ESTUDIO DE SEGURIDAD INFORMÁTICA PARA LAS BASES DE DATOS DEL CAMPUS VIRTUAL DE LA UNAD.

CARLOS JAVIER URIBE OTÁLORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA.
BUCARAMANGA
2016

ESTUDIO DE SEGURIDAD INFORMÁTICA PARA LAS BASES DE DATOS DEL CAMPUS VIRTUAL DE LA UNAD.

CARLOS JAVIER URIBE OTÁLORA

Proyecto de grado presentado como requisito para optar al título de Especialista en Seguridad Informática

Asesor
JOHN FREDDY QUINTERO TAMAYO
M.Sc. Seguridad Informática.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA.
BUCARAMANGA
2016

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Bucaramanga, Septiembre 2016.

DEDICATORIA

A Dios por darme cada día fortaleza, salud y sabiduría para luchar día a día; A mis padres por su apoyo; A mis hermanos Víctor y Patricia por todo su apoyo y palabras de ánimo; A mis tutores y Director de proyecto por sus orientaciones.

C. Javier

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Dios, porque gracias a él se logró esta nuevo peldaño en mi vida profesional.

A mis padres y hermanos, por el apoyo moral que me brindaron de una manera desinteresada.

A los tutores y docentes de la Universidad Nacional Abierta y a Distancia – UNAD, a quienes debo los conocimientos y la formación como profesional.

A John Freddy Quintero Tamayo, Msc Seguridad Informática y Director del proyecto, por su disposición para hacer de este proyecto una meta alcanzada.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Título: Estudio de seguridad informática para las bases de datos del campus virtual de la UNAD.

Autor: Carlos Javier Uribe Otálora

Palabras Claves: Bases de Datos, Redes Informáticas, Vulnerabilidades, Seguridad Informática, MySQL, OpenSSH, Kali Linux, Nessus, Zenmap, Nmap, SQL Map.

Línea De Investigación: Administración y Seguridad en Redes.

Descripción:
Actualmente el mundo informático se mueve entre un creciente escenario de anomalías electrónicas, unas regulaciones débiles, unas tecnologías de protección cada vez más limitadas, y una mayor dependencia de la tecnología dentro de la forma de hacer negocios.

En el caso latinoamericano, se debe agregar la falta de presupuesto asignado a la seguridad de la información, esto hace que los encargados de ella tengan que buscar estrategias poco confiables o simplemente la limiten al mínimo aceptable (Antivirus – Firewalls), lo que incrementa la vulnerabilidad y los riesgos de ataques.

En el caso particular de la UNAD, su campus virtual se convierte en espacio vital de la interacción de sus 70 mil estudiantes, ya que a través de éste se desarrollan cursos, se actualiza información personal, se envían actividades, se comunican con tutores y compañeros, además de presentar evaluaciones y consultar notas. Este entorno ha hecho que su plataforma tecnológica haya comenzado a ser blanco de ataques informáticos como el robo de identidad y algunas caídas sospechosas del sistema.

La problemática descrita anteriormente, permitió la formulación de un estudió de seguridad informática para las bases de datos del campus virtual de la UNAD, con el fin de evaluar las vulnerabilidades que existen en el acceso directo a su SGBD, y a los medios usados para acceder a él, buscando formular estrategias y políticas que ayuden a reducir las amenazas.

El estudio se desarrolló usando la metodología de análisis de vulnerabilidad, usando como herramientas de ataques programas de software libre como: Kit de Seguridad de Kali Linux, Nessus, Nmap, SQL Map, entre otras. También de detallan entrevistas con expertos en campus virtuales y seguridad en redes, quienes aportaron ideas para evaluar la seguridad del campus..

Los resultados finales del estudio demostraron que el nivel de seguridad del acceso al SGBD usado por el campus virtual y sus redes de acceso, se puede catalogar como bueno. Sin embargo se dejan plasmadas unas recomendaciones basadas en lo encontrado en el estudio.

ABSTRACT

Title: Study on information security for the databases of the virtual campus at UNAD

Author: Carlos Javier Uribe Otálora

Keywords: Databases, informatic networks, vulnerability, information security, MySQL, OpenSSH, Kali Linux, Nessus, Zenmap, Nmap, SQL Map.

Research lines: Administration and network security

Description:
Currently computing world moves among a growing scene of electronic anomalies, weak regulations, more limited protective technologies, and a greater dependence on technology when doing business.

Besides the above, it is necessary to mention the lack of money allocated to information security in Latin America. All of these situations have force the information security commissioned to look for strategies that are not very reliable or to implement a minimum security (firewalls, antivirus) which increases vulnerability and cyber-attacks.

At UNAD particularly, its virtual campus is a very important setting for the interaction of its 70.000 students because they do all the activities of their courses, update their personal information, activities are submitted, interact with their tutors and peers, take quizzes and review grades. This situation has propitiate attacks on its technological platform like identity theft and suspicious system problems.

The problems describe above were the reasons why a study on information security for the virtual campus databases at UNAD was proposed, in order to evaluate the vulnerabilities in its SGBD shortcut, the media used to enter in it, so that, some strategies and policies to decrease attacks can be designed.

This study was developed using the ethodology of vulnerability analysis, implementing some free software programs like Kali Linux, Nessus, Nmap, SQL map as preventing tools. There are also some interviews with some experts in virtual campuses and network security, who helped with some ideas to evaluate the virtual campus security system.

The final results of the study showed that the level of security of the access to the SGBD used by the virtual campus and its access networks are good and acceptable. Nevertheless there are some useful recommendations based on the findings of the study.

INTRODUCCIÓN

Actualmente la información que se maneja en una compañía de cualquier tipo, es fundamental, pues ésta es sinónimo de poder; poder para controlar los negocios, las tácticas y el mercado de sus productos y/o servicios, por tanto es lo que más preocupa a las organizaciones hoy en día.

La viabilidad de los negocios de una organización basados en sistemas de información no está determinada por las cualidades de la tecnología usada, porque el desarrollo de ésta conlleva un nuevo campo de acción a conductas delictivas, otorgando facilidades para cometer delitos tradicionales en formas inusuales, atentando contra la confidencialidad, disponibilidad y seguridad de la infraestructura y de los datos. Por tanto, se ocasiona un aumento del grado de vulnerabilidad e incertidumbre sobre la eficacia de los sistemas que guardan y protegen la información, lo cual ha ocasionado que la seguridad informática se convierta en una prioridad para cualquier empresa.

En este orden de ideas, este trabajo documenta a través de cinco capítulos, un análisis de vulnerabilidades, realizado a las bases de datos de la plataforma tecnológica de la UNAD, con el fin de identificar brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la institución. El estudio busca reducir la efectividad de los ataques que pueden aprovechar las mismas. De igual manera entrega un conjunto de recomendaciones que permitan mitigar los riesgos a los que se encuentra expuesta la institución en el campo de las bases de datos de la plataforma.

1. DESCRIPCION DEL PROYECTO

Este capítulo tiene por objetivo presentar el título del proyecto, el planteamiento del problema y el equipo de trabajo conformado para garantizar la ejecución del mismo.

1.1 TÍTULO

Teniendo en cuenta la temática tratada y los lineamientos de investigación establecidos por la UNAD en su documento "Investigación en la Escuela de Ciencias Básicas, Tecnología e Ingeniería", el título establecido para el trabajo es: ESTUDIO DE SEGURIDAD INFORMÁTICA PARA LAS BASES DE DATOS DEL CAMPUS VIRTUAL DE LA UNAD.

1.2 PLANTEAMIENTO DEL PROBLEMA

Según un artículo publicado por ACIS[1] en el 2013 y elaborado por el experto en seguridad informática Andrés Almanza[2], "Un creciente escenario de anomalías electrónicas, unas regulaciones vigentes, unas tecnologías de protección cada vez más limitadas, y una mayor dependencia de la tecnología dentro de la forma de hacer negocios, muestra cómo la necesidad de proteger la información es más relevante. Bajo esa misma óptica vemos unos ejecutivos de la seguridad más preocupados por utilizar lenguajes más cercanos a la organización e interesados en tratar de entregar soluciones que armonicen las relaciones de funcionalidad y protección dentro del marco del negocio. Encontramos responsables de seguridad más preocupados en ver cómo la seguridad de la información debe aportar valor a la empresa y de esta forma se diseñan planes para tener una sensación adecuada de confianza frente a los negocios". De lo anterior se puede concluir que la seguridad de la información se vuelve más importante para las organizaciones, por lo que contemplan los escenarios de protección de la información, como parte de las preocupaciones internas.

[1] ACIS. Encuesta Seguridad Informática En Colombia. Tendencia [en línea] [Fecha de consulta: 05/06/2014] Disponible en: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013

[2] ALMANZA, Andrés. Perfil Profesional. [en línea] [Fecha de consulta: 05/06/2014] Disponible en: http://co.linkedin.com/pub/andres-ricardo-almanza-junco/23/339/ba8

El artículo antes referenciado, también permite recomendar a los encargados de seguridad en la organización que el factor clave de la seguridad, no es la cantidad de tecnologías alrededor del tema, sino una adopción clara de una cultura, encaminada a proteger el activo estratégico de la organización, denominado información.

Otro factor determinante en el medio colombiano es la falta de presupuesto asignado a la seguridad de la información, esto hace que los encargados de ella tengan que buscar estrategias poco confiables o simplemente la limiten al mínimo aceptable (Antivirus – Firewalls), lo que incrementa la vulnerabilidad y los riesgos de ataques.

En Colombia los sectores que demuestran más preocupación por el incremento de los ataques a sus plataformas son: el Financiero, el Gubernamental y el Educativo. A nivel estatal se ve cómo el estado se preocupa cada vez más por el ciberespacio (ley Lleras, Gobierno en línea, entre otros). Por otro lado, el sector educativo ve con preocupación la seguridad, teniendo en cuenta los repetidos ataques a sus infraestructuras, originados por los débiles diseños que exigen mejorar los esquemas. Por su parte, el sector financiero se ven enfrentados a satisfacer una serie de controles para cumplir con ese competido negocio, considerando la globalización de las economías y la normatividad nacional e internacional.

En el caso particular la UNAD, una institución de carácter oficial, que cuenta actualmente con cerca de 70 mil estudiantes matriculados en sus diferentes programas, los cuales tienen acceso al campus virtual, desde muchos municipios del país y desde otros países (estudiantes radicados en otros países). Para ellos el campus se convierte en el espacio vital de interacción, a través del cual desarrollan los cursos que matriculan, actualizan información personal, envían actividades, se comunican con tutores y compañeros, además de presentar evaluaciones y consultar notas. Este entorno ha hecho que la plataforma tecnológica de la institución haya empezado a ser objeto de ataques informáticos como el robo de identidad y algunas caídas sospechosas del sistema.

Por otro lado, los incidentes de seguridad son una tendencia mundial, y se presentan en las organizaciones sin importar el tamaño ni el tipo de negocio que manejan; lo inquietante es que en la realidad colombiana es poco el registro que dejan del mismo. Hecho que puede obedecer a que no todas las partes estén involucradas y que se asuma, como un tema secreto dentro de las empresas, lo que cuestiona el modelo adoptado para la atención de incidentes puesto que lo

recomendado por la industria es que ante un incidente, las partes interesadas estén debidamente informadas, para no generar falsas versiones al respecto.

Sumado a lo anterior, se tiene que las instituciones que ofrecen programas en informática a nivel pregrado y postgrado, están entregando información a sus estudiantes sobre seguridad informática, lo cual hace que a estos, les sea fácil vulnerar sistemas. El argumento anterior es confirmado por expertos en delitos informáticos[3], los cuales establecen que los ataques provenientes de empleados deshonestos o personas con acceso a datos privilegiados de las empresas están creciendo en los países latinoamericanos, algunos de estos expertos establecen la cifra de ataques en aproximadamente el 80%.

En este orden de ideas, se propone este trabajo con el fin de dar respuesta a la siguiente pregunta: ¿Qué medidas de seguridad informática son necesarias para la gestión y consulta de las bases de datos del Campus Virtual de la UNAD, con el fin de reducir amenazas?

1.3 EQUIPO DE TRABAJO

El equipo encargado del desarrollo del trabajo está conformado por dos personas con los siguientes cargos y funciones:

- **Ingeniero.** Estudiante en proyecto de grado de la Especialización en Seguridad Informática de la UNAD. Su función es ejecutar cada una de las tareas establecidas en el plan del proyecto.

- **Asesor.** Ingeniero de Sistemas y Especialista en Seguridad Informática. Tutor de la UNAD. Su función es la coordinación de cada una de las tareas del proyecto.

[3] EL TIEMPO. Crecen los ataques informáticos internos. [en línea] [Fecha de consulta: 08/06/2014] Disponible en: http://www.eltiempo.com/archivo/documento/MAM-1003031

2. OBJETIVOS

Para el desarrollo del proyecto se plantea un objetivo general y cuatro específicos, los cuales se presentan a continuación.

2.1 OBJETIVO GENERAL.

Determinar los niveles de seguridad que tienen las bases de datos del Campus Virtual de la UNAD, mediante un análisis de penetración usando herramientas de software libre, con el fin de reducir sus vulnerabilidades.

2.1. OBJETIVOS ESPECÍFICOS

- Definir los tipos de ataques a bases de datos más comunes en Colombia y el mundo con el fin de establecer un estado del arte sobre el tema mediante una investigación exploratoria.

- Especificar tres herramientas de software libre que pueden ser útiles en pruebas de penetración a base de datos en entornos web, mediante un análisis de funcionamiento de las cinco más usadas para ello.

- Determinar las posibles vulnerabilidades que existan en las bases de datos que maneja el Campus Virtual de la UNAD mediante pruebas de penetración.

- Especificar las políticas de seguridad para el manejo de las base de datos del Campus Virtual que permitan minimizar las vulnerabilidades en el acceso a dichas bases de datos.

3. JUSTIFICACIÓN

Hoy en día es común escuchar a través de los medios de comunicación, noticias sobre ataques cibernéticos a organizaciones tanto estatales como privadas. Dentro de estos ataques, están los dirigidos a uno de los activos más valioso de la compañía, los datos; específicamente a las base de datos, que es el lugar donde reposa éste activo en las compañías. .

La realización de este proyecto entregará como resultado principal un documento que especifica a la UNAD, las vulnerabilidades y riesgos a los que están sometidas las bases de datos que hacen parte de su campus virtual. De igual manera entrega una serie de recomendaciones (políticas de seguridad) sobre la forma como se pueden reducir o mitigar estos riesgos, teniendo en cuenta los recursos disponibles en la universidad para ello. La viabilidad de la pruebas, en un escenario real es alta teniendo en cuenta que la UNAD autorizó el uso de su plataforma para ello (ver carta de autorización adjunta).

Desde el punto de vista institucional, la entidad beneficiada con el desarrollo del proyecto, podrá evidenciar la mejora de sus políticas de seguridad informática en el campo de la protección de los datos. Además la UNAD podrá mostrar a la comunidad la capacidad y habilidad de los profesionales que egresan de su especialización en seguridad informática.

Desde el punto de vista teórico, el desarrollo de este trabajo permitirá validar fundamentos teóricos sobre: seguridad informática y auditoría en bases de datos. Esta validación se logrará al llevar a realidad las políticas de políticas de seguridad y auditoria en el campo de las bases de datos del campus virtual de la UNAD, para lo cual será necesario aplicar teorías y conceptos que involucran estas disciplinas.

De igual manera, el proyecto entregará una documentación que puede ser usada por estudiantes de la UNAD, para el desarrollo de futuros proyectos en el área de seguridad informática.

4. FUNDAMENTOS TEÓRICOS DEL PROYECTO

A continuación se presentan una serie de conceptos y teorías que serán referencia para el desarrollo de este trabajo.

4.1 MARCO CONCEPTUAL

a. Amenaza[4]. Se puede definir como todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

b. Ataque Informático[5]. Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera). Cuando estos van enfocados directamente a cualquier grupo colectivo de información y registros de una empresa o compañía, entonces se realiza un ataque a base de datos.

c. Base de Datos[6]. Una base de datos es un "almacén" que permite guardar grandes cantidades de información de forma organizada para ser luego encontrada y consultada fácilmente. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos. Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.

---

[4] UNLU. Amenazas a la seguridad de la información. [en línea] [Fecha de consulta: 03/03/2015] Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[5] NeaSTDL. Métodos de ataques y vulnerabilidades de las bases de datos. [en línea] [Fecha de consulta: 06/03/2015] Disponible en: http://www.buenastareas.com/ensayos/M%C3%A9todos-De-Ataque-y-Vulnerabilidades-De/25016957.html

[6] MAESTROS DE LA WEB. ¿Qué son las bases de datos?. [en línea] [Fecha de consulta:10/04/2015] Disponible en: http://www.maestrosdelweb.com/editorial/%C2%BFque-son-las-bases-de-datos/

d. NVD (*National Vulnerability Database*)[7]. Es un repositorio estandarizado del gobierno de los Estados Unidos en el cual se encuentra almacenada información acerca de la gestión de vulnerabilidades. Estos datos permiten la automatización de la gestión de vulnerabilidades y la toma de medidas de seguridad. NVD incluye bases de datos con listas de control de seguridad, fallos de seguridad relacionados con software, errores de configuración, nombres de productos y métricas de impacto. En la actualidad cada día se adiciona a la NVD un promedio de 12 nuevas vulnerabilidades.

e. CVE (*Common Vulnerabilities and Exposures*)[8]. El código CVE (vulnerabilidades y amenazas comunes) es un identificador que se asigna a cada vulnerabilidad que se conoce públicamente con el fin de que pueda ser identificada de forma unívoca. Este código fue creado por la corporación MITRE y permite que los usuarios puedan conocer de forma objetiva las vulnerabilidades de un sistema computacional. Los identificadores CVE se presentan en el formato CVE-AÑO-NUMERO y están acompañados de una breve descripción de la vulnerabilidad o amenaza y un grupo de referencias pertinentes.

f. Motor de base de datos[9]. Es un servicio de la base de datos usado para almacenar, procesar y proteger los datos. El motor proporciona acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de su empresa. Se usa generalmente para crear bases de datos relacionales para el procesamiento de transacciones en línea o datos de procesamiento analíticos en línea. Algunos de los motores de base de datos más reconocidos son: Microsoft Access, MySql Server, PostGresql, MySql, Oracle DataBase.

g. Riesgo[10]. El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. El riesgo permite tomar decisiones para proteger mejor al sistema.

[7] FRANCO, David. Herramienta para detectar vulnerabilidades. [en línea] [Fecha de consulta: 05/08/2015] Disponible en: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext
[8] Ibid
[9] MICROSOFT. Motor de base de datos de SQL Server. [en línea] [Fecha de consulta: 10/04/2015] Disponible en: http://msdn.microsoft.com/es-es/library/ms187875.aspx
[10] CODEJOBS. Qué es una vulnerabilidad, una amenaza y un riesgo?. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.D2RDznkO.dpbs

h. Vulnerabilidades[11]. Las vulnerabilidades son errores de diseño, configuración, o implementación, que exponen al riesgo los sistemas informáticos. Algunas vulnerabilidades permiten a los atacantes explotar el sistema comprometido, permitiendo la ejecución de código malicioso controlado por el atacante pero sin el conocimiento del usuario. Otros autores definen la vulnerabilidad informática[12] como un estado de un sistema (o conjunto de sistemas) que puede:

- Permitir a un atacante acceder a información confidencial
- Permitir a un atacante modificar información
- Permitir a un atacante negar un servicio

Existen numerosas vulnerabilidades en aplicaciones, sistemas operativos ó navegadores, que son aprovechadas por atacantes para acceder a información confidencial, realizar una intrusión, instalar un malware, etc. El estándar más común de las vulnerabilidades conocidas y documentadas se denomina CVE (*Common Vulnerabilities and Exposures*) y son mantenidas y publicadas por el NIST en la Base de Datos de Vulnerabilidades conocida como NVD.

La gestión de indicadores de vulnerabilidades permite medir el grado de exposición a las mismas, así como la capacidad de "aguante" de las organizaciones ante distintos ataques/amenazas o incidentes reales que puedan sufrir, su nivel de preparación y su capacidad para mantener la continuidad de su negocio y recuperarse de posibles impactos.

Algunos de estos indicadores son:

- Número de incidentes ocurridos debido a vulnerabilidades en los sistemas.
- Número de vulnerabilidades de nivel alto, medio, o bajo en sistemas críticos.
- Porcentaje de sistemas con vulnerabilidades conocidas.
  Tiempo medio para corregir las vulnerabilidades.
- Costo promedio para corregir las vulnerabilidades.

Un adecuado cuadro de mando de indicadores alimentados en los procesos de auditoría técnica mediante la ejecución de herramientas automáticas, es de gran ayuda para la detección de vulnerabilidades y de los valores de las mismas. El cuadro de mando permite a las organizaciones tener bajo control su grado de exposición a los riesgos de las vulnerabilidades de sus sistemas.

[11] INCIBE. ¿Mi empresa es vulnerable a un ataque informático?. [en línea] [Fecha de consulta: 05/04/2015] Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/empresa_vulnerable_ataque_informatico

[12] FERRER, Rodrigo. Análisis de Vulnerabilidades. [en línea] [Fecha de consulta: 10/04/2015] Disponible en: http://www.sisteseg.com/

Con base en el conocimiento de estos indicadores se puede aplicar el denominado ARTE (Asumir el riesgo, o tomar medidas para Reducirlo, o Transferirlo a un tercero o Eliminarlo), para gestionar los riesgos de las vulnerabilidades existentes en los sistemas de información de la organización.

4.2 MARCO TEÓRICO

a. Anatomía de un ataque informático[13]. A continuación se presenta los pasos de un ataque.

- *Reconocimiento.* En esta etapa se estudia la posible víctima, por medio de diferentes técnicas que proporcionen la información necesaria para un posible ataque.
- *Exploración.* La información obtenida anteriormente es utilizada para lograr datos más relevantes como la dirección IP, contraseñas, host entre otros.
- *Obtener el acceso.* Ahora se analiza las debilidades del sistema, permitiendo así una elaboración inicial del ataque, ataque de los cuales se hablara más adelante en este documento.
- *Mantener el acceso.* Como ya se ha logrado el ataque, los usuarios maliciosos pretenderán mantener el acceso permanente para cuando lo deseen utilizar, usando herramientas como puertas traseras, gusanos, etc.
- *Borrar huella.* Habiendo logrado los objetivos que se ha propuesto, el atacante buscará la manera de no ser detectado borrando cualquier rastro de lo que haya hecho.

b. Análisis de Vulnerabilidades[14]. Una preocupación constante de los profesionales de la seguridad informática es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de herramientas de software cada vez más poderosas en su capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.

El análisis de vulnerabilidades el cual complementa el proceso de análisis de riesgo, es una actividad fundamental con el fin de orientar hacia un sistema de gestión de la seguridad de la información, el cual debería comprender las siguientes actividades:

[13] CIBERINFORMATICO. Anatomía de un ataque. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: http://ciberinfosystem.blogspot.com.co/2012/03/anatomia-de-un-ataque.html
[14] FERRER, Op. Cit.

- *Entendimiento de la infraestructura*. En esta fase se busca, identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos del negocio. Esta selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos. A manera de ejemplo, dentro de los posibles elementos de la infraestructura que un momento dado pudieran llegar a albergar vulnerabilidades a nivel de software tenemos: Servidores, Aplicaciones, Estaciones de trabajo, Bases de datos, Firewalls y Enrutadores

- *Determinación de pruebas*. En esta fase se realizará una clasificación de activos con base en la confidencialidad de la información que guardan y la importancia del activo para la continuidad del proceso en estudio. Se recomienda que para seleccionar las pruebas a realizar, se tenga en cuenta herramientas para la detección de vulnerabilidades[15]. También se debe contar con una base de datos actualizada de vulnerabilidades aceptadas por la industria (CERT, SANS) y con un criterio común de clasificación como el CVE[16] (common vulnerabilities and exposure). Con la herramienta se busca detectar vulnerabilidades presentes en activos y evitar futuros incidentes de seguridad.

