ESTUDIO DE VULNERABILIDADES A LAS APLICACIONES PREFIS Y SIVICOF DE LA CONTRALORÍA DE BOGOTÁ D.C.

OSBALDO CORTÉS LOZANO

LENIN HERRERA MONCADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2018

ESTUDIO DE VULNERABILIDADES A LAS APLICACIONES PREFIS Y SIVICOF DE LA CONTRALORÍA DE BOGOTÁ D.C.

OSBALDO CORTÉS LOZANO

LENIN HERRERA MONCADA

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Mariano Esteban Romero Torres

Director de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.,

2018

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Bogotá D.C., 2018

EXCLUSIÓN DE RESPONSABILIDAD

Las ideas, opiniones y conclusiones expresadas en este proyecto son de exclusiva responsabilidad de sus autores y de ninguna manera comprometen la ideología de la Universidad Nacional Abierta y a Distancia UNAD.

AGRADECIMIENTOS

A mi familia en especial a mi Papá que, a pesar de no estar con nosotros, siempre me guía.

Al equipo de profesores de la UNAD por su apoyo irrestricto y a Lenin por su apoyo.

Osbaldo Cortes Lozano

Agradezco a Dios por su amor, su misericordia y fidelidad, y a su Hijo Jesús que murió por mí, tomado en la Cruz el lugar que yo merecía. A mi amada esposa y a mis hijas por su amor, apoyo y tiempo, a mi estimado amigo y socio en este proyecto por su comprensión y tolerancia y a mis tutores y director de proyecto por su disposición y valiosa ayuda.

Lenin Herrera Moncada

CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

INTRODUCCIÓN

La contraloría de Bogotá D.C., es la entidad encargada de vigilar la gestión Fiscal de la Administración del Distrito Capital, y de los particulares que manejan fondos o bienes públicos, en las diferentes etapas de los procesos de contratación[1]. En resumen, es quién garantiza la correcta utilización de los recursos económicos en Bogotá D.C.

Par lograr sus objetivos y gracias al componente tecnológico la Contraloría de Bogotá Cuenta entre otras herramientas con Sivicof “Aplicación de vigilancia y Control de Procesos” y Prefis “Sistema de Información para el Manejo y Control del Proceso de Responsabilidad Fiscal”, programas que son neurálgicos para la Misión Institucional, convirtiéndolos en objetivos a los ataques.

La seguridad de la información es un tema actual, por ejemplo, el pasado16 de mayo de 2017, los medios de comunicación dieron a conocer a la opinión pública que más de 230.000 equipos en 179 países fueron infectados por un malware que empezó a propagarse desde el viernes 12 de mayo del mismo año. Este programa malicioso se conoce con el nombre de “WannaCry” y se tipifica como un ‘ransomware’, cuyo objetivo es cifrar los archivos de interés de una persona, que generalmente son de tipo Word, Excel, PowerPoint, videos, imágenes, fotografías, bases de datos, etc., para luego pedir rescate por ellos, en otras palabras, pagar para recobrarlos.

Aquí en Colombia se conoció que varias empresas privadas y Entidades del Estado se vieron afectadas por este ataque. Entonces podemos afirmar que nadie está exento de ser el objetivo de uno de estos delincuentes informáticos.

La Contraloría de Bogotá D.C., no está exenta de ser víctima de estos tipos de ataques y en consecuencia verse seriamente afectada desde el punto de vista de la integridad, disponibilidad y confidencialidad de la información que maneja y de los servicios que debe prestar a los ciudadanos de Bogotá D.C.

---

[1] ACUERDO 519 de diciembre de 2012 Normas sobre la organización de la Contraloría de Bogotá D.C., Internet:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51049)

Una de las maneras de conocer el estado actual de la seguridad informática en la Contraloría de Bogotá, es por medio de la práctica de test de penetración[2], que permitan identificar y explotar las brechas de seguridad o vulnerabilidades en los diferentes componentes del sistema informático, con el objetivo de implementar los controles para mitigar el riesgo.

En consecuencia, se plantea realizar, un estudio de Vulnerabilidades en la fase recolección pasiva de información, se buscarán los posibles puntos de acceso para luego identificar y enumerar las factibles vulnerabilidades y por último, diseñar y planificar el aprovechamiento de vulnerabilidades.

La realización del test se basa en la Metodología PTES (Penetration Testing Execution Standard)[3], que es un framework o marco de referencia que sus inicios datan a principios del año 2009, fue diseñado para suministrar a las Organizaciones y a los proveedores de servicios de seguridad un ambiente común para realizar pruebas de penetración con el objetivo de evaluar la seguridad de un sistema.

La metodología para el desarrollo de este proyecto es el de investigación aplicada, que está orientada a la solución de problemas locales, regionales o nacionales, partiendo del conocimiento específico del programa que se cursa. Se emplearán herramientas para la recogida pasiva de la información del sistema como entrevistas y correos anónimos, así mismo se emplearán herramientas de software libres para la búsqueda, enumeración y planificación de ataques.

Como producto final del estudio de Vulnerabilidades en la fase de recolección de información en el sistema de la Contraloría de Bogotá, serán los informes técnicos y ejecutivos de los resultados obtenidos de las pruebas de penetración.

---

[3] Penetration Testing Execution Standard. disponible en: http://www.pentest-standard.org/index.php/FAQ

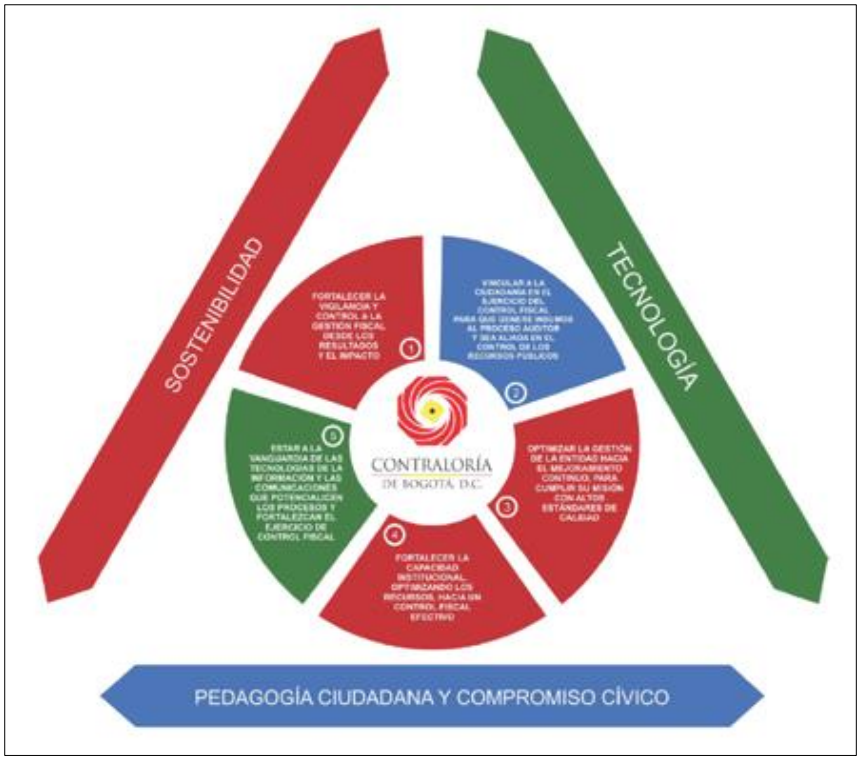
1. PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

Teniendo presente que los sistemas de información de la Entidad enfrentan, cada día más riesgos e inseguridad procedente de varias fuentes, incluyendo espionaje, fraudes tecnológicos, sabotaje, vandalismo; o naturales como temblores e incendios. Algunas fuentes de daños como los son el malware y ataque de intrusión o negación de servicios, son más frecuentes, dañinos y especializados.

La Contraloría de Bogotá D.C., de acuerdo con su Plan estratégico, establece tres pilares fundamentales que son; la Sostenibilidad, Pedagogía Ciudadana y Compromiso Cívico y Tecnología, en este entendido la dependencia a los sistemas y servicios de información implica que la Contraloría de Bogotá D.C., sea más vulnerable a las amenazas a su seguridad informática, la cual se incrementa al conectar las redes privadas con las redes públicas y al compartir recursos de información por medios electrónicos.

Ilustración 1. Plan Estratégico - Contraloría de Bogotá



Fuente:
http://www.contraloriabogota.gov.co/intranet/contenido/planes/planes/Estrategico/2016-2020/DIAGN%C3%93STICO%20ESTRATEGICO%202016-2020.pdf

En la actualidad la Contraloría de Bogotá, D.C., no cuenta con un estudio reciente de análisis de riesgos de sus sistemas de información Prefis y Sivicof, que le permita conocer el estado real de la seguridad de este y de las vulnerabilidades que pueden ser explotadas por un atacante, comprometiendo gravemente la confidencialidad, integridad, disponibilidad y autenticidad de la información.

1.2. FORMULACIÓN DEL PROBLEMA

Evidenciando la posibilidad de ocurrencia de un ataque informático que pueda afectar los sistemas informáticos Prefis y Sivicof, es pertinente tomar acciones.

¿Cómo la realización de un estudio de vulnerabilidades a los sistemas de Información Prefis y Sevicof, permitirá identificar las posibles amenazas y vulnerabilidades, a los que están expuestos, para con base en los resultados proponer un plan de contingencia que brinde seguridad al sistema?.

1.3. OBJETIVO GENERAL

Realizar el estudio de penetración en las fases de recolección (activa y pasiva) de información y análisis de vulnerabilidades, para el sistema de información de la Contraloría de Bogotá, D.C, y en particular a los aplicativos Prefis y Sivicof.

1.4. OBJETIVOS ESPECÍFICOS

- Identificar la información que gestiona los aplicativos Prefis y Sivicof.
- Realizar la recolección de información para obtener la mayor información de forma pasiva y activa del sistema (Recolección de Inteligencia).
- Enumerar las vulnerabilidades existentes en el sistema y que pueden ser explotadas (Enumeración).
- Diseñar la ejecución del ataque, seleccionando las herramientas apropiadas para explotar una posible vulnerabilidad.
- Desarrollar el informe técnico con destino a la Dirección de las TIC de la Contraloría de Bogotá. D.C., del resultado del estudio de Ethical Hacking en la fase de recolección de información.

1.5. JUSTIFICACIÓN

Los delitos informáticos cada día van en aumento, ninguna organización privada o estatal está exenta de verse gravemente afectada por esta causa.

El Sistema de Información -PREFIS-, es uno de los sistemas de más importantes, por no decir el más importante con el que cuenta la Contraloría de Bogotá, D.C., este sistema soporta la gestión misional de la Entidad, es el repositorio de información de todas las actuaciones procesales de responsabilidad fiscal, la información allí almacenada y procesada es de carácter sensible y antes de que haya un fallo legal, esta información es de carácter reservada.

Debido a la importancia de este sistema de información, es de vital importancia implementar las medidas necesarias que garanticen la seguridad de este, así como confidencialidad, integridad y disponibilidad de la información.

