aircrack-ng

Aircrack-ng es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK ("*es:aircrack-ng [Aircrack-ng]", 2019*). Este software es utilizado para auditar redes inalámbricas, trata de romper las claves y contraseñas capturando paquetes cifrados con algunas de sus herramientas.

Las herramientas más utilizadas para la auditoría inalámbrica son:

- Aircrack-ng (descifra la clave de los vectores de inicio)
- Airodump-ng (escanea las redes y captura vectores de inicio)
- Aireplay-ng (inyecta tráfico para elevar la captura de vectores de inicio)
- Airmon-ng (establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores).

La suite está diseñada para trabajar con una distribución Linux, aunque también existe una versión para Windows que no es muy estable debido a conflictos con drivers. Esta suite está diseñada para trabajar con tarjetas inalámbricas con circuitos integrados Atheros y con algunas con circuitos Ralink sin necesidad de configurarlas (Ilustración 3).

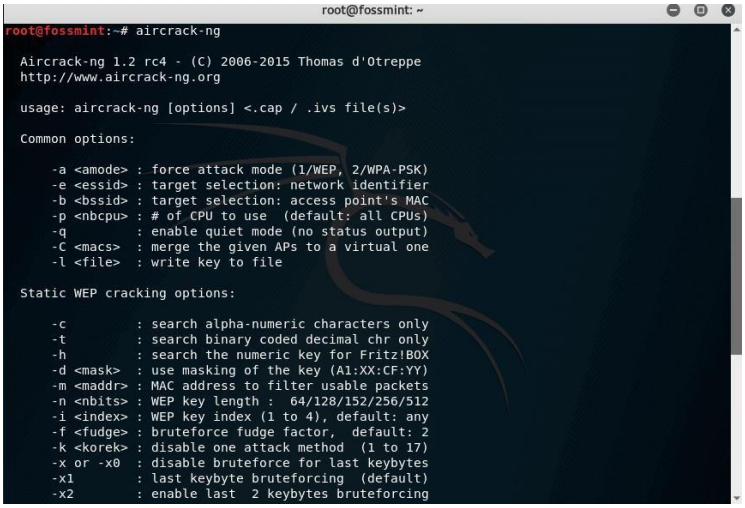

Ilustración 3 - Interfaz Aircrack-ng

THC Hydra

Hydra es un cracker de inicio de sesión de red en paralelo. Hydra funciona mediante el uso de un conjunto de métodos para descifrar contraseñas utilizando diferentes enfoques para generar contraseñas posibles, utiliza métodos como ataques de lista de palabras, ataque de fuerza bruta y muchos otros métodos. Hydra es comúnmente utilizado por los evaluadores de penetración junto con un software llamado Crunch, que se utiliza para generar la lista de palabras. Crunch se usaría para generar listas de palabras, mientras que Hydra se usa para probar los ataques usando las mismas listas de palabras que Crunch creó. Hydra está programado para actualizar las horas extraordinarias a medida que se respalden más y más servicios. (Ilustración 4).

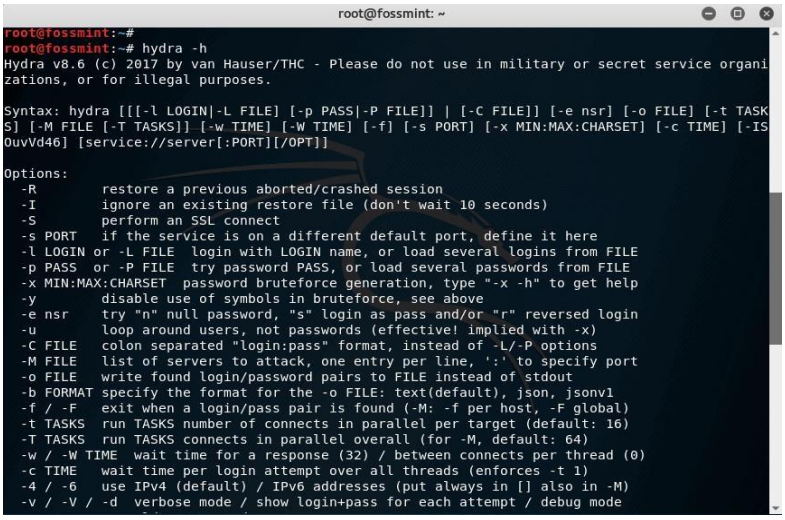

Ilustración 4 - Interfaz Hydra

John the Ripper

Es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas (*"John the Ripper", 2020*).

Esta es una de las herramientas de descifrado de contraseñas más popular utilizada por los administradores de sistemas para detectar contraseñas débiles de los usuarios en una red.

John the Ripper usa un ataque por diccionario: tiene un diccionario con palabras, que pueden ser contraseñas típicas, y las va probando todas. Para cada palabra, la cifra y la compara con el hash a descifrar. Si coinciden, es que la palabra era la correcta.

Esto funciona bien porque la mayor parte de las contraseñas que usa la gente son palabras de diccionario. Pero John the Ripper también prueba con variaciones de estas palabras: les añade números, signos, mayúsculas y minúsculas, cambia letras, combina palabras, etc. Además ofrece el típico sistema de fuerza bruta en el que se prueban todas las combinaciones posibles, sean palabras o no. Éste es el sistema más lento, y usado sólo en casos concretos, dado que los sistemas anteriores (el ataque por diccionario) ya permiten descubrir muy rápidamente las contraseñas débiles. (Ilustración 5).

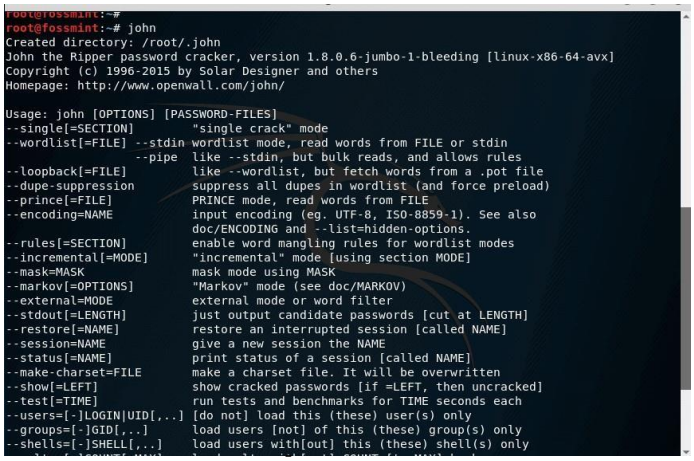

Ilustración 5 - Interfaz John the Ripper

Nmap

Nmap ("Network Mapper") es una utilidad gratuita y de código abierto (licencia)para la detección de redes y la auditoría de seguridad *("Nmap: the Network Mapper - Free Security Scanner", 2020*). Fue desarrollada inicialmente para sistema operativo Linux pero en la actualidad es multiplataforma. Sirve para efectuar rastreo de puertos mediante escaneos para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Posee una gran variedad de funciones para sondear redes de computadores, algunas de ellas como la detección de equipos, servicios y sistemas operativos. Estas funciones pueden ser extendidas mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. También es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma.

Algunas de las características principales son:

- El descubrimiento de servidores.
- Identifica puertos abiertos en un host dentro de la red.
- Determina los servicios que se ejecuta.

- Determina que sistema operativo y su versión utiliza el host, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Nmap es una herramienta muy utilizada por los administradores de un sistema ya que permite encontrar fallos en los sistemas y corregirlos así como detectar usuarios y/o programas no autorizados que se dentro de la red o el servidor (Ilustración 5).

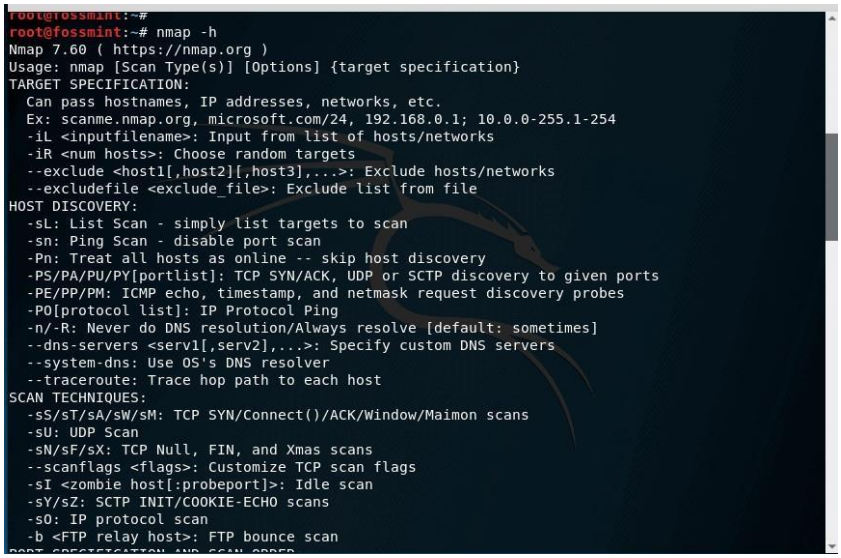

Ilustración 6 - Interfaz Nmap

Nessus

Nessus es un software de escaneo de vulnerabilidades en diversos sistemas operativos (*Marqués, 2020*).

Nessus escanea los puertos del objetivo utilizando Nmap o su propio escáner para posteriormente lanzar Exploits.

Los resultados obtenidos del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

El uso de Nessus para pruebas de vulnerabilidades puede causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

Actualmente existen dos versiones: "Home" y "Work" Esta última de pago y sin restricciones. (Ilustración 7)

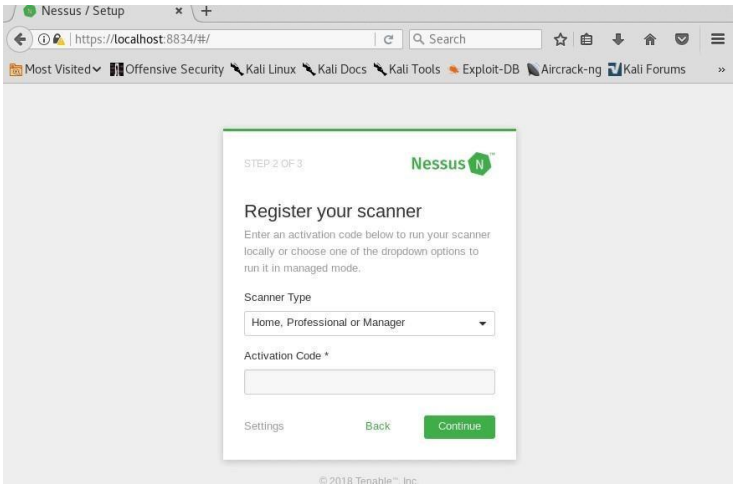

Ilustración 7 - Interfaz Nessus

WireShark

Se trata de un potente sniffer de red de software libre heredero de Ethereal que nos permite capturar y monitorizar todos los paquetes de red que pasan por nuestro equipo con el solo hecho de poner nuestra tarjeta de red a escuchar en modo promiscuo, es decir, diciéndole a nuestra tarjeta que capture todo el tráfico que pase por ella. (*Relancio, 2013*).