- *Medidas preventivas*. Una vez determinado el conjunto de activos a probar, se tomarán las medidas preventivas adecuadas para su ejecución, con el fin de prevenir efectos negativos en el funcionamiento correcto del negocio. Entre estas medidas se pueden contar: Definir horas de bajo tráfico o horarios de no prestación de servicios; Análisis sobre la no disponibilidad de activos críticos de la prueba; Estimar impactos; Tomar algunas medidas de contingencia (Definir estrategias de contingencia para activos críticos, Involucrar personal clave, Realizar copias de seguridad de los activos implicados antes de la prueba); Realizar monitoreo de activos durante las pruebas; Informar al personal operativo y "dueños" de los activos.

  Realización de las pruebas. Una vez clasificadas las vulnerabilidades más críticas, se debe realizar una prueba sobre ellas, con el fin de realizar su explotación. En la medida en que la herramienta seleccionada sea más sofisticada (inteligente y estructurada) el proceso será más corto. Se estima que el tiempo de explotación de 15 vulnerabilidades debe estar del orden de 3 horas, incluyendo la realización del informe. Las pruebas se pueden realizar suministrando información al responsable de su ejecución o se pueden realizar también sin suministrar esta información. También estas pruebas se pueden clasificar según si se hacen de manera interna o se

[15] SECTOOLS. *Top 125 Network Security Tools* [en línea] [Fecha de consulta: 13/04/2015] Disponible en: http://sectools.org/
[16] Common Vulnerabilities and Exposures. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: https://cve.mitre.org/.

intentan ataques desde fuera, es decir, intentar llegar a recursos internos desde por ejemplo Internet.

- *Análisis de resultados.* Terminadas las pruebas se debe realizar una reunión técnica para el análisis formal y detallado de los resultados obtenidos. Este análisis debe incluir una revisión de cada una de las vulnerabilidades encontradas por la herramienta.

- *Plan de mejoramiento de vulnerabilidades*. Identificadas las vulnerabilidades se debe plantear un plan de mejoramiento específico para cada una de ellas. Este plan puede hacer parte del plan de tratamiento general de riesgos. Además debe determinar la criticidad de cada una de las vulnerabilidades encontradas y sugiere cuales deben ser solucionadas en el corto, mediano o largo plazo.

c. Ataques a bases de datos. La gran mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server entre otros, y atacar una bases de datos es uno de los objetivos favoritos para los ciber-criminales. Esto puede explicar el por qué los ataques externos, tales como inyección de SQL, subieron 56.2% en 2012, "Esta tendencia es prueba adicional de que los agresores tienen éxito en hospedar páginas web maliciosas, y de que las vulnerabilidades y explotación en relación a los navegadores web están conformando un beneficio importante para ellos. Para empeorar las cosas, según un estudio publicado en febrero de 2012 *The Independent Oracle Users Group* (IOUG), casi la mitad de todos los usuarios de Oracle tienen al menos dos parches sin aplicar en sus manejadores de bases de datos"[17].

Mientras que la atención generalmente se ha centrado en asegurar los perímetros de las redes por medio de, firewalls, IDS / IPS y antivirus, cada vez más las organizaciones se están enfocando en la seguridad de las bases de datos con datos críticos, protegiéndolos de intrusiones y cambios no autorizados.

Expertos en temas de seguridad como la *Open Security Foundation* han identificado las 9 amenazas más comunes para las base de datos[18].

[17] CHÁVEZ, Jenny. Ataque a la base de datos. [en línea] [Fecha de consulta: 13/04/ 2015] Disponible en: http://ataquebd.blogspot.com/2012/07/ataque-la-base-de-datos-introduccion-la.html

[18] TICBEAT. Las 10 grandes amenazas de seguridad en las bases de datos. [en línea] [Fecha de consulta: 13/04/2015] Disponible en: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

- *Privilegios excesivos e inutilizados*. Cuando a alguien se le otorgan privilegios de base de datos que exceden los requerimientos de su puesto de trabajo se crea un riesgo innecesario. Los mecanismos de control de privilegios de los roles de trabajo han de ser bien definidos o mantenidos.

- *Abuso de Privilegios*. Los usuarios pueden llegar a abusar de los privilegios legítimos de bases de datos para fines no autorizados, por ejemplo, sustraer información confidencial. Una vez que los registros de información alcanzan una máquina cliente, los datos se exponen a diversos escenarios de violación.

- *Malware y spear phising*. Se trata de una técnica combinada que usan los cibercriminales, hackers patrocinados por estados o espías para penetrar en las organizaciones y robar sus datos confidenciales.

- *Auditorías débiles*. No recopilar registros de auditoría detallados puede llegar a representar un riesgo muy serio para la organización en muchos niveles.

- *Exposición de los medios de almacenamiento para backup*. Éstos están a menudo desprotegidos, por lo que numerosas violaciones de seguridad han conllevado el robo de discos y de cintas. Además, el no auditar y monitorizar las actividades de acceso de bajo nivel por parte de los administradores sobre la información confidencial puede poner en riesgo los datos.

- *Explotación de vulnerabilidades y bases de datos mal configuradas*. Los atacantes saben cómo explotar estas vulnerabilidades para lanzar ataques contra las empresas.

- *Datos sensibles mal gestionados*. Los datos sensibles en las bases de datos estarán expuestos a amenazas si no se aplican los controles y permisos necesarios.

- *Denegación de servicio (DoS).* En este tipo de ataque se le niega el acceso a las aplicaciones de red o datos a los usuarios previstos. Las motivaciones suelen ser fraudes de extorsión en el que un atacante remoto repetidamente atacará los servidores hasta que la víctima cumpla con sus exigencias.

- *Limitado conocimiento y experiencia en seguridad y educación*. Muchas firmas están mal equipadas para lidiar con una brecha de seguridad por la falta de conocimientos técnicos para poner en práctica controles de seguridad, políticas y capacitación.

Entre los ataques más comunes y que tienen como fin llegar a las a base de datos están[19]:

- *Ataque por Session Hijacking*. Conocido también como “secuestro o robo de sesión”, se refiere a que un individuo (atacante) consigue el identificador de sesión entre una página web y un usuario, de forma que puede hacerse pasar por este y acceder a su cuenta en esa página web. Esto es posible dado que la única forma que tiene la página web de reconocer a un usuario es por medio de su identificador de sesión. Si un atacante consigue el identificador de sesión de un usuario que ya está autenticado, puede hacerse pasar por él y entrar en su cuenta sólo con hacer que su navegador envíe el identificador a la página web, ya sea a través de la URL o de una cookie.

- *Robo en Servidor Compartido*. Si se tiene una página web alojada en un servidor compartido, los archivos físicos de las sesiones se guardan, por defecto, en un directorio común para todas las páginas web del servidor. Esto quiere decir que todas las personas que tengan su página web en ese mismo servidor, tienen acceso a todos los archivos de sesiones. Dado que el nombre de los archivos es "sess_" más el identificador de sesión, cualquier atacante tendrá una lista de identificadores de sesión válidos con sólo leer la lista de archivos del directorio común.

- *Ataque Por Inyección De Código*. La inyección SQL consiste en la modificación del comportamiento de consultas mediante la introducción de parámetros no deseados en los campos a los que tiene acceso el usuario. Este tipo de errores permite a usuarios malintencionados acceder a datos a los que de otro modo no tendrían acceso y, en el peor de los casos, modificar el comportamiento de nuestras aplicaciones.

d. Auditorias Para Vulnerabilidades[20]. Los procesos de auditorías técnicas realizadas de manera continua, y apoyadas en herramientas para descubrir vulnerabilidades y brechas de seguridad, pueden ayudar a las organizaciones a mantener controladas y reducir las amenazas y riegos de sufrir incidentes de seguridad debido a la posible explotación de las vulnerabilidades en sus sistemas de información.

Algunas soluciones multipropósito de escaneo de vulnerabilidades son:

[19] CHAVEZ, Op. Cit.
[20] PELAEZ, Juan. ¿Mi empresa es vulnerable a un ataque informático? [en línea] [Fecha de consulta: 13/04/2015) Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/empresa_vulnerable_ataque_informatico

- *Acunetix (https://www.acunetix.com/). Herramienta para búsqueda de vulnerabilidades mediante técnicas de hacking como, por ejemplo, inyección SQL, ataques de ejecución de código y ataques de autentificación, entre otros.*

- *Faast (https://www.elevenpaths.com/es/tecnologia/faast/). Es un servicio de persistent pentesting que implementa y automatiza todas las técnicas de pruebas de penetración mediante un proceso continuo de evaluación.*

- *GFI Languard (http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard). Herramienta que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad en una red informática.*

- *Nessus (http://www.tenable.com/products/nessus-vulnerability-scanner): Detecta numerosos fallos de seguridad.*

- *Nexpose (http://www.rapid7.com/products/nexpose/). Herramienta para realizar escaneo de vulnerabilidades.*

- *OpenVAS (http://www.openvas.org/). Escáner de vulnerabilidades, muy similar al Nessus, desarrollado por la comunidad de software libre.*

Existen listados de herramientas de seguridad, entre ellos SecTools (http://sectools.org/tag/vuln-scanners/), donde se enlazan herramientas de escaneo de vulnerabilidades, o para pruebas específicas y utilizadas en procesos de auditoría técnica.

e. Bases de la seguridad informática[21]. En general, un sistema será seguro o fiable si se puede garantizar tres aspectos: Confidencialidad, Integridad y Disponibilidad.

- *Confidencialidad.* Hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. Su objetivo es prevenir la divulgación no autorizada de la información. En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos.

- *Integridad*. Este término hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado. Su objetivo es prevenir modificaciones no

[21] MIFSUD, Elvira. Introducción a la seguridad informática. [en línea] [Fecha de consulta: 25/04/2015] Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

autorizadas de la información. La integridad hace referencia a: la integridad de los datos (el volumen de la información) e integridad del origen (la fuente de los datos, llamada autenticación).

- *Disponibilidad*. En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. Su objetivo es prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En ambientes educativos es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer las notas de otro usuario a que pueda modificarlas.

f. Seguridad de la información del estado[22]. En lo referente a seguridad de la información, la Ley 1341 de 2009“ por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC- se crea la agencia nacional de espectro y se dictan otras disposiciones”, señala en su artículo dos (2), como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno en Línea. Adicional a lo expuesto, el Gobierno Nacional, a través del documento CONPES 3701 del 14 de julio de 2011, estableció la Estrategia Nacional de Ciberseguridad y Ciberdefensa, con el fin de desarrollar medidas que aseguren la información de los ciudadanos frente a las amenazas informáticas, estableciendo compromisos a cargo del Ministerio de las TIC, entre otras entidades relacionados con el diseño e implementación de planes, políticas, estrategias, gestión, capacitación y sensibilización en lo referente a seguridad de la información.

Con la expedición del decreto 2618 del 2012, se modifica la estructura del Ministerio de las TIC, se crea la Subdirección de Seguridad y Privacidad de TI, la cual tiene entre otras las siguientes funciones:

- Liderar la implementación en el Estado de plataformas con estándares de seguridad y privacidad de la información en coordinación con las autoridades pertinentes.

[22] MINTIC. Modelo de seguridad de la información. [en línea] [Fecha de consulta: 25/04/2015] Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

- Definir, conjuntamente con las autoridades competentes, una estrategia de seguridad y privacidad de la información desde la perspectiva de la tecnología en las dimensiones de la protección de bienes, activos, servicios, derechos y libertades dependientes del Estado y que coordine las agencias y entidades público - privadas relacionadas con este fin.

- Elaborar una estrategia de seguridad de la información que soporte un marco normativo específico para las entidades del orden nacional y en coordinación con las entidades del orden territorial respetando la autonomía administrativa.

- Definir los lineamientos de política y estándares de protección de la información pública, para su preservación en situaciones de desastre.

- Promover en la dinámica del Estado una cultura de la ciberresponsabilidad, basada en la concientización y formación continua en ciberseguridad, a través de planes de estudio que desarrollen teoría práctica aplicable en las organizaciones y provean empleo cualificado.

Este mismo decreto, le da facultades al Ministerio de las TIC, para generar estrategias de implementación y evaluación del modelo de seguridad y privacidad de la información, en las entidades del Estado. Que el 12 de diciembre del año 2014, fue expedido el Decreto 2573, “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”. El Decreto tiene como objeto “Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad”.

5. RECOLECCIÓN DE INFORMACIÓN

A través de este capítulo se presenta de manera general la infraestructura de la plataforma de la UNAD, las herramientas que se usaran para los ataques y las recomendaciones de los expertos en seguridad.

Es necesario aclarar que por petición de directivas de la UNAD y de los profesionales entrevistados, alguna información es presentada de manera muy general en éste documento, pero que en el proceso de desarrollo del trabajo se contó con toda la información pertinente.

5.1 ENTREVISTAS

Con el fin de facilitar la documentación del proyecto, se presenta en el Anexo A, las preguntas formuladas a los profesionales y se entrega un CD los audios de cada entrevista.

Por motivos de seguridad, no se presenta toda la información suministrada por los profesionales, ya que alguna es sensible y puede afectar la seguridad de su organización.

A continuación se documentan las entrevistas realizadas.

Tabla 1. Entrevista 1.

Profesional	José Gregorio Hernández Sánchez.
Cargo	Jefe de Infraestructura Tecnológica de la Universidad Autónoma de Bucaramanga - UNAB.
Formación Académica	Ingeniero de Sistemas, Especialista en Telecomunicaciones Maestría en E-learning
Soporte	CD\Entrevistas\Juan Sánchez

Fuente: Autor del proyecto.

El ingeniero José Gregorio Hernández Sánchez está encargado de la administración de las plataformas de servidores, lo relacionado con el procesamiento y almacenamiento de datos, además de la parte de conectividad.

La entrevista realizada al Ingeniero José Gregorio Hernández Sánchez, permitió establecer lo siguiente:

a. La mayoría de los casos a nivel de seguridad en los cuales se ha visto comprometida las bases de datos de la universidad, ha sido a nivel de MySQL por inyección de código a través de los sitios web.

b. Como mejores prácticas comenta que han tenido que separar la base de datos de los aplicativos web; para tener un direccionamiento privado al acceso a la base de datos y el aplicativo como tal, envía el direccionamiento público, esto ayuda a mitigar un poco ese tipo de ataques por inyección que se han presentado.

c. Otra buena práctica, ha sido los respectivos parches y actualizaciones de los respectivos motores de bases de datos y de los aplicativos que hacen acceso a estos.

d. Con respecto al campus virtual de la Universidad UNAB, manejan dos plataformas virtualmente por cuestiones de rendimiento, se ofrece directamente el servicio en la nube a los estudiantes y la seguridad está a cargo del proveedor.

Tabla 2. Entrevista 2.

Profesional	**Gerardo Granados Acuña**
Cargo	Docente de planta de la UNAD, adscrito a la Escuela de Ciencias Básicas Tecnología e Ingeniería, del CEAD Bucaramanga
Formación Académica	Ingeniero de Sistemas, Especialista en Telecomunicaciones, Maestría en Telecomunicaciones. Instructor CISCO para los módulos CCAN1, CCAN2, CCAN3, CCAN4 Certificaciones ICONTEC en el manejo de normas ISO 9000 y 27001.
Soporte	CD\Entrevistas\Gerardo Granados

Fuente: Autor del proyecto.

El Msc. Gerardo Granados Acuña es **d**ocente de planta de la UNAD, quien además cuenta con experiencia como asesor de seguridad en empresas públicas y privadas.

De su entrevista, se destacan los siguientes apartes.

a. Ha realizado estudios de seguridad informática para algunas empresas, en las cuales ha podido constatar que muchas veces, no se aplica las normas esenciales, básicas o mínimas, de seguridad informática.

b. Conoce de caso de empresas, en los que las Bases de Datos por ejemplo: se actualizan directamente desde un lenguaje SQL y no, desde programas.

c. Ha encontrado casos, en donde se aplica un usuario root y el usuario root de la base de datos que maneja el master de la base de datos, lo tienen personas no autorizadas.

d. Como usuario por más de 10 años de la plataforma Tecnológica de la UNAD, particularmente no ha tenido ningún inconveniente serio, relacionado con la seguridad informática en las Bases de Datos. Pero, sí ha podido determinar que muchas veces se han presentado situaciones en las cuales por ejemplo: los docentes hacen grabaciones de notas o trabajo colaborativo y en uno o dos días las notas desaparecen completamente del campus, le da la impresión de que los backups no se manejan con la debida seriedad.

e. En otras oportunidades, ha podido constatar que algunos estudiantes han ingresado desde sitios externos de la Universidad a las Bases de Datos y han alterado notas, eso le parece muy delicado, en lo que respecta a la seguridad de las Bases de Datos.

f. Sugiere que la UNAD debería trabajar más en la cultura de la seguridad de la información, donde se den algunos tics necesario de seguridad informática a los estudiantes pero, también es importante que los docentes se les haga una preparación mucho más formal, en lo que se refiere a cómo mantener seguro su curso, como sacar copias de seguridad del curso a cargo, es bueno que todos sepan cómo realizarlo de una manera muy controlada.

Tabla 3. Entrevista 3.

Profesional	**Javier Medina Cruz**.
Cargo	Docente asistente de planta de la UNAD, adscrito a la Escuela de Ciencias Básicas Tecnología e Ingeniería, del CEAD Bucaramanga.
Formación Académica	Ingeniero de Sistemas, Especialista en Docencia Universitaria, Especialista en Finanzas, Maestría en Ingeniería de Sistemas e Informática
Soporte	CD\Entrevistas\Javier Medina

Fuente: Autor del proyecto.

El ingeniero Javier Medina Cruz es docente de planta de la UNAD, quien además tiene experiencia de 15 años como jefe de sistemas de la alcaldía de Floridablanca (Santander). Siendo el encargado de todos los procesos que conllevaron a tener una confidencialidad, integridad y una disponibilidad de la información. Sobre todo lo relacionado con los datos del impuesto predial unificado, de industria y comercio, nómina y la administración de personal, presupuesto almacén e inventarios entre otras.

A continuación, se presentan los fragmentos más relevantes de su entrevista.

a. La estructura tecnológica de la UNAD, permite afirmar que la Universidad cuenta con procesos y procedimientos muy bien establecidos. No solamente a nivel interno sino, también a nivel de usuario. De tal manera que se podría decir que se garantiza estas tres características (confidencialidad, integridad y disponibilidad) de toda seguridad, sobre todo, en las bases de datos.

b. Se puede ver un trabajo continuo de actualización de la seguridad informática, por lo cual puede decirse que se puede garantizar que esta información es segura, tanto a nivel físico como a nivel de usuario.

c. Se podría comentar que la idea es hacer mucho énfasis en lo que tiene que ver en la seguridad cuando se manejan servidores de Bases de Datos específicos, como es el caso por ejemplo: Oracle, MYSQL, u otro manejador de Base de Datos, de tal manera, que se sigan los lineamientos y parámetros claros que puedan garantizar la seguridad de la información.

Tabla 4. Entrevista 4.

Profesional	Juan Carlos Vesga.
Cargo	Docente de planta de la UNAD, adscrito a la Escuela de Ciencias Básicas Tecnología e Ingeniería, del CEAD Bucaramanga.
Formación Académica	Ingeniero Electrónico, Ingeniero de Sistemas, Especialista en Docencia Universitaria, Especialista en Telecomunicaciones, Maestría en Telecomunicaciones, Doctorado en Telecomunicaciones
Soporte	CD\Entrevistas\Juan Vesga.

Fuente: Autor del proyecto.

El Dr. Juan Carlos Vesga, es docente de planta de la UNAD y adscrito a la Escuela de Ciencias Básicas Tecnología e Ingeniería, del CEAD Bucaramanga.

A continuación se extracta algunos comentarios de su entrevista.

a. Uno de los mayores problemas que se ha detectado a nivel de Bases de Datos está relacionado con la integridad de la información. Actualmente en aplicaciones Web, utilizan diversos motores como por ejemplo: MySQL o Postgressl pero, lastimosamente, la mayoría de los sistemas de información están soportados en que operan sobre Moodle, MySQL y estos, no manejan entidad referencial lo que hace que se presente, duplicidad en la información, por ende, sea fácilmente Vulnerable para algún ataque que haga referencia a Base de Datos.

b. Uno de los aspectos que considero de vital importancia, es que no hay una integración de los sistemas de Información al interior de la institución y como lo

mencionaba anteriormente, la mayoría están soportados en Moodle, el cual hace uso de MySQL como motor de Base de Datos, por lo que maneja una falencia de entidad referencial que incluso, puede ser Vulnerado, no solamente, bajo ataques comunes en relación con la identificación de llaves dentro de los campus, como es el caso de adición de líneas de sql o incluso obtener las respectivas credenciales de accesos, lo cual en este caso vulnera el sistema fácilmente.

Tabla 5. Entrevista 5.

Profesional	Fernando Morales Carvajal
Cargo	Profesional Arquitectura de Seguridad - Banco Bogotá
Formación Académica	Ingeniero de Sistema y Especialista En Seguridad Informática
Soporte	CD \Entrevistas\Fernando Morales

Fuente: Autor del proyecto.

El ingeniero Fernando Morales hace parte del equipo de profesionales que define y gestiona la Arquitectura de la Seguridad del Banco Bogotá. Se encuentra radicado en la ciudad de Bogotá.

La entrevista se realizó a través de un cuestionario, el cual se le hizo llegar a través de un correo electrónico. Las respuestas dadas, permitió establecer lo siguiente:

a. Su experiencia en seguridad informática se adquirido en empresas del sector de las telecomunicaciones y del sector financiero.

b. Ha analizado situaciones de empresas a nivel mundial del sector retail que han sido víctimas de ataques, como el caso de Home Depot´s y Target, las cuales han sido afectadas con el robo de información financiera asociada a tarjetas-crédito de sus clientes, impactando la imagen de las compañías, la credibilidad de sus compradores y aumentando el fraude.

c. Conoce de casos en Colombia de incidentes en el sector público asociados a ataques de denegación de servicio a portales de la Registraduría Nacional y la Policía.

d. En cuanto a recomendaciones para proyectos que usen MySQL y Moodle, establece que las herramientas de libre distribución o de código abierto son tan buenas como las herramientas de pago, la recomendación es que si se usan estas herramientas lo importante es contar con versiones actualizadas

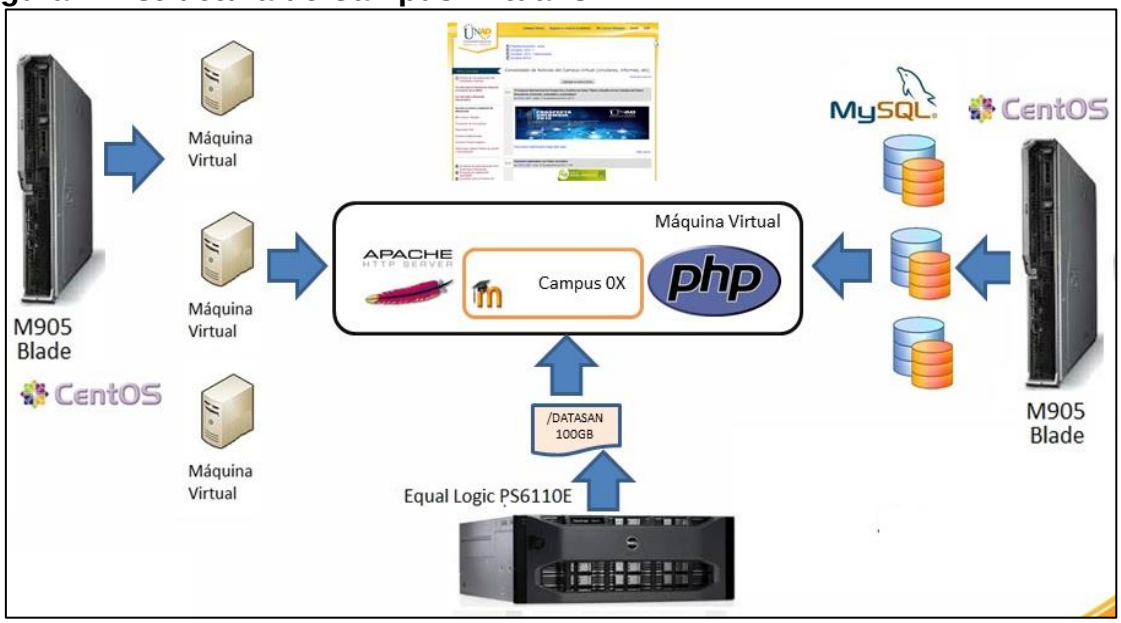
para evitar la explotación de vulnerabilidades, adicionalmente realizar las validaciones necesarias a nivel de la aplicación para evitar ataques de *SQL injection*.