En el proyecto DE ACUERDO No. 037 DE 2013.[4] "Por medio del cual se establece la Estrategia de Ciberseguridad para enfrentar ciberdelitos y amenazas contra el Distrito Capital", se describe que las entidades distritales no han sido exentas a los ataques informáticos. Entre las entidades afectadas y los ataques recibidos se mencionan entre otras las siguientes:

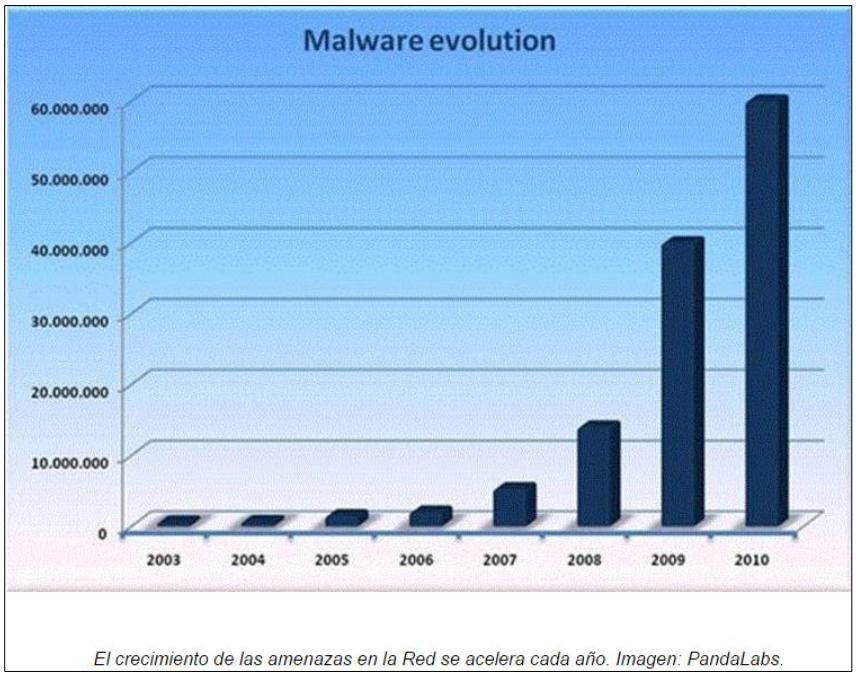
Registraduría Nacional: Ataque de hackers durante las elecciones parlamentarias del 2010, que hizo colapsar al sistema de datos.

Empresa de Acueducto de Bogotá: Ataque a la página web de la E.A.A.B., en el 2012, exactamente al sitio donde se publican las licitaciones.

Este documento también muestra la tendencia de los ataques informáticos en el Distrito Capital.

[4] Proyecto de Acuerdo No. 037 de 2013, disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

Ilustración 2. Proyección de Crecimiento de amenazas en Internet en Bogotá



Fuente: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

Por lo anterior es de vital necesidad e importancia que la Contraloría de Bogotá realice cuanto antes un estudio del estado de la seguridad de su sistema informático, que le permita blindar sus procesos con el fin de poder cumplir los objetivos misionales para lo cual fue creada.

1.6. ALCANCE Y DELIMITACIÓN

El alcance del proyecto consiste en efectuar algunas pruebas de penetración en la fase de recolección de información al sistema de información de la Contraloría de Bogotá, D.C., que permitan identificar las posibles vulnerabilidades existentes el sistema a nivel general y a nivel particular en los aplicativos Sivicof y Prefis; y dejar planificados los ataques para poder explotarlas en un futuro. En este proyecto se realizarán las siguientes pruebas:

- Recolección pasiva de información (Passive Footprinting)
- Recolección activa de información (Active Footprinting)
- Escaneo y análisis de puertos
- Escaneo y análisis de vulnerabilidades
- Auditoria de contraseña
- Análisis de seguridad web

- Análisis de direcciones IP públicas para identificar vulnerabilidades

El proyecto estará delimitado por el siguiente entregable:

- Realizar el informe técnico, especificando las vulnerabilidades encontradas y las recomendaciones para su tratamiento.

2. MARCO DE REFERENCIA

2.1. ANTECEDENTES

Para el estudio de posibles vulnerabilidades de la infraestructura tecnológica de la Contraloría de Bogotá D.C., es de vital importancia contar con los antecedentes actuales, confiables y de calidad de esta área del conocimiento, y con esta información realizar un estudio que logre cubrir la mayoría de las amenazas actuales y así mitigar la incidencia de estas en los pilares de la seguridad informática de la Contraloría de Bogotá D.C.

Según[5] Luis Alcides Mendaño y María Elena Hurtado Saldoval, en su tesis "Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de las redes de una cartera de estado" en la ciudad de Quito en 2016, afirman que un estudio de Ethical Hacking permite detectar fallas en la seguridad perimetral de una Organización que facilite a un atacante obtener información relevante del sistema, identificar servicios o acceder al sistema por medio de usuarios y contraseñas por defecto.

También, Daniel Iván Quirumbay Yagual[6], en su tesis "Desarrollo del Esquema de Seguridad, Plan de Recuperación Ante Desastres Informáticos y Solución para el Nivel de Exposición de Amenazas y Vulnerabilidades Aplicada a los Servidores y Equipos de Comunicación del Centro de Datos de la Municipalidad de la Ciudad Del Este" en la ciudad de Guayaquil en 2015, afirma que un estudio de Ethical Hacking permite detectar las vulnerabilidades de un sistema de información, medir el nivel de seguridad y aplicar las medidas preventivas y correctivas para prevenir y mitigar los riesgos.

Así mismo, Bharath Kumar Koopari Roopkumar[7], en su tesis "Ethical Hacking using penetration testing" en la ciudad de Luisiana en 2012, afirma que la implementación de un laboratorio de Ethical Hacking, permite a las organizaciones testear y monitorear en tiempo real tanto el software como el hardware y enfatiza en la fase

[5] Fuente: http://bibdigital.epn.edu.ec/bitstream/15000/16836/1/CD-7415.pdf

[6] Fuente: https://www.dspace.espol.edu.ec/retrieve/88647/D-84693.pdf

[7] Fuente: http://digitalcommons.lsu.edu/gradschool_theses/3238

de la recopilación y análisis de información como fundamental para el logro del objetivo.

Por otro lado, Andrés Fernando Castañeda Suárez[8], en su tesis “Identificación y explotación de vulnerabilidades en aplicaciones web de un entorno académico” en la ciudad de Bogotá en 2015, enfatiza en la necesidad creciente del desarrollo de pruebas de Ethical Hacking, que permita controlar y verificar el estado de las diferentes redes, que cubra desde las conexiones WAN hasta las redes LAN.

Según, David Kennedy[9], Jim O’Gorman y Devon Kearns, Mati Aharoni, en su libro “Metasploit The Penetration Tester’s Guide” en la ciudad de San Francisco en 2011, afirman que la forma de probar que una vulnerabilidad encontrada en un sistema informático se pueda considerar realmente como un riesgo de seguridad, es mediante la explotación de esta.

También, Christopher Hadnagy[10], en su libro “Social Engineering – The Art of Human Hacking” en la ciudad de Indianápolis en 2011, afirma que en un proyecto de Ethical Hacking, la fase de recolección de información es de vital importancia, ya que es la que provee la información inicial para perfilar el objetivo y de esta forma poder diseñar, planificar y desarrollar el ataque.

Por otro lado, Lee Brotherston y Amanda Berlin[11], en su libro “Defensive Security Handbook - Best Practices for Securing Infrastructure” en 2017, afirman que la educación y la conciencia de los usuarios a cerca de la seguridad informática de las compañías en las cuales laboran es un punto de alto impacto y evidencian lo anteriormente dicho con una investigación que arrojo que el Phishing, se ha convertido en un ataque popular. También, recomiendan que los planes de

---

[8]Fuentehttp://repository.unimilitar.edu.co/bitstream/10654/16513/3/CastanedaSuarezAndresFernando2017.pdf

[9] (David Kennedy, Jim O’Gorman, Devon Kearns, Mati Aharoni. Metasploit The Penetration Tester’s Guide. San Francisco. 2011. Cap 2, P 7-14.)

[10] (Christopher Hadnagy. Social Engineering – The Art of Human Hacking. Wiley Publishing, Inc. Indianapolis. 2011. Cap 2, P 47-85.)

[11] (BROTHERSTON, Lee – BERLIN, Amanda. Defensive Security Handbook - Best Practices for Securing Infrastructure, 2017 firts edition – EEUU, OREILLY, pag: 149-169, “Chapter 5. User Education”)

capacitación deben convertirse en talleres vivenciales, en el que, haciendo uso de técnicas de sensibilización y concientización, al igual que el uso de estímulos y simular escenarios de la vida real, permite aumentar las habilidades de los usuarios, y esto redunda en el refuerzo de la seguridad en las compañías.

También, Domenic Antonucci[12], en su libro "The Cyber Risk Handbook – Creating and Measuring Effective Cybersecurity Capabilities" en 2017, afirma que las organizaciones deben despertar y tomar conciencia sobre los riesgos cibernéticos a los que están expuestos, y desarrollar diferentes estrategias que les permitan mitigar estos riesgos y garantizar así la sostenibilidad.

2.2. MARCO TEÓRICO CONCEPTUAL

El concepto de 'hacker' se encuentra actualmente en boca de todos. Paredes Flores Carlos Iván, en su libro hacking[13] define a un hacker como un individuo apasionado por las computadoras y que traspasa los límites normales de interés por ellas. También dice que los hackers son personas con alto sentido de curiosidad, quieren acceder a todas las partes del sistema, todo lo prueba, no paran hasta lograrlo y no se retiran ante el primer problema.

La situación es que varias de estas personas usan las actitudes y cualidades descritas anteriormente para acceder a los sistemas informáticos de forma abusiva para realizar acciones ilícitas convirtiéndose en delincuentes informáticos. En el argot de la tecnología informática se denominan "Black Hacker".

En contraposición, también existen hacker que usan sus conocimientos para acceder a los sistemas informáticos en búsqueda de las vulnerabilidades existentes para explotarlas, pero con propósitos diferentes a los anteriores. Estas personas se denominan "White Hacker".

---

[12] (ANTONUCCI Domenic. The Cyber Risk Handbook – Creating and Measuring Effective Cybersecurity Capabilities, 2017 – EEUU, WILEY, pag: 2-4, "Introduction. Toward an Effectively Cyber Risk-Managed Organization")

[13] Paredes Flores, Carlos Iván. (2009). Hacking. El Cid Editor | apuntes. Pág. 7 -9 ProQuest ebrary. Web.

El concepto Ethical Hacking se deriva de este último tipo de hacker, y su función básicamente es la de evaluar la seguridad de un sistema informático, para lo cual utiliza métodos de pruebas o test de penetración en búsqueda de las falencias de seguridad con el objetivo de corregirlas y mejorar el nivel de seguridad del sistema.