Tener la información detallada que nos facilita este programa nos permite poder analizar el tráfico que pasa por nuestra red y así poder solucionar o incluso prevenir los posibles problemas que puedan surgir (*Relancio, 2013*).
Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD,

Android, y macOS, así como en Microsoft Windows. Para capturar paquetes directamente de la interfaz de red, generalmente se necesitan permisos de ejecución especiales (Ilustración 8).

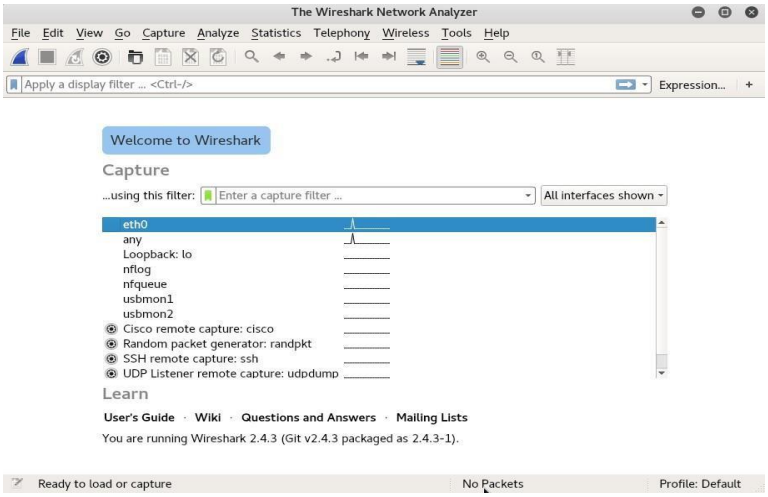

Ilustración 8 - Interfaz Wireshark

Nikto2

Nikto2 es un escáner web gratuito y de código abierto para realizar pruebas rápidas y completas contra elementos en la web (*"Las mejores 20 herramientas de hacking y penetración para Kali Linux", 2020*) (Ilustración 9).

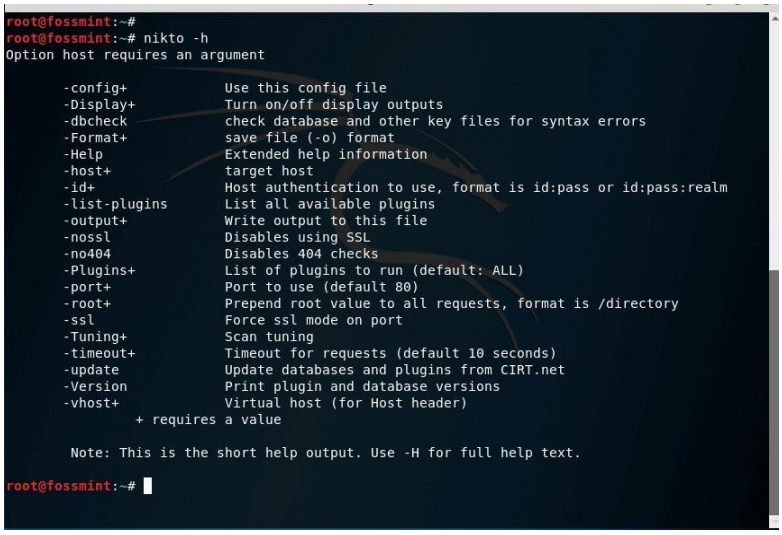

Ilustración 9 - Interfaz Nikto2

DNSenum - enumerador de servidores

Los primeros mapas de alto nivel de la red de una organización provendrán de la ubicación de sus servidores DNS. Comenzar con una buena base aquí lo ayudará a encontrar los puntos de apoyo clave que necesitará más adelante. DNSenum es una herramienta de alto nivel que a menudo es el primer paso para mapear su red de objetivos. Usando el formato...

./dnsenum enum [NOMBRE DE DOMINIO OBJETIVO] ...

Dmitry – “El telemetro de red”

Una vez que la información de su DNSenum haya regresado, tendrá un rango de servidores utilizados por su objetivo. El objetivo de Dmitry rangefinder es averiguar qué IP se utilizan en esos servidores. Esto se realiza mediante un comando de traceroute TCP que puede enhebrarse y mostrarse gráficamente con los comandos Dmitry.

INSTALACION DE SISTEMAS OPERATIVOS

Para la realización de las pruebas se requiere un ambiente controlado por lo cual se destinó un laboratorio de pruebas, Se le instalo el sistema operativo anfitrión, para posteriormente instalar kali Linux de la forma habitual (Ilustración 10,
Ilustración 11), Se procedió a instalar los sistemas victimas Ubuntu (Ilustración 12, Ilustración 13) y Windows (Ilustración 14, Ilustración 15).