5.2 INFRAESTRUCTURA DEL CAMPUS VIRTUAL.

El objetivo de esta sección es presentar la estructura y gestión de la base de datos que hace parte del campus virtual de la UNAD. Para facilitar esta tarea se tramitó la autorización por parte del Jefe De La Plataforma Tecnológica Integrada – PTI (Ver Anexo B), quien es el encargado del Campus Virtual.

a. Base de datos y servidores. La UNAD cuenta con un Campus Virtual (ver figura 1) donde interactúan estudiantes, personal académico y funcionarios administrativos de la institución. Éste campus está estructurado tecnológicamente por servidores con configuración en Linux, con tres versiones de Moodle y un gestor de base de datos, llamado MySQL (por seguridad se omiten la versiones), que se utiliza para la interconexión con el administrador de base de datos.

Figura 1. Estructura de Campus virtual UNAD.



Fuente: Tomado de Presentación PTI Unad

Además cuenta con una herramienta para el monitoreo del comportamiento de las bases de datos, llamada *Mysql monitoring tool* (ver figura 2).

Figura 2. Monitoreo de servidores de bases de datos.

Fuente: Pantallas capturadas del programa *Mysql monitoring tool*

La gráficas que aparecen en la figura 2, muestran un monitoreo de las bases de datos, de los 3 servidores o *blade*. Cada servidor administra 14 motores. Con esta herramienta se pueden visualizar la cantidad de conexiones que se realizan, en un momento determinado, a la base de datos.

El Campus también cuenta con tres servidores de acceso identificados como: campus0a, campus0b y campus0c. Estos servidores están vinculados a un servidor balanceador que nivela las cargas entre ellos.

El número de registros por ingreso de usuarios, que se hacen en el día oscila entre 27.000 y 39.000, generando un promedio mensual de consultas de 848.639.

Las copias de seguridad de la información son realizadas tres veces al día (1:30 a.m., 10:30 a.m., y 3:30 p.m). Las horas seleccionadas para hacer las copias son franjas de bajo tráfico, con el fin de no saturar el servidor con éste proceso.

Normalmente, se tiene un promedio entre 25 y 30 conexiones simultáneas; en las horas con mayor flujo se puede incrementar hasta 50. Cuando estas

conexiones simultáneas se pasan de 100, es una alarma y se tiene que entrar a revisar que está pasando.

Mysql monitoring tool cuenta con una pestaña llamada *process list*, que permite visualizar lo qué se está ejecutando en determinado momento. De esta forma se puede determinar, si se tienen consultas encoladas o si se está atacando la base de datos.

La grafica de monitoreo de base de datos (figura 2), no fue diseñada para entregar información detallada de un ataque; fue creada para visualizar el comportamiento, seguimiento y alertas del funcionamiento de la base de datos. Con esta información el personal encargado debe revisar si lo que está pasando, es el resultado de encolamiento de peticiones u otras consultas que se pueden realizar pero que no se pueden revelar en este documento por protocolos de seguridad.

b. ***Moodle***. Es un LCMS (*Learning Content Management System*), creado por Martin Dougiamas, un administrador de WebCT en Curtin University, Australia, y graduado en Ciencias de la Computación y Educación. En su Ph.D. examinó el uso del software abierto para el soporte de una epistemología construccionista social de enseñanza y aprendizaje con comunidades, basadas en Internet. Su investigación tiene fuerte influencia en el diseño de Moodle, proporcionando aspectos pedagógicos perdidos en muchas otras plataformas de aprendizaje virtual.

El campus de la UNAD, usa *Moodle* para crear y administrar la información de sus cursos. Este LCMS no crea relaciones entre tablas ni genera un diccionario de datos como lo haría cualquier SGBD, en lugar de ello, crea una estructura acorde a las necesidades del usuario. Moodle genera documentación relacionada con objetos creados *Stored Procedure,* Vistas, y Disparadores o *Trigger*.

La instalación de Moodle requiere una plataforma que soporte PHP y la disponibilidad de una base de datos. Moodle tiene una capa de abstracción de bases de datos por lo que soporta los principales sistemas gestores de bases de datos.

Moodle tiene desventajas asociadas a la seguridad, que dependen del lugar dónde se esté alojando su instalación, de las políticas de seguridad y la infraestructura tecnológica con la cual se cuente durante la instalación.

c. Personal. Las bases de datos de Campus Virtual UNAD, son administradas por tres Ingenieros de Sistemas con Especialización en un área del conocimiento a fin a sus funciones. El personal desempeña las siguientes funciones:

Ingeniero De Base De Datos 1. Administra la base de datos

Ingeniero De Base De Datos 2. Migra y Restaura Cursos del Campus Virtual de periodos académicos ya culminados; Gestiona la solución de los casos tecno-pedagógicos correspondientes a bases de datos de la PTI; documenta procedimientos y actividades inherentes a su cargo. También monitorea el espacio en disco de los *blade* asignados a bases de datos del campus virtual. Actualiza información de estudiantes de campus virtual y Recupera Información borrada accidentalmente (foros, quices, actividades).

Ingeniero De Base De Datos 3. Sus funciones son: el análisis del comportamiento de la base de datos; el monitoreo de servidores; la realización de copias de seguridad y el desarrollo de consultas en el motor de la base de datos. También realiza tareas de programación en MySQL y PHP.

De las charlas realizadas para reconocer el entorno de trabajo, se pudo extractar lo siguiente:

a. Los procesos y procedimientos de base de datos están documentados en un 70%.

b. No se cuenta con una política de seguridad establecida para la base de datos.

c. La documentación existente es fácil de consultar por parte de los Ingenieros y personal autorizado por GIDT[23] de la UNAD.

d. El DBA[24] por cumplimiento a la política de seguridad, cambia cada 90 días la contraseña o password. La contraseña maneja letras (mayúsculas y minúsculas), números, caracteres especiales y tiene una extensión de 12 caracteres.

e. Las contraseñas se cambian por defecto, para evitar ataque de privilegios.

[23] GIDT: Gerencia de Innovación y Desarrollo Tecnológico.
[24] DBA: Administrador de la Base de Datos

f. Cuando la página web está offline, no se muestra la versión de SGBD utilizado por la UNAD.

g. Se tiene nociones del *NoSql* pero, nunca se ha trabajado con ellas fuera de las prácticas académicas.

d. Seguridad. En cuanto a la seguridad del Campus Virtual de la UNAD, se pudo establecer que se cuenta con algunas políticas, que impiden entregar información clasificada. Tan solo se puede mencionar algunas reglas de seguridad que se utilizan, entre ellas están los certificados SSL (https://www.unad.edu.co/ y https://campus0b.unadvirtual.org/campus0/login/index.php).

También se realiza mensualmente un análisis de vulnerabilidades a los servidores del campus Virtual de la UNAD, si se encuentran vulnerabilidades automáticamente se realiza el plan de mejora. Otro control que se hace es por un firewall que tiene la universidad ya configurado.

5.3 HERRAMIENTAS A UTILIZAR.

El objetivo de esta sección es dar unas orientaciones sobre las herramientas que se podrían usar para el desarrollo de las pruebas de vulnerabilidad. Para ello se realizará un análisis tomando como base una serie de criterios y aspectos técnicos relevantes.

a. Criterios para selección. Tomando como base la información consultada, la colaboración de algunos expertos en seguridad y las características del proyecto, se establecieron tres criterios para seleccionar las herramientas que se usaron para el análisis de vulnerabilidades de la base de datos. A continuación se describen los criterios seleccionados:

Criterio 1. Es multiplataforma (incluye Linux)
Criterio 2. De libre distribución.
Criterio 3. Uso en el mercado de la seguridad.
Criterio 4. Documentación disponible (tutoriales, manuales y videos).
Criterio 5. Interfaz amigable.

b. Herramientas analizar. Para realizar esta tarea fue necesario hacer una serie de consultas en internet, y material trabajado en la Especialización, con el fin de determinar las herramientas más promovidas en el mundo de la seguridad informática. Entre los sitios consultados en internet están:

Las 75 herramientas de seguridad más usadas.
http://insecure.org/tools/tools-es.html

Seis escáneres de vulnerabilidades de red gratuitos
http://cioperu.pe/articulo/15863/6-escaneres-de-vulnerabilidades-de-red-gratuitos/

50 herramientas top de seguridad
http://www.zonagratuita.com/a-cursos/utilidades/50_herramientas_top.htm

Las 8 mejores herramientas de seguridad y hacking
http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

Top 5 de las mejores herramientas para seguridad informática
https://hacknicla.wordpress.com/2014/09/16/top-5-de-las-mejores-herramientas-para-seguridad-informatica/

Clasificación de herramientas de vulnerabilidad por costos
http://www.clcert.cl/repCosto.php

La revisión de las fuentes antes citadas y la asesoría de expertos en seguridad informática, permitió identificar seis herramientas muy usadas en el ámbito del análisis de vulnerabilidades. A continuación se hace una pequeña descripción de cada una.

Core Impact[25]. Es considerada a nivel mundial como la herramienta de explotación más poderosa existente. Soporta una gran cantidad de exploits profesionales en una base de datos que se actualiza con regularidad, y puede realizar trucos como realizar ataques redirigidos usando una máquina afectada con un *exploit* como esclavo. El principal inconveniente de esta herramienta es su precio: Puede llegar a varios miles de dólares.

GFI LANguar.[26] Es un escáner de red no-libre para Windows. LANguard escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches {patches} de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro {"key registy entries"}, passwords débiles, usuarios y grupos; y más. Los resultados del escaneo se muestran en un reporte en formato HTML, que puede

[25] CORE SECURITY. Core Impact. [en línea] [Fecha de consulta: 05/07/2015] Disponible en: http://www.coresecurity.com/core-impact-pro
[26] ASI. GFI LanGuard. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://www.auditoria.com.mx/GFI-LanGuard

ser modificado a gusto propio o consultado. Aparentemente, una versión gratuita está disponible para prueba y usos no comerciales.

Kali Linux.[27] Es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Fue construida pensando en profesionales de la seguridad. Es un software libre y totalmente gratuito. Kali Linux dispone de más de 300 herramientas de penetración.

Nessus.[28] Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad. Nessus se ha convertido es el escáner de vulnerabilidades y evaluación de configuraciones más utilizado del mundo, por su gran velocidad a la hora de realizar sus descubrimientos.[29].

Nmap (Network Mapper).[30] Es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.

Sqlmap.[31] Es una de las herramienta más conocidas para hacer ataques SQLi (SQL Injection) escrita en Python. SQLmap se encarga de realizar peticiones a los parámetros de una URL que se le indiquen, ya sea mediante una petición GET, POST, en las cookies, etc. Es capaz de explotar todo tipo de SQLi como union-base, time-base-blind, base-blind-injection, heavy-queries, etc.

SQL Injection es una técnica de ataque a páginas o aplicaciones, que intenta inyectar código SQL dentro de la aplicación destino, para acceder a información sensible. Inyección SQL es un método de infiltración de código intruso que se

[27] KALI. Documentación Oficial Kali Linux. [en línea] [Fecha de consulta: 10/08/ 2015] Disponible en: http://es.docs.kali.org/introduction-es/que-es-kali-linux
[28] INSECURE. Las 75 herramientas de seguridad más usadas. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://insecure.org/tools/tools-es.html
[29] Ibid.
[30] CAPACITY. Las 8 Mejores Herramientas de Seguridad y Hacking. [en línea] [Fecha de consulta: 05/08/2015] Disponible en: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/
[31] EL HACKER.NET. Tutorial Sqlmap. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://blog.elhacker.net/2014/06/sqlmap-automatizando-ataques-sqli-injection.html

vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

c. Elección de herramienta. Para elegir las tres herramientas que se emplearían para las pruebas se aplicaron los criterios preestablecidos en cada una de las preseleccionadas. Para realizar esta tarea se contó con la información de los sitios oficiales de cada herramienta, además de los sitios web citados en la sección anterior. En la Tabla de la figura 3 se pueden ver los resultados de esta tarea.

Tabla 6. Aplicación de criterios a herramientas preseleccionadas

Herramienta	Criterio 1	Criterio 2	Criterio 3	Criterio 4	Criterio 5
Core Impact	**Si**	**No**	**No**	**Poca**	**Gráfica**
GFI LANguar	**No**	**No**	**Si**	**Poca**	**Gráfica**
Kali Linux	**Si**	**Si**	**Si**	**Mucha**	**Gráfica y Comandos**
Nessus	**Si**	**No**	**Si**	**Mucha**	**Gráfica**
Nmap	**Si**	**Si**	**Si**	**Mucha**	**Gráfica**
Sqlmap	**Si**	**Si**	**No**	**Poca**	**Gráfica y Comandos**

Fuente: Autor del proyecto

Tomando como base los resultados mostrados en la tabla 6, se determinó usar las siguientes herramientas: Kali Linux, Nmap y Sqlmap.

d. Ajustes finales a herramientas. Terminado el proceso de elección de herramientas, se presentó el documento al asesor del proyecto, quien de acuerdo a su experiencia considero necesario dejar las herramientas **SQL Map** y **Nmap** e incluir **BBSQL**, que es un Framework de inyección SQL diseñado específicamente para ser hiper rápido, hacer diagnóstico de bases de datos, y es fácil de configurar y modificar. Esta herramienta es muy eficaz en la explotación de un determinado tipo de fallo de inyección SQL.

6. DESARROLLO DE PRUEBAS

En este capítulo se describen las pruebas realizadas, especificando herramientas, comandos y mostrando los resultados obtenidos a través de pantallas capturadas de la consola de cada herramienta. Es necesario aclarar que no se entró en muchos detalles de las pruebas y sus resultados, debido a las condiciones de confidencialidad de la información que coloco el personal de la universidad.

6.1 CONDICIONES ESTABLECIDAS POR LA UNAD

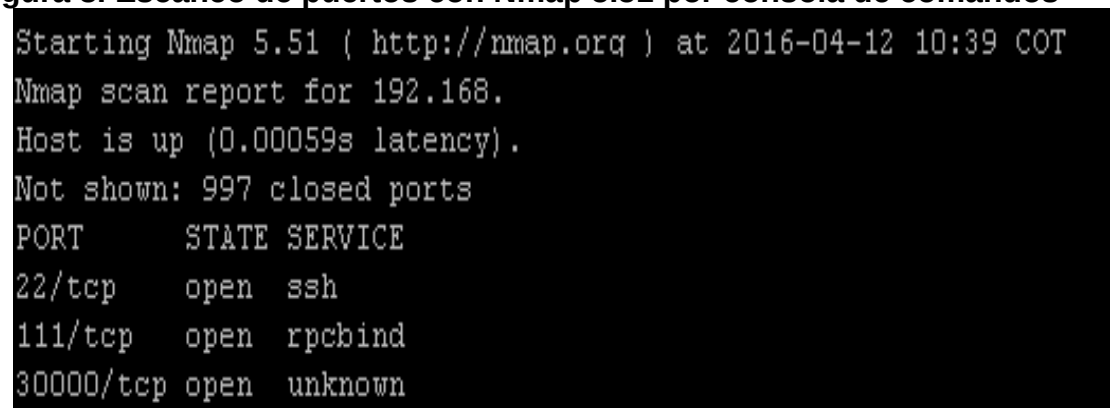
Por la sensibilidad de la información que se almacena y gestiona el Campus Virtual, la Universidad asignó al Ing. Miguel Pinto (Coordinador Del Campus) para establecer los lineamientos sobre los cuales se realizaría el análisis de vulnerabilidad. Entre los principales lineamientos están los siguientes:

a. Debe existir una autorización escrita de la universidad para realizar las pruebas. Esta carta debe ser emitida por el funcionario que asigne la UNAD.
b. La Universidad asignará un equipo de cómputo donde se configurará un servidor de pruebas con características similares a los servidores utilizados en el Campus Virtual.
c. El personal responsable de los servidores de la Unad, realizará una copia de la base de datos del campus virtual y la montará en el servidor de prueba.
d. La Universidad solicita se hagan las pruebas desde accesos internos, ya que no asignará direcciones públicas para pruebas externas, ello por políticas de seguridad.
e. La UNAD solo autoriza pruebas pasivas con la base de datos. Estas pruebas no deben incluir modificación de configuraciones de la base de datos ni de servidores.
f. La universidad autoriza usar en las pruebas copia de datos reales de cursos, estudiantes y tutores, pero de semestres anteriores.

6.2. ESCANEO DE PUERTOS

Para realizar esta prueba se usó la herramienta Nmap de Kali Linux. La prueba se realizó para determinar los puertos que tiene abiertos el Servidor. En la figura 3 se puede ver los resultados que arrojó la prueba a través de la pantalla de la consola. Se utiliza el comando **nmap 192.168.X.X**

Figura 3. Escaneo de puertos con Nmap 5.51 por consola de comandos



Fuente: Terminal Kali Linux - Nmap

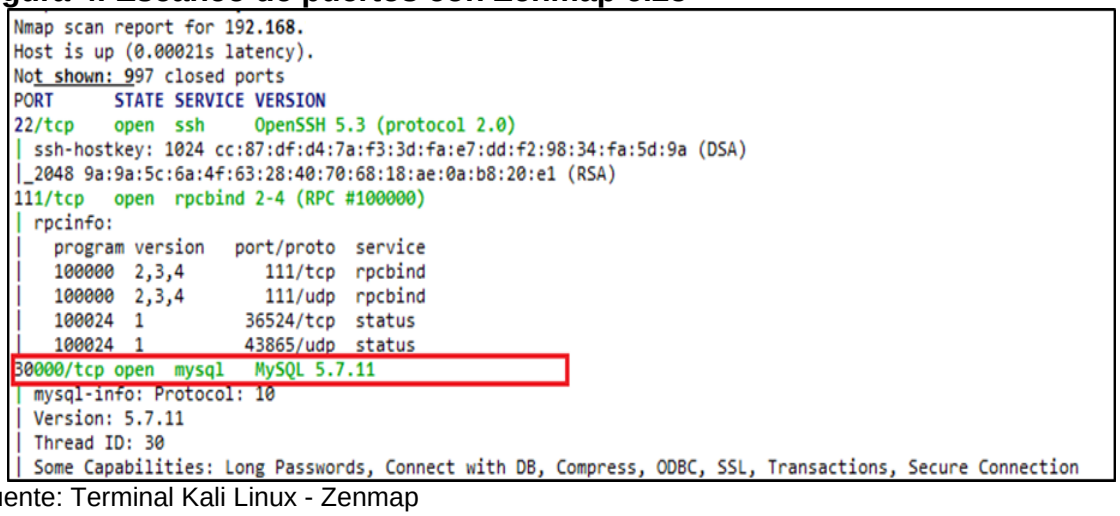
Conociendo los puertos abiertos se procedió a confirmar los servicios que se atendían por los puertos, para ello ejecuto un comando de Nmap para conocer el servicio que se ejecutaba por el puerto 30000 (Desconocido).

Para realizar un escaneo completo del puerto se empleó la herramienta *Zenmap*, y el comando:

nmap -T4 -A -v -Pn **192.168.29.98**

Una vez ejecutado el comando, se encontró que por el puerto 30000, se ejecuta un servicio de **Mysql versión 5.7.11** (ver figura 4).

Figura 4. Escaneo de puertos con Zenmap 6.25

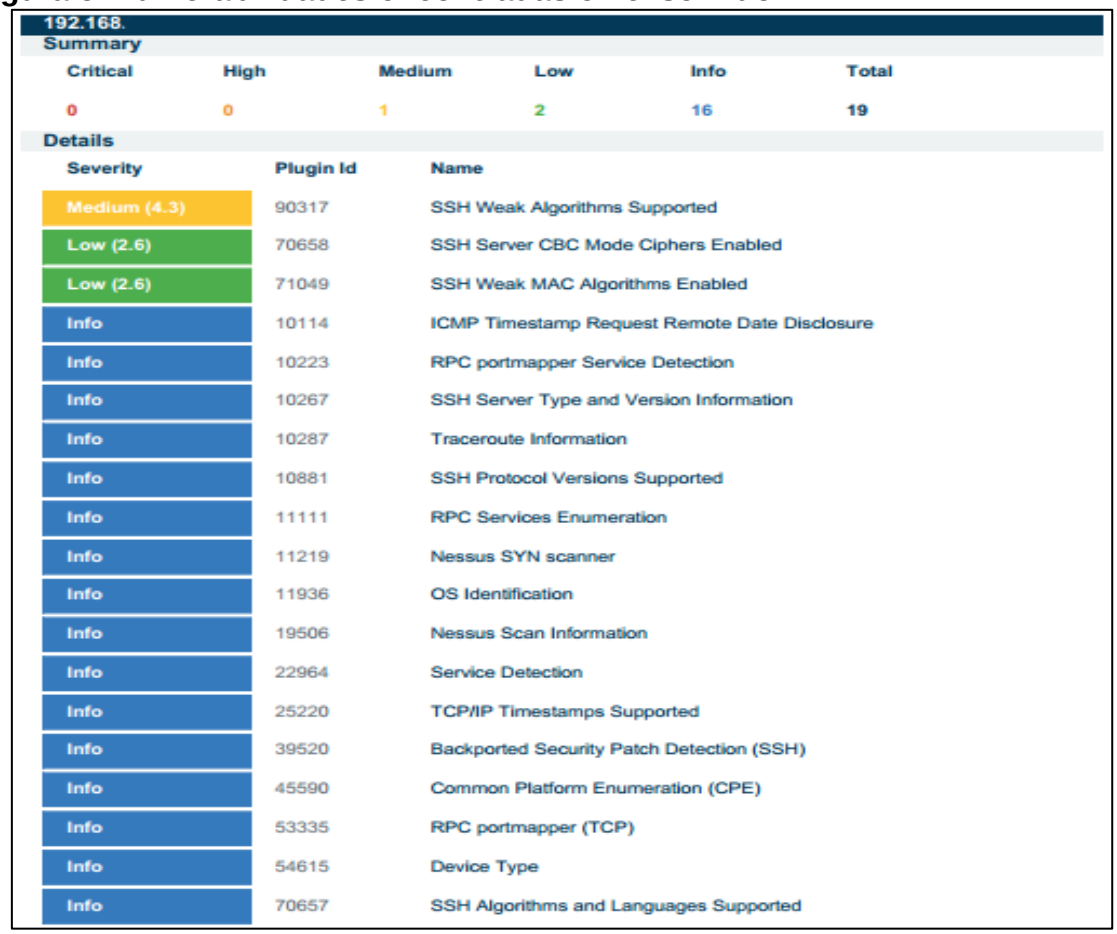


Fuente: Terminal Kali Linux - Zenmap

6.2.1. Análisis de vulnerabilidades del servidor 192.168.29.98. Una vulnerabilidad es un elemento de un sistema que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado. A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos[32].