El autor Carlos Tori en su libro Hacking Ético[14] dice que para simular la forma de ataque de un hacker y no serlo, esta persona tiene que tener un valor humano que se denomina ética. En este sentido Tori tiene toda la razón, si una organización contrata una persona para realizar un hacking ético con el objetivo de mejorar la seguridad de su sistema y esté se aprovecha de la situación por ejemplo para incrustar una puerta trasera, con el fin de tener acceso al sistema posteriormente y de forma no autorizada para sacar provecho, esta forma de actuar no corresponde a un Hacking Ético.

Este autor resume el proceso de Ethical Hacking en las siguientes etapas:

- Selección y contratación servicio de Ethical Hacking por parte de la organización
- Autorización y convenios de confidencialidad
- Planificación estratégica, objetivos, alcance, metodologías, etc.
- Análisis vulnerabilidades, acciones de ataque sin comprometer el sistema
- Análisis de resultados de evaluación de seguridad
- Diseño, entrega y sustentación de informes
- Implementación de controles para corregir vulnerabilidades o para mitigar el riesgo
- Adopción de políticas de seguridad por parte de la organización.

2.2.1 Vulnerabilidad

Según Escrivá Gasco en su libro Seguridad Informática[15], define vulnerabilidad como “cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la

---

[14] Tori, Carlos. (2008) Hacking Ético. Rosario Argentina. El Autor, Pág. 13-16. Disponible en: https://www.maestrodelacomputacion.net/libro-gratuito-de-hacking-etico-en-espanol/

[15] Escrivá Gascó, Gema. Romero Serrano, Rosa María. Ramada, David Jorge. (2013) Seguridad Informática.Editorial Macmillan Iberia, S.A. Pág. 8-10, ProQuest ebrary. Web.

implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas".

Es de vital importancia tomar las medidas necesarias para corregir una vulnerabilidad detectada, ya que esta es pone en peligro potencial la seguridad y estabilidad del sistema informático.

2.2.2 Amenaza

Según Escrivá Gasco en su libro Seguridad Informática, define una amanezca como "cualquier entidad o circunstancia que atenta contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria como por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño".

En función de las acciones realizadas por parte del atacante, las amenazas se clasifican en pasivas y activas:

- Amenaza Pasiva: Su finalidad es averiguar y obtener información generalmente capturada de una comunicación.
- Amenaza Activa: Cuando se intenta realizar alguna actividad que altere, sustraiga, consulte, o realice algún cambio no autorizado en el estado del sistema o en alguno de sus objetos.

Magerit presenta la siguiente clasificación de amenazas:

Ilustración 3. Amenazas según Magerit

Grupos de amenazas	Ejemplos
Desastres naturales	Fuego, daños por agua, desastres naturales.
Desastres industriales	Fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
Errores y fallos no intencionados	Errores de usuarios, errores de configuración, etc.
Ataques deliberados	Manipulación de la configuración, suplantación de la identidad del usuario, Difusión de software dañino, etc.

Fuente:http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=2&docID=10820963&tm=1466006456772

2.2.3 Ataque

Según Escrivá Gasco en su libro Seguridad Informática, define un ataque como "una acción que trata de aprovechar una vulnerabilidad de un sistema informático para

provocar un impacto sobre él e incluso tomar control de mismo. Se tratan de acciones tanto intencionales como fortuitas que pueden llegar poner en riesgo el sistema".

Normalmente un proceso de ataque considera los siguientes pasos:

- Reconocimiento: En este paso se obtiene la información necesaria de la víctima
- Exploración: Se intenta conseguir información del sistema a atacar direcciones IP, sistemas operacionales, sistema de seguridad, contraseñas, usuarios, etc.
- Obtención d acceso: Aquí se intenta acceder al sistema con base a la información anteriormente obtenida y el uso de herramientas para este propósito.
- Mantener acceso: Ya dentro del sistema, se debe tratar por un lado permanecer acceso evitando ser detectados y por otro lado realizar las modificaciones en el sistema que le permita acceder nuevamente sin mayor complejidad, pudiera ser con la creación de un usuario.
- Borrar huellas: Por último, el atacante evitara dejar huellas, por tanto intentara eliminar las evidencias que pudiera haber dejado la intrusión, como por ejemplo eliminar archivos logs.

2.2.4 Firewall

Herramientas que permiten administrar, controlar y filtrar el tráfico de la red. Se trata de una aplicación que restringe el acceso a la maquina desde el exterior, o sea de la red externa, la Web o desde cualquier otra máquina que esté conectada al mismo segmento de la red. Por ello. Por tanto, si la maquina tiene acceso a Internet, un dispositivo físico o lógico tipo firewall es esencial para prevenir el acceso no autorizado de una persona, o de un programa que quiera tomar el control de esta.

Esta herramienta nos permite visualizar, crear, eliminar y modificar las reglas o directrices de entrada y salida del tráfico de datos que el sistema operacional debe aplicar.

En sistemas operativos Linux, se implementa el firewall llamado IPtables. Iptables es un firewall que esta embebido en el kernel del sistema operacional. Este firewall está basado en reglas, su operación consiste en aplicar reglas que el mismo firewall ejecuta. Por lo general la interfaz para la creación de reglas del firewall en Linux es por la línea de comando, pero también se encuentran gráficas para administrar Iptables.

2.2.5 Acceso a la Red

Es un factor que pone en riesgo latente la información almacenada en cualquier dispositivo conectado a la red, hay muchas técnicas que son efectivas, y son técnicas de intrusión que aprovechan las vulnerabilidades o bugs de los sistemas operativos para realizar ataques que pueden afectar seriamente los activos de información de un sistema de una organización y por ende la perdida de información vital para el funcionamiento de esta.

2.2.6 Configuraciones del Sistema

Cuando se instala por primera vez el sistema operativo en una maquina o en un servidor, las variables de configuración de los accesos a la red vienen configuradas por defecto, y en muchas ocasiones esta configuración hace que el sistema sea vulnerable a ataques. Estas configuraciones poden ser modificadas por el encargado de la seguridad o el administrador del sistema para que esas vulnerabilidades no puedan ser aprovechadas y debe estar atento a realizar las actualizaciones provistas por el fabricante.

2.2.7 Control de Contraseñas

El control de contraseñas puede analizarse desde dos puntos de vista. Desde el punto de vista del administrador del sistema, quien tiene la responsabilidad de configurar los parámetros del sistema para no permitir la creación de contraseñas y que estén alineadas a las políticas de seguridad de la organización. Desde el punto de vista del usuario, el cual debe participar activamente de la seguridad del sistema formándose en una cultura organizativa, entendiendo la importancia de tener contraseñas seguras, de la importancia de la seguridad de la información y de los recursos que tienen a su cargo.

2.2.8 Controles de Acceso

Son los elementos, configuraciones o acciones que permiten la autorización, autenticación y auditoria de un usuario al sistema y que le permiten acceder a los objetos de este. La autenticación es la que define si el usuario es aceptado o rechazado, la autorización es la que le permite acceder a los recursos u objetos de la red y la auditoria son los registros que dan evidencia de las actividades y acciones que un usuario realizó en el sistema después de haber sido autenticado.

Existen varias formas de autenticación que involucran contraseñas, llaves físicas, métodos biométricos como huella dactilar, llaves electrónicas, monitoreo, etc.

2.2.9 Privilegios

Los privilegios son los permisos que se le otorga a un usuario sobre un objeto o conjunto de objetos de un sistema de información o de un sistema operacional. En un sistema operacional como Windows, los privilegios dependen al tipo de cuenta que tenga asociado el usuario, por ejemplo, si es tipo administrador, normal o invitado el usuario tiene permisos o no para realizar ciertas acciones en o sobre el sistema. En un sistema operacional como Linux los privilegios de acceso están definidos de acuerdo con el grupo de trabajo que se asocie. De todas formas, siempre hay un usuario o tipo de usuario que es el que administra y otorga los privilegios a las demás cuentas.

2.2.10 Puertos Lógicos y Servicios

Un puerto es una conexión lógica, y en el marco de Internet y utilizando el protocolo de Internet, es la manera en que un programa cliente solicita un determinado servicio (HTTP, Apache, FTP, SSH, Correo, etc.) a una máquina que puede estar en la red interna o en la red externa web. Por tanto, podemos decir que los puertos son los puntos o canales de acceso que proveen las máquinas para el uso de servicios y el flujo de datos entre ellos.

Existen 65535 puertos lógicos de red. Se puede asignar cualquiera de estos a cualquier protocolo o servicio, pero existe la entidad denominada IANA que es la encargada de la asignación de los números de puertos a los servicios, La IANA creó tres grupos de puertos:

Puertos bien conocidos: del 0 al 1023, reservados al sistema operativo y usados por Protocolos bien conocidos como por ejemplo HTTP (servidor Web), SSH, POP3/SMTP (servidor de e-mail), Telnet y FTP.

Puertos registrados: Son los puertos que en al rango de 1024 y 49151, pueden ser usados por cualquier aplicación.

Puertos dinámicos o privados: Comprendidos entre los números 49152 y 65535 son denominados, asignados en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Generalmente son usados en conexiones peer to peer (P2P).

Los puertos y servicios son una variable crítica de los sistemas operativos, debido a que en la medida de su incorrecta configuración y administración son puertas

abiertas de acceso al sistema vulnerables y son aprovechadas por atacantes para realizar acciones delictivas que atentan contra la seguridad del sistema.

Por tanto, el administrador de seguridad del sistema debe cerrar todos los puertos y servicios que no se proveen o debe diseñar e implementar las reglas de acceso (entrada y salida) a ellos por medio de la configuración y puesta en marcha del firewall.

2.2.11 Software de Seguridad

Es el software que en conjunto con el sistema operativo brindan y proveen controles en cuanto al riesgo en el tema de la intrusión y la violación de la información almacenada, en este ámbito encontramos una serie de software para este propósito como lo son los antivirus, anti spam, antimalware, IDS/IPS, Firewall y otras herramientas de detección y prevención de acciones maliciosas que pretender proteger los recursos TI y a la misma información.

2.2.12 Políticas de Seguridad

Entendida como el conjunto de elementos, acciones, normas y procedimientos establecidos por una organización y que tienen por objetivo regular y definir las reglas del uso de los recursos TI y de la información con el fin de mitigar o reducir el riesgo de pérdida de información y de accesos no autorizados al sistema.

Las políticas de seguridad en un sistema operacional son todas las acciones, y procedimientos que se establecen para garantizar la integridad, disponibilidad y confidencialidad de la información. Por ejemplo, una política que se puede establecer a nivel del sistema operacional es, la de configurarlo para que bloquee un usuario o un acceso desde una IP determinada después de tres intentos de autenticación rechazadas, otra política puede ser, no aceptar contraseñas débiles, otra puede ser, establecer la periodicidad de actualizaciones automáticas del sistema, etc.

2.3. MARCO CONTEXTUAL

2.3.1 Reseña Histórica

En 1923, la Misión Kemmerer, impulsadora de la fundación del Banco de la República bajo el gobierno del general Pedro Nel Ospina, recomendó también la creación de la Contraloría General de la República, con el fin de dotar al país de una gran oficina de control. Al demostrarse la bondad de esta medida se determinó instituir la Contraloría Municipal de Bogotá, con una delimitación clara de independencia y de la función fiscalizadora.