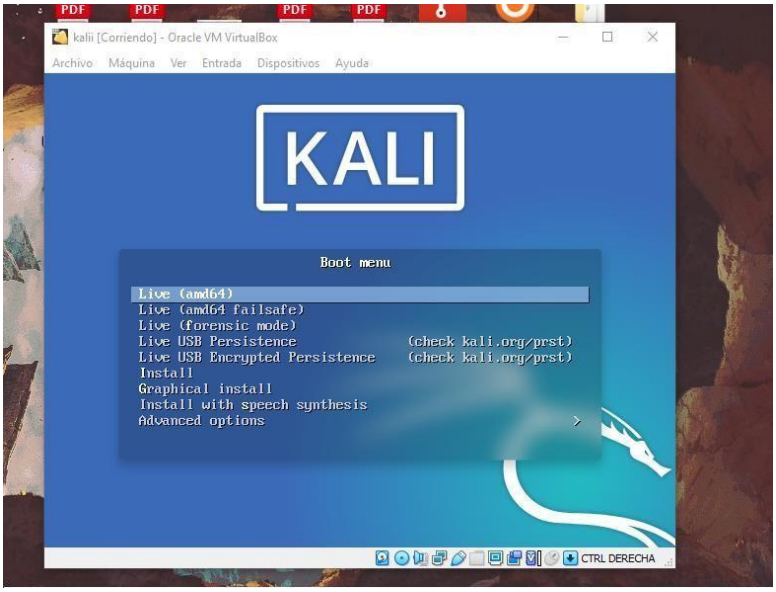

Ilustración 10 - Ventana de Instalación Kali

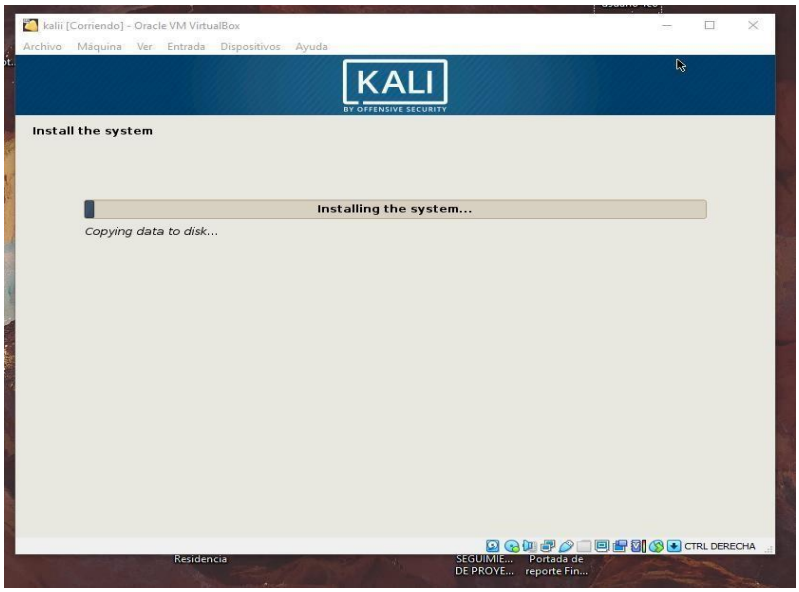

Ilustración 11 - Progreso de instalación Kali

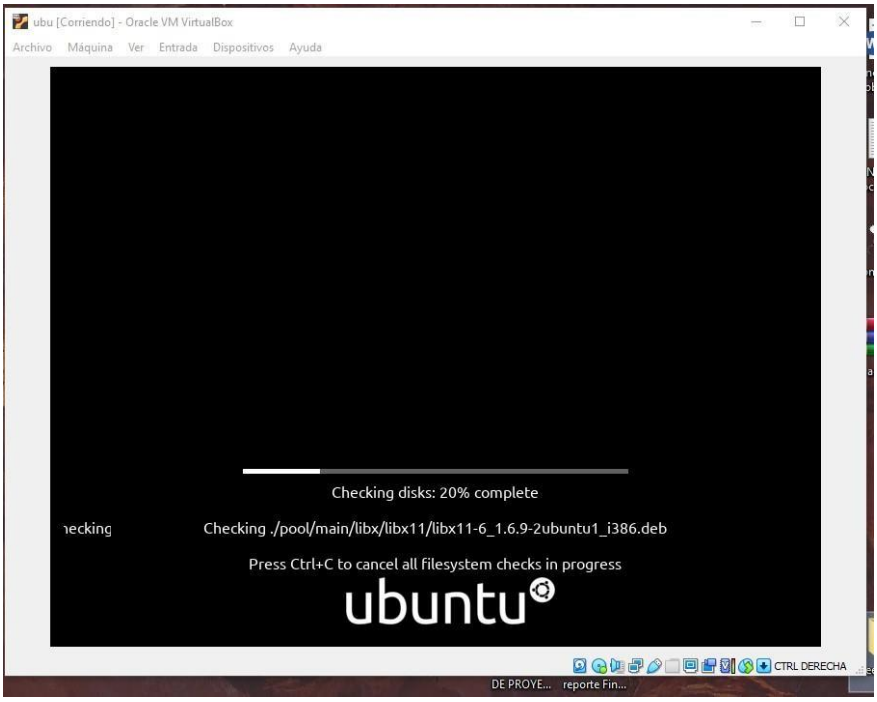

Ilustración 12 – Ventana Instalación Ubuntu

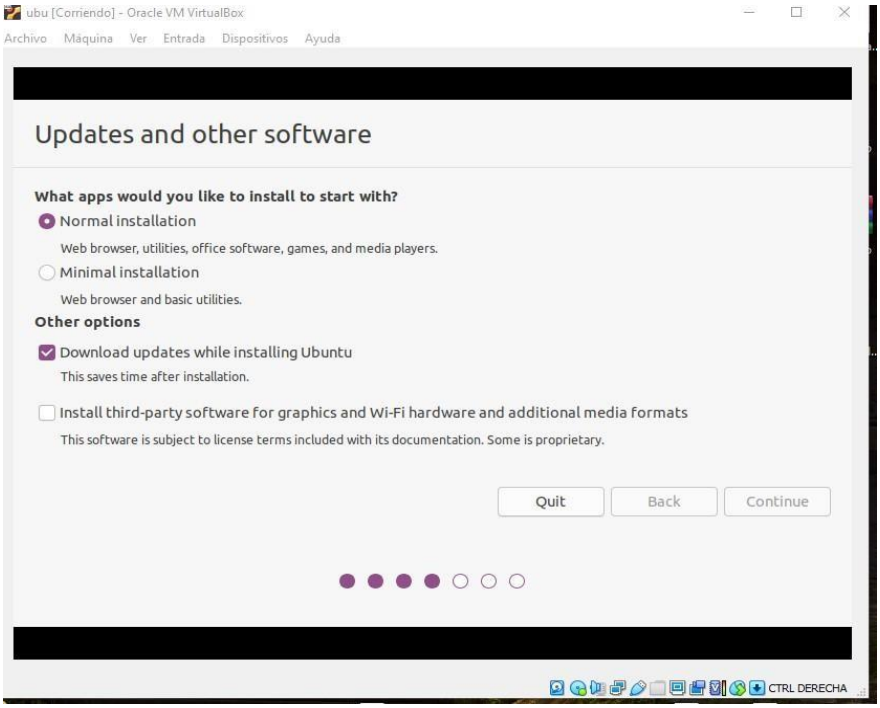

Ilustración 13 – Instalación de actualizaciones Ubuntu

Ilustración 14 – Ventana instalación Windows 7

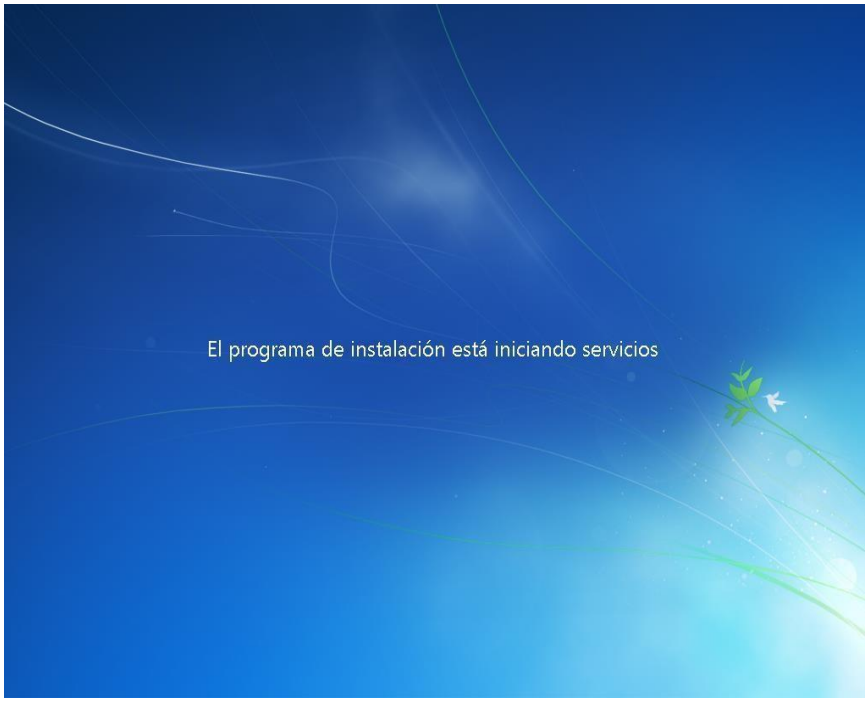

Ilustración 15 – Proceso de instalación Windows 7

Configuración de servicios de red y comunicaciones seguras

El primer paso para poder usar Kali es garantizar que tenga conectividad a una red cableada o inalámbrica para admitir actualizaciones y personalización. Primero, se confirma la dirección IP usando el comando ifconfig desde una ventana de terminal (Ilustración 16)

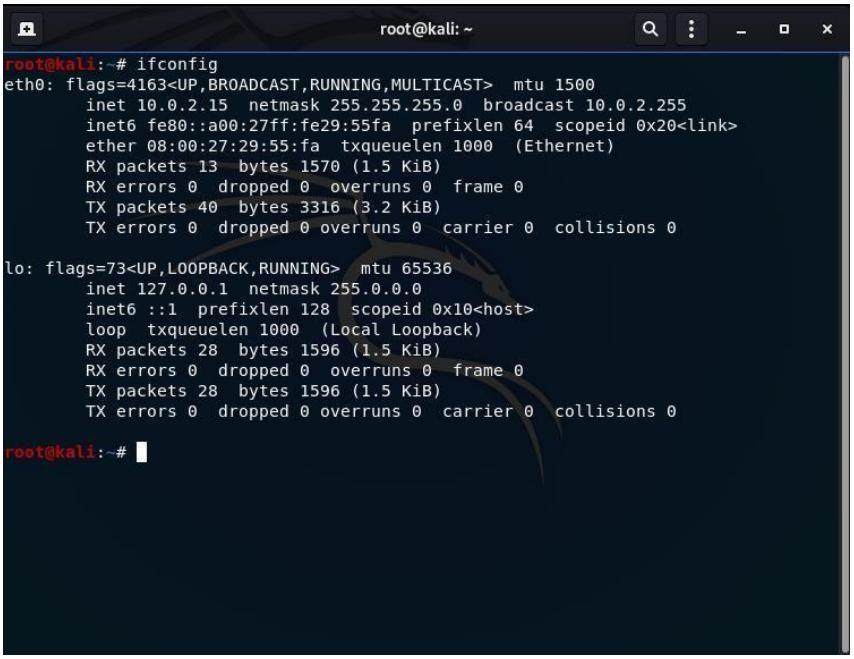

Ilustración 16 - Configuración Conectividad Kali

Si estamos conectados con una conexión proxy autenticada o no autenticada se debe modificar bash.bashrc y apt.conf. Ambos archivos se encuentran en el directorio / root / etc.

Usar el editor de texto para agregar las siguientes líneas al final del archivo bash.bashrc: export ftp_proxy = "ftp: //usuario: contraseña @ proxyIP: puerto" export http_proxy =" http: //usuario: contraseña @ proxyIP: puerto" export https_proxy =" https: //usuario: contraseña @ proxyIP: puerto" export socks_proxy =" https: //usuario: contraseña @ proxyIP: puerto"

Reemplazar proxyIP y puerto con su dirección IP proxy y número de puerto respectivamente, y reemplace el nombre de usuario y la contraseña con su nombre de usuario y contraseña de autenticación. Si no es necesario autenticarse, escriba solo la parte que sigue al símbolo @. (Ilustración 17)

Ejemplo: export ftp_proxy = "ftp:
//rabbits:123456@192.168.16.120:80” export ftp_proxy =
"ftp: // @192.168.16.120:80”

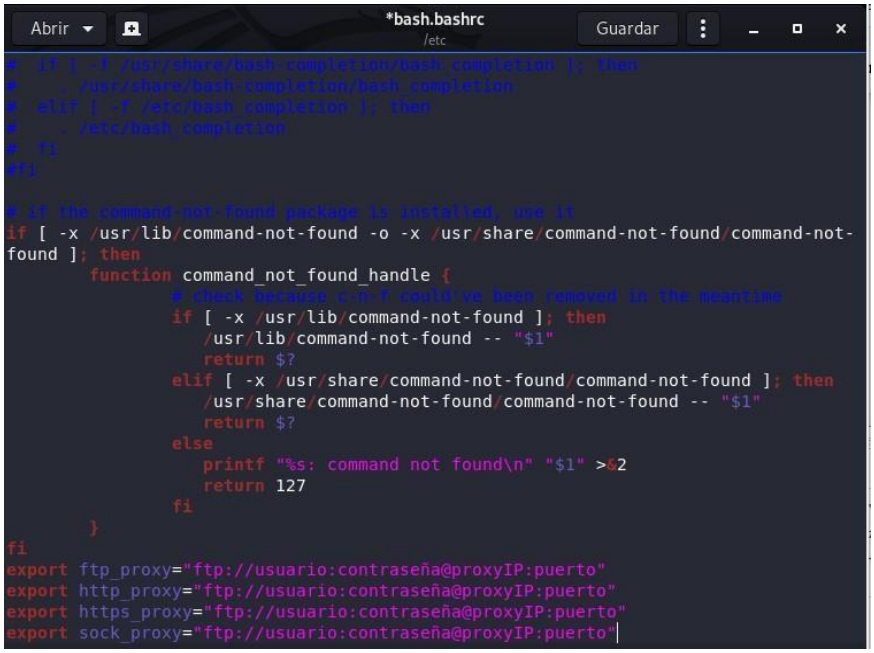

Ilustración 17 - Ingreso de proxy en bash.bashrc Kali

En el mismo directorio, se debe crear el archivo apt.conf e ingresar las siguientes líneas de comando

Acquire::ftp::proxy "ftp: //usuario: contraseña @ proxyIP: puerto”

Acquire::http::proxy " http: //usuario: contraseña @ proxyIP: puerto”

Acquire::https::proxy " https: //usuario: contraseña @ proxyIP: puerto”

Acquire::socks::proxy " https: //usuario: contraseña @ proxyIP: puerto”

PRUEBAS DE PENETRACIÓN IDENTIFICANDO A NUESTRO OBJETIVO

Prueba 1

Reconocimiento pasivo

Objetivo: Identificar a nuestro objetivo.

Herramienta: Terminal kali, comando who is

Ejecución:

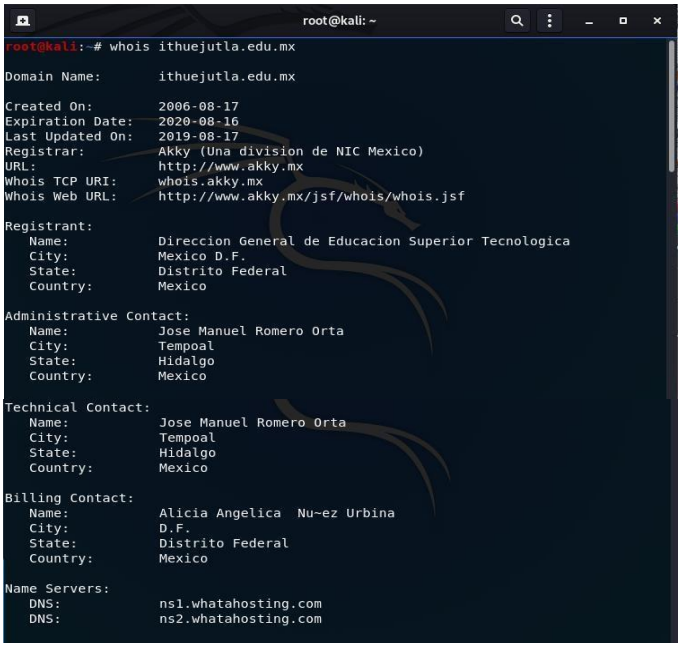

Ilustración 18 - Uso comando whois

Resultados:

Al hacer una consulta whois al dominio ithuejutla.edu.mx nos muestra la fecha en que fue creado el dominio, la fecha de expiración, datos de quien registro el dominio, datos de contacto administrativo, datos de contacto técnico y datos de la persona que realiza el pago del dominio, así también se puede observar los DNS los cuales son ns1.whatahosting.com y ns2.whatahosting.com

¿Cómo podemos usar la información de una consulta whois?

- En el caso en la fecha de expiración del dominio, se puede intentar apoderarse del dominio y crear un parecido sitio web para comprometer a los visitantes que piensan que están en el sitio web original.
- Se puede utilizar los servidores DNS autorizados, que son los registros para las búsquedas de ese dominio, para facilitar el reconocimiento de DNS.

Recomendaciones:

Al ser información pública, toda consulta realizada por el comando whois a cualquier dominio no puede ser registrada, y cualquier persona puede acceder a ella sin problemas, lo recomendable es configurar el servidor para exponer la menor cantidad de información pública posible.