Para identificar las vulnerabilidades del Servidor del Campus Virtual, se usó la versión 5.2.1 de la herramienta Nessus. El objetivo de la prueba es identificar las vulnerabilidades del servidor para luego explotarlas e intentar acceder a éste. En la figura 5 se puede ver un cuadro con las vulnerabilidades detectadas por la herramienta.

Figura 5. Vulnerabilidades encontradas en el servidor



192.168.

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Details

Severity	Plugin Id	Name
Medium (4.3)	90317	SSH Weak Algorithms Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

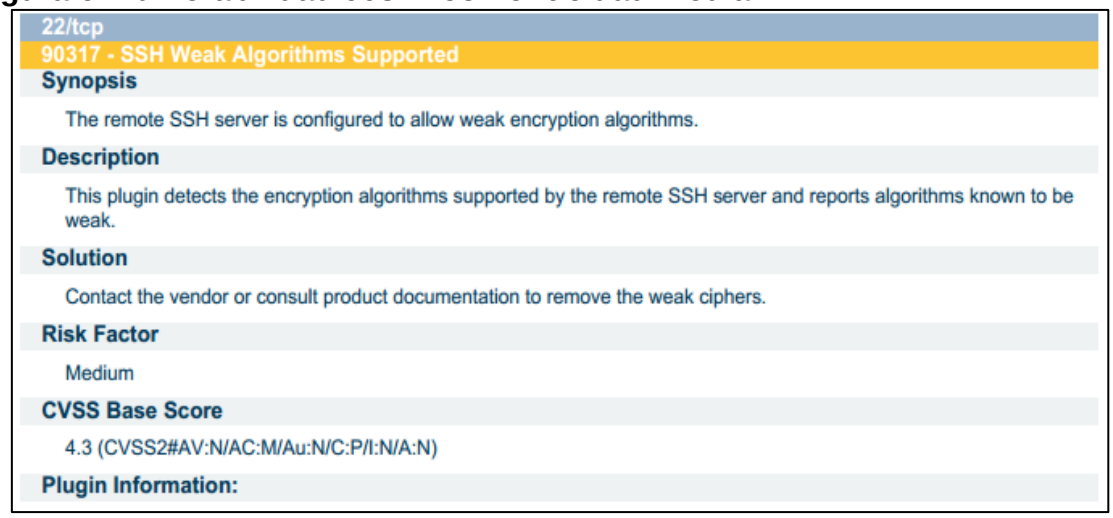
Fuente: Terminal Kali Linux - Nessus

[32] UNAM. Tutorial de Seguridad Informática - Amenazas y vulnerabilidades. [en línea] [Fecha de consulta: 13/05/2016] Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html.

A continuación se describen algunas de las vulnerabilidades encontradas:

- **Vulnerabilidad 90317 SSH Weak Algorithms Supported**. Se evidencia una vulnerabilidad de *criticidad media*, asociada con el puerto 22, servicio SSH; la cual permite el uso de algoritmos de cifrado débiles u obsoletos. La solución es configurar el servidor para que no permita estos algoritmos obsoletos de 128 o 256 bits. Ver detalles en figura 6.

Figura 6. Vulnerabilidad 90317 con criticidad media.

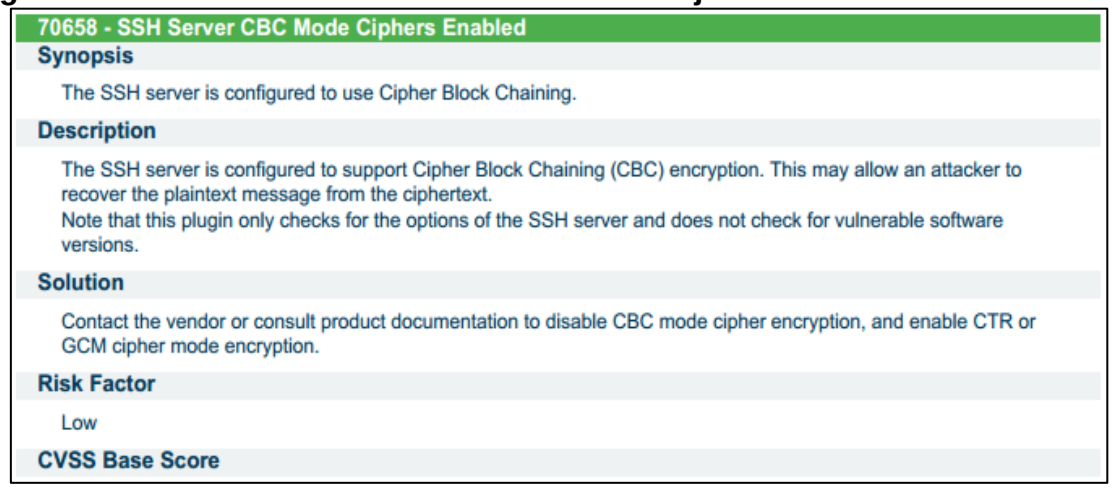


Fuente: Terminal Kali Linux - Nessus

- **Vulnerabilidad 70658 SSH Server CBC Mode Ciphers Enabled**. Se encuentra vulnerabilidad de criticidad baja asociada con el puerto 22, y el servicio SSH; la cual soporta el encadenamiento de bloques de cifrado (CBC, Cipher Block Chaining). Esta vulnerabilidad permite que un atacante recupere información en texto plano de un texto cifrado previamente, basado en la vulnerabilidad de algoritmos de cifrado obsoletos como (DES, 3DES, AES 128 ó *Rijndael*, AES 256, MD5, SHA1, etc.). Ver detalles técnicos de la vulnerabilidad en la figura 7.

Para solucionar esta vulnerabilidad, el administrador del servidor debe deshabilitar el modo CBC y habilitar el modo de cifrado GCM (Galois/Counter Mode).

Figura 7. Vulnerabilidad 70658 con criticidad baja.



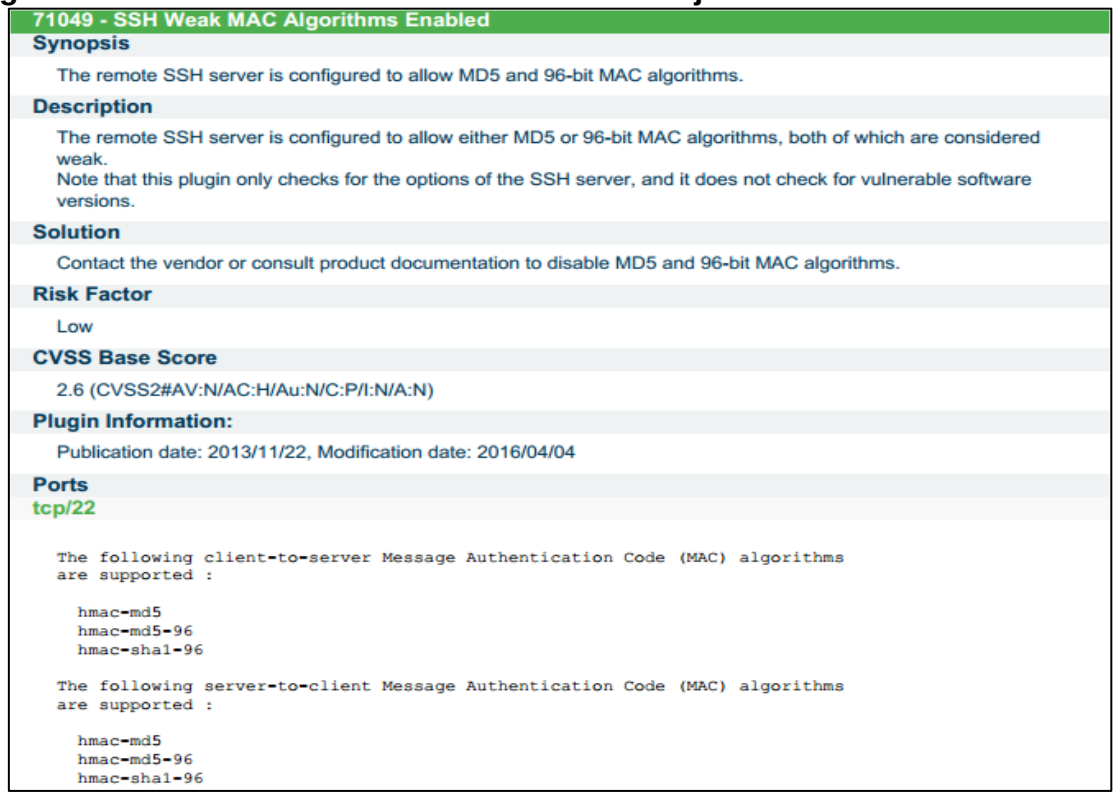
Fuente: Terminal Kali Linux - Nessus

- **Vulnerabilidad 71049 SSH Weak MAC Algorithms Enabled**[33]. El servidor SSH remoto está configurado para permitir ya sea MD5 o MAC algoritmos de 96 bits, los cuales se consideran débiles. Tenga en cuenta que este plugin sólo aplica para las opciones del servidor SSH, y no comprueba las versiones del software vulnerables. La vulnerabilidad es catalogada de criticidad baja. La solución a este inconveniente es desactivar MD5 y algoritmos MAC de 96 bits. En la figura 8 se pueden ver detalles técnicos de la vulnerabilidad.

- **Vulnerabilidad 10114 ICMP Timestamp Request Remote Date Disclosure**[34]. El host remoto responde a una solicitud de registro de tiempo. Esto le permite a un atacante conocer la fecha de reinicio de la máquina objetivo, lo que ayudar a un atacante remoto no autenticado, a “saltar” protocolos de autenticación de reinicio. El factor de riesgo de esta vulnerabilidad es nulo. La solución es filtrar las respuestas a solicitudes de registro de tiempo y las respuestas ICMP a solicitudes de registro de tiempo.

[33] TENABLE. Nessus Plugin. [en línea] [Fecha de consulta: 05/06/2016] Disponible en: https://www.tenable.com/plugins/index.php?view=single&id=71049.
[34] Ibid

Figura 8. Vulnerabilidad 71049 con criticidad baja.



Fuente: Terminal Kali Linux - Nessus

- **Vulnerabilidad 10223 RPC portmapper Service Detection**[35]. Indica que el mapeador de puertos RPC se está ejecutando en este puerto. El mapeador de puertos permite a alguien obtener el número de puerto de cada servicio RPC que se ejecuta en el host remoto. Esta vulnerabilidad no está ligada con factores de riesgo.

- **Vulnerabilidad 10267 SSH Server Type and Version Information**[36]. A través de esta vulnerabilidad es posible obtener información sobre el servidor SSH remoto, mediante el envío de una solicitud de autenticación vacía. No existe factor de riesgo asociado a esta vulnerabilidad.

- **Vulnerabilidad 10287 Traceroute Information**. Hace un traceroute a una máquina remota. No existe factor de riesgo asociado a esta vulnerabilidad.

[35] Ibid.
[36] Ibid

- **Vulnerabilidad 10881 SSH Protocol Versions Supported**. Este plugin determina las versiones del protocolo SSH soportadas en un ***daemon*** SSH remoto. No existe factor de riesgo asociado a esta vulnerabilidad.

También se encontraron otras vulnerabilidades como: 11219 Nessus SYN scanner, 22964 Service Detection, entre otras, las cuales no representaban riesgos para el sistema, por lo cual no se documentaron.

6.2.2. Vulnerabilidades asociadas con la versión del Open SSH Versión 5.3 usada por los administradores del servidor. En las tablas 7, 8 y 9, se describen las vulnerabilidades encontradas en la versión OpenSSH 5.3 usada en el servidor; éstas podrían llegar a ser explotadas por personal externo a la institución.

Tabla 7. CVE-2016-0778

CVE-2016-0778	
(1) ***roaming_read*** y (2) funciones ***roaming_write*** en ***roaming_common.c*** en el cliente de OpenSSH 5.x, 6.x, 7.x antes 7.1p2, cuando ciertos proxy y las opciones de desvío están habilitadas, no mantienen adecuadamente la conexión descriptores de archivos , que permite a los servidores remotos provocar una denegación de servicio (basado en heap desbordamiento de memoria) o posiblemente tener un impacto no especificado de otro mediante la solicitud de muchas expediciones.	
Tipo de vulnerabildiad	DoS por Desbordamiento
Impacto:	6.5
Acceso	Remoto
Autenticación	Sistema simple
Fecha de publicación:	**2016-01-14**

Fuente: Common Vulnerabilities and Exposures. Adaptado de http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2010-4478

Tabla 8. CVE-2014-1692

CVE-2014-1692	
La función ***hash_buffer*** en schnorr.c en OpenSSH a través de 6,4, cuando Makefile.inc se modifica para activar el protocolo J - PAKE, no inicializar ciertas estructuras de datos, lo que podría permitir que atacantes remotos provoquen una denegación de servicio (corrupción de memoria) o que tienen impacto no especificado a través de vectores que provocan una condición de error	
Tipo de vulnerabildiad	DOS por Desbordamiento de memoria
Impacto:	7.5
Acceso	Remoto
Autenticación	No requiere
Fecha de publicación:	**2014-01-29**

Fuente: Common Vulnerabilities and Exposures. Adaptado de http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2010-4478

Tabla 9. CVE-2010- 4478

CVE-2010-4478	
En OpenSSH 5.6 y anteriores, cuando J - PAKE está habilitada, no valida correctamente los parámetros públicos, lo que permite a atacantes remotos evitar la necesidad de conocimiento del secreto compartido y autenticándose con éxito, mediante el envío de los valores trabajados en cada ronda del protocolo.	
Tipo de vulnerabildiad	Por Contraseña
Impacto:	7.5
Acceso	Remoto
Autenticación	No requiere
Fecha de publicación:	**2010-12-29**

Fuente: Common Vulnerabilities and Exposures. Adaptado de http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2010-4478

6.2.3 EXPLOITS Encontrados. Al realizar el escaneo de puertos para el puerto 22, servicio SSH con versión Openssh 5.3 los exploits disponibles en Kali linux y ejecutando en comando search openssh 5.3 en metasploit, se hallaron los exploits que se ven en la figura 9. La descripciòn de los principales exploit se puede ver en la tabla 10.

Figura 9. Exploits para Openssh 5.3

```
msf > search openssh 5.3

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/scanner/http/apache_activemq_source_disclosure                normal     Apache ActiveMQ JSP Fil
es Source Disclosure
   auxiliary/scanner/http/apache_activemq_traversal                        normal     Apache ActiveMQ Directo
ry Traversal
   auxiliary/scanner/ssh/ssh_enumusers                                     normal     SSH Username Enumeratio
n
   exploit/aix/rpc_ttdbserverd_realpath                  2009-06-17       great      ToolTalk rpc.ttdbserver
d _tt_internal_realpath Buffer Overflow (AIX)
   exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      FreeBSD Telnet Service
Encryption Key ID Buffer Overflow
   exploit/multi/http/op5_license                        2012-01-05       excellent  OP5 license.php Remote
Command Execution
   exploit/multi/http/op5_welcome                        2012-01-05       excellent  OP5 welcome Remote Comm
and Execution
   exploit/multi/http/php_cgi_arg_injection              2012-05-03       excellent  PHP CGI Argument Inject
ion
   exploit/multi/http/vtiger_php_exec                    2013-10-30       excellent  vTigerCRM v5.4.0/v5.3.0
 Authenticated Remote Code Execution
   exploit/osx/arkeia/type77                             2005-02-18       average    Arkeia Backup Client Ty
pe 77 Overflow (Mac OS X)
   exploit/unix/http/lifesize_room                       2011-07-13       excellent  LifeSize Room Command I
njection
   exploit/unix/webapp/tikiwiki_unserialize_exec         2012-07-04       excellent  Tiki Wiki unserialize()
 PHP Code Execution
   exploit/unix/webapp/wp_infusionsoft_upload            2014-09-25       excellent  Wordpress InfusionSoft
Upload Vulnerability
   exploit/windows/arkeia/type77                         2005-02-18       good       Arkeia Backup Client Ty
pe 77 Overflow (Win32)
   exploit/windows/browser/honeywell_tema_exec           2011-10-20       excellent  Honeywell Tema Remote I
nstaller ActiveX Remote Code Execution
   exploit/windows/browser/inotes_dwa85w_bof             2012-06-01       normal     IBM Lotus iNotes dwa85W
 ActiveX Buffer Overflow
   exploit/windows/browser/notes_handler_cmdinject       2012-06-18       excellent  IBM Lotus Notes Client
URL Handler Command Injection
   exploit/windows/browser/novelliprint_datetime         2009-12-08       great      Novell iPrint Client Ac
tiveX Control Date/Time Buffer Overflow
   exploit/windows/browser/novelliprint_target_frame     2009-12-08       great      Novell iPrint Client Ac
tiveX Control target-frame Buffer Overflow
   exploit/windows/browser/softartisans_getdrivename     2008-08-25       normal     SoftArtisans XFile File
Manager ActiveX Control Buffer Overflow
   exploit/windows/browser/tom_sawyer_tsgetx71ex552      2011-05-03       normal     Tom Sawyer Software GET
 Extension Factory Remote Code Execution
   exploit/windows/emc/replication_manager_exec          2011-02-07       great      EMC Replication Manager
 Command Execution
   exploit/windows/fileformat/scadaphone_zip             2011-09-12       good       ScadaTEC ScadaPhone Sta
ck Buffer Overflow
   exploit/windows/ftp/filewrangler_list_reply           2010-10-12       good       FileWrangler 5.30 Stack
 Buffer Overflow
   exploit/windows/games/racer_503beta5                  2008-08-10       great      Racer v0.5.3 Beta 5 Buf
fer Overflow
   exploit/windows/http/efs_fmws_userid_bof              2014-05-20       normal     Easy File Management We
b Server Stack Buffer Overflow
   exploit/windows/http/ibm_tsm_cad_header               2007-09-24       good       IBM Tivoli Storage Mana
ger Express CAD Service Buffer Overflow
   exploit/windows/isapi/rsa_webagent_redirect           2005-10-21       good       Microsoft IIS ISAPI RSA
 WebAgent Redirect Overflow
   exploit/windows/local/trusted_service_path            2001-10-25       excellent  Windows Service Trusted
 Path Privilege Escalation
   exploit/windows/misc/fb_svc_attach                    2007-10-03       average    Firebird Relational Dat
abase SVC_attach() Buffer Overflow
   exploit/windows/misc/ibm_tsm_cad_ping                 2009-11-04       good       IBM Tivoli Storage Mana
ger Express CAD Service Buffer Overflow
   exploit/windows/misc/ibm_tsm_rca_dicugetidentify      2009-11-04       great      IBM Tivoli Storage Mana
ger Express RCA Service Buffer Overflow
   post/multi/gather/ssh_creds                                            normal     Multi Gather OpenSSH PK
  Credentials Collection
```

Fuente: Pantalla programa Openssh 5.3

Tabla 10. Descripción de exploit de Openssh 5.3

Exploit	Confiabilidad	Descripción
Exploit/windows/http/efs_fmws_userid_bof	Normal	Fácil gestión de archivos v4.0 y v5.3. Servidor Web contiene una condición de desbordamiento de pila que se desencadena como entrada proporcionada por el usuario. No se valida correctamente al manipular la cookie de identificación de usuario. Esto puede permitir a un atacante remoto ejecutar código arbitrario.
Exploit/Windows/browser/notes_handler_cmdinject	Excelente	Aprovecha una vulnerabilidad de inyección de comandos en el controlador de URL para el cliente de IBM Lotus Notes < = 8.5.3. El manejador registrado puede ser objeto de abuso con una nota especialmente diseñados: //URL para ejecutar comandos arbitrarios con argumentos también arbitrarios. Este módulo ha sido probado con éxito en Windows XP SP3 con IE8, Google Chrome 23.0.1271.97 m e IBM Lotus Notes Client 8.5.2.
Exploit/Windows/emc/replication_manager_exec	Muy Bueno	Aprovecha una vulnerabilidad de inyección de comandos remotos en el cliente de EMC Replication Manager (irccd.exe). Mediante el envío de un mensaje especialmente diseñado. Invocando la función RunProgram un atacante puede ser capaz de ejecutar código arbitrario con privilegios de SYSTEM. Los productos afectados son EMC Replication Manager < 5,3. Este módulo ha sido probado con éxito en contra de EMC Replication Manager 5.2.1 en XP / W2003. EMC NetWorker Module para aplicaciones de Microsoft 2.1 y 2.2 pueden ser vulnerables también.
Exploit/Windows/arkeia/type77	Bueno	Aprovecha un desbordamiento de pila en el cliente de la copia de seguridad Arkeia para la plataforma Windows. Esta vulnerabilidad afecta a todas las versiones hasta e incluyendo 5.3.3.
Exploit/multi/http/vtiger_php_exec	Excelente	vtiger CRM permite a un usuario autenticado subir archivos para integrarlos dentro de los documentos. Debido a los privilegios suficientes sobre la carpeta ' ' archivos cargados, un atacante puede cargar un script PHP y ejecutar código PHP arbitrario en forma remota.
Exploit/unix/http/lifesize_room	Excelente	Este módulo explota un recurso vulnerable en las versiones de LifeSize Room 3.5.3 y 4.7.18 para inyectar commmands OS.
Post/multi/gather/ssh_creds	Normal	En este módulo se recogerá el contenido de directorios .ssh de todos los usuarios en la máquina objetivo. Este módulo se basa en gran medida en firefox_creds.rb.
Exploit/Windows/misc/fb_svc_attach	Regular	Este módulo se aprovecha de un desbordamiento de pila en Borland InterBase mediante el envío de un servicio especialmente diseñado para adjuntar la solicitud.
Exploit/freebsd/telnet/telnet_encrypt_keyid	Muy Bueno	Este módulo explota un desbordamiento de búfer en el manejador de opción de cifrado del servicio telnet FreeBSD.

Fuente: Autor del proyecto

Del mismo modo, según el escaneo de puertos, para el puerto 30000, el cual se identificó con un servicio Mysql con versión 5.7.11, los exploits disponibles se pueden ver en la tabla que se ve en la figura 10 y la descripción de los principales exploits se ve en la tabla 11.

Del mismo modo, según el escaneo de puertos, para el puerto 30000, el cual se identificó con un servicio Mysql con versión 5.7.11, los exploits disponibles se pueden ver en la tabla que se ve en la figura 10 y la descripción de los principales exploits se ve en la tabla 11.