Fue así, como en septiembre de 1929, el Concejo Municipal de Bogotá, presidido por el eminente médico y hombre público profesor Jorge E. Cavelier, aprobó por unanimidad el Acuerdo 23 del citado año, por medio del cual se creó la Contraloría de Bogotá. Desde ese luminoso día en que el cabildo capitalino creó la entidad, la ciudad se vistió de gala para recibir el viento fresco de la modernidad.

Han pasado ya quince lustros, casi 80 años, y la institución ha cambiado de nombre -lo mismo que la ciudad, que por mandato constitucional se denominó Santa Fe de Bogotá entre 1991 y 2000-, sin embargo, no sus objetivos y empeños de establecimiento del control como requisito indispensable de equilibrio y ética para el desarrollo de la suprema metrópoli de Colombia.

Primero se llamó Contraloría Municipal de Bogotá, posteriormente Contraloría de Bogotá Distrito Especial (a partir de 1955), luego Contraloría de Santa Fe de Bogotá, y finalmente, su denominación actual, Contraloría de Bogotá, Distrito Capital. Sus sedes han variado desde que se localizaba en el Edificio “Condominio” en la Avenida Jiménez, corazón de Colombia, pasando por el Centro Administrativo Distrital, hasta la actual sede principal en el Edificio de la Lotería de Bogotá y sus ramificaciones en diversos espacios de la capital.

Desde su creación, la Contraloría de Bogotá ha sido dirigida por destacadas figuras de la vida pública colombiana, como los doctores Hernando Carrizosa Pardo, Carlos Didacio Álvarez, Gustavo Samper Bernal, Eduardo García Badel, Rodrigo Marín Bernal, César Montoya Ocampo, Germán Rueda Escobar, Enrique Low Murtra, Iván Duque Escobar, Augusto Gaitán Quijano y Rosa Natale Rodríguez.

2.3.2 Misión

La Contraloría de Bogotá, D.C., es la entidad que vigila la gestión fiscal de la administración distrital y de los particulares que manejan fondos o bienes públicos, en aras del mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital.

2.3.3 Visión

En el año 2020, la Contraloría de Bogotá, D.C., será reconocida por los ciudadanos como una entidad confiable por su efectividad en la vigilancia y control del uso adecuado de los recursos públicos, fundada en la participación ciudadana, la sostenibilidad y el uso de la tecnología.

2.3.4 Políticas de calidad

Somos un equipo comprometido con la vigilancia a la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, a través del mejoramiento continuo de los procesos, el fortalecimiento de la capacidad institucional, la optimización de los recursos, la actualización de las tecnologías de la información y las comunicaciones y el cumplimiento de los requisitos aplicables, generando productos con calidad y oportunidad que satisfagan las necesidades y expectativas de nuestros clientes, en un ambiente de trabajo seguro y responsable con el medio ambiente y de este modo contribuir al mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital.

2.3.5 Objetivos de calidad

- Fortalecer la vigilancia y control a la gestión fiscal desde los resultados y el impacto.
- Vincular a la ciudadanía en el ejercicio del control fiscal para que genere insumos al proceso auditor y sea aliada en el control de los recursos públicos
- Fortalecer la capacidad institucional, optimizando los recursos, hacia un control fiscal efectivo.
- Estar a la vanguardia de las tecnologías de la información y las comunicaciones - Tics, que potencialicen los procesos y fortalezcan el ejercicio de control fiscal.

2.3.6 Estructura organizacional

La Contraloría de Bogotá, D. C., tiene la siguiente estructura interna:

El Despacho del Contralor, es el nominador y la oficina de mayor jerarquía; la cual está compuesta por la Dirección de Apoyo al Despacho, y la Dirección de Reacción Inmediata.

La Dirección de Participación Ciudadana y Desarrollo Local, oficina misional encargada de realizar las auditorías de control fiscal en las diferentes alcaldías de

la ciudad de Bogotá; está compuesta por la Subdirección de Gestión Local y las Gerencias de Localidades.

La Oficina de Control Interno oficina de apoyo encargada de los temas de control y gestión de calidad.

La Oficina de Asuntos Disciplinarios, oficina de apoyo encargada del control disciplinario de los funcionarios.

La Oficina Asesora de Comunicaciones, oficina de apoyo encargada de velar por la imagen y las comunicaciones al interior y exterior de la Contraloría de Bogotá.

Oficina Asesora Jurídica, oficina encargada de la defensa de la contraloría de Bogotá D.C.

Despacho del Contralor Auxiliar, oficina encargada de apoyar la gestión del Contralor de Bogotá D.C.

Dirección de Planeación, oficina encargada de fijar los lineamientos y gerencia de proyectos de la Contraloría.

Subdirección de Análisis, Estadísticas e Indicadores, oficina de apoyo encargada de establecer y analizar los indicadores estadísticos.

Dirección de Tecnologías de la Información y las Comunicaciones está compuesta por la Subdirección de la Gestión de la Información y la Subdirección de Recursos Tecnológicos.

La Dirección de Estudios de Economía y Política Pública compuesta por: la Subdirección de Estudios Económicos y Fiscales, la Subdirección de Estadística y Análisis Presupuestal y Financiero, la Subdirección de Evaluación de Política Pública.

La Dirección Sector Movilidad compuesta por Subdirección de Fiscalización Movilidad y la Subdirección de Fiscalización Infraestructura.

La Dirección Sector Hábitat y Ambiente compuesta por la Subdirección de Fiscalización Hábitat, la Subdirección de Fiscalización Ambiente y la Subdirección de Fiscalización Control Urbano.

La Dirección Sector Servicios Públicos compuesta por la Subdirección de Fiscalización de Acueducto y Saneamiento Básico, la Subdirección de Fiscalización de Energía y la Subdirección de Fiscalización de Comunicaciones.

La Dirección Sector Salud compuesta por la Subdirección de Fiscalización Salud.

La Dirección Sector Integración Social.

La Dirección Sector Gobierno compuesta por la Subdirección de Fiscalización Gestión Pública y Gobierno.

La Dirección Sector Educación compuesta por la Subdirección de Fiscalización Educación.

La Dirección Sector Hacienda.

La Dirección Sector Desarrollo Económico, Industria y Turismo.

La Dirección Sector Cultura Recreación y Deporte compuesta por la Subdirección de Fiscalización Cultura, Recreación y Deporte.

La Dirección Sector Gestión Jurídica.

La Dirección Sector Equidad y Genero.

La Dirección Sector Seguridad, Convivencia y Justicia

La Dirección de Responsabilidad Fiscal y Jurisdicción Coactiva compuesta por la Subdirección del Proceso de Responsabilidad Fiscal y la Subdirección de Jurisdicción Coactiva.

La Dirección Administrativa y Financiera compuesta por la Subdirección Financiera, la Subdirección de Contratación, la Subdirección de Recursos Materiales y la Subdirección de Servicios Generales.

La Dirección de Talento Humano compuesta por la Subdirección de Carrera Administrativa, la Subdirección de Gestión de Talento Humano, la Subdirección de Capacitación y Cooperación Técnica y la Subdirección de Bienestar Social

2.3.7 Referente Nacional

Según lo establecido en el artículo 3 del acuerdo 519 de 2012, emitido por el concejo de Bogotá, los objetivos generales de la contraloría de Bogotá D.C., son:

"..1. Ejercer en representación de la comunidad la vigilancia de la gestión fiscal de la administración del Distrito Capital y los particulares que manejen bienes o fondos del Distrito Capital, evaluando los resultados obtenidos por las diferentes organizaciones y entidades del Sector Público Distrital, en la correcta, eficiente, económica, eficaz y equitativa administración del patrimonio público, de los recursos naturales y del medio ambiente.

“Somos una entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejen fondos o bienes públicos, en aras del mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital.” “A 2015 la Contraloría de Bogotá, D.C., será reconocida como un organismo de control respetable, confiable, técnico y oportuno en el ejercicio de la función de vigilancia del manejo de los recursos públicos del Distrito Capital.”

2. Generar una cultura del control del patrimonio del Sector Público Distrital y de la gestión pública.

3. Evaluar el cumplimiento y conformidad de las acciones de la Administración Distrital en sus diferentes niveles y sectores con los objetivos, planes, programas y proyectos que constituyen en un período determinado, las metas y propósitos de la administración; realizar el balance social de las políticas públicas del Distrito Capital y de sus finanzas, así como la elaboración de estudios e investigaciones de impacto en la ciudad.

4. Establecer si las operaciones, transacciones, acciones jurídicas, financieras y materiales en las que se traduce la gestión fiscal se cumplieron de acuerdo con las normas prescritas por las autoridades competentes, los principios de contabilidad universalmente aceptados o señalados por el Contador General de la República.

5. Contribuir con los informes de auditoría en el mejoramiento de la gestión administrativa y fiscal de las entidades distritales.

6. Establecer las responsabilidades fiscales e imponer las sanciones administrativas pecuniarias que corresponda y las demás acciones derivadas del ejercicio de la vigilancia y control fiscal; así como procurar el resarcimiento del daño al patrimonio público a través de la jurisdicción coactiva…”

2.3.8 Marco Legal

La naturaleza de la Contraloría de Bogotá fue establecida en el Decreto 1421 de 1993, artículo 105 “Titularidad y naturaleza del control fiscal”, en los siguientes términos:

“La vigilancia de la gestión fiscal del Distrito y de los particulares que manejen fondos o bienes de este, corresponde a la Contraloría Distrital.

Dicho control se ejercerá en forma posterior y selectiva, conforme a las técnicas de auditoría, e incluirá el ejercicio de un control financiero, de gestión y de resultados, en la eficiencia, la economía, la equidad y la valoración de los costos ambientales, en los términos que señalen la ley y el Código Fiscal.

El control o evaluación de resultados se llevará a cabo para establecer en qué medida los sujetos de la vigilancia logran sus objetivos y cumplen los planes, programas y proyectos adoptados para un período determinado.

La Contraloría es un organismo de carácter técnico, dotado de autonomía administrativa y presupuestal. En ningún caso podrá ejercer funciones administrativas distintas a las inherentes a su propia organización.

La vigilancia de la gestión fiscal de la contraloría se ejercerá por quien designe el tribunal administrativo que tenga jurisdicción en el Distrito."

3. METODOLOGÍA

3.1. TIPO DE INVESTIGACIÓN

El tipo de investigación para desarrollar este proyecto es aplicado, ya que parte de la aplicación de los conocimientos específicos en el área de la Seguridad de la Información, contribuyendo con el desarrollo empresarial y tecnológico de las Entidades del Distrito Capital.

3.2. DISEÑO DE INVESTIGACIÓN

El diseño de esta investigación es de tipo descriptivo ya que se podrá observar la conducta del sistema ante un ataque de penetración en la fase de recolección de información, ordenar y analizar los resultados con el objetivo de determinar posibles vulnerabilidades de seguridad.

3.3. HIPÓTESIS

Un sistema de información se hace más seguro en la medida que se conozcan y se mitiguen las debilidades y vulnerabilidades de seguridad existentes.