En este caso se debe de hablar a soporte técnico del hosting para solicitar ocultar la información personal de las personas que operan el dominio.

Prueba 2

Reconocimiento pasivo - Reconocimiento IP

Objetivo: Reconocer la IP de nuestro dominio objetivo

Herramientas: Terminal Kali, comando nslookup

Ejecución:

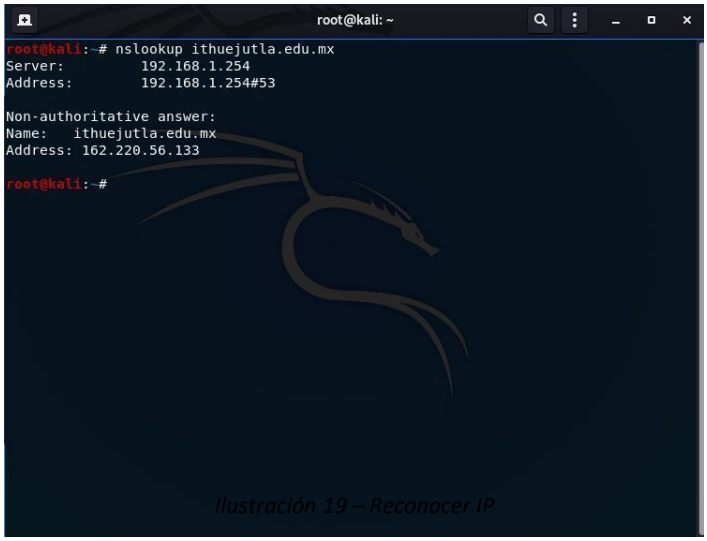

Ilustración 19 – Reconocer IP

Resultados:

Al consultar con el comando nslookup ithuejutla.edu.mx nos devuelve la información de nuestra puerta de enlace que en este caso es 192.168.1.254 así también podemos apreciar que la dirección IP de www.ithuejutla.edu.mx es 162.220.56.133 La información IP se puede usar para dirigir todos los ataques a ella.

Recomendaciones.

Es inevitable mostrar la IP de un dominio.

Usar VPN el cual retrasara el ataque para poder ser anticipado y tomar las respectivas medidas.

Prueba 3

Reconocimiento pasivo - Escaneo de DNS

Objetivo: obtener las direcciones de DNS

Herramientas: terminal kali, dnsrecon

Ejecución: dnsrecon –t std –d ithuejutla.edu.mx

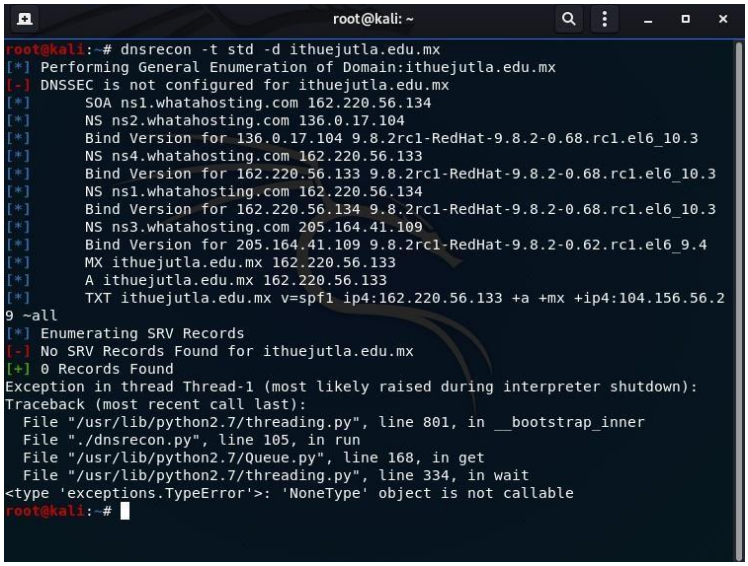

Ilustración 20 - Reconocimiento DNS

Resultados:

Al realizar el escaneo de tipo (-t) estándar (std) al dominio (-d) ithuejutla.edu.mx, por lo cual obtenemos el registro SOA el cual es el encargado de la transferencia de información entre servidores que en este caso es el 162.228.56.134 , los servidores de nombres NS: 136.0.17.104, 162.220.56.133-134 y los hosts del intercambiador de correo MX, 162.220.56.133, también nos damos cuenta que dichos servidores usan seguridad de enlace RedHat 9.8.2-0.62.rc1, por lo que nos hace suponer que el sistema base es RedHat.

¿Cómo puedo usar esta información?

Con esta información obtenemos la dirección de los servidores dns por lo que podríamos realizar ataques de fuerza bruta de subdominio, búsqueda de Google, búsqueda inversa, transferencia de zona y denegación de servicios.

Recomendaciones:

Como se mencionó en la prueba anterior es inevitable que se muestre la IP de nuestros servidores, lo que se podría realizar es enmascarar y ocultar las direcciones IP con un VPN.

Prueba 4

Reconocimiento activo - Mapeo de ruta

Objetivo: Mapear la ruta que toman los datos hasta llegar al dominio objetivo
Herramientas: terminal kali, hping3

Ejecución:

Por cuestiones legales esta prueba se realizara en el sitio *scanme.nmap.org*

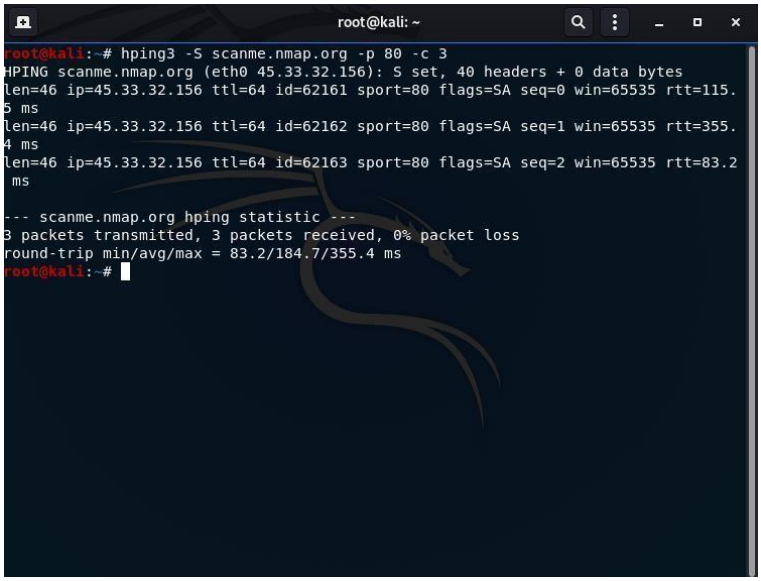

Ilustración 21 – Mapeo de Ruta

Resultados:

Debido a que la herramienta de diagnóstico nos mapea la red usando el tiempo de vida (**TTL**) en un paquete IP, cada salto desde un punto al siguiente genera un mensaje ICMP TIME_EXCEEDED del enrutador receptor. Los paquetes cuentan el número de saltos y la ruta tomada pero en esta prueba lo que se alcanza a ver es que un solo paquete fue enviado directo al dominio y recibido del mismo.

Recomendaciones:

Entre más saltos de un paquete hasta llegar al dominio es más difícil de reconocer el servidor final en donde se aloja el dominio. Para esto se ocuparían VPN. Si se requiere un poco más de seguridad para nuestro servidor lo que tendremos que hacer es colocar un VPN a dicho servidor el cual retrasara, mas no evitara ser encontrado por los atacantes, al realizar el escaneo queda expuesto el atacante; los firewall mandaran una alerta que se está tratando de escanear la red de la empresa.

Prueba 5

Reconocimiento activo - Escaneo de red

Objetivo: Mostrar los dispositivos conectados a la red para identificar al objetivo.

Herramientas: terminal kali, Nmap

Ejecución: nmap –sP 192.168.1.0/24

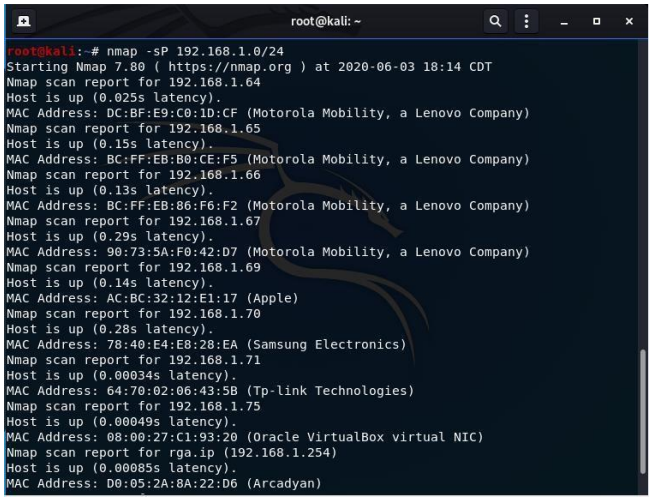

Ilustración 22 - Escaneo de Red, búsqueda de victima local

Resultados:

Al ejecutar el comando nos muestra cada uno de los dispositivos que están conectados a la red, podemos apreciar que la dirección 192.168.1.64 con dirección MAC DC:BF:E9:C0:1D:CF pertenece a un dispositivo Motorola, lo mismo con la dirección 192.168.1.165, 192.168.1.66, 192.168.1.67, un dispositivo Apple con dirección IP 192.168.1.67, un dispositivo Samsung, la máquina virtual VirtualBox y la máquina virtual victima con la que trabajaremos con dirección IP 192.168.1.75 Tp-link, por lo tanto nos muestra a todos los dispositivos que están en la red exceptuándonos a nosotros.

Recomendaciones:

Este tipo de escaneo solo se da si tienen acceso a la red, se recomienda ampliamente a reforzar la seguridad de su red inalámbrica. Ya que todo el que esté conectado a la red podrá realizar un escaneo.

Prueba 6

Reconocimiento activo - Escaneo de puertos e identificación de BD

Objetivo: Encontrar puertos abiertos e identificar BD

Herramientas: Terminal Kali,

Nmap

Ejecución: nmap –O 192.168.1.75

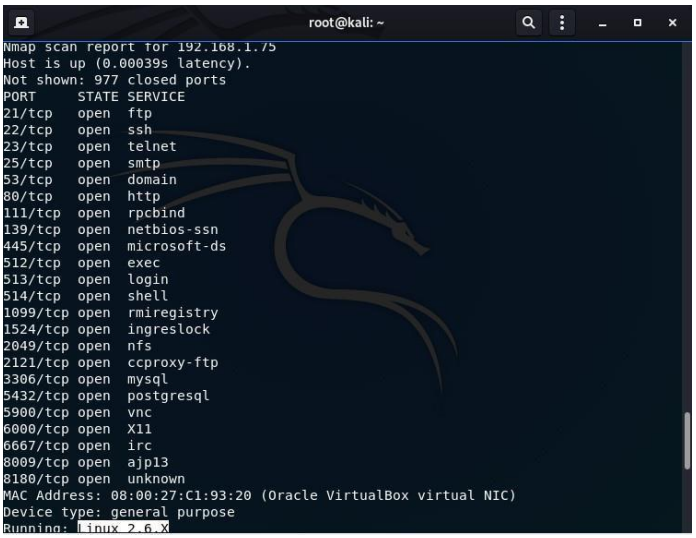

Ilustración 23 - Escaneo de puertos y SO

Resultados:

Tras haber ejecutado el comando anterior se aprecia que los puerto 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009 y 8180 están abiertos, se podría decir que son bastantes pero la mayoría de esos puertos están a la escucha para poder dar respuesta a los usuario que lo consultan, la búsqueda rindió frutos ya que podemos ver que nuestra victima tiene los puertos 3306 de MySQL y el puerto 5432 de PostgreSQL ambos abiertos.