Figura 10. Exploits para Mysql

```
msf > search mysql

Matching Modules
================

   Name                                                Disclosure Date  Rank       Description
   ----                                                ---------------  ----       -----------
   auxiliary/admin/http/manageengine_pmp_privesc       2014-11-08       normal     ManageEngine Password Manag
er SQLAdvancedALSearchResult.cc Pro SQL Injection
   auxiliary/admin/http/rails_devise_pass_reset        2013-01-28       normal     Ruby on Rails Devise Authen
tication Password Reset
   auxiliary/admin/mysql/mysql_enum                                     normal     MySQL Enumeration Module
   auxiliary/admin/mysql/mysql_sql                                      normal     MySQL SQL Generic Query
   auxiliary/admin/tikiwiki/tikidblib                  2006-11-01       normal     TikiWiki Information Disclo
sure
   auxiliary/analyze/jtr_mysql_fast                                     normal     John the Ripper MySQL Passw
ord Cracker (Fast Mode)
   auxiliary/gather/joomla_weblinks_sqli               2014-03-02       normal     Joomla weblinks-categories
Unauthenticated SQL Injection Arbitrary File Read
   auxiliary/scanner/mysql/mysql_authbypass_hashdump   2012-06-09       normal     MySQL Authentication Bypass
 Password Dump
   auxiliary/scanner/mysql/mysql_file_enum                              normal     MYSQL File/Directory Enumer
ator
   auxiliary/scanner/mysql/mysql_hashdump                               normal     MYSQL Password Hashdump
   auxiliary/scanner/mysql/mysql_login                                  normal     MySQL Login Utility
   auxiliary/scanner/mysql/mysql_schemadump                             normal     MYSQL Schema Dump
   auxiliary/scanner/mysql/mysql_version                                normal     MySQL Server Version Enumer
ation
   auxiliary/server/capture/mysql                                       normal     Authentication Capture: MyS
QL
   exploit/linux/mysql/mysql_yassl_getname             2010-01-25       good       MySQL yaSSL CertDecoder::Ge
tName Buffer Overflow
   exploit/linux/mysql/mysql_yassl_hello               2008-01-04       good       MySQL yaSSL SSL Hello Messa
ge Buffer Overflow
   exploit/multi/http/manage_engine_dc_pmp_sqli        2014-06-08       excellent  ManageEngine Desktop Centra
l / Password Manager LinkViewFetchServlet.dat SQL Injection
   exploit/unix/webapp/kimai_sqli                      2013-05-21       average    Kimai v0.9.2 'db_restore.ph
p' SQL Injection
   exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     WordPress Plugin Google Doc
ument Embedder Arbitrary File Disclosure
   exploit/windows/mysql/mysql_mof                     2012-12-01       excellent  Oracle MySQL for Microsoft
Windows MOF Execution
   exploit/windows/mysql/mysql_payload                 2009-01-16       excellent  Oracle MySQL for Microsoft
Windows Payload Execution
   exploit/windows/mysql/mysql_start_up                2012-12-01       excellent  Oracle MySQL for Microsoft
Windows FILE Privilege Abuse
   exploit/windows/mysql/mysql_yassl_hello             2008-01-04       average    MySQL yaSSL SSL Hello Messa
ge Buffer Overflow
   exploit/windows/mysql/scrutinizer_upload_exec       2012-07-27       excellent  Plixer Scrutinizer NetFlow
and sFlow Analyzer 9 Default MySQL Credential
   post/linux/gather/enum_configs                                       normal     Linux Gather Configurations
   post/linux/gather/enum_users_history                                 normal     Linux Gather User History
   post/multi/manage/dbvis_add_db_admin                                 normal     Multi Manage DbVisualizer A
dd Db Admin
```

Fuente: Pantalla programa Openssh 5.3

Tabla 11. Descripción de exploit de MySql

Exploit	Confiabilidad	Descripción
Exploit/linux/mysql/mysql_yassl_getname	Bueno	Aprovecha un desbordamiento de pila en el ya SSL (1.9.8 y anteriores) aplicación incluido con MySQL. Mediante el envío de un certificado de cliente especialmente diseñado. Un atacante puede ejecutar código arbitrario. Esta vulnerabilidad está presente dentro de la función CertDecoder :: GetName dentro "taocrypt / src / asn.cpp". Sin embargo, el búfer de pila que se escribe existe dentro del marco de pila de una función madre. NOTA: Esta vulnerabilidad requiere una configuración no predeterminada. En primer lugar, el atacante debe ser capaz de pasar la autenticación basada en host. A continuación, el servidor debe estar configurado para escuchar en una interfaz de red accesible. Por último, el servidor debe estar configurado manualmente para utilizar SSL. El binario a partir de la versión 5.5.0-m2 fue construida con / GS y / SafeSEH. Durante las pruebas en Windows XP SP3, estas protecciones tenido éxito en evitar la explotación.
Exploit/linux/mysql/mysql_yassl_hello	Bueno	Este módulo se aprovecha de una desbordamiento de pila en el ya SSL (1.7.5 y anteriores) aplicación incluido con MySQL < = 6,0. Mediante el envío de un paquete de saludo especialmente diseñado, un atacante puede ser capaz de ejecutar código arbitrario.
Exploit/multi/http/manage_engine_dc_pmp_sqli	Excelente	Aprovecha una inyección SQL ciega sin autenticación en LinkViewFetchServlet, que se expone en ManageEngine Desktop Central V7 construcción de 70200 a 90033 v9 construir y Password Manager Pro v6 build 6500 para construir v7 7002 (incluyendo las versiones MSP). La inyección SQL se puede utilizar para lograr la ejecución de código remoto como del sistema en Windows o como el usuario en Linux. En este módulo se explota tanto PostgreSQL como en MySQL. La inyección sólo es explotable a través de una solicitud GET, lo que significa que la carga útil tiene que ser enviado en trozos más pequeños de 8000 caracteres (limitación de tamaño URL).
Exploit/unix/webapp/kimai_sqli	Promedio	Aprovecha una vulnerabilidad de inyección SQL en Kimai versión 0.9.2.x. El archivo 'db_restore.php' permite a los usuarios no autenticados para ejecutar consultas SQL de su elección. Este módulo escribe una carga útil de PHP en el disco si se cumplen las siguientes condiciones: La configuración de PHP debe tener ' ' display_errors habilitadas, Kimai debe estar configurado para utilizar una base de datos MySQL se ejecuta en el servidor local; y el usuario MySQL debe tener permiso de escritura en el directorio de la Kimai "temporal".
Exploit/Windows/mysql/mysql_mof	Excelente	Este módulo aprovecha un problema de mala configuración de privilegios de archivos de Windows específicamente en contra de los servidores MySQL (debido al uso de un archivo MOF). Esto puede dar lugar a la ejecución de código arbitrario en el contexto del SISTEMA. Este módulo requiere una cuenta válida de MySQL en el equipo.

Exploit	Confiabilidad	Descripción
Exploit/Windows/mysql/mysql_payload	Excelente	Crea y habilita una UDF de encargo (función definida por el usuario) en el host de destino a través de la instrucción SELECT... en el método de la inyección DUMPFILE binario. Por defecto instalaciones de Microsoft Windows de MySQL (= < 5.5.9), los permisos de directorio de escritura no se hacen cumplir, y el servicio MySQL se ejecuta como LocalSystem. NOTA: En este módulo se dejará un ejecutable de carga útil del sistema de destino cuando se termina el ataque, así como la DLL de UDF, y será definir o redefinir las funciones ( ) sys_eval () y sys_exec.
Exploit/Windows/mysql/mysql_Start_up	Excelente	Aprovecha un problema de mala configuración de privilegios de archivos de Windows específicamente en contra de los servidores MySQL. Este módulo abusa del privilegio archivo para escribir una carga útil para todos los usuarios de Microsoft Start Up directorio que ejecutará cada vez que un usuario inicie sesión. El valor predeterminado Todos los usuarios comienzan a este directorio utilizado por el módulo está presente en Windows 7.
Exploit/Windows/mysql/mysql_yassl_hello	Promedio	Aprovecha un desbordamiento de pila en el ya SSL (1.7.5 y anteriores) aplicación incluido con MySQL < = 6,0. Mediante el envío de un paquete de saludo especialmente diseñado, un atacante puede ser capaz de ejecutar código arbitrario.
Exploit/Windows/mysql/scrutinizer_upload_exec	Excelente	Esto explota una configuración insegura que se encuentra en Scrutinizer NetFlow & sFlow Analyzer. Por defecto, el software se instala una contraseña por defecto en MySQL, y se une al servicio de "0.0.0.0". Esto permite a cualquier usuario remoto para iniciar sesión en MySQL, y luego ganar ejecución remota de código arbitrario en el contexto del "sistema". Ejemplos de credenciales predeterminadas incluyen: ' escrutador: admin', y ' scrutremote: admin'.

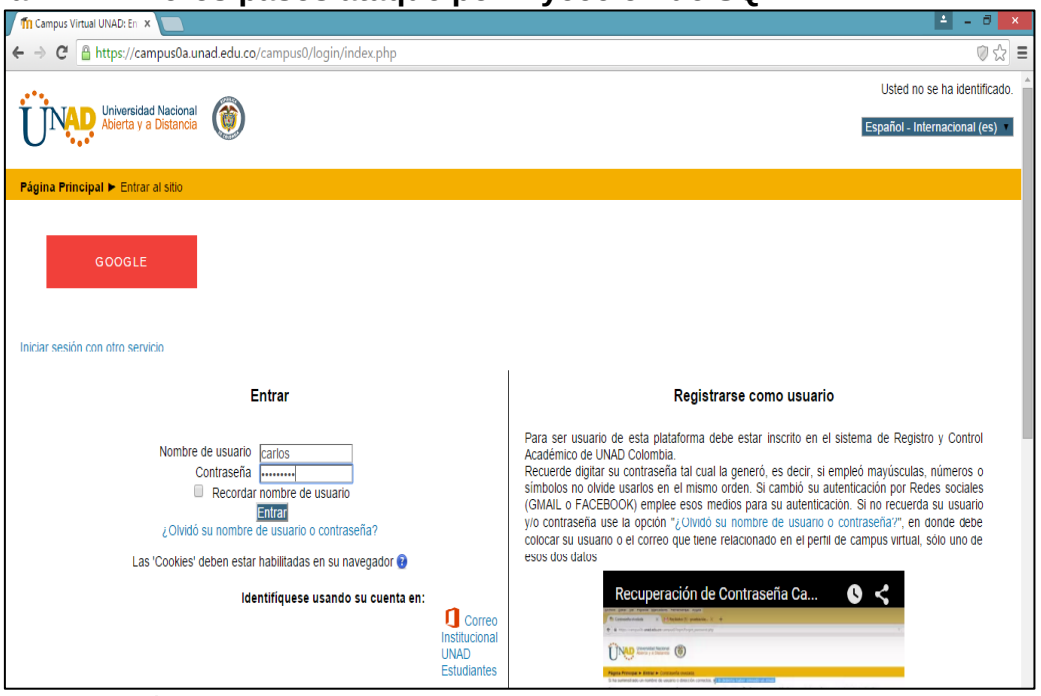
Fuente: Autor del proyecto

6.3 PRUEBAS DE ATAQUE SQL INJECTION

Para verificar si la página era vulnerable a inyección SQL, se realizó el siguiente procedimiento: Usando el Usuario: carlos y la contraseña: 'or '1'='1 (ver figura 11).

Mediante este proceso se verifica si es vulnerable o no. Si arroja un error, la base de datos es segura, de otra manera este código SQL permitiría el acceso al sistema con el primer usuario que esté en tabla de Usuarios

Figura 11. Primeros pasos ataque por inyección de SQL



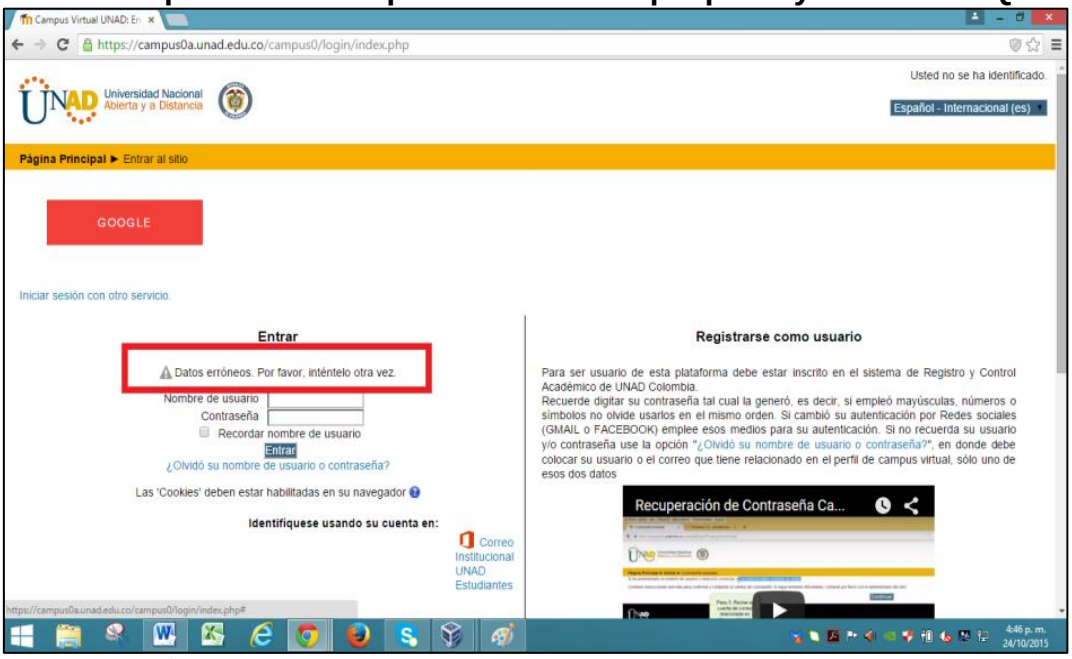
Fuente: Pantalla página web campus virtual Unad.

Al ejecutar el ataque el sitio respondió con un mensaje de DATOS ERRÓNEOS (Ver figura 12), lo cual significa que la base es segura. Revisando la seguridad se encontró que en la UNAD los datos no se manejan por GET, sino por POST, lo cual contrarresta esa vulnerabilidad.

La prueba se realizó con el programa Sqlmap ejecutado desde Kali linux, y usando el siguiente código:

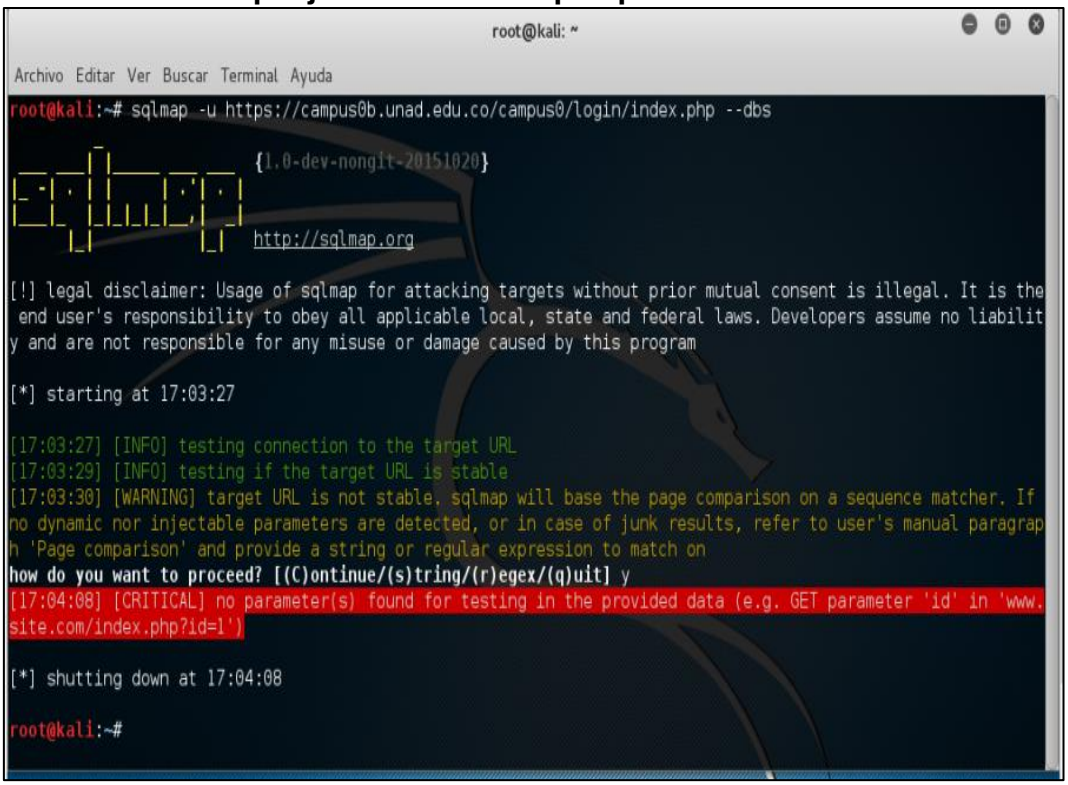
Sqlmap -u https://campus0a.unad.edu.co/campus0/login/index.php --dbs, en la figura 13 se muestra la información obtenida:

Figura 12. Respuesta de campus virtual al ataque por inyección de SQL



Fuente: Pantalla página web campus virtual Unad.

Figura 13. Prueba Sql Injection desde Sqlmap

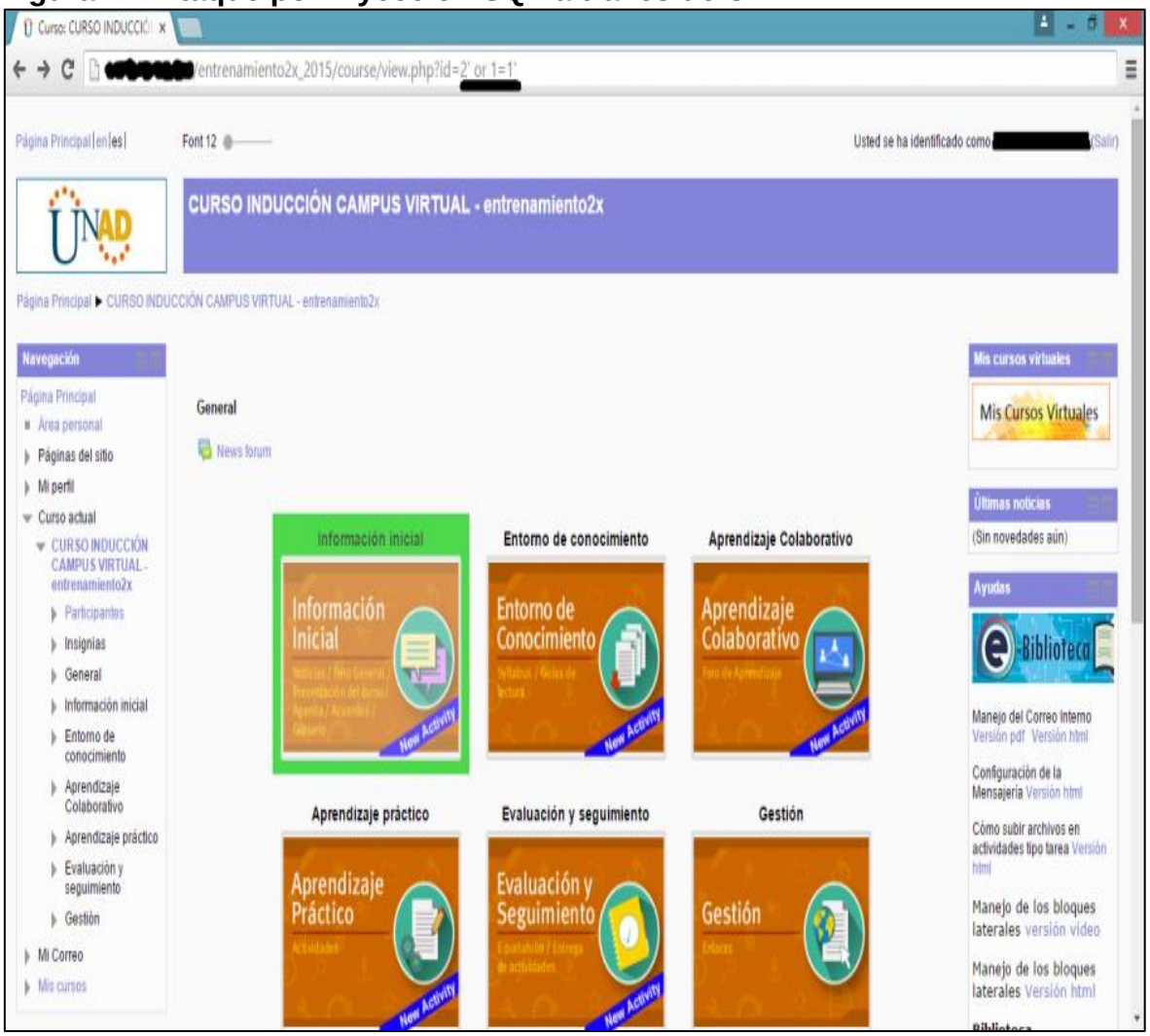


Fuente: Pantalla programa Sqlmap.

La consulta arrojó un error crítico en el cual hace mención de no encontrar un parámetro que funcione para detectar la vulnerabilidad en la página, debe tener una variable tipo GET como el parámetro id como se muestra en la página web que da como ejemplo: www.site.com/index.php?id=1

Otro ataque por inyección realizado es ingresando a la plataforma de la página como tal y digitando código sql en la URL (ver figura 14):

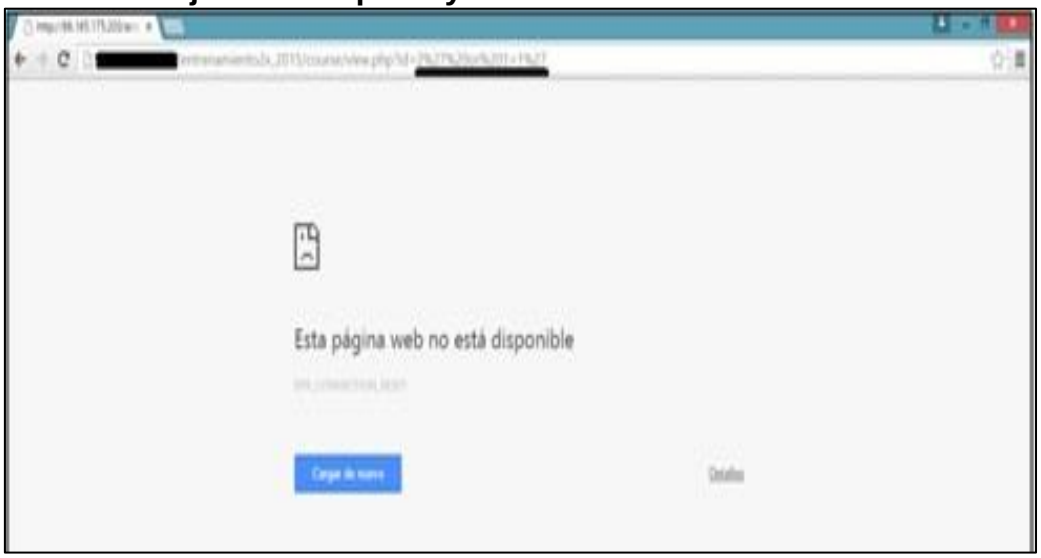
Figura 14. Ataque por Inyección SQL a través de URL



Fuente: Pantalla Campus Virtual UNAD.

Como resultado la página arroja error y no da resultados (ver figura 15).