3.4. VARIABLES

Parámetros de seguridad instalados en la Red Empresarial.

3.5. POBLACIÓN

El universo objeto de la muestra son los servidores que alojan el sistema de información de la Contraloría de Bogotá, D.C., y en particular de los aplicativos Prefis y Sivicof.

3.6. MUESTRA

El presente trabajo estará enmarcado en la técnica de caja blanca, la que define que el total de las pruebas será acompañado por la Contraloría de Bogotá D.C., y en ese entendido las pruebas serán realizadas a la totalidad de direcciones IP que

ellos nos suministran y a los servidores y equipos expresamente autorizados por el departamento de las Tecnologías de la Información y las Comunicaciones.

3.7. INSTRUMENTOS O TÉCNICAS PARA LA RECOLECCIÓN DE LA INFORMACIÓN

Para el desarrollo de este proyecto se aplicará la técnica de observación estructurada[16], la cual consiste en observar de forma cuidadosa y atenta el fenómeno, evento, acción, hecho o situación con el objeto de adquirir información y registrarla para ser analizada y valorada.

El tipo de observación científica, que consiste en ver la situación, evento o cosa con un objetivo definido, claro, y preciso. El investigador identifica claramente lo que desea observar y con que propósito lo hace, o quiere hacerlo, esto involucra que el investigador debe cuidadosamente preparar la observación.

En relación con las pruebas de penetración a realizarse en el sistema de la Contraloría de Bogotá, se seguirían los pasos que debe seguir la técnica de la Observación a saber: Determinar el objeto y los objetivos de observación, establecer la forma de salida de los resultados, observar cuidadosamente y analíticamente, registrar los resultados, interpretar y analizar los resultados, desarrollar las conclusiones y elaborar informe de observación.

Los instrumentos que utilizar para recopilar información son; la elaboración y aplicación de entrevistas libres, de comprobación, de exploración, y entrevistas informales. En lo concerniente al pentesting y su análisis se registrarán las pruebas a realizar, herramienta utilizada y resultado obtenido, todo esto en al marco de referencia de la metodología PTES (The Penetration Testing Execution Standard).

3.8. FUENTES DE INFORMACIÓN

De acuerdo con la metodología PTES las fuentes de información se dividen en Activas y Pasivas.

---

[16] Puente Wilson. TÉCNICAS DE INVESTIGACIÓN [en línea]. Disponible en: http://www.rrppnet.com.ar/tecnicasdeinvestigacion.htm

3.9. RECURSOS

3.9.1 Recursos Materiales

Los recursos necesarios para el desarrollo del proyecto se enumeran, en la siguiente tabla:

Tabla 1. Recursos necesarios para el desarrollo del Proyecto valores en millones de pesos.

ÍTEM	RECURSO	DESCRIPCIÓN	PRESUPUESTO
1	Equipo Humano	Servicios Profesionales de Ingeniera de Sistemas y Tecnología de Redes de Datos	20,000,000
2	Equipos y Software	Licencias Sistema Operacional, Ofimática y de Pentesting, Equipos Portátiles y periféricos	5,000,000
3	Viajes y Salidas de Campo	Transporte e imprevistos	2,000,000
4	Materiales y suministros	Elementos de papelería, fotocopias, etc.	1,000,000
5	Bibliografía	Adquisición de Manuales y Normas	2,000,000
		TOTAL:	30,000,000

3.9.2 Recursos Institucionales

Para el desarrollo del proyecto se cuenta con la autorización para realizar las pruebas sobre un delimitado grupo de recursos informáticos previa concertación con el departamento TIC de la Contraloría de Bogotá D.C.

Se cuenta para el desarrollo del proyecto con el acompañamiento de la UNAD en cabeza de sus tutores y con el apoyo de la Contraloría de Bogotá D.C. en cabeza de las direcciones TIC y Talento Humano.

3.10. PROPONENTES O PERSONAS QUE PARTICIPAN EN EL PROYECTO

El proyecto es una propuesta desarrollada por Lenin Herrera Moncada y Osbaldo Cortés Lozano, para acceder al título de Especialista en Seguridad Informática, con el apoyo de los instructores, compañeros de la UNAD y de la Contraloría de Bogotá.

3.10.1 Proponentes Primarios

El desarrollo del proyecto será ejecutado por: Lenin Herrera Moncada, Osbaldo Cortés Lozano; bajo los lineamientos de la Universidad Abierta y a Distancia representada por el Ingeniero: Juan José Cruz.

3.10.2 Proponentes Secundarios

El proyecto cuenta con el apoyo de las directivas de la Contraloría de Bogotá, en cabeza de la Ingeniera Carmen Rosa Mendoza; Directora de Tecnologías de Información y las Comunicaciones.

3.11. CRONOGRAMA

Tabla 2. Cronograma de Actividades

ITEM	CRONOGRAMA DE ACTIVIDADES	SEMANAS															
	ACTIVIDAD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Reunión y comunicación previa	X	X														
2	Recolección pasiva de información (Passive Footprinting)		X	X	X	X	X										
3	Recolección activa de información (Active Footprinting)		X	X	X	X	X										
4	Enumeración						X	X	X	X							
5	Análisis de vulnerabilidades								X	X	X	X	X				
6	Diseño y planificación de la ejecución del ataque											X	X	X	X		
7	Elaboración y Entrega de informes		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

4. RESULTADOS

4.1. IDENTIFICACIÓN INFORMACIÓN APLICATIVOS SIVICOF Y PREFIS

4.1.1 Aplicativo Sivicof

El Sistema de Información Sivicof (Sistema de Vigilancia de Control Fiscal) es el aplicativo por medio del cual las entidades distritales de Bogotá, las cuales son sujetos de control fiscal por parte de la Contraloría de Bogotá, D.C., presentan la redición de cuentas de todas sus actuaciones fiscales y administrativas.

La información que rinden los sujetos de control a través del Sistema SIVICOF mediante formularios electrónicos y documentos electrónicos se constituye en una prueba para cualquier proceso que adelante la Contraloría de Bogotá D.C.

Los sujetos de control rinden cuentas a cerca de sus actuaciones en áreas como:

- Presupuestales
- Contratación
- Planes de Mejoramiento
- Control Fiscal
- Gestión y Resultados
- Contabilidad

Sivicof es el sistema de información con el que cuenta la Contraloría de Bogotá, D.C., para realizar los siguientes procesos tendientes al control Fiscal:

1. Auditor: Planeación y ejecución de las auditorías de investigación
2. Plan de Mejoramiento: Formulación de hallazgos, solicitud al sujeto de control de la formulación del plan de mejoramiento con base a los hallazgos encontrados y evaluación de las actividades realizadas o dejadas de realizar por el sujeto de control según el plan de mejoramiento.

El Sistema Sivicof se compone básicamente de 3 módulos:

- StormUser: Módulo LOCAL que permite gestionar y cargar información para alimentar el módulo StormWeb.
- StormWeb: Módulo WEB que permite subir la información generada por StormUser a la Base de Datos.
- StormReport: Módulo WEB que permite consultar y generar reportes de la información almacenada en la Base de Datos.
-

4.1.2 Aplicativo Prefis

El Sistema de Información PREFIS es el aplicativo que utiliza la Contraloría de Bogotá, D.C., para la gestión y control del Proceso de Responsabilidad Fiscal amparados bajo la ley 610 de 2000, función que esta a cargo de la dependencia Dirección de Responsabilidad Fiscal y Jurisdicción Coactiva de la Contraloría de Bogotá D.C.

El sistema de Información PREFIS permite el almacenamiento, la gestión y procesamiento de toda la información asociada a los procesos de responsabilidad fiscal que se adelantan en la Dirección de Responsabilidad Fiscal y Jurisdicción Coactiva, provenientes de las diferentes dependencias o Direcciones Sectoriales y del Grupo GAE (Grupo de Actuaciones Especiales).

Las principales funcionalidades del sistema PREFIS son las siguientes:

- Registro, gestión y control de cada una de las actuaciones realizadas sobre un proceso de responsabilidad fiscal tramitado por la Dirección de Responsabilidad Fiscal y Jurisdicción Coactiva, que permita conocer en cualquier momento el estado real del proceso.
- Consulta y generación de información y reportes que permitan retroalimentar el proceso de Responsabilidad y que sirven de insumo para la toma de decisiones por la alta dirección.

Por tanto, el sistema PREFIS apalanca los objetivos estratégicos de la Contraloría de Bogotá, D.C., tendiente al fortalecimiento de la vigilancia y control a la gestión fiscal de los sujetos de control que permitan identificar el daño patrimonial causado a la ciudad, la cuantificación de este, la plena identificación de los responsables y el resarcimiento del daño causado.

4.2. RECOLECCIÓN DE INFORMACIÓN

En esta fase se realiza la inteligencia a los sistemas, para guiar las acciones de evaluación, se precisa recopilar información acerca de empleados, instalaciones, productos y planes[17], según la OSINT existen dos fuentes de recopilación de información:

[17] Penetration Testing Execution Standard. disponible en: http://www.pentest-standard.org/index.php/FAQ

1. Fuentes externas: (external footprinting) es toda la información que se puede recolectar del medio, competencia, funcionarios que en algún momento pueden afectar la organización.
2. Fuentes internas: (internal footprinting) luego de tener acceso a la red de la compañía y haciendo uso de técnicas y herramientas diversas se recopila información que se encuentra al interior de la red.

Adicional, enuncia las técnicas para la recopilación de fuentes externas:

1. Activa: si hay contacto con la empresa auditada.
2. Pasiva: si no hay contacto directo con la empresa auditada, en esta se hace uso del método OSINT (open source intelligence) que se basa en la obtención de datos de fuentes de acceso público.

4.2.1 Recolección pasiva de información

Herramientas que se van a utilizar en la fase:

- HTTrack: crea una copia idéntica de las páginas web a auditar, para su exploración y recolección de información offline
- Whois: este servicio brinda información como: dirección IP, DNS (servicio de nombre de dominio) e información de contacto de la compañía, entre otra.
- Google hacking[18]: técnicas para la obtención de datos, ejemplo el comando “allintitle” ejemplo “alltintle: index of otro comando útil es “inurl”, anexo 1.
- Existe otras fuentes de información como lo son las redes sociales, donde podemos encontrar datos personales, que en muchas ocasiones son utilizadas para la creación de las contraseñas.
- The harvester: potente buscador de direcciones de correo, usuarios y dominios y gracias a esta información recolectada podemos intentar el ingreso mediante servidores SSH, VPN o FTP.
- MetaGoofil: su función es buscar en Internet archivos pertenecientes a la compañía auditada y obtener sus metadatos.
- robtex.com: esta web, es una herramienta útil para la recolección de diferente tipo de información acerca de la infraestructura de red de la compañía.
- Wireshark: herramienta que intercepta las conexiones entrantes y salientes, analizando los protocolos y obteniendo información.

[18] Exploit Database. Disponible en: https://www.exploit-db.com/google-hacking-database/

- Nesssus: sistema de análisis de vulnerabilidades que cuenta con varios filtros.