Recomendaciones:

Al poner en línea un servidor ya sea local o en red por defecto vienen los puertos 3306 para MySQL o 5432 para PostgreSQL y al usar base de datos los puertos tendrán que estar abiertos. La recomendación es tener un firewall para evitar comprometer el equipo, usar puertos que no sean estándar y usar IDS (Sistema de detección de intrusos).

Prueba 7

Reconocimiento activo – Identificación de base de Datos

Objetivo: Identificar que GBD está ejecutando nuestro objetivo

Herramientas: Terminal kali, Nmap

Ejecución: nmap –sTV –Pn –n –p3306,5432 192.168.1.75

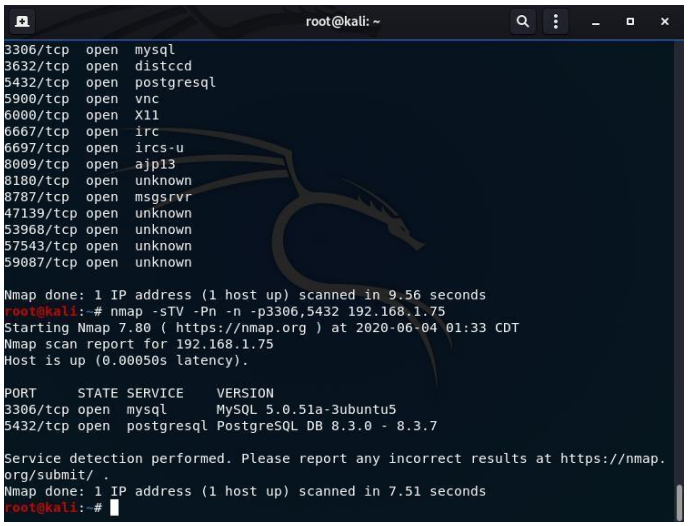

Ilustración 24 - Identificación de BD

Resultados:

En el puerto 3306 está a la escucha MySQL en su versión 5.0.51ª para Ubuntu, en el puerto 5432 está a la escucha PostgreSQL versión DB 8.3.0 - 8.3.7, de esta manera obtuvimos las versiones en ejecución de los GBD que se encuentran en la maquina objetivo.

Recomendaciones:

Tener un firewall para evitar comprometer el equipo, usar puertos que no sean estándar y usar IDS (Sistema de detección de intrusos).

Prueba 8

Reconocimiento activo – Identificación BD con Metasploit

Objetivo: Identificar que GBD está ejecutando nuestro objetivo

Herramientas: Terminal kali, Metasploit

Ejecución:

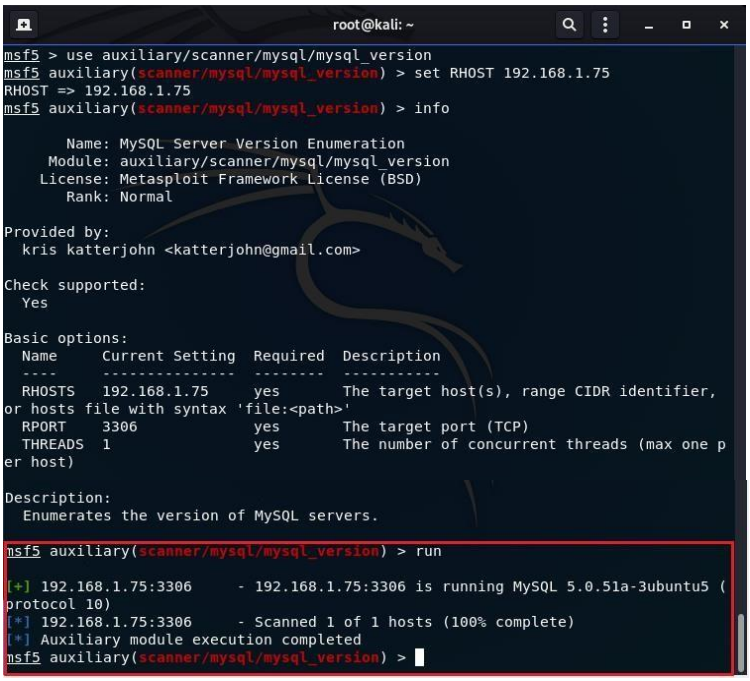

Ilustración 25 - Identificación de BD con Metasploit

Resultados:

Al usar un escáner auxiliar de Metasploit podemos ver el resultado, el cual es idéntico al de Nmap, el objetivo está ejecutando MySQL 5.0.51ª para Ubuntu.

Recomendaciones:

Tener un firewall para evitar comprometer el equipo, usar puertos que no sean estándar y usar IDS (Sistema de detección de intrusos).

Prueba 9

Ataque de Fuerza bruta a base de datos.

Objetivo: Poder obtener claves de acceso root a la base de datos del servidor objetivo

Herramientas: Terminal kali, python, mysqlbrute

Ejecución: python mysqlbrute.py –i 192.168.1.75 –u root – p/root/Desktop/pass.txt

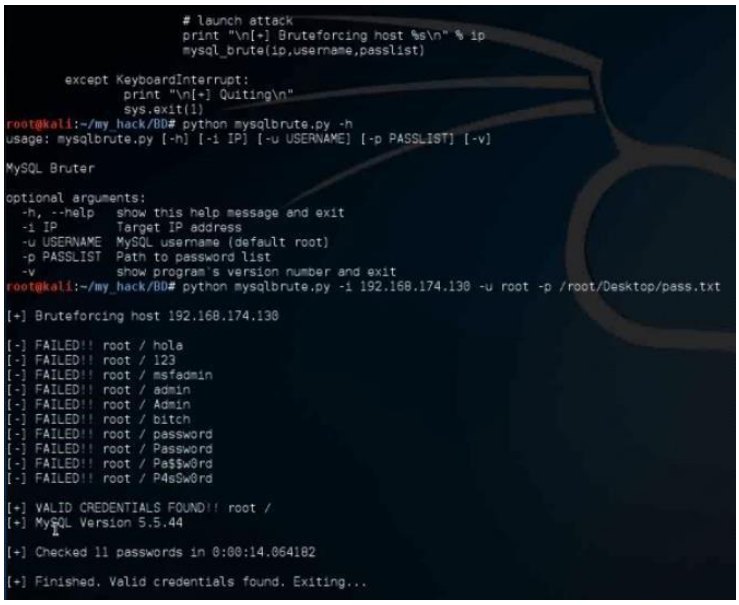

Ilustración 26 - Ataque de Fuerza Bruta a BD

Resultados:

En esta prueba lo que se hace es encontrar un Password para el usuario root, el script comprueba 1 a 1 las claves que contiene el archivo txt llamado pass hasta encontrar la clave correcta, y nos devuelve la siguiente línea de texto VALID CREDENTIALS FOUND: root/

El usuario y contraseña están divididos por la diagonal en este caso el usuario no tiene Password, es una base de datos a la cual no se le elimino el usuario root o se le puso una contraseña

Recomendaciones:

Si se decide poner en línea un servidor de base de datos, lo más adecuado es cambiar la contraseña de root, cambiar el nombre de usuario root, eliminar el usuario y crear uno el cual deberá tener permisos root.

Estos errores son comunes, por lo cual se debe de tener mucho cuidado.

Prueba 10

Explotando Base de datos

Objetivo: Entrar a la base de datos y eliminar tablas, modificar, crear, etc.

Herramientas: Terminal kali, MySQL.

Ejecución: mysql –h 192.168.1.75 –u root show databases;

use dvwa; show tables;

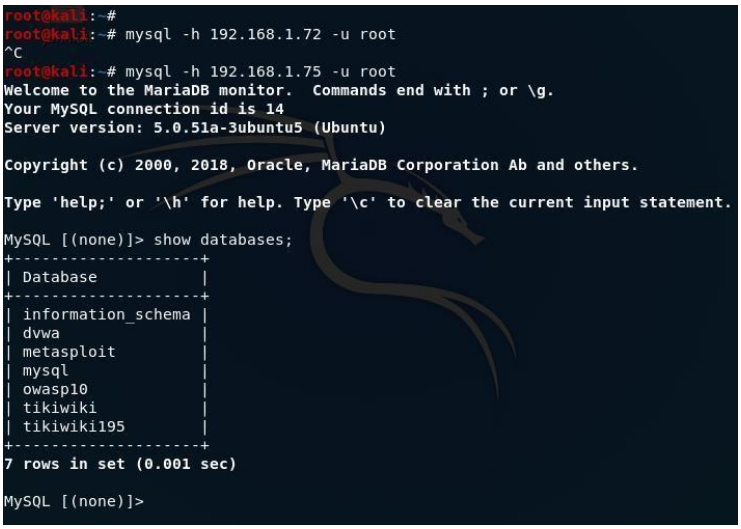

Ilustración 27 - Ingreso remoto a BD

select *from users;

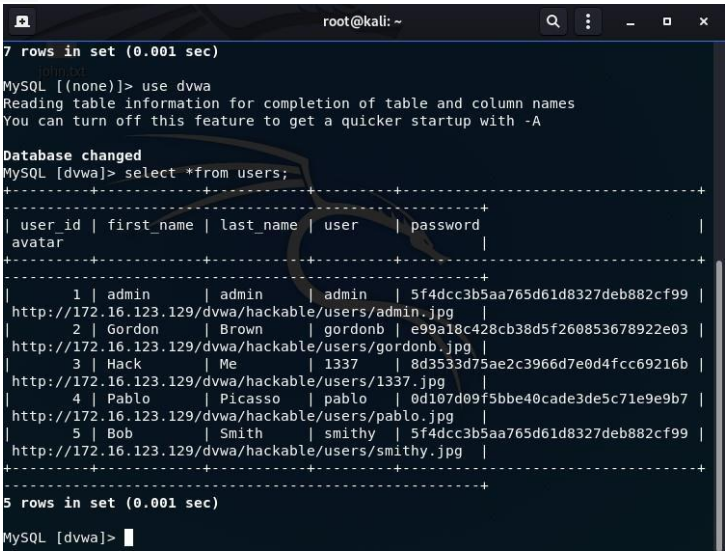

Ilustración 28 - Select a tabla usuarios de BD dvwa

Resultados:

Como se muestra en las imágenes tenemos conexión con las bases de datos, pedimos que nos muestre las bases de datos, seleccionamos una, pedimos que nos muestre las tablas y realizamos un select a la tabla usuario el cual nos muestra el id de usuario, nombre, apellido, usuario y las Password. A partir de aquí podemos realizar lo que queramos con las bases de datos si lo deseamos hasta podemos eliminarla para que nuestra victima pierda todos los datos.