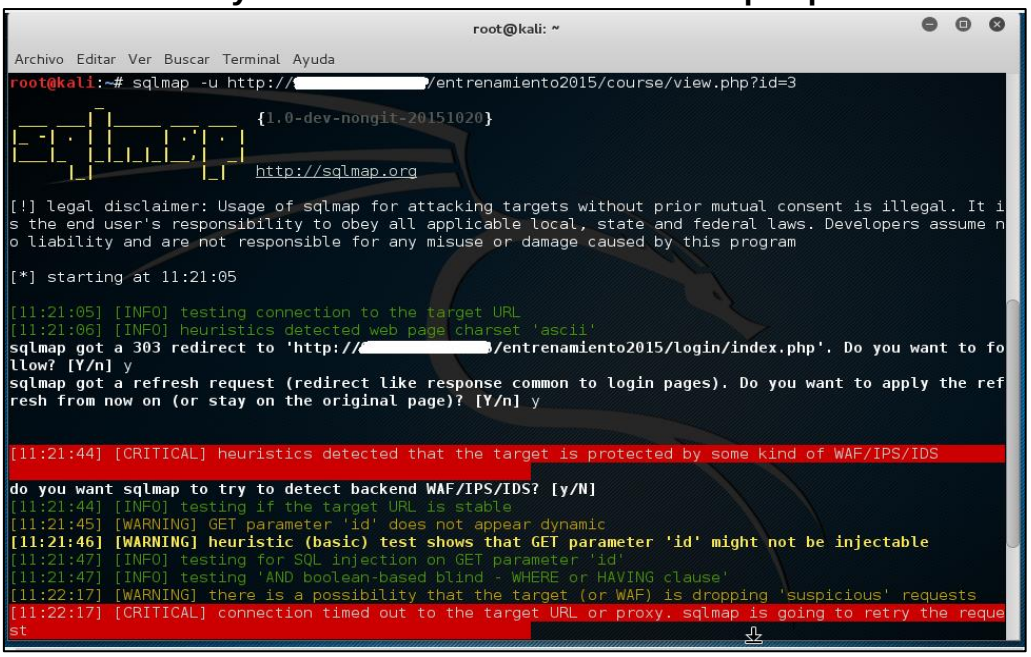
Figura 15. Mensaje de error por inyección a través de URL



Fuente: Pantalla Sitio Web Campus Virtual UNAD

Luego se ingresó la información de la URL a la herramienta Sqlmap como se puede ver en la figura 16.

Figura 16. Prueba inyección a través de URL desde Sqlmap



Fuente: Pantalla Herramienta Sqlmap

Lo primero que informa ***sqlmap*** es que al ingresar se redirecciona a otra URL y pregunta que si se quiere seguir con el proceso, a lo cual se digita “Y” para

informar Si. El siguiente mensaje que se muestra indica que se quiere refrescar la página, esto debido a la página de inicio de sesión, e indica si se quiere aplicar actualización o quedarse en la página actual. Se informa que si se desea aplicar.

Posteriormente el programa arroja un error donde informa que existe protección por algún tipo de WAF/IPS/IDS. A continuación pregunta: ¿usted desea que ***sqlmap*** trate de detectar backend WAF/IPS/IDS?. Se le indica que si y el programa continua el escaneo. Luego de lo anterior, el programa realiza una verificación e informa que la variable ID podría ser no inyectable, finalmente arroja un aviso critico donde no tiene respuesta por conexión.

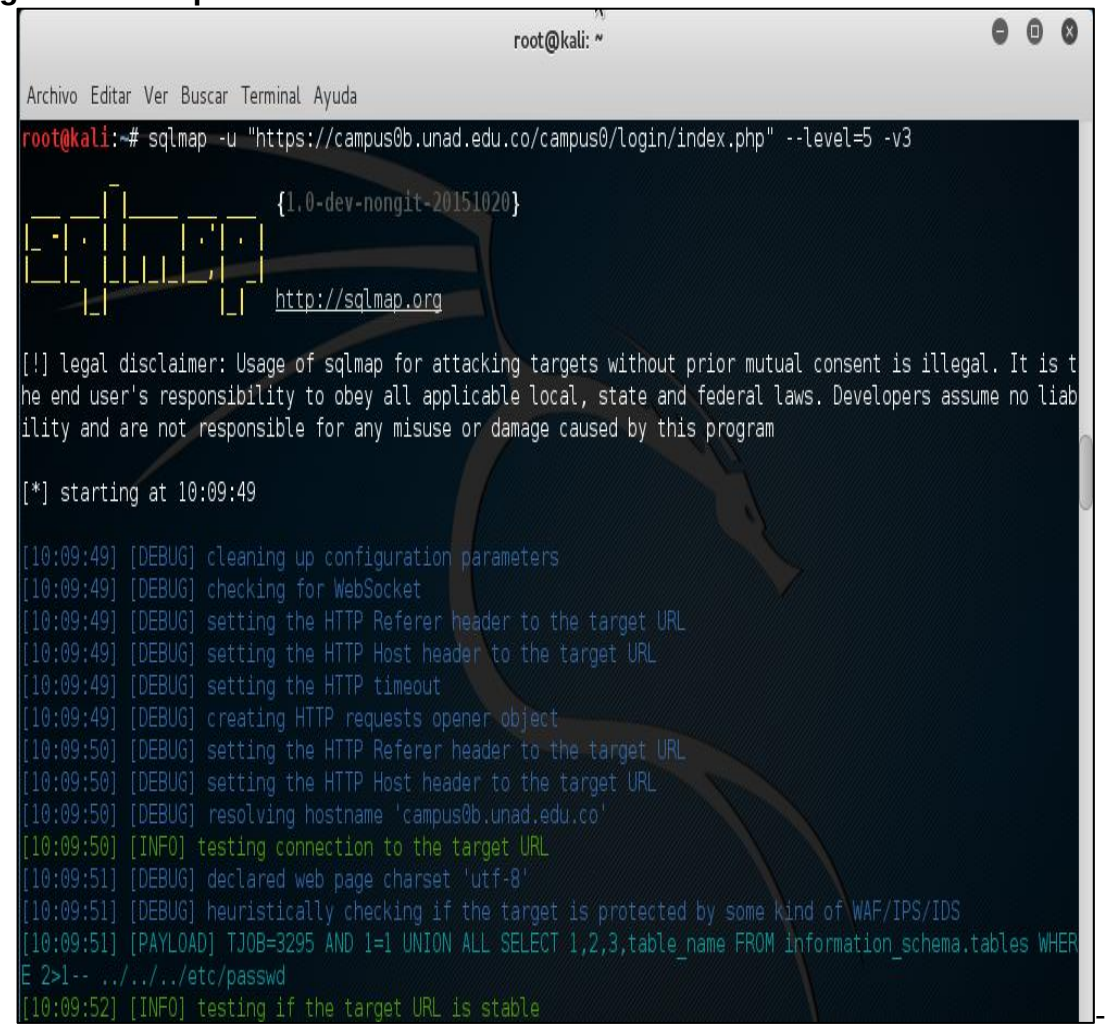
Con las anteriores pruebas se comprueba que la página tiene protección ante los ataques con Inyección de SQL, sin embargo para evitar que una web sea vulnerada con ***sql injection*** es necesario hacer lo siguiente:

- Tener un adecuado filtrado de las variables en las aplicaciones WEB.
- Aplicar mecanismos de detección de escaneo y ataques ***sql injection*** (usando IPS/IDS (sistema de prevención y detección de intrusos)).
- Evitar mostrar información específica de la base de datos.

Luego de realizar la anterior prueba y observar que no dio ningún resultado, se realizó un ataque a diccionario usando el parámetro "--level=5 –v3", es decir, aumentando al máximo nivel de búsqueda de vulnerabilidades. En otras palabras, el programa realizará constantes consultas con cada una de las variables en la URL y si encuentra una vulnerabilidad arrojará la información correspondiente y permitirá ingresar a la base de datos.

La consulta se realizó a través de ***sqlmap*** usando el siguiente código:
Sqlmap –u "url" –level=5 –v3 (ver figura 17)

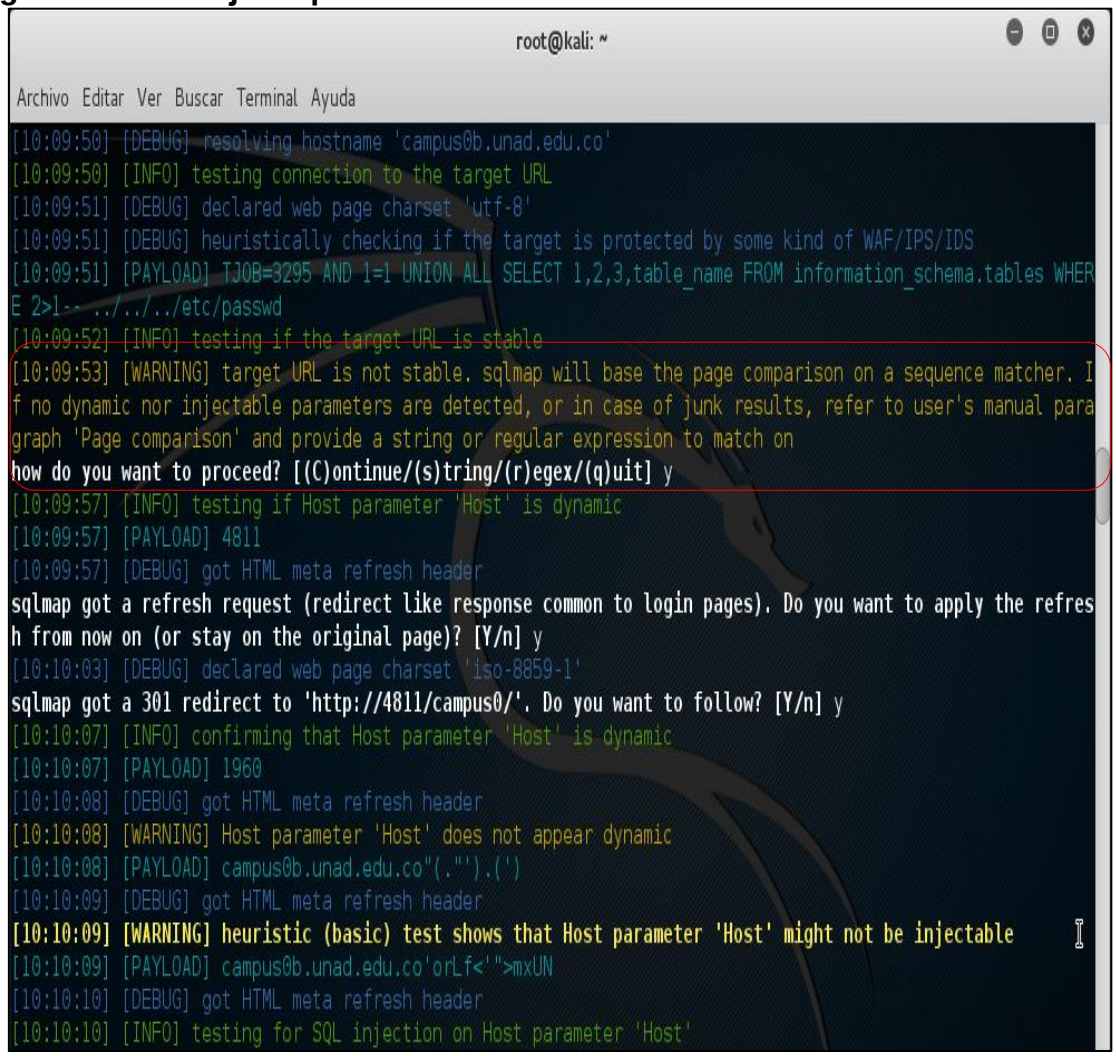
Figura 17. Ataque a diccionario de la base de datos



Fuente: Pantalla programa Sqlmap

Luego de ser ejecutado el escaneo en ***sqlmap*** arrojo un mensaje de precaución donde informa que la url insertada no era estable e informa que si no da resultados deseados, se sebe consultar el manual de usuarios de ***sqlmap.*** A continuación pregunta si desea proceder. Lo anterior se puede ver en la figura 18.

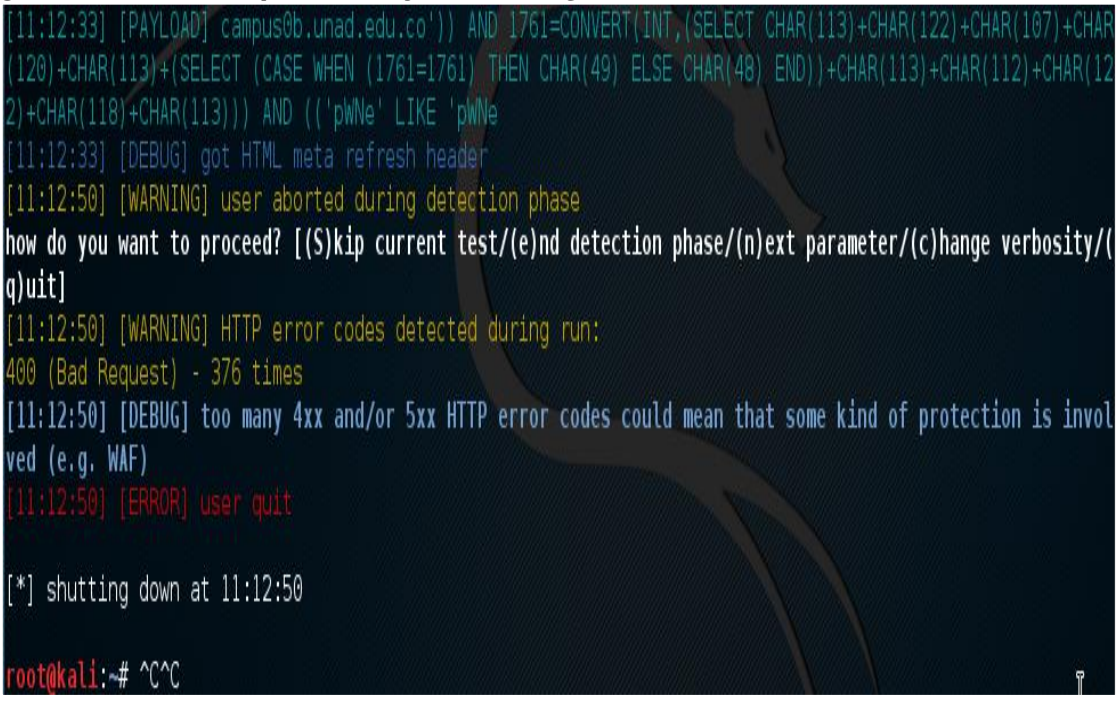
Figura 18. Mensaje se precaución “URL no estable“



Fuente: Pantalla programa Sqlmap

Después de una hora, tres minutos y un segundo de ejecución, ***sqlmap*** arrojo un error donde informa; el usuario abortó durante la búsqueda o posiblemente fue detectado por un WAF (herramienta para proteger los servidores web de los ataques informáticos). En automático dio por terminado el proceso como se ve en la figura 19.

Figura 19. Final de prueba inyección SQL.



Fuente: Pantalla programa Sqlmap

6.4. PRUEBAS CON EXPLOITS

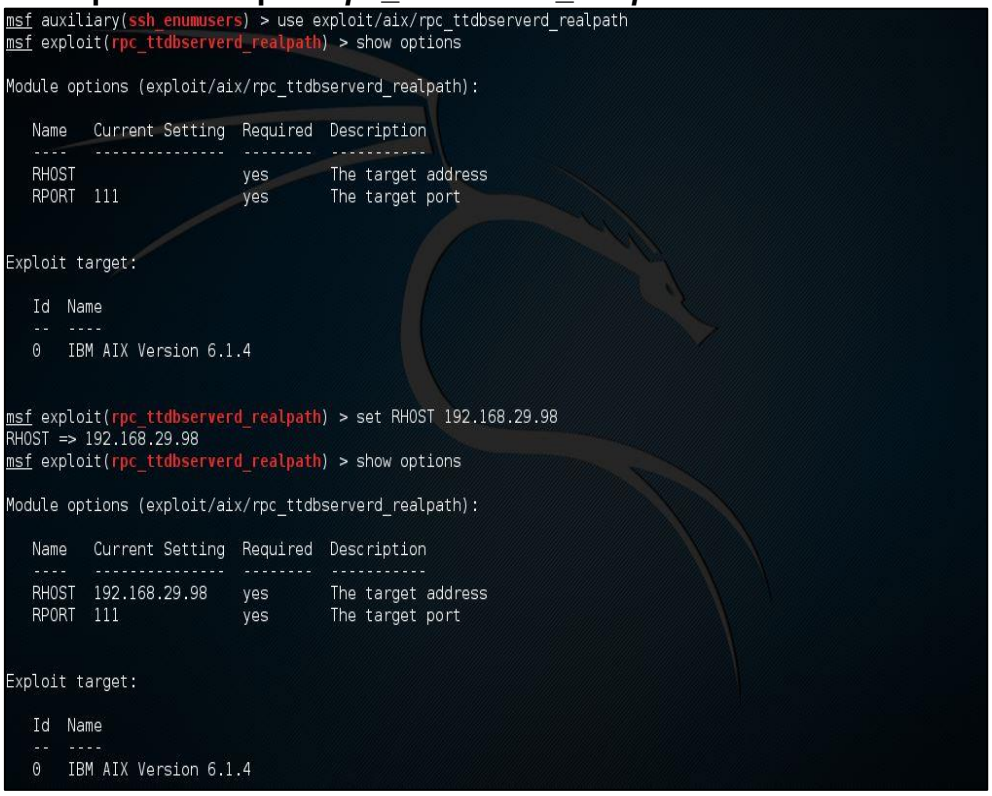
Un exploit es un fragmento de software o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

En este trabajo se realizaron pruebas con exploit disponibles para OpenSSh y Mysql. A continuación se detallan las pruebas y exploits usados.

6.4.1 OpenSSH. En la ejecución de las pruebas para OpenSSh se usaron cuatro tipos de e*xploits.* Los detalles de cada prueba se presentan a continuación.

- ***rpc_ttdserverd_realpatch.*** Hace parte de las opciones de exploits del Openssh 5.3. Su función es tratar de vulnerar el puerto 111, con el fin de aprovechar una vulnerabilidad de desbordamiento de búfer en ***_tt_internal_realpath,*** función del servidor de base de datos ToolTalk (rpc.ttdbserverd). En la figura 20 se pueden ver las opciones de este exploit.

Figura 20. Opciones exploit *rpc_ttdserverd_realpatch*



Fuente: Pantalla exploit *rpc_ttdserverd_realpatch*

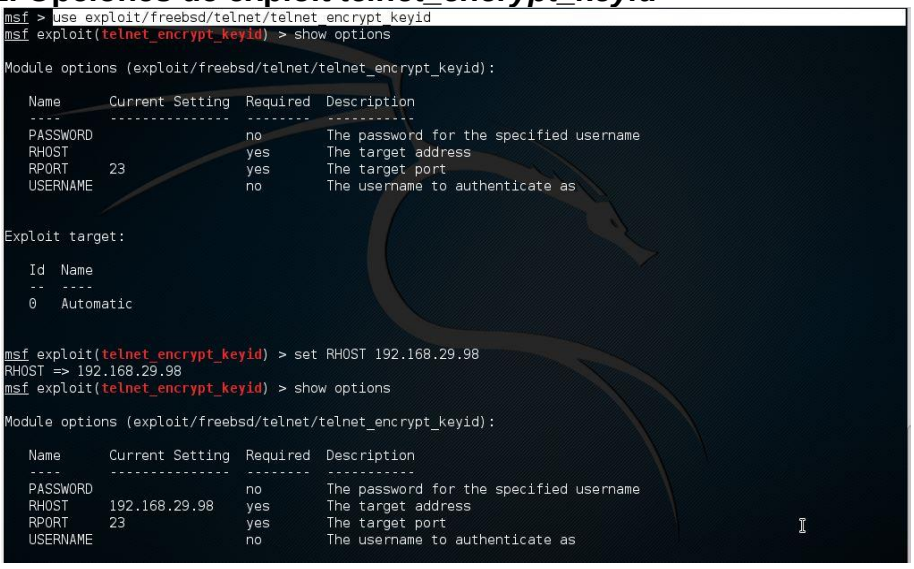
Una vez ejecutado el exploit, se observó que la conexión fue rechazada porque el puerto 111 no está abierto en el servidor. Ver figura 21.

Figura 21. Conexión rechazada de exploit *rpc_ttdserverd_realpatch*

Fuente: Pantalla exploit *rpc_ttdserverd_realpatch*

- ***telnet_encrypt_keyid.*** Hace parte de las opciones de exploits del Openssh 5.3; su función es intentar vulnerar el puerto 23, con el fin de explotar un desbordamiento de búfer en el manejador de opción de cifrado del servicio telnet FreeBSD (ver figura 22).

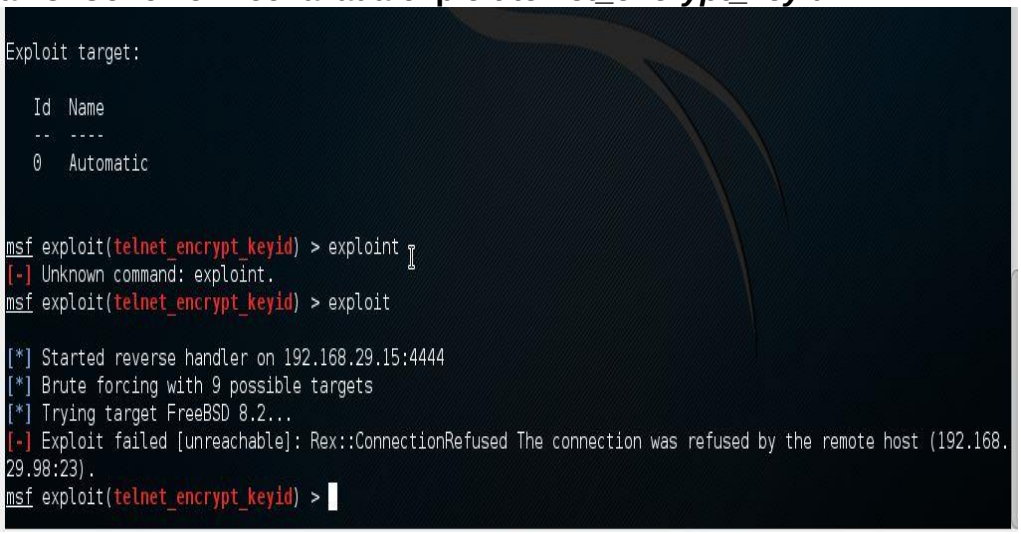
Figura 22. Opciones de exploit *telnet_encrypt_keyid*



Fuente: Pantalla exploit *telnet_encrypt_keyid*

Una vez ejecutado el exploit, se observó que la conexión fue rechazada porque el puerto 23 no está abierto en el servidor (ver figura 23).

Figura 23. Conexión rechazada exploit *telnet_encrypt_keyid*



Fuente: Pantalla exploit *telnet_encrypt_keyid*

- **type77**. Hace parte de las opciones de exploits del Openssh 5.3. Su función es intentar explotar el puerto 617 aprovechando un desbordamiento de pila en el cliente de copia de seguridad Arkeia para la plataforma Windows. Esta vulnerabilidad afecta a todas las versiones de Openssh, incluyendo la 5.3.3. La figura 24 muestra las opciones de este exploit.