Herramientas que se van a utilizar en la fase:

- Nmap: herramienta para el escaneo de redes y auditoría de seguridad en redes y su extensión NSE (nmap scripting engine) que amplía las opciones de Nmap.
- Comando Dig: permite realizar consultas DNS.
- Matelgo: permite la obtención de datos como servidores de correo asociados a un dominio.

Herramientas utilizadas para la recolección de información sobre los servicios web:

- Identificación del servidor web: esta tarea se puede facilitar leyendo la información del banner del servicio, usando herramientas como:
  - Ncat
  - Nmap
  - Zenmap
  - WhatWeb
- Identificación de vulnerabilidades y plugins de los CMS: podemos detectar vulnerabilidades usando:
  - Nikto

Ingeniería Social, es otra técnica para recopilar información; existe muchas tácticas para este fin como suplantación por corro o llamadas, olvidar una memoria USB en un lugar donde un funcionario la encuentre y la conectarla a su computador pueda ser implantado un troyano.

Después de recopilada la información debe ser contrastada con el cliente para estructurarla dentro del alcance del proyecto.

Cómo se explicó en el punto 6.8.4; gracias a diferentes técnicas, se va a realizar el acopio de información estratégica de la página Web de la Contraloría de Bogotá D.C., que sirva de insumo para perfilar las diferentes auditorías a los sistemas de Información.

4.2.1.1 Foca

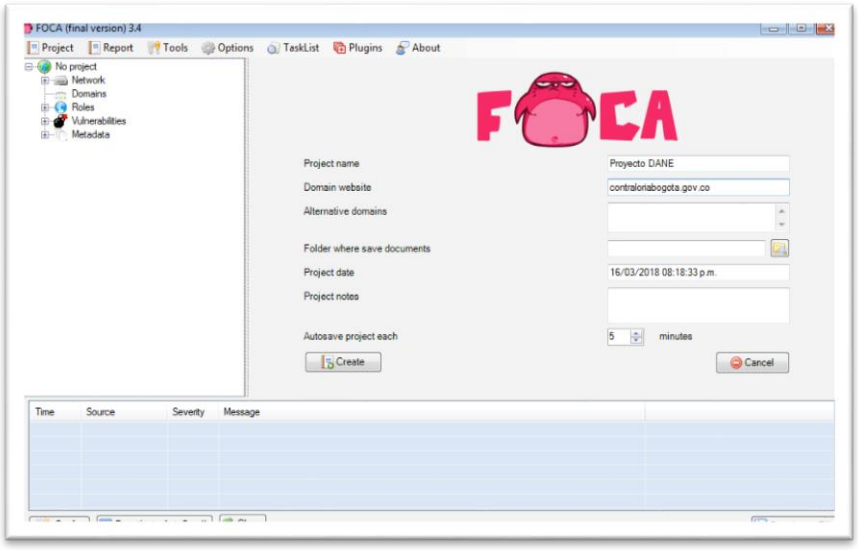
Gracias a esta herramienta se ha recolectado información de calidad, que permite deducir ciertas políticas; como la de creación de usuarios, nombres, cargos, teléfonos y otro tipo de información que explicaremos posteriormente.

La aplicación gratuita en su versión 3.0, se descargó de su página oficial: https://www.elevenpaths.com/es/labstools/foca-2/index.html, en la que también se acceden a diferentes recursos y plugins adicionales para aumentar su funcionalidad.

La extracción de metadatos es otra de las funciones importantes ya que en estos se puede encontrar información importante acerca de la compañía a auditar, como se va a comprobar a continuación.

- Creación de la compañía: Diligenciamos los datos de la compañía y el dominio (contraloriabogota.gov.vo)

Ilustración 4. Creación del usuario



Fuente: propia

- Después de realizado el análisis arrojo los siguientes resultados:
- Usuarios: encontró dos usuarios, para los que muestra información como usuario de red, sistema operativo

Ilustración 5. Usuarios

Fuente propia

- Servidores: se encontraron cuatro;

Ilustración 6. Servidores

Fuente propia

Con la siguiente información: dirección IP, dominios, direcciones ip de origen, HTP, SMTP y FTP, con sus respectivos puertos y dirección IP.

- Dominios: se evidencia que la página auditada tiene cinco dominios, como se observa a continuación:

Ilustración 7. Dominios

Fuente propia

- Servidores de correo: la empresa auditada cuenta con los siguientes servidores de correo con sus respectivas direcciones:

Ilustración 8. Mail

Fuente propia

- Metadatos: se encontraron 1214 documentos entre; .doc, .xls, .ppt y pdf, de los cuales se extrajeron los siguientes metadatos; 239 usuarios, 101 nombre y ruta de carpetas, 77 impresoras con su ruta, 55 tipos de software, 84 cuentas de correo electrónico y 5 sistemas operativos:

Ilustración 9. Metadatos

Fuente propia

4.2.1.2 Whois

Protocolo TCP, cuyo funcionamiento es basado en petición – respuesta, actualmente lo tienen integrado páginas web que realizan búsqueda de datos públicos de un dominio, a continuación, se observa que información arrojada por el dominio de la empresa auditada:

DOMAIN NAME: CONTRALORIABOGOTA.GOV.CO
REGISTRY DOMAIN ID: D618381-CO
REGISTRAR WHOIS SERVER:
REGISTRAR URL: WWW.COINTERNET.COM.CO
UPDATED DATE: 2018-01-03T13:55:59Z
CREATION DATE: 1999-12-27T00:00:00Z

REGISTRY EXPIRY DATE: 2022-12-28T23:59:59Z
REGISTRAR: .CO INTERNET S.A.S.
REGISTRAR IANA ID: 111111
REGISTRAR ABUSE CONTACT EMAIL: SOPORTE@COINTERNET.COM.CO
REGISTRAR ABUSE CONTACT PHONE: +57.16169961
DOMAIN STATUS: OK HTTPS://ICANN.ORG/EPP#OK
REGISTRY REGISTRANT ID: C548983-CO
REGISTRANT NAME: CONTRALORIA DE SANTA FE DE BOGOTA D.C.
REGISTRANT ORGANIZATION: CONTRALORIA DE SANTA FE DE BOGOTA D.C.
REGISTRANT STREET: CRA.35 NO.26 A 10
REGISTRANT STREET:
REGISTRANT STREET:
REGISTRANT CITY: BOGOTA , D.C
REGISTRANT STATE/PROVINCE:
REGISTRANT POSTAL CODE:
REGISTRANT COUNTRY: CO
REGISTRANT PHONE: +57.003378087
REGISTRANT PHONE EXT:
REGISTRANT FAX:
REGISTRANT FAX EXT:
REGISTRANT EMAIL: ADMINISTRATIVA@CONTRALORIA.GOV.CO
REGISTRY ADMIN ID: C548991-CO
ADMIN NAME: CESAR ORLANDO CAMACHO PEQA
ADMIN ORGANIZATION:
ADMIN STREET: CRA.35 NO.26-18 P.10
ADMIN STREET:
ADMIN STREET:
ADMIN CITY: SANTAFE DE BOGOTA
ADMIN STATE/PROVINCE:
ADMIN POSTAL CODE:
ADMIN COUNTRY: CO
ADMIN PHONE: +57.003378065
ADMIN PHONE EXT:
ADMIN FAX:
ADMIN FAX EXT:
ADMIN EMAIL: ADMINISTRATIVA@CONTRALORIA.GOV.CO
REGISTRY TECH ID: C548997-CO
TECH NAME: ROCIO PINZON / LUIS ARMANDO SANCHEZ
TECH ORGANIZATION:
TECH STREET: CARRERA 35 NO. 26 A 18 PISO 7
TECH STREET:
TECH STREET:
TECH CITY: SANTA FE DE BOGOTA
TECH STATE/PROVINCE:

TECH POSTAL CODE:
TECH COUNTRY: CO
TECH PHONE: +571.0000000
TECH PHONE EXT:
TECH FAX:
TECH FAX EXT:
TECH EMAIL: CCOMPUTO@CONTRALORIABOGOTA.GOV.CO
NAME SERVER: NS2-AUTH.ETB.NET.CO
NAME SERVER: NS1-AUTH.ETB.NET.CO
DNSSEC: UNSIGNED
URL OF THE ICANN WHOIS INACCURACY COMPLAINT FORM:
HTTPS://WWW.ICANN.ORG/WICF/
>>> LAST UPDATE OF WHOIS DATABASE: 2018-03-16T00:06:06Z <<<

Cómo se observa se han subrayado los datos que permiten recopilar información; como cuentas de correo y nombres de los encargados de la página web de la empresa auditada.

4.2.1.3 Google Gathering

Gracias a algunas opciones del buscador Google, se puede obtener información importante acerca de la empresa auditada:

“intitle:"admin" site:contraloriabogota.gov.co” con esta búsqueda nos despliega el índice del registro de aplicaciones, permite entrar a gran parte de estos archivos de los cuales se pueden extraer datos y metadatos:

Ilustración 10. Google

Fuente propia

Otra búsqueda que permite acceder al índice de directorios padre; “intitle:"index of /" Parent Directory site:contraloriabogota.gov.co”

Ilustración 11. Google2

Fuente propia

Con la información descargada y con procesos de análisis se pueden obtener datos sensibles de la organización, los cuales se pueden perfilar para las posteriores etapas de auditoría:

Ejemplo:

Se evidencian los nombres y cargos de los servidores, y como se ha visto anteriormente, los usuarios se conforman de la primera letra del nombre más el primer apellido, así que se puede crear una base de correos, para realizar un ataque de pishing o ingeniería social.

Ilustración 12. Ejemplo1

Tomado de búsqueda en Google. Fuente propia

4.2.1.4 Robtex.com

Página web que apoya la búsqueda pasiva de información suministrando datos de servidores de dominio, IPs, y muestra una aproximación de la infraestructura de la red.

Ilustración 13. Aproximación Red

Fuente propia

Ilustración 14 - robotex

Fuente propia https://www.robtex.com/dns-lookup/contraloriabogota.gov.co

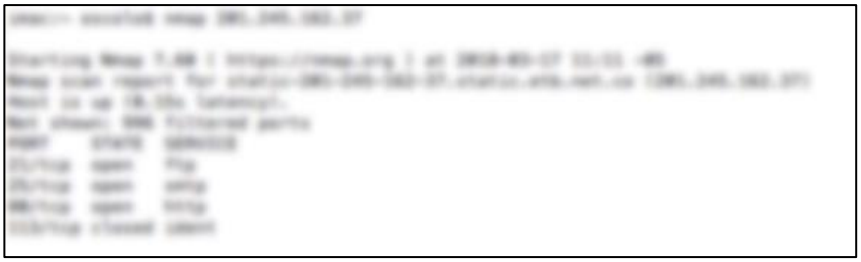
4.2.1.5 NMAP, toma pasiva de información:

Escaneo a las direcciones halladas con FOCA:

Tabla 3. Evidencia FOCA.