Recomendaciones:

Se recomienda realizar una instalación y configuración correcta de los gestos, se recomienda ampliamente a modificar o eliminar a los usuarios predeterminados ya que por medios de estos se puede ingresar, se debe de tener una contraseña altamente fuerte combinada con caracteres, números, letras mayúsculas y minúsculas.

Prueba 11

Escaneo de Vulnerabilidades – Script auth

Objetivo: Identificar vulnerabilidades en la victima.

Herramientas: Terminal kali, Nmap, script auth.

Ejecución: nmap –f –sS –sV –script auth 192.168.1.75

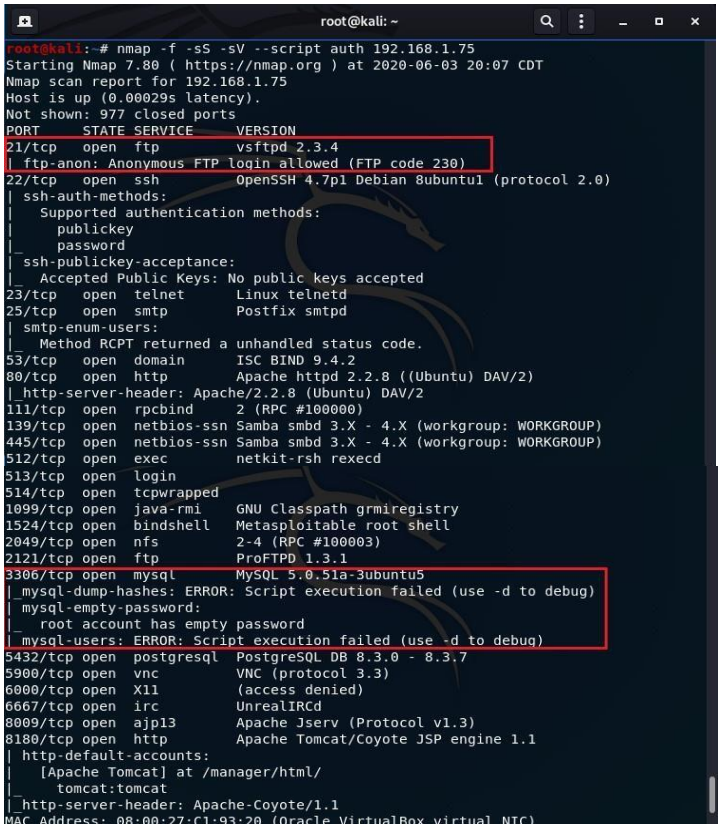

Ilustración 29 - Escaneo de vulnerabilidades de Autenticación

Resultados:

En este análisis se puede observar que el ingreso de usuarios anónimos está autorizado por el puerto 21, también podemos ver que la cuenta root de MySQL no tiene contraseña, este script nos permite realizar análisis de autenticación, el cual nos mostrara todas las vulnerabilidades por autenticación que tenga la víctima.

Recomendaciones:

Solo dejar abierto los puertos que en realidad se utilizan y cerrar los demás, nunca dejar sin contraseña o por defecto las contraseñas de los servidores y los GBD, realizar una configuración adecuada para evitar estos simples errores de usuario.

Prueba 12

Escaneo de vulnerabilidades – script default

Objetivo:

Herramientas: Terminal kali, Nmap, script default

Ejecución: nmap –f –sS –sV --script default 192.168.1.75

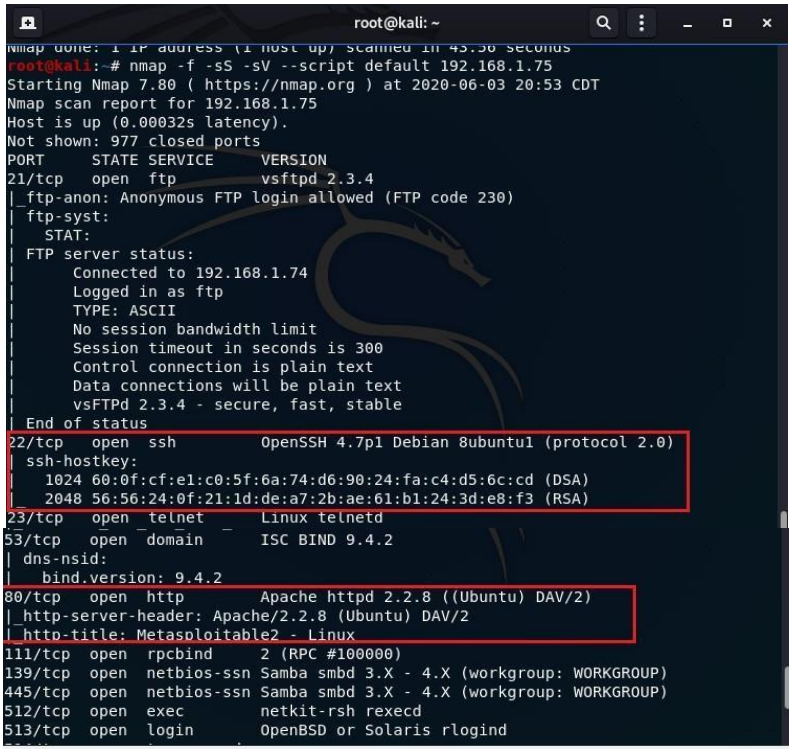

Ilustración 30 - Escaneo de vulnerabilidades script default

Resultados:

Al ejecutar los scripts por default podemos apreciar que el puerto 22 SSH nos arroja la información de la llave para la conexión ssh, esta llave nos permite el control remoto del servidor, en el puerto 80 nos muestra la información de la pc, nos indica que el SO es Ubuntu.

Recomendaciones:

Cerrar puertos que no se ocupen o que sean innecesarios, de esta forma el puerto 22 no permitirá conexiones remotas ni mucho menos mostrara la llave de conexión remota.

Prueba 13

Escaneo de vulnerabilidades – script vuln

Objetivo: Identificar todas las vulnerabilidades de la víctima

Herramientas: Terminal kali, Nmap, script vuln

Ejecución: nmap –f --script vuln 192.168.1.75

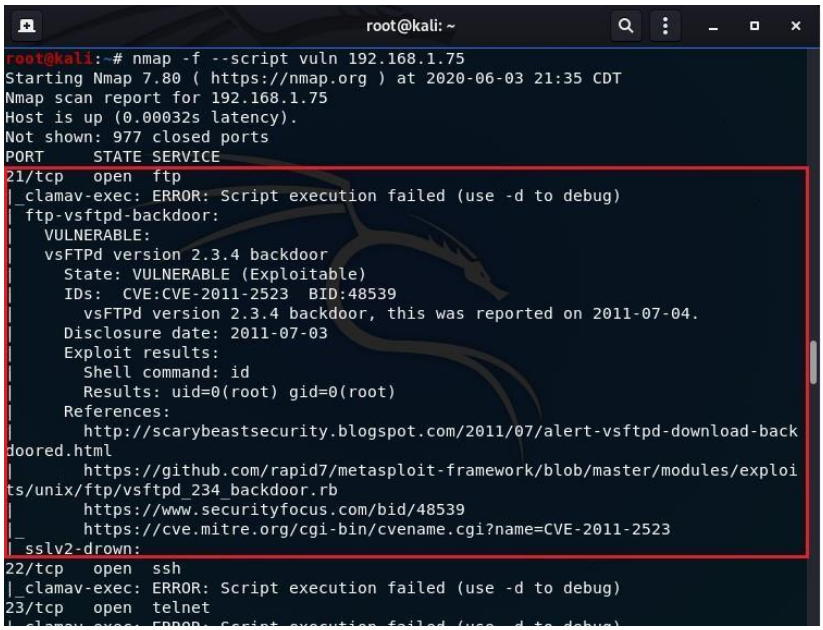

Ilustración 31 - Escaneo de vulnerabilidades script vuln - Backdoor en aplicación vsFTPd

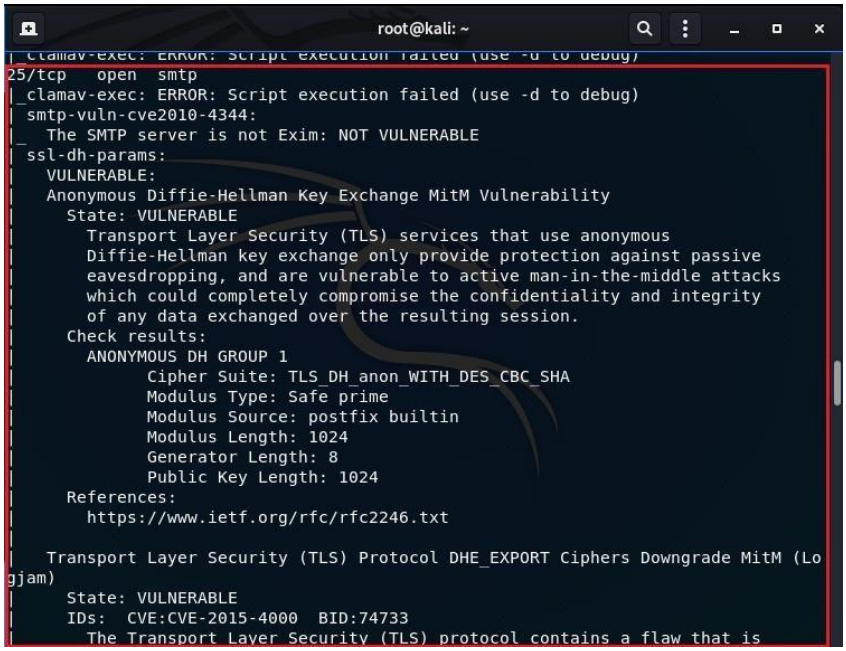

Ilustración 33 - Vulnerabilidad a MitM (Ataque de hombre de en medio) conexiones cifradas

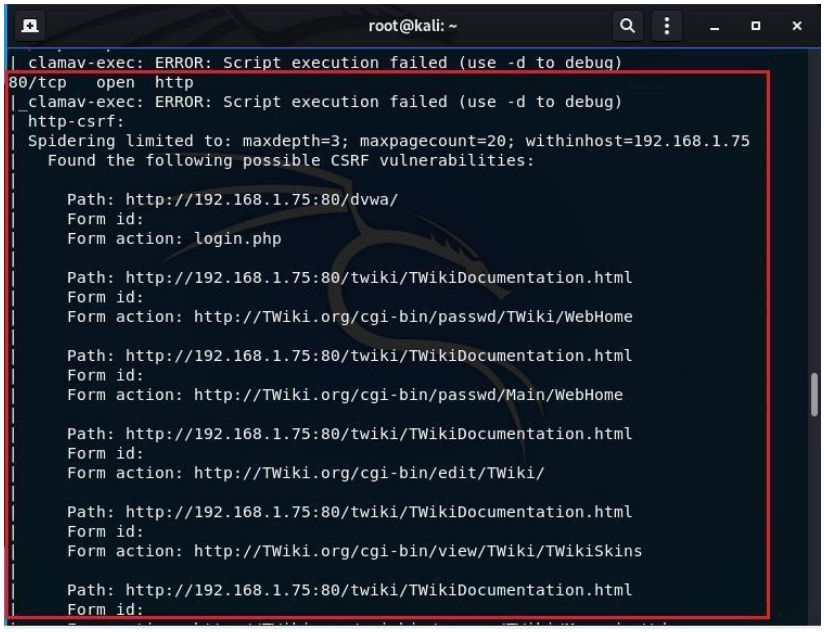

Ilustración 32 - Vulnerabilidad CSRF (falsificación de petición en sitios cruzados)