Figura 24. Ventana de opciones de exploit type77

Fuente: Pantalla exploit type77

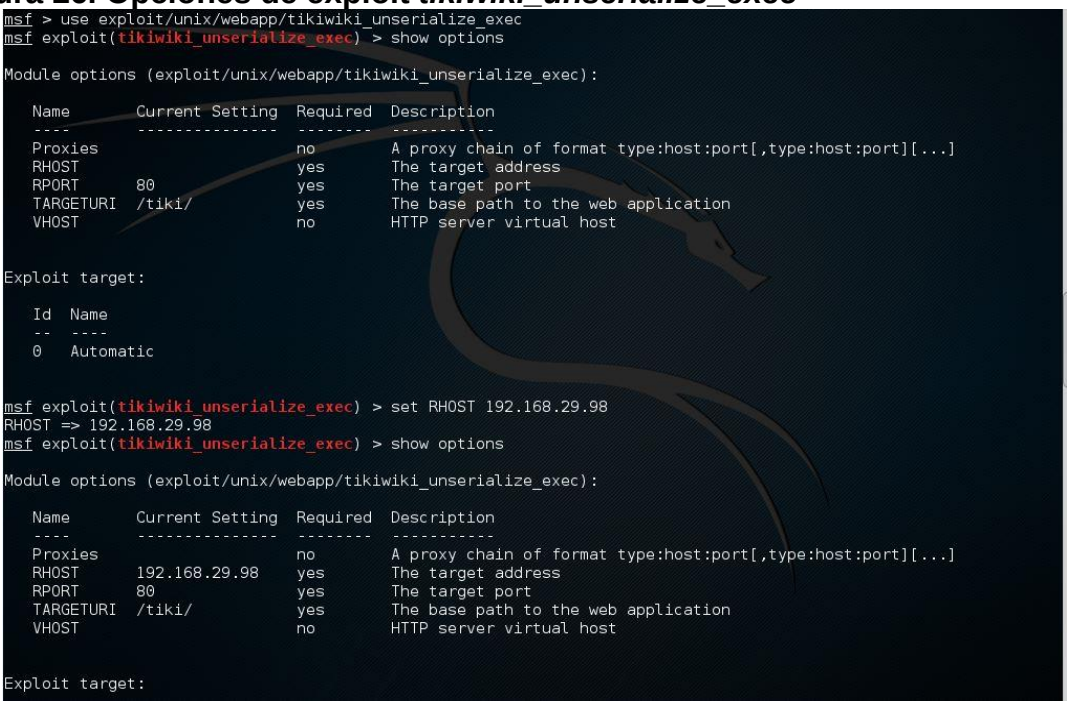
Una vez ejecutado el exploit, se observó que la conexión fue rechazada porque el puerto 617 no está abierto (Ver figura 25).

Figura 25. Conexión rechazada de exploit *type77*

Fuente: Pantalla exploit type77

- ***tikiwiki_unserialize_exec.*** Hace parte de las opciones de exploit del Openssh 5.3 (ver figura 26). Este módulo aprovecha una vulnerabilidad php, que podría ser objeto de abuso para que los usuarios no autenticados ejecuten código arbitrario en el contexto de usuario de servidor web. Las versiones de php anteriores a 5.3.4 son vulnerables a este exploit. La vulnerabilidad ha sido probada con éxito en Ubuntu 9.10 y Tiki Wiki 8.3.

Figura 26. Opciones de exploit *tikiwiki_unserialize_exec*

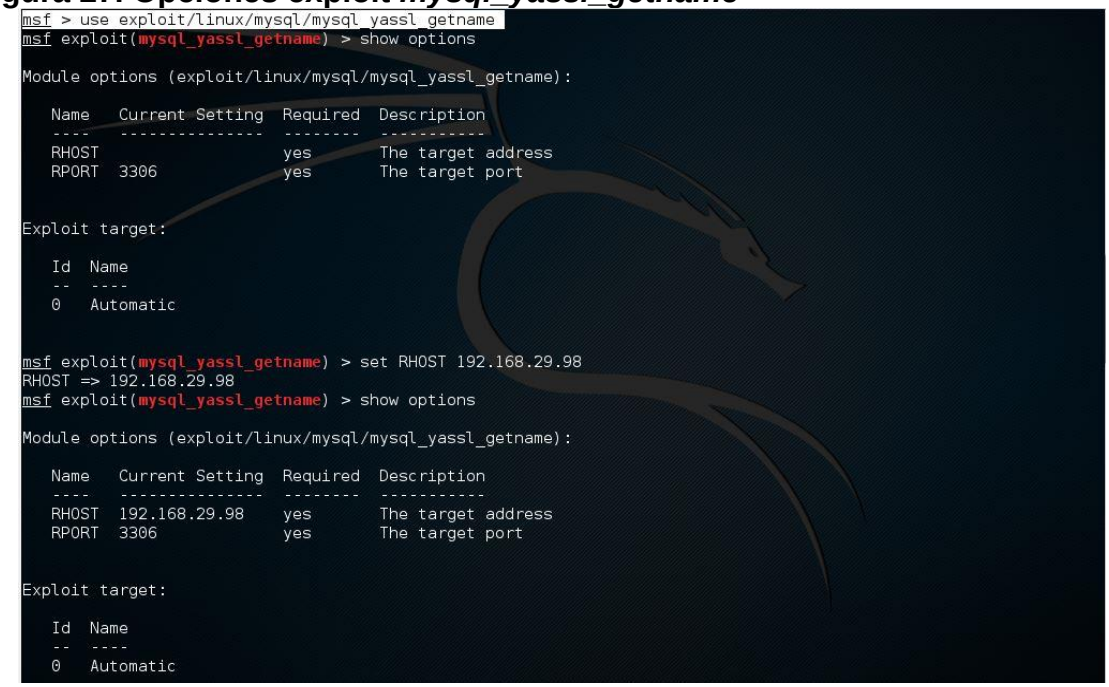


Fuente: Pantalla exploit *tikiwiki_unserialize_exec*

6.4.2. Mysql. En la ejecución de las pruebas para Mysql se usaron dos tipos de e*xploits.* Los detalles de cada prueba se presentan a continuación.

- ***Mysql_yassl_getname.*** Hace parte de las opciones de exploits de Mysql. Este módulo se aprovecha de una desbordamiento de pila en el yaSSL (1.9.8 y anteriores) aplicación incluido con MySQL (ver figura 27). Mediante el envío de un certificado cliente especialmente diseñado, un atacante puede ejecutar código arbitrario. Esta vulnerabilidad está presente dentro de la función CertDecoder: GetName dentro "taocrypt / src / asn.cpp".

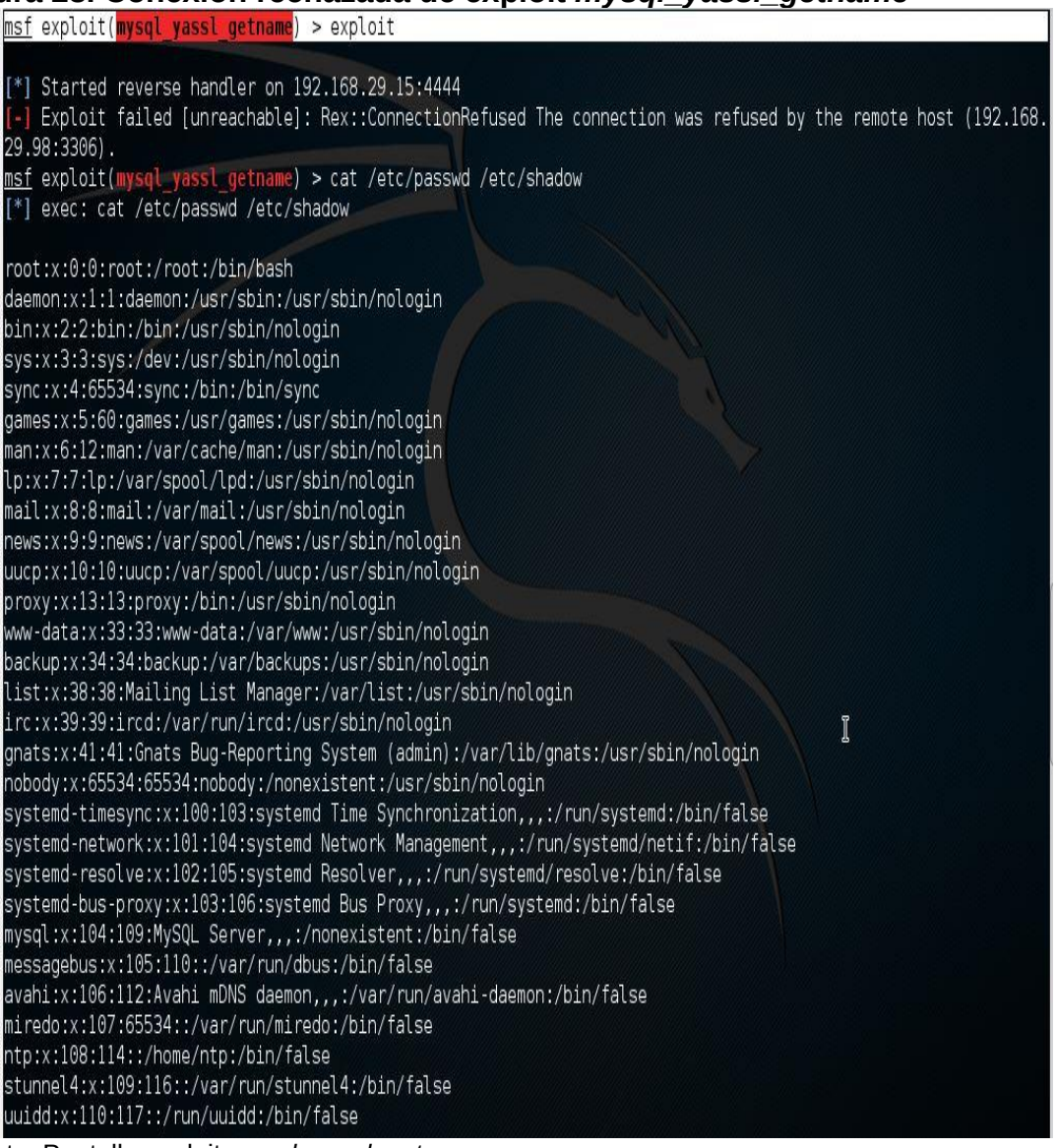
Figura 27. Opciones exploit *mysql_yassl_getname*



Fuente: Pantalla exploit *mysql_yassl_getname*

Una vez ejecutado el exploit, se observó que la conexión fue rechazada porque el puerto predeterminado de Mysql (3306) no está abierto en el servidor. Esto significa que dispone de un control para el manejo de puertos. Detalles de la prueba con este exploit se ve en la figura 28.

Figura 28. Conexión rechazada de exploit *mysql_yassl_getname*

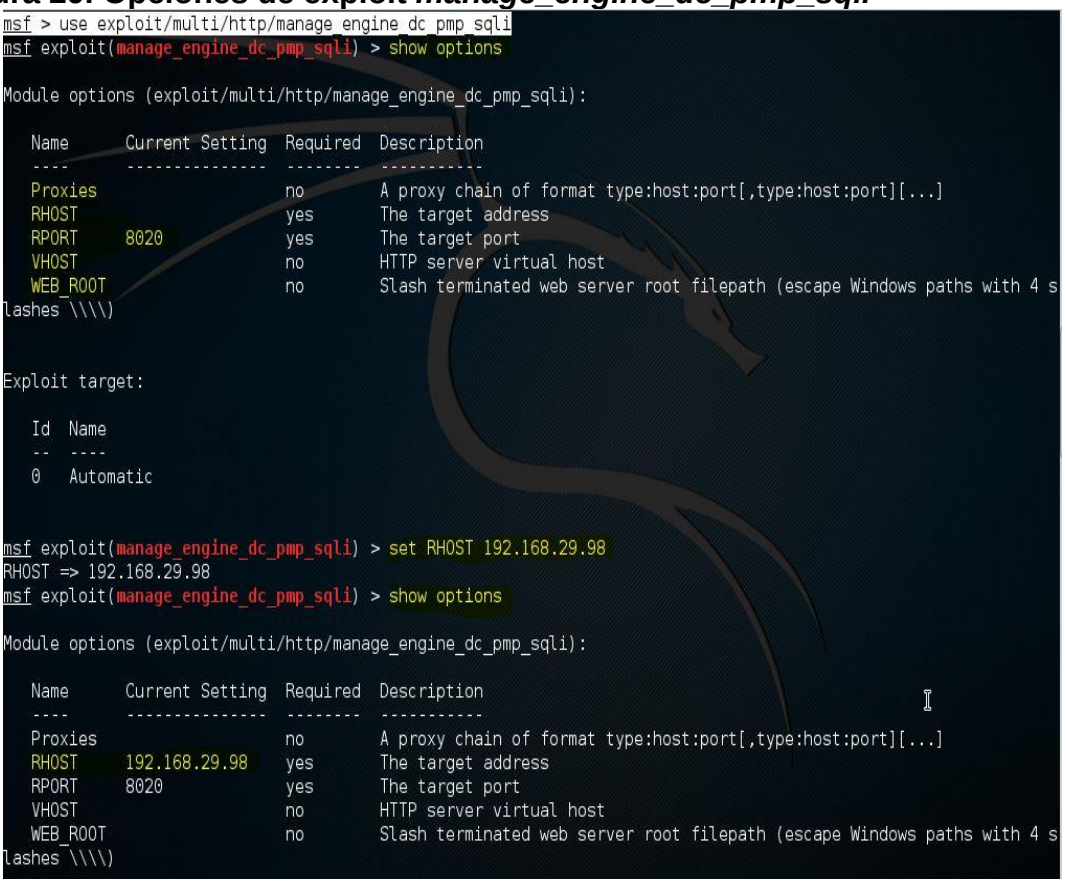


Fuente: Pantalla exploit *mysql_yassl_getname*

- ***Manage_engine_dc_pmp_sqli.*** Hace parte de las opciones de exploits de Mysql; este módulo aprovecha una inyección SQL ciega sin autenticación que se puede utilizar para lograr la ejecución de código remoto del sistema Windows o de Linux (ver figura 29). En este módulo se explota tanto en PostgreSQL como en MySQL. En MySQL son más confiables debido al uso de rutas relativas; con PostgreSQL se debe encontrar la ruta raíz web a través de otros medios y especificar con WEB_ROOT. La inyección sólo es explotable a través de una solicitud GET, lo que significa que la carga útil tiene que ser enviada en

trozos más pequeños de 8000 caracteres (limitación de tamaño URL). Esta vulnerabilidad existe en todas las versiones publicadas desde 2006.

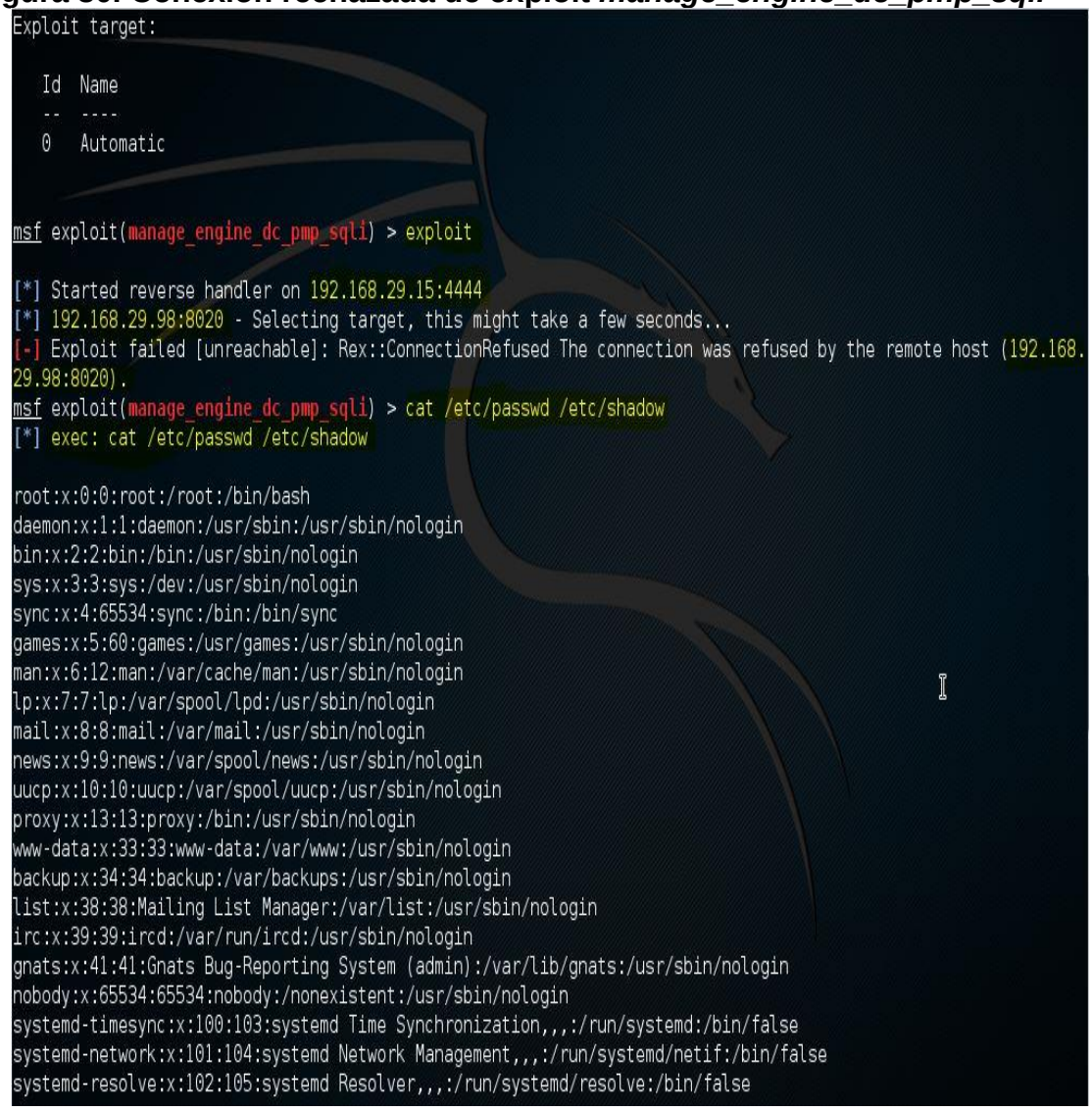
Figura 29. Opciones de exploit *manage_engine_dc_pmp_sqli*



Fuente: Pantalla exploit *manage_engine_dc_pmp_sqli*

Una vez ejecutado el exploit, se observó que la conexión fue rechazada porque el puerto 8020 no está abierto en el servidor, ni existe una política definida en el firewall institucional que permita tráfico a través de este puerto (ver figura 30).

Figura 30. Conexión rechazada de exploit *manage_engine_dc_pmp_sqli*



Fuente: Editor KDE Linux

6.5. PRUEBAS DE ATAQUE DE DICCIONARIO HACIA EL SERVIDOR CON METASPLOIT

Inicialmente, se identificó el puerto de bases de datos usado, en este caso el puerto fue el 30000. A través de este puerto hay comunicación con *Mysql 5.7.11.*

En la figura 31 se puede ver el escaneo que se realizó para ubicar el puerto.

Figura 31. Escaneo de puertos con nmap 6.4 Beta

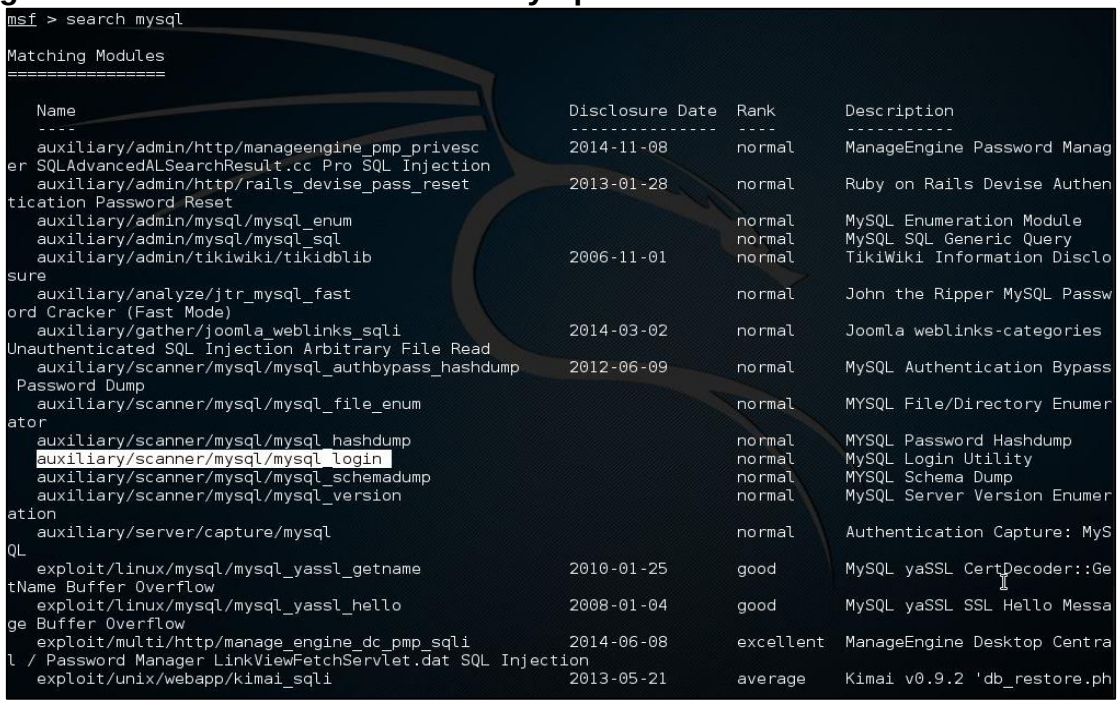
Fuente: Ventana programa nmap 6.4 Beta

A continuación se realizó la búsqueda de ***exploits*** por categoría, para identificar el exploit *mysql_login* e intentar realizar el ataque de diccionario.

Usando la herramienta *Metasploit*, se ingresó al *exploit* de ***mysql_login****,* donde se encuentran las diferentes opciones del módulo anteriormente mencionado (ver figura 32).

Luego se ingresó usando el comando:
Use auxiliary/scanner/mysql/mysql_login

Figura 32. Ventana de módulos de mysql.

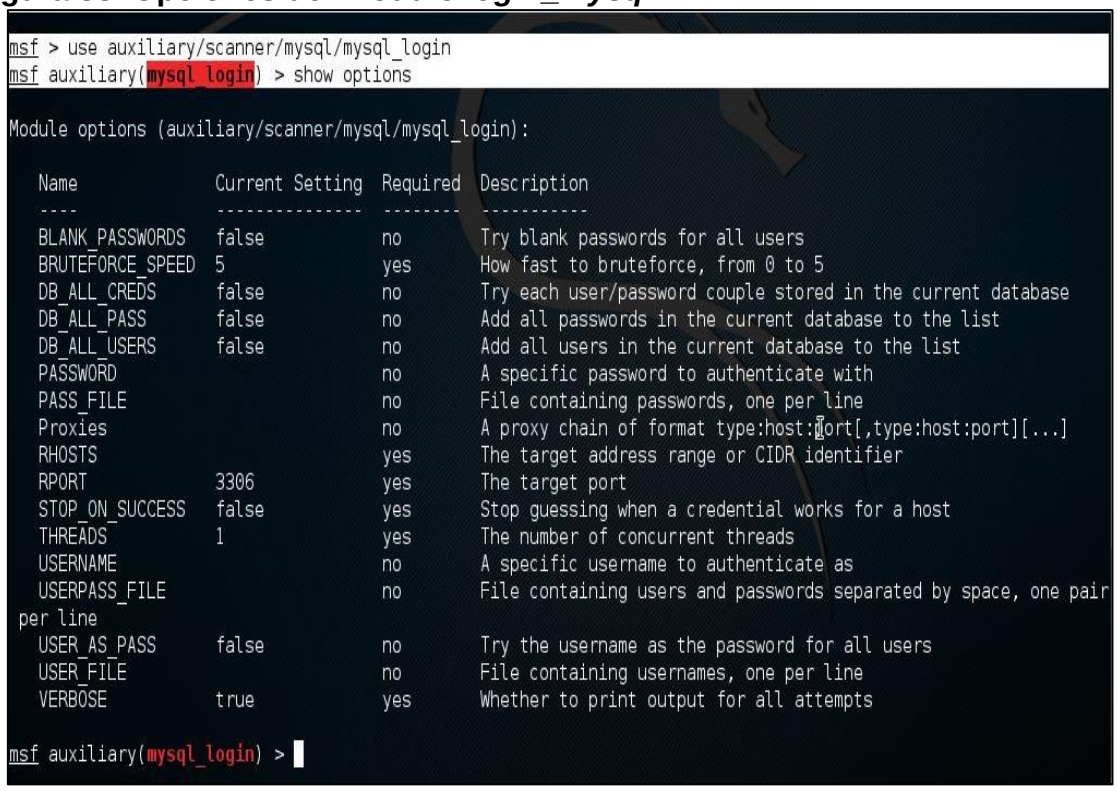


Fuente: Editor Kali Linux

Al ejecutar RPORT dentro del módulo ***login_mysql***, mostró la existencia de un puerto abierto para bases de datos *Mysql*. Este puerto se identifica como predeterminado (3306), sin embargo según el escaneo de puertos realizado al inicio sabemos que el puerto habilitado es el 30000 y se debe modificar el puerto.