Dirección IP	Servicio	Estado

Ilustración 15. NMAP-passive



Fuente propia

4.2.1.6 The Harvester

Esta herramienta disponible en Kali o Mac OS; permite recolectar información de manera pasiva de datos cómo: emails, subdominios, puertos, hosts, funcionarios, entre otros, utilizando fuentes como buscadores, SHODAN y redes sociales.

Iniciamos con escaneo de correos y direcciones IP

“theHarvester -d contraloriabogota.gov.co -l 100 -b google”

Ilustración 16. The Harvester

Fuente propia

4.2.1.7 Wireshark

Herramienta de análisis de protocolos de red, que permite interceptar y analizar el tráfico entrante. Se realizó una captura de datos al momento de tratar de ingresar al sistema Sivicof con las siguientes credenciales:

Usuario	contraseña
Admin	admin

El resultado de la captura muestra que los datos viajan en texto plano, evidenciando una falta de encriptado de información ocasionada por el uso de protocolos inseguros como HTTP.

Ilustración 17. Análisis con wireshark.

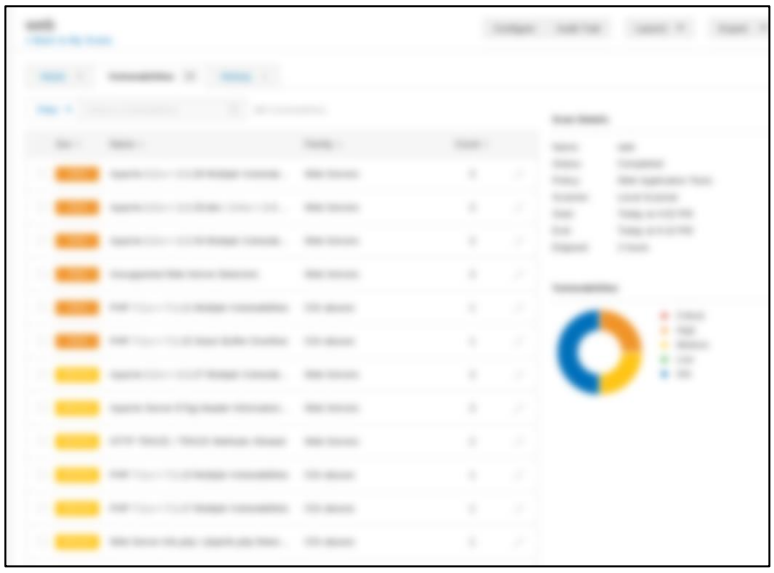
Fuente propia

4.2.1.8 Nessus

Programa de escaneo utilizado para encontrar vulnerabilidades de infraestructura de red, protocolos, aplicaciones, malware y otros, para el caso de las direcciones analizadas nos arrojó los siguientes resultados:

14 vulnerabilidades de alto impacto y 12 vulnerabilidades de medio.

Ilustración 18. Resultados Nessus



Fuente propia

En el detalle de cada vulnerabilidad se observa la descripción, la solución, links a información sobre la vulnerabilidad y la salida del informe, como se observa a continuación y la que servirá de insumo para el diseño y planificación de ataques:

Ilustración 19. Reporte vulnerabilidad

Fuente propia

4.2.2 Recolección Activa de Información

El objetivo es recolectar la mayor cantidad de información posible de la Contraloría de Bogotá D.C., de forma directa, es decir conectado a la misma red donde está el objetivo.

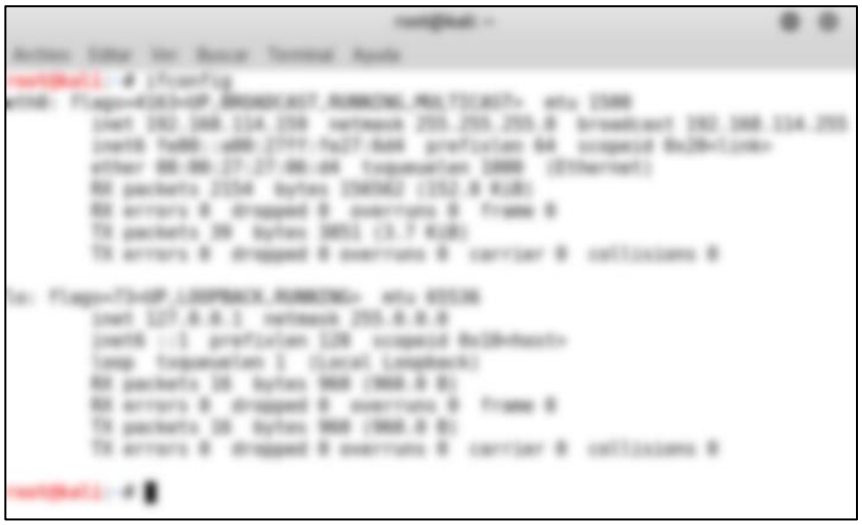
En primer lugar, se identifica la red sobre la cual se está realizando la recolección activa de información.

Ilustración 20. Interfaz de Red Recolección de Información

Fuente propia

Identificación del Nodo desde el cual se está realizando la búsqueda de información:

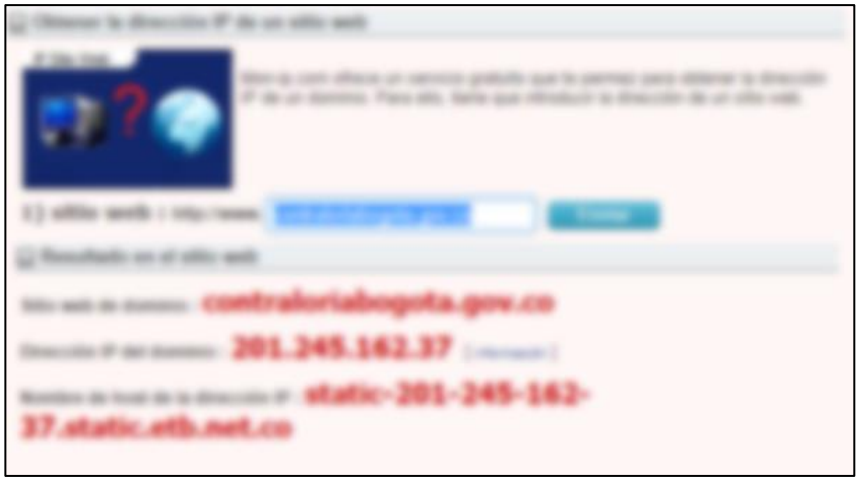
Ilustración 21. Nodo de Recolección de Información



Fuente propia

Mediante la página: www.mon-ip.com, se puede obtener información acerca del servidor de dominio asociado, como se puede observar en la siguiente imagen:

Ilustración 22. IP Pública Sitio Web Objetivo



Fuente propia

A partir de los datos obtenidos anteriormente, se realiza la recolección de información en búsqueda de datos relevantes que permitan develar brechas de la seguridad o que pueda mostrar información sensible, para lo cual se utilizaron las siguientes herramientas clasificadas así:

4.2.2.1 Captura de Información

DNSeunm

El propósito de DNSenum es capturar toda la información que sea posible sobre un dominio, realizando una diversidad de operaciones. Opción –enum

Ilustración 23. DNsenum

Fuente propia

Fierce

Fierce es un escáner que permite realizar un proceso de enumeración, que ayuda a los profesionales de seguridad a localizar direcciones IP y nombres de host para dominios específicos, utilizando DNS, Whois y ARIN.

Ilustración 24. Fierce

Fuente propia

Dmitry

Es una herramienta en línea de comandos para Linux, que permite capturar tanta información como sea posible sobre un host, desde ejecutar un simple Whois hasta generar reportes del tiempo de funcionamiento o escaneo de puertos.

Ilustración 25.Dmitry

Fuente propia

Netcraf.com

Este sitio web genera información valiosa de un determinado dominio, como por ejemplo: ip pública, sistema operacional del servidor donde está implementado, servidor web utilizado y última fecha de actualización.

Ilustración 26. Información Dominio con Netcraf

Fuente propia

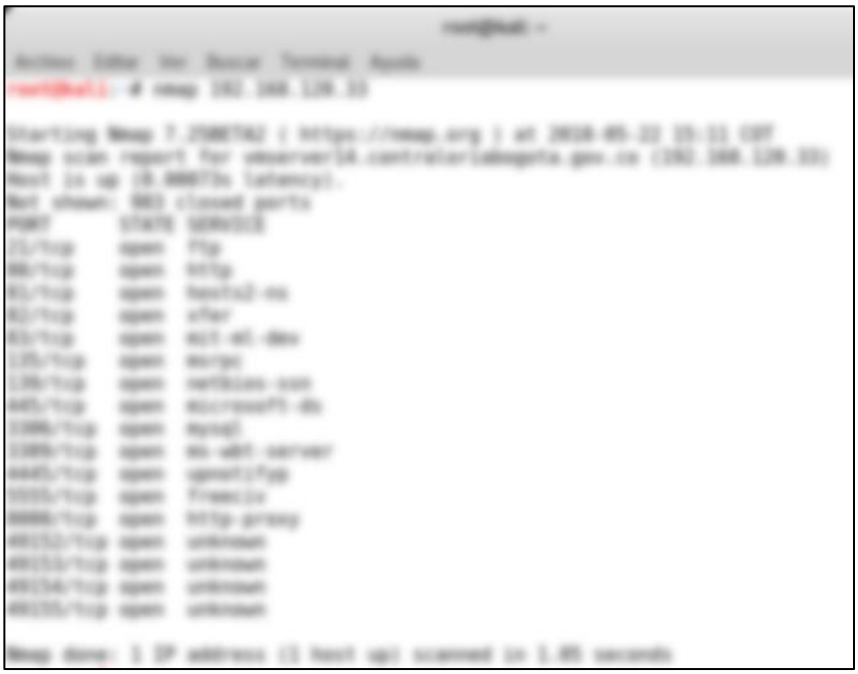
4.2.2.2 Descubriendo el Objetivo

Nmap

Nmap “Network Mapper” o Mapeador de Puertos, es una herramienta Open Source utilizada para la exploración de redes y auditorías de seguridad. Se diseño para escanear rápidamente redes de gran tamaño, así como también maquinas individuales.