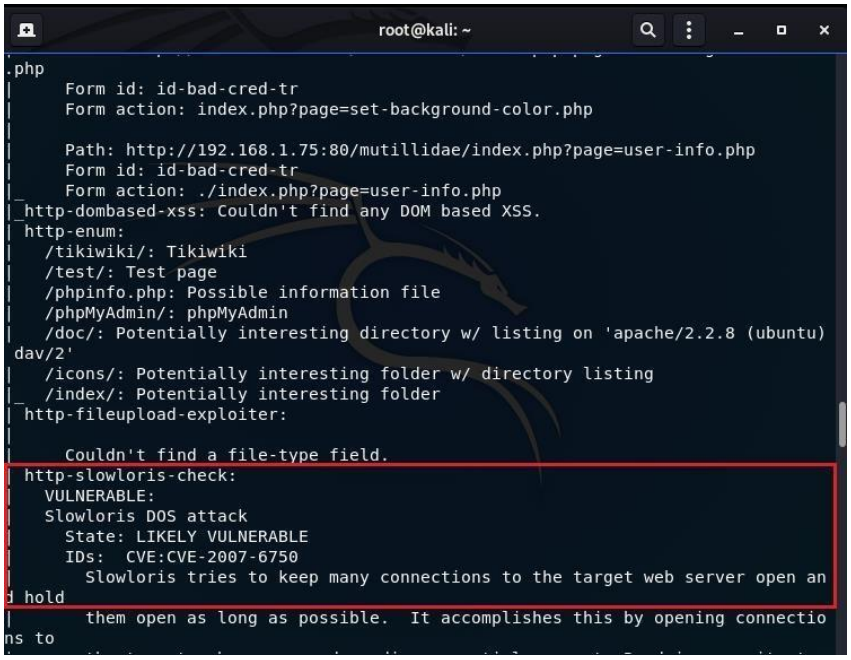

Ilustración 34 - Vulnerabilidad a ataques DDoS de slowloris

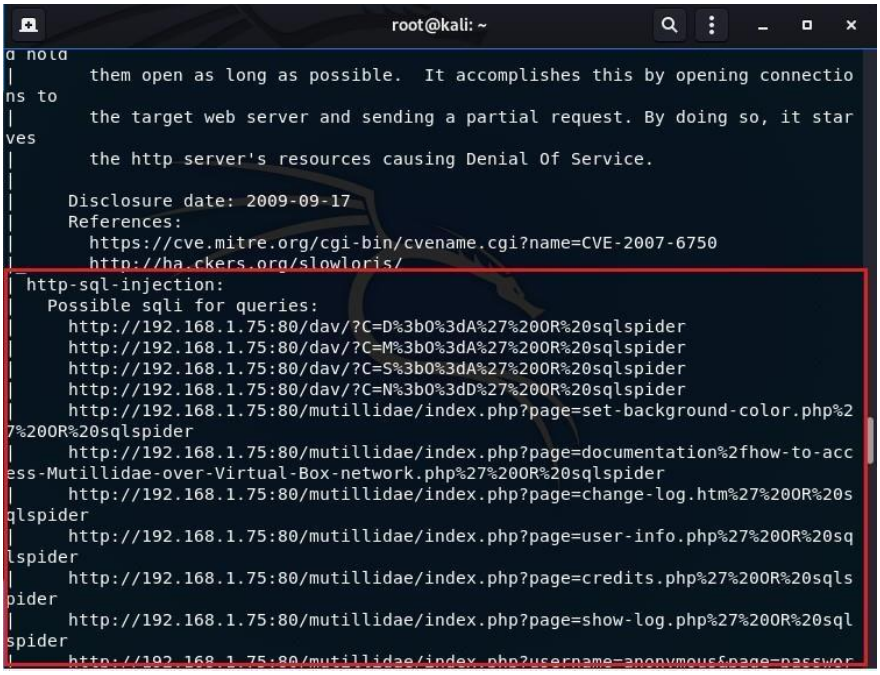

Ilustración 35 - Vulnerabilidad a ataques SQL Injection

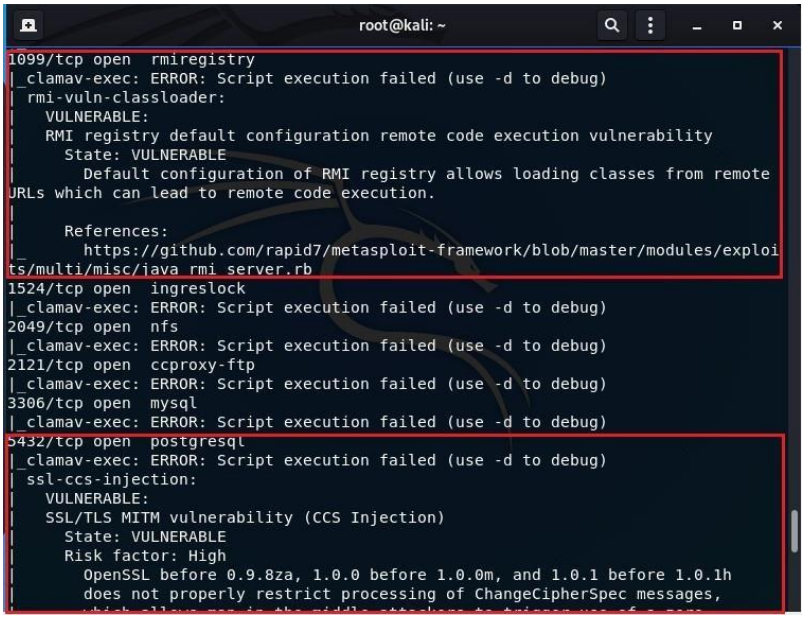

Ilustración 37 - Vulnerabilidad de carga clases desde URL remotas

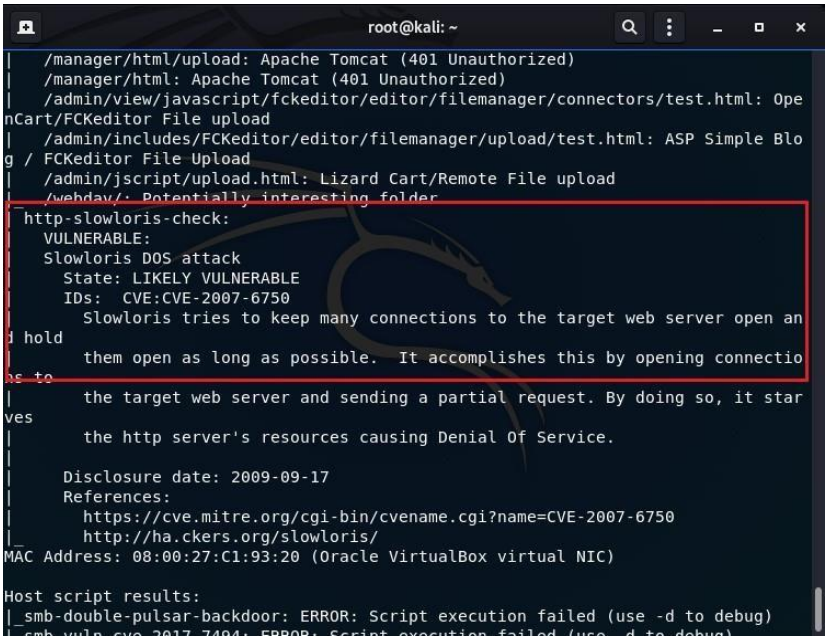

Ilustración 36 - Vulnerabilidad a ataque DDoS de slowloris

Resultados:

Al ejecutar el script de vulnerabilidades, nos muestra que en el puerto 21 tcp es vulnerable el vsFTPd (Servidor ftp para sistemas Unix) nos muestra que el tipo de vulnerabilidad es un Backdoor es cuál puede ser explotado (Ilustración 31), la siguiente vulnerabilidad que encontramos en el SO es en el puerto 25 Anonymous Deffie-Hellman(Protocolo criptográfico para comunicaciones) el cual es vulnerable al ataque MitM (Man in the Middle) (Ilustración 32), en el puerto 80 encontramos vulnerabilidad **CSRF** (Cross-site request forgery) falsificación de petición en sitios cruzados(Ilustración 33), puerto 80 encontramos que es vulnerable a ataques DDoS (Ilustración 34), puerto 80 posible vulnerabilidad a inyección SQL (Ilustración 35), puerto 1099 la configuración predeterminada del registro RMI(Java Remote Method Invocation) permite cargar clases desde URL remotas que pueden conducir a la ejecución remota de código (Ilustración 36), puerto 5432 OpenSSL vulnerable a inyección CSS por medio de MitM (Ilustración 36), puerto 8180 vulnerabilidad a ataque DDoS (Ilustración 37).

Recomendaciones:

La mayoría de todas las vulnerabilidades encontradas, son debido a la falta de actualización de los programas que se utilizan, errores del propio sistema operativo e incluso errores básicos de usuario.

Se recomienda actualizar los programas utilizados diariamente, actualizar el sistema operativo a la versión más actual, colocar un firewall, un IDS, cambiar contraseñas predeterminada, cambiar usuarios predeterminados, crear nuevos usuarios, usar contraseña complejas, si es posible utilizar un generador de contraseñas y cambiarla cada mes.

CONCLUSIÓN

Los resultados sobrepasaron las expectativas, debido a que hay demasiada información acerca del Pentesting no se pudieron realizar todas las pruebas que se tenían pensadas, aun así la información obtenida mediante las pruebas nos hace ver que todo sistema o programa es propenso a tener fallas, y así también como administradores podemos realizar malas prácticas y dejar un hueco de seguridad por error.

Tanto las bases de datos de Linux como Windows son propensas a ser comprometidas de la misma manera que explicamos en este proyecto.

Se debe de tomar en cuenta que antes de realizar las pruebas se debió de configurar nuestro entorno de trabajo.

Se logró cumplir el objetivo que era comprometer una base de datos en cualquier sistema operativo.