A continuación se ejecutó el comando: set **RPORT 30000** para establecer el nuevo puerto (ver figura 33).

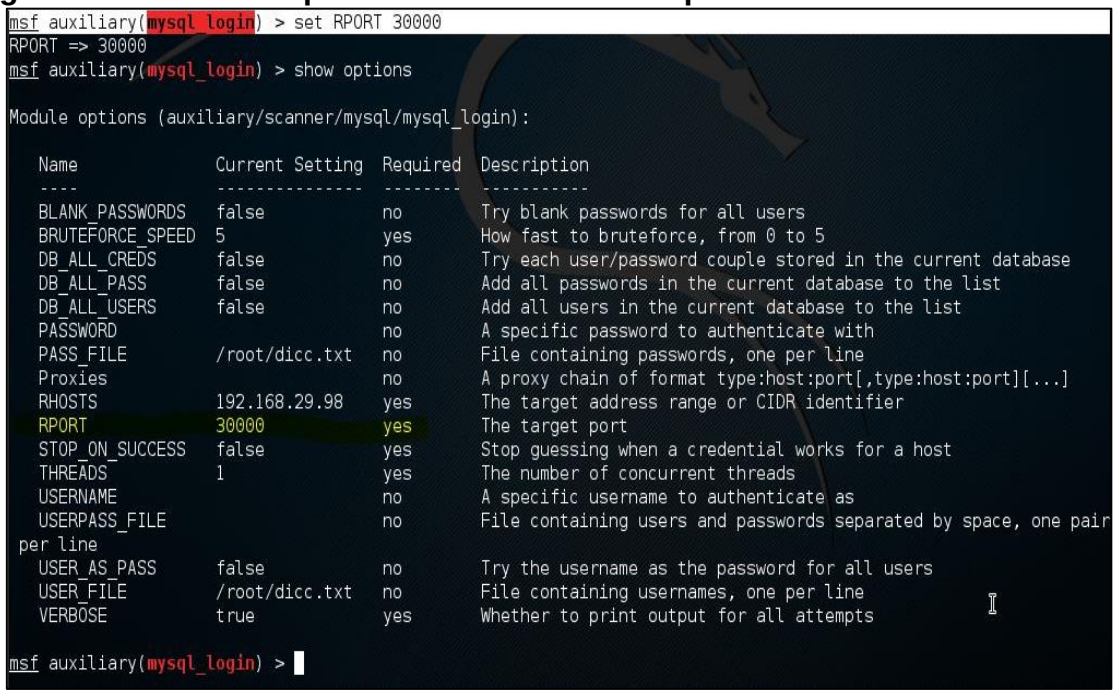
Figura 33. Opciones del módulo *login_mysql.*



Fuente: Editor Kali Linux

En la figura 34, se puede ver el cambio de puerto mediante el comando *RPORT*

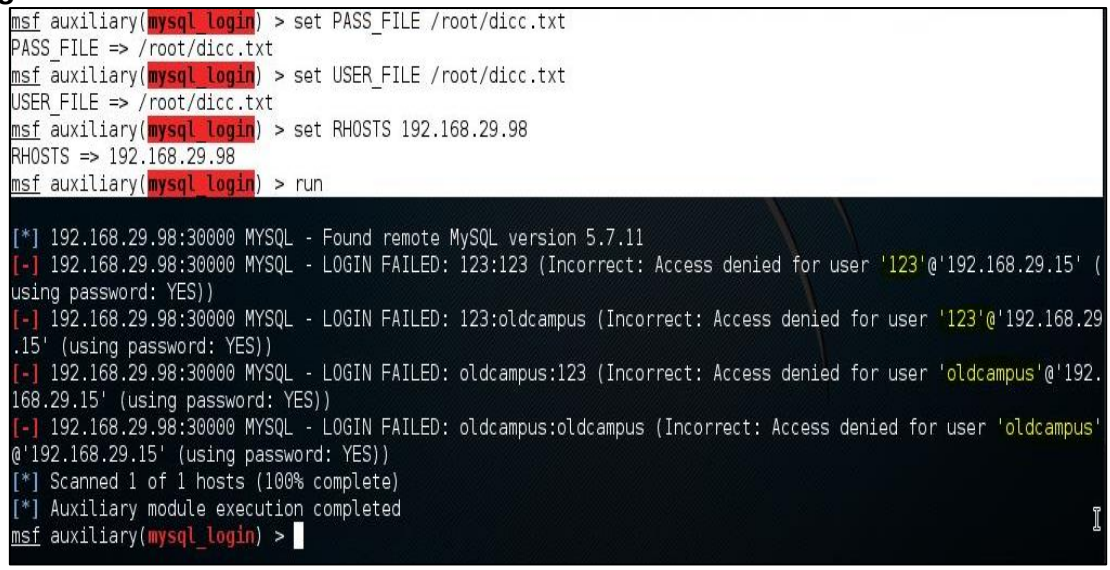
Figura 34. Cambio de puerto de escucha con Rport



Fuente: Editor Kali Linux

Para dar continuidad a la prueba se usó un diccionario de datos con 227 millones de palabras, intentando *crackear* la contraseña por fuerza bruta, pero no fue satisfactorio porque las credenciales de acceso no son comunes y no se encontraron en el archivo *dicc.txt (*ver figura 35*).*

Figura 35. Usando el diccionario de datos *dicc.txt*



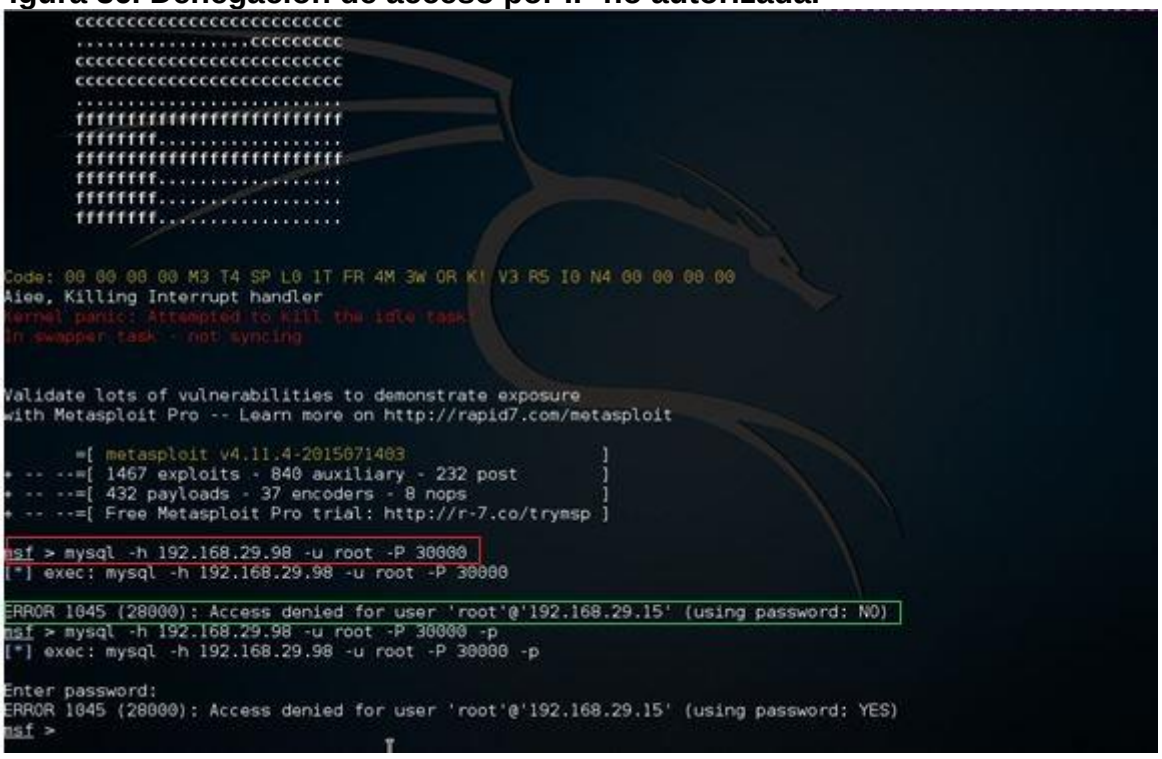
Fuente: Editor Kali Linux

También se intentó hacer conexión con la base de datos por el puerto conocido, probando el usuario *"root"*, un usuario predeterminado, sin embargo el acceso fue denegado, lo cual puede haber sucedido porque la IP, desde donde se intenta acceder, no se encuentra autorizada para acceder a la base de datos en cuestión (ver figura 36). Este control es muy importante y lo aplica el equipo administrador de la base de datos.

Otro aspecto importante a tener en cuenta es la versión usada de *Mysql*; a partir de la versión 5.6 se hace necesario proveer de una contraseña para la instalación del gestor de bases de datos.

Msf> mysql –h 192.168.29.98 –u root –P 30000

Figura 36. Denegación de acceso por IP no autorizada.



Fuente: Editor Kali Linux

Se intentó acceder al usuario "*root*" del servidor definiendo el puerto conocido 30000 del servidor, pero la conexión fue rechazada, debido a los módulos de seguridad que mantiene el servidor Mysql, los cuales no permiten el ingreso de IP diferentes.

Con paquetes RPM, es necesario que después de la instalación y de iniciar el servidor, se haga la conexión como usuario *root* con la contraseña inicial, y

asignar una nueva contraseña root. Esto debe hacerse para cada cuenta root que se vaya a utilizar. Esto proporciona más seguridad a las bases de datos de *Mysql.*

7. COMENTARIOS FINALES

El objetivo de este capítulo es presentar algunos resultados y recomendaciones, deducidos del análisis de los resultados de las pruebas. Se busca que estas recomendaciones se pueden usar en el plan de mejoramiento del área bajo pruebas.

7.1. RESULTADOS

A continuación se presentan algunos ítems encontrados al terminar las pruebas:

a. Las versiones de Mysql usadas por la universidad, son versiones que exigen una contraseña para la instalación del paquete rpm, lo cual se considera adecuado para evitar brechas de seguridad.

b. El ataque de SQL injection no fue satisfactorio, desde el punto de vista del atacante, porque los servidores analizados mantienen un estricto nivel de aseguramiento o “hardening”, además que los datos se manejan por método POST y mantienen certificados digitales con un algoritmo criptográfico muy robusto (RSA) SHA-512.

c. En las bases de datos no se usan puertos predeterminados, y se usan versiones modernas que ayudan a mitigar los riesgos de ser atacados.

d. Las contraseñas establecidas en los servidores y bases de datos, cumplen la política de complejidad y robustez; no son palabras comunes que puedan aparecer en un diccionario de datos y por ende ser vulneradas por fuerza bruta.

e. Los exploits utilizados para intentar vulnerar el Openssh 5.3 y el Mysql 5.7.11 son escasos y los usados no fueron eficientes porque las versiones mantienen una seguridad interna que dificultad la explotación de las vulnerabilidades asociadas a estos activos. Entre otras cosas porque Openssh 5.3 cifra su llave con 2048 bits y porque la versión de Mysql 5.7.11 exige contraseña para ser instalado.

f. Se mantiene un estricto control sobre los puertos necesarios y usados tanto en los servidores como en las políticas del firewall institucional lo que dificulta que los exploits puedan ejecutarse apropiadamente y cumplir el objetivo del atacante. Esta es una medida de control muy importante implementada por la universidad para eliminar los riesgos de ataques a la plataforma.

g. Con las pruebas de Vulnerabilidad realizadas al campus virtual y las cuales se enfocaron a las Bases de Batos se puede concluir que el nivel de seguridad es alto y se recomienda continuar aplicando las actualizaciones de Mysql y la seguridad en los servidores.

7.2. RECOMENDACIÓN GENERAL.

Fortalecer la política de actualización de versiones de programas de *PHP, Apache*, *Mysql*, *Moodle*, métodos de seguridad para servidores, parches de actualización en los servidores, depuración de usuarios, actualización de claves para funcionarios internos del campus, el monitoreo de las bases de datos, todo ello con el fin de prevenir posibles ataques.

7.3. RECOMENDACIONES ORIENTADAS A POLÍTICAS DE SEGURIDAD

a. Es importante definir en la topología de red, una zona desmilitarizada *(DMZ)*, con el fin de aislar y proteger los activos (Servidores-Servicios) más importantes de la organización, con el fin de evitar accesos no autorizados por brechas identificadas en otros puntos de la red.

b. Definir canales dedicados para los procesos más críticos de la organización, con el fin de prevenir saturación de paquetes y por ende alguna denegación de servicio que pueda generar un impacto catastrófico para la universidad.

c. Mantener un plan de continuidad del negocio (BCP) donde se involucren todos los posibles escenarios, en los cuales los riesgos sean identificados y controlados de manera correcta, minimizando el impacto para la universidad.

d. Realizar una depuración de puertos en todos los servidores de la universidad, de manera que únicamente se permita el tráfico por puertos necesarios para la continuidad del negocio y debidamente documentados.

e. Documentar formalmente los procesos y procedimientos, que realizan los Ingenieros de Base de Datos y Servidores, porque se están llevando en cuadernos, drives y hojas de Excel, que tiene cada uno de los funcionarios.

8. CONCLUSIONES

La mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos (Oracle, MySQL, SQL Server, PostGreSQL entre otros), razón por la cual son permanentes los ataques a bases de datos almacenadas en ellos. De acuerdo con estudios de entidades especializadas las amenazas más comunes en este campo son: *Privilegios excesivos e inutilizados*, *Abuso de Privilegios, Explotación de vulnerabilidades, Bases de daros mal configuradas, Malware y spear phising, Denegación de servicio (DoS), Auditorías débiles y Datos sensibles mal gestionados.* Estas mismas entidades han establecido como los ataques más comunes: Ataques p*or Session Hijacking, Robo en Servidor Compartido* y *Ataque Por Inyección De Código.*

Existen muchas herramientas de licencia libre, que ayudan en el proceso de identificación de vulnerabilidades de sistemas informáticos; en el caso particular de la tesis, se realizó un análisis para establecer las más adecuadas para el tipo de ataque que se quería ejecutar, siendo seleccionadas: Nmap, SQL Map y Nessus teniendo en cuenta que además de su efectividad son fáciles de descargar y de usar. Con Nmap se atacó el servidor donde se alojaba la base de datos del campus para determinar los puertos abiertos y poder hacer ataques; con Nessus se escaneo el servidor para determinar las vulnerabilidades y evaluar su configuración; con SQL Map se hicieron los ataques de inyección de código al servidor del Campus donde están los Backup de la base de datos.

Las vulnerabilidades detectadas para las herramientas OpenSSH y MySql por Nessus, fueron atacadas usando los sploits: rpc_ttdserverd_realpatch, tikiwiki_unserialize_exec, telnet_encrypt_keyid, type77, Mysql_yassl_getname y Manage_engine_dc_pmp_sqli, los cuales arrojaron resultados negativos a la prueba. De igual manera las pruebas de inyección de código salieron negativas por el tipo de codificación utilizada en el Campus. Lo anterior permitió validar el grado de seguridad del Campus al fracasar todos los ataques.

Aunque el estudio mostró que la seguridad de campus en general es buena, se sugiere fortalecer las políticas de actualización de: versiones de programas (PHP, Apache, Mysql y Moodle); métodos de seguridad para servidores junto con los parches de actualización; depuración de usuarios; actualización de claves para funcionarios internos del campus; y monitoreo de las bases de datos.

BIBLIOGRAFÍA

ASI. GFI LanGuard. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://www.auditoria.com.mx/GFI-LanGuard

ACIS. Encuesta Seguridad Informática En Colombia. Tendencia [en línea] [Fecha de consulta: 05/06/2014] Disponible en: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013

ALMANZA, Andrés. Perfil Profesional. [en línea] [Fecha de consulta: 05/06/2014] Disponible en: http://co.linkedin.com/pub/andres-ricardo-almanza-junco/23/339/ba8

CAPACITY. Las 8 Mejores Herramientas de Seguridad y Hacking. [en línea] [Fecha de consulta: 05/08/2015] Disponible en: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

CIBERINFORMATICO. Anatomía de un ataque. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: http://ciberinfosystem.blogspot.com.co/2012/03/anatomia-de-un-ataque.html

CODEJOBS. Qué es una vulnerabilidad, una amenaza y un riesgo?. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.D2RDznkO.dpbs

COMMON VULNERABILITIES AND EXPOSURES. [en línea] [Fecha de consulta: 12/04/2015] Disponible en: https://cve.mitre.org/.

CORE SECURITY. Core Impact. [en línea] [Fecha de consulta: 05/07/2015] Disponible en: http://www.coresecurity.com/core-impact-pro

CHÁVEZ, Jenny. Ataque a la base de datos. [en línea] [Fecha de consulta: 13/04/ 2015] Disponible en: http://ataquebd.blogspot.com/2012/07/ataque-la-base-de-datos-introduccion-la.html

EL-TIEMPO. Crecen los ataques informáticos internos. [en línea] [Fecha de consulta: 08/06/2014.] Disponible en: http://www.eltiempo.com/archivo/documento/MAM-1003031

FERRER, Rodrigo. Análisis de Vulnerabilidades. [en línea] [Fecha de consulta: 10/04/2015] Disponible en: http://www.sisteseg.com/

FRANCO, David. Herramienta para detectar vulnerabilidades. [en línea] [Fecha de consulta: 05/08/2015] Disponible en: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext

HACKER.NET. Tutorial Sqlmap. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://blog.elhacker.net/2014/06/sqlmap-automatizando-ataques-sqli-injection.html

INCIBE. ¿Mi empresa es vulnerable a un ataque informático?. [en línea] [Fecha de consulta: 05/04/2015] Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/empresa_vulnerable_ataque_informatico

INSECURE. Las 75 herramientas de seguridad más usadas. [en línea] [Fecha de consulta: 10/08/2015] Disponible en: http://insecure.org/tools/tools-es.html

KALI. Documentación Oficial Kali Linux. [en línea] [Fecha de consulta: 10/08/ 2015] Disponible en: http://es.docs.kali.org/introduction-es/que-es-kali-linux

MAESTROS DE LA WEB. ¿Qué son las bases de datos?. [en línea] [Fecha de consulta: 10/04/2015] Disponible en: http://www.maestrosdelweb.com/editorial/%C2%BFque-son-las-bases-de-datos/

MIFSUD, Elvira. Introducción a la seguridad informática. [en línea] [Fecha de consulta: 25/04/2015] Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

MINTIC. Modelo de seguridad de la información. [en línea] [Fecha de consulta: 25/04/2015] Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

MICROSOFT. Motor de base de datos de SQL Server. [en línea] [Fecha de consulta: 10/04/2015] Disponible en: http://msdn.microsoft.com/es-es/library/ms187875.aspx

NeaSTDL. Métodos de ataques y vulnerabilidades de las bases de datos. [en línea] [Fecha de consulta: 06/03/2015] Disponible en: http://www.buenastareas.com/ensayos/M%C3%A9todos-De-Ataque-y-Vulnerabilidades-De/25016957.html

PELAEZ, Juan. ¿Mi empresa es vulnerable a un ataque informático? [en línea] [Fecha de consulta: 13/04/2015] Disponible en:

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/empresa_vulnerable_ataque_informatico

SECTOOLS. Top 125 Network Security Tools [en línea] [Fecha de consulta: 13/04/2015] Disponible en: http://sectools.org/

TENABLE. Nessus Plugin. [en línea] [Fecha de consulta: 05/06/2016] Disponible en: https://www.tenable.com/plugins/index.php?view=single&id=71049.

TICBEAT. Las 10 grandes amenazas de seguridad en las bases de datos. [en línea] [Fecha de consulta: 13/04/2015] Disponible en: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

UNAM. Tutorial de Seguridad Informática - Amenazas y vulnerabilidades. [en línea] [Fecha de consulta: 01 Mayo 2016] Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html.

UNLU. Amenazas a la seguridad de la información. [en línea] [Fecha de consulta: 03/03/2015] Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

ANEXOS

ANEXO A.

ESQUEMA Y PREGUNTAS PARA ENTREVISTAS CON EXPERTOS

Introducción
Buenas Días/Tardes:
Como autor del trabajo de grado titulado ESTUDIO DE SEGURIDAD INFORMÁTICA PARA LAS BASES DE DATOS DEL CAMPUS VIRTUAL DE LA UNAD de la Especialización en Seguridad Informática de la UNAD, me encuentro realizando entrevistas a profesionales de Área de Sistemas con el fin de conocer su apreciaciones en el campo de la seguridad informática en el campo de las bases de datos.

Hoy me encuentro con profesional: _____
Cargo: _____

Preguntas

1. Ing/Msc/Dr. _____ podría usted hacernos un resumen de su formación académica y experiencias profesional.

2. Podría indicar si ha tenido conocimiento de un caso que haya afectado la seguridad informática de una base de datos.

3. Como usuario experto en el campo de los sistemas de información y plataformas tecnológicas, puede comentarnos algunas inquietudes o sugerencias que tenga sobre la seguridad informática en el campus virtual de instituciones educativas?.

4. Podría usted sugerir acerca de algún material bibliográfico o multimedia que maneje temas relacionados con la seguridad informática en Bases de datos?

5. El proyecto está enfocado a las vulnerabilidades que puede presentar o presentan la Base de Datos en campus virtuales que tiene como herramienta sistema operativo Moodle y motor de BD MySQL.
   ¿Qué recomienda para tener una mejor seguridad con estas dos herramientas (Moodle y MySQL)?
   ¿Considera recomendables y seguras estas dos herramientas para entornos de campus virtuales?

ANEXO B.

UNAD
Universidad Nacional Abierta y a Distancia

Bucaramanga, 16 de Junio de 2014

Doctor
ARTURO ERAZO
Director del Curso Proyecto de Seguridad Informática I
Pasto

Asunto: Autorización para realizar escaneo de vulnerabilidades en Bases de Datos del Campus Virtual UNAD

Cordial saludo.

Con la presente me permito confirmarle que el ing Carlos Javier Uribe Otálora, actualmente como coordinador del equipo de soporte de la Plataforma Tecnológica Integrada (PTI), tiene autorización para realizar el escaneo de vulnerabilidades a uno de los servidores dedicados a las bases de datos del campus virtual de la UNAD. Este procedimiento se realizará con el acompañamiento del equipo de base de datos y de seguridad informática de la PTI para evitar contratiempos

Cordialmente,

Ing. Miguel Pinto Aparicio
Coordinador Plataforma Tecnológica Integrada

Universidad Nacional Abierta y a Distancia UNAD
Zona Centro Oriente. Carrera 27 número 40-43 Bucaramanga
Teléfono: 635 85 77 Fax 635 83 32