Nmap: 192.168.120.33/ contraloria

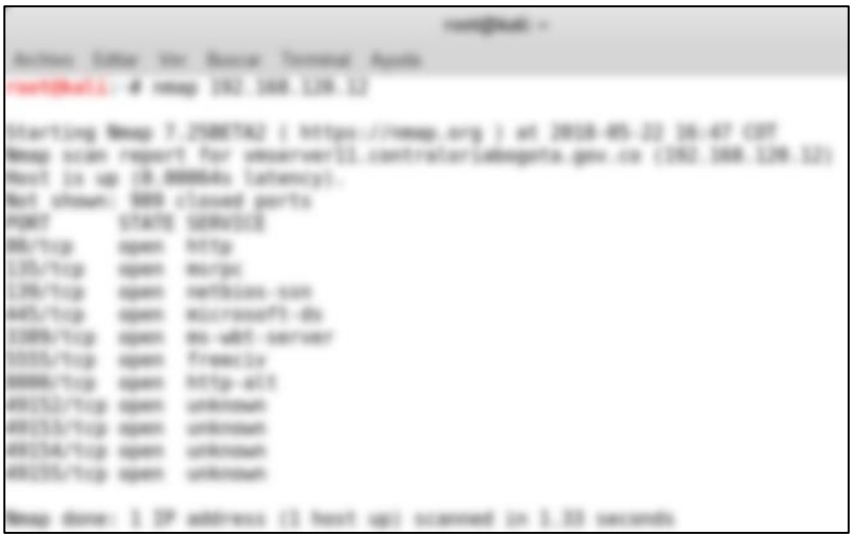
Ilustración 27. Nmap a contraloriabogota.gov.co



Fuente propia

Nmap: 192.168.120.12 / sivicof

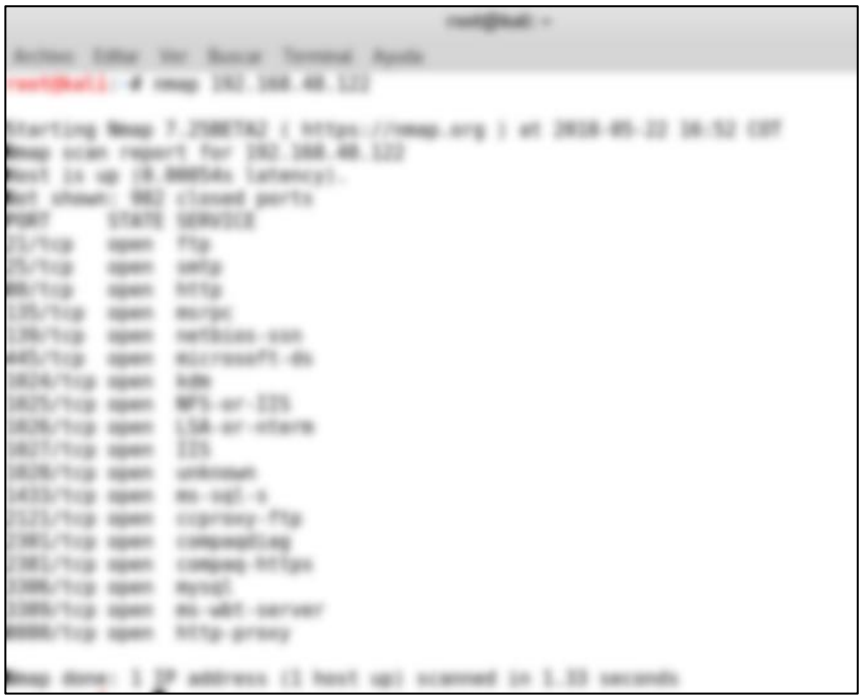
Ilustración 28. Nmap a sivicof.contraloriabogota.gov.co



Fuente propia

Nmap: 192.168.48.122/ prefis

Ilustración 29. Nmap a Prefis



Fuente propia

Nmap -O

El parámetro “-O” permite la identificación del Sistema Operativo de la máquina objetivo, mediante el envío de una serie de paquetes TCP y UDP al host remoto, con el propósito de examinar el paquete de bit en las respuestas.

Ilustración 30. Nmap -O

Fuente propia

4.2.2.3 Enumerar el Objetivo

Nmap -p

Una herramienta muy utilizada es nmap utiliza un escaneo SYN, pero este es substituido por un escaneo tipo Connect si el usuario no tiene los privilegios necesarios para enviar paquetes en bruto. Si en los parámetros de entrada de no definen los puertos, a escanear, entonces, nmap escanean los 1,000 puertos más populares.

Si se quiere definir un conjunto de puertos a escanear, se utiliza la opción “-p” seguido de la lista de puertos o rango de puertos.

Ilustración 31. Nmap -P

Fuente propia

Zenmap

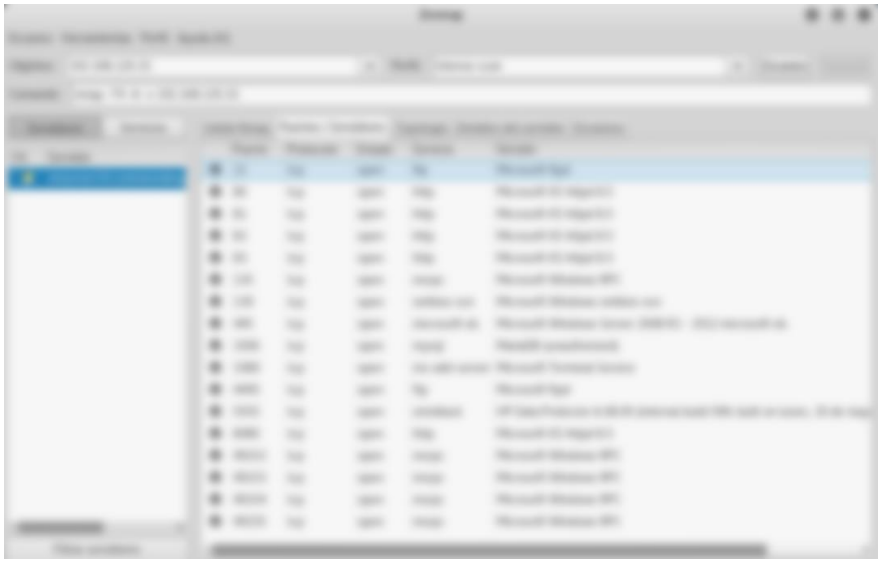
Zenmap es un Interfaz Gráfica para nmap. Es una aplicación de licencia Open Source que facilita el uso de nmap.

La identificación de los servicios activos en un puerto específico puede asegurar que una prueba de penetración tenga éxito. También elimina cualquier duda que se haya generado durante el proceso de reconocimiento acerca de la huella del sistema operativo.

Ilustración 32. Zenmap – contraloriabogota.gov.co

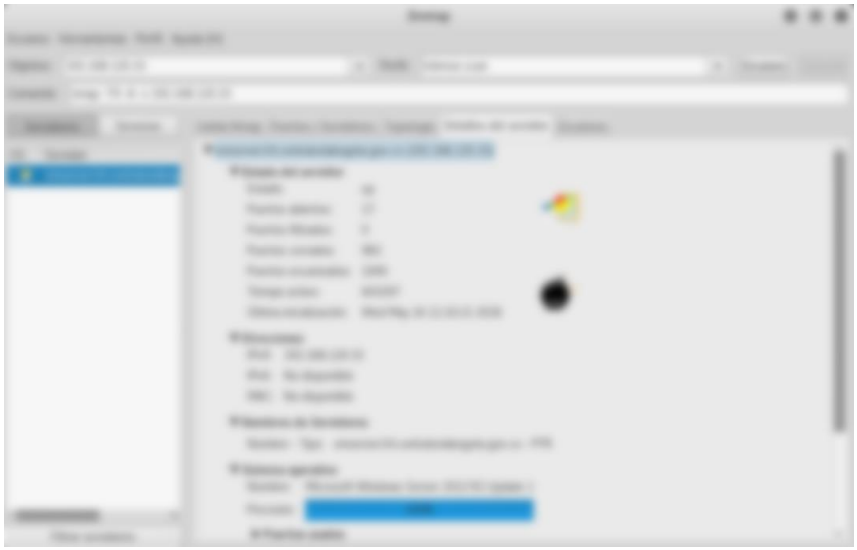
Fuente propia

Ilustración 33. Zenmap - contraloriabogota.gov.co - Puertos Abiertos



Fuente propia

Ilustración 34. Zenmap - contraloriabogota.gov.co - Información Servidor

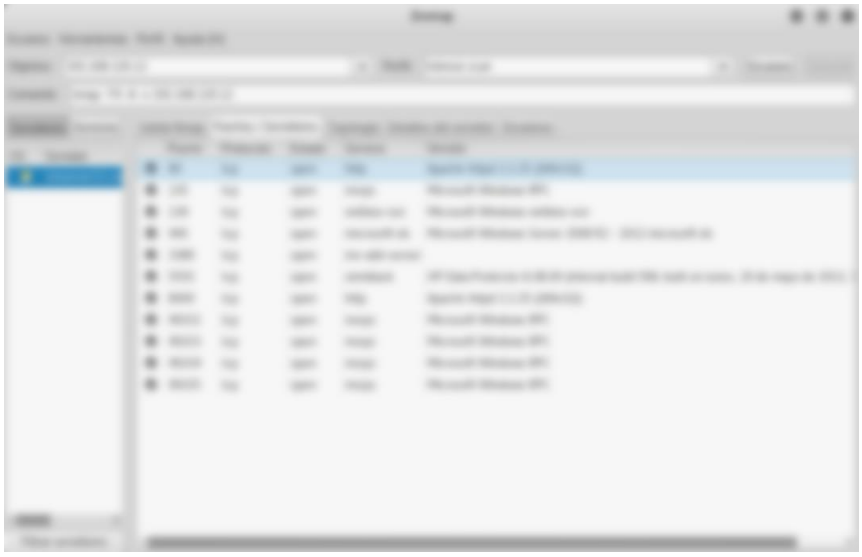


Fuente propia

Ilustración 35. Zenmap – SIVICOF

Fuente propia

Ilustración 36. Zenmap - SIVICOF - Puertos Abiertos



Fuente propia

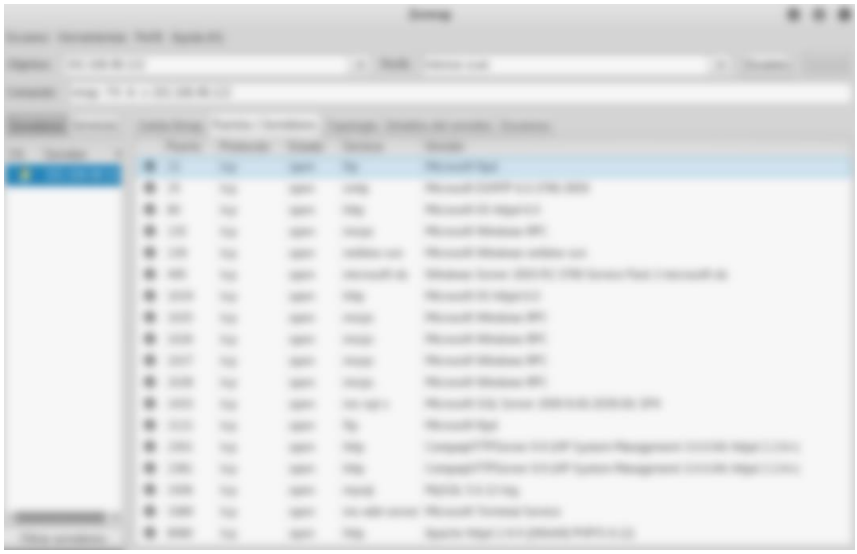
Ilustración 37. Zenmap - SIVICOF - Detalle Servidor

Fuente propia

Ilustración 38. Zenmap - PREFIS

Fuente propia

Ilustración 39. Zenmap - PREFIS - Puertos Abiertos



Fuente propia