TABLA DE PRUEBAS

PRUEBA	SO	RESULTADO
Reconocimiento Pasivo (Recopilación de información personal)	RedHat	Error de Usuario (Mala Configuración)
Reconocimiento Pasivo (Recopilación de información personal)	Ubuntu	Error de Usuario (Mala Configuración)
Reconocimiento Pasivo (Recopilación de información personal)	Windows 7	Error de Usuario (Mala Configuración)
Reconocimiento Pasivo (Reconocimiento de IP)	RedHat	Carencia de VPN
Reconocimiento Pasivo (Reconocimiento de IP)	Ubuntu	Carencia de VPN
Reconocimiento Pasivo (Reconocimiento de IP)	Windows 7	Carencia de VPN
Reconocimiento Pasivo (Escaneo de DNS)	RedHat	DNS(Protocolo no cifrado)
Reconocimiento Pasivo (Escaneo de DNS)	Ubuntu	DNS(Protocolo no cifrado)
Reconocimiento Pasivo (Escaneo de DNS)	Windows 7	DNS(Protocolo no cifrado)
Reconocimiento Activo (Mapeo de Ruta)	RedHat	No se Realizo
Reconocimiento Activo (Mapeo de Ruta)	Ubuntu	No se generó ninguna ruta
Reconocimiento Activo (Mapeo de Ruta)	Windows 7	No se generó ninguna ruta

Reconocimiento Activo (Escaneo de Red)	RED	Se Mostraron todos los dispositivos conectados y la IP de cada uno
Reconocimiento Activo (Escaneo de puertos e Identificación de SO)	Jbuntu	Puertos Abiertos, Sistema Operativo Identificado
Reconocimiento Activo (Escaneo de puertos e Identificación de SO)	Windows 7	Puertos Abiertos, Sistema Operativo Identificado
Reconocimiento Activo (Identificación de BD)	Jbuntu	Gestor de BD identificado MySQL 5.0.5
Reconocimiento Activo (Identificación de BD)	Windows 7	Gestor de BD identificado MySQL 5.0.5
Reconocimiento Activo (Identificación de BD Metasploit)	Jbuntu	Gestor de BD identificado MySQL 5.0.51a
Reconocimiento Activo (Identificación de BD Metasploit)	Windows 7	Gestor de BD identificado MySQL 5.0.51ª
Ataque fuerza bruta	Jbuntu	Error de administrado Usuario redeterminado, claves encontradas
Ataque fuerza bruta	Windows 7	Error de administrado Usuario redeterminado, claves encontradas

Explotación de BD	Jbuntu	Acceso a todas las BD control total.
Explotación de BD	Windows 7	Acceso a todas las BD control total.
Escaneo de Vulnerabilidades script auth	Jbuntu	Ingreso anónimo al sistema puerto 21.
Escaneo de Vulnerabilidades script auth	Windows 7	Gestor BD (Usuario root no tiene contraseña).
Escaneo de Vulnerabilidades script default	Jbuntu	Puerto 22 llave de conexión ssh encontrada.
Escaneo de Vulnerabilidades script default	Windows 7	No se encontró información.
Escaneo de Vulnerabilidades script vuln	Jbuntu	Vulnerabilidades en: puerto 21, 25,80, 1099 y 5432.
Escaneo de Vulnerabilidades script vuln	Windows 7	Vulnerabilidad en: puerto 21 25, y múltiples vulnerabilidades puerto 80.

RECOMENDACIONES GENERALES

Control de acceso a la información sensible: Desarrolladores de aplicaciones web no deben colocar información predecible o sensible en cualquier página web de acceso libre, dentro de un registro de Internet.

Establecer fuertes controles sobre la entrada: La regla más importante es nunca confiar en las transmisiones de datos entre el browser, el servidor web y los dispositivos de red. Siempre debe existir validación y revalidación en los controles de entrada.

Establecer pruebas de vulnerabilidad en el ciclo de vida del desarrollo de sistemas: La mayoría de las empresas de auditoría y consultoría de Tecnologías de la Información proveen económicas pruebas para testear la vulnerabilidad. Estas pruebas permiten identificar debilidades en seguridad que pueden permitir el acceso a intrusos a la aplicación web y a las bases de datos. La incapacidad de identificar las vulnerabilidades en la Web a través de un testing estandarizado puede generar un impacto significativo en el proceso de solicitud del cliente.

Por lo regular se suelen testear las funcionalidades de un sitio, sin observar la seguridad. Además, existen software automatizado que monitorean continuamente el Uptime de un sitio web y todas sus páginas, sin detectar el Hackeo. Una vez más y posiblemente en todo el mundo, la detección de intromisiones en los sitios web raramente atrae la atención de los especialistas en seguridad para protegerlos de los infractores.

El sistema operativo que se recomienda es cualquier distribución Linux siempre y cuando se actualice constantemente, esto debido a su robustez, todos los programas que se usaran en el servidor se deberán actualizar igualmente; los puertos que no se utilicen se deben de cerrar y abrir los que si se utilizan.

Usar VPN para poder camuflar su IP, IDS para detectar intrusos, Firewall para detectar y bloquear cualquier actividad sospechosa. No poner información de carácter confidencial en la información pública.

COMPETENCIAS DESARROLLADAS

Durante la realización del proyecto se utilizaron y desarrollaron las siguientes competencias:

- Planificación
- Comunicación
- Compromiso
- Liderazgo
- Adaptabilidad
- Análisis de problemas
- Autoconocimiento
- Autoconfianza
- Trabajo en equipo
- Pro actividad
- Autocrítica
- Gestión del tiempo

FUENTES DE INFORMACIÓN

Fuentes Electrónicas

- Olaya, V. (2020). *Sistemas de Información Geográfica*. Volaya.github.io. Consultado el 8 de Marzo de 2020, de http://volaya.github.io/librosig/chapters/Bases_datos.html.
- *¿Qué es un servidor?* Onyxsystems.es. (2020). Consultado el 15 de Marzo 2020, de http://www.onyxsystems.es/que-es-un-servidor.html.
- *Sistema operativo - EcuRed*. Ecured.cu. (2020). Consultado el 17 de Marzo 2020, de https://www.ecured.cu/Sistema_operativo.
- *Qué es el Pentesting*. OpenWebinars.net. (2020). Consultado el 18 de Marzo 2020, de https://openwebinars.net/blog/que-es-el-pentesting/.
- la Red Martínez, M. (2020). Sistop.gwolf.org. Consultado el 7 de Abril 2020, de http://sistop.gwolf.org/html/biblio/Sistemas_Operativos__Luis_La_Red_Martinez.pdf.
- *Arquitectura del Sistema Operativo*. Users.dcc.uchile.cl. (1999). Consultado 18 Abril 2020, de https://users.dcc.uchile.cl/~jpiquer/Docencia/SO/aps/node16.html.
- *¿Qué es un sistema operativo?* | *Desarrollar Inclusión*. Desarrollar Inclusión | Portal de tecnología inclusiva de CILSA. (2020). Consultado 18 Abril 2020, de https://desarrollarinclusion.cilsa.org/tecnologia-inclusiva/que-esunsistema-operativo/.
- *SGBD - EcuRed*. Ecured.cu. (2020). Consultado 18 Junio 2020, de https://www.ecured.cu/SGBD.

- *INTRODUCCIÓN — Gestión de Bases de Datos*. (2020). Consultado 18 Abril 2020, de https://gestionbasesdatos.readthedocs.io/es/latest/Tema1/Teoria.html.
- *¿Qué es un servidor?* Onyxsystems.es. (2020). Consultado 15 Marzo 2020, de http://www.onyxsystems.es/que-es-un-servidor.html.
- Academy, B. (2020). *BacktrackAcademy: Sqlmap Parte 1: Automatizando Inyección SQL*. Backtrack Academy. Consultado el 6 de Mayo de 2020, de https://backtrackacademy.com/articulo/sqlmap-parte-1automatizandoinyeccion-sql.
- *es:aircrack-ng [Aircrack-ng]*. Aircrack-ng.org. (2019). Consultado el 8 de Mayo de 2020, de https://www.aircrackng.org/~~V:/doku.php?id=es:aircrack-ng.
- *John the Ripper*. Es.wikipedia.org. (2020). Consultado el 20 de Mayo de 2020, de https://es.wikipedia.org/wiki/John_the_Ripper.
- *Las mejores 20 herramientas de hacking y penetración para Kali Linux*. Linux en español. (2020). Consultado el 24 de Mayo de 2020, de https://www.xnlinuxenespaol-skb.com/noticias/mejores-20-herramientashackingpenetracion-kali-linux/.
- Marqués, J. (2020). *¿Escáner de vulnerabilidades en sistemas operativos en red?; necesitas NESSUS | Javier Marqués, Grupo INVACI. Profesor Técnico de FP. Ingeniero Telemático*. Javiermarques.es. Consultado el 24 de Mayo de 2020, de https://javiermarques.es/nessus.
- *Nmap: the Network Mapper - Free Security Scanner*. Nmap.org. (2020). . Consultado el 25 de Mayo de 2020, de https://nmap.org/.
- Relancio, A. (2013). Wireshark, un gran analizador de protocolos. Consultado el 11 de Mayo de 2020, de https://www.seas.es/blog/informatica/wiresharkun-gran-analizador-deprotocolos/.

Fuentes Bibliográficas

- Bertino, E., & Martino, L. (1995). *Sistemas de bases de datos orientadas a objetos*. Addison-Wesley/Díaz de Santos.
- Cesar H. Tarazona T.. (2007). Derecho Penal y Criminología. Revista del Instituto de Ciencias Penales y Criminológicas, 28, 146.
- Silberschatz, A., Galvin, P., & Gagne, G. (2007). *Sistemas operativos* (7th ed.). Limusa Wiley.
- Stallings, W. (2005). *Sistemas operativos* (5th ed.). Pearson Educación.
- Camps Paré, R., Casillas Santillán, L., Costal Costa, D., Gibert Ginestà, M., Martín Escofet, C., & Pérez Mora, O. (2007). *Bases de datos: Software libre* (2nd ed.). Barcelona (España) : Fundació per a la Universitat Oberta de Catalunya, 2007.
- Muños Mogrobejo, B. (2012). *taller auditoria y pentest 2012*. Manual.

GLOSARIO

OSINT: son datos recogidos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia

Doxing: Practica en la cual se adquieren datos personales por medio de Ingeniería social o búsquedas en bases de datos de acceso público y redes sociales, tales como Facebook o Twitter.

DomainKeys Identified Mail (DKIM): es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario.

Sender Policy Framework (SPF): es una protección contra la falsificación de direcciones en el envío de correo electrónico. Identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes.

ANEXO XXXIII. FORMATO DE LIBERACION DE PROYECTO PARA LA TITULACION INTEGRAL

Lugar y Fecha: **06 de Noviembre de 2020**

Asunto: Liberación de Proyecto para la titulación integral

C. **Ing. Blanca Arguelles Arguelles**
Jefe(a) de la División de Estudios Profesionales
PRESENTE

Por este medio informo que ha sido liberado el siguiente proyecto para la titulación integral:

Nombre del estudiante y/o egresado	Christopher Romero Hernández Everardo Salinas Salvador
Carrera:	Ingeniería en Sistemas Computacionales
No. de control:	16840432 16840010
Nombre del proyecto:	Pentesting a base de datos en sistemas operativos de gratuita de paga.
Producto	Tesis

El Vocal Suplente para la presentación del Acto de recepción profesional será:

Vocal Suplente:	M. en C. José Manuel Romero Orta.

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados.

ATENTAMENTE

S.E.P.
TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE HUEJUTLA
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

M.T.I. JACOBO ANTONIO CRUZ
Nombre y firma del (de la) Jefe (a)
De Departamento Académico de: **Sistemas y Computación**

M. en C. Leodegario Redondo Martínez	M. en C. Juan de Viniegra Vargas.	Ing. Jesús Hernández Aguilera
Nombre y firma del asesor	Nombre y firma del revisor*	Nombre y firma del revisor*

*Solo aplica para el caso de tesis o tesina

c.c.p.- Expediente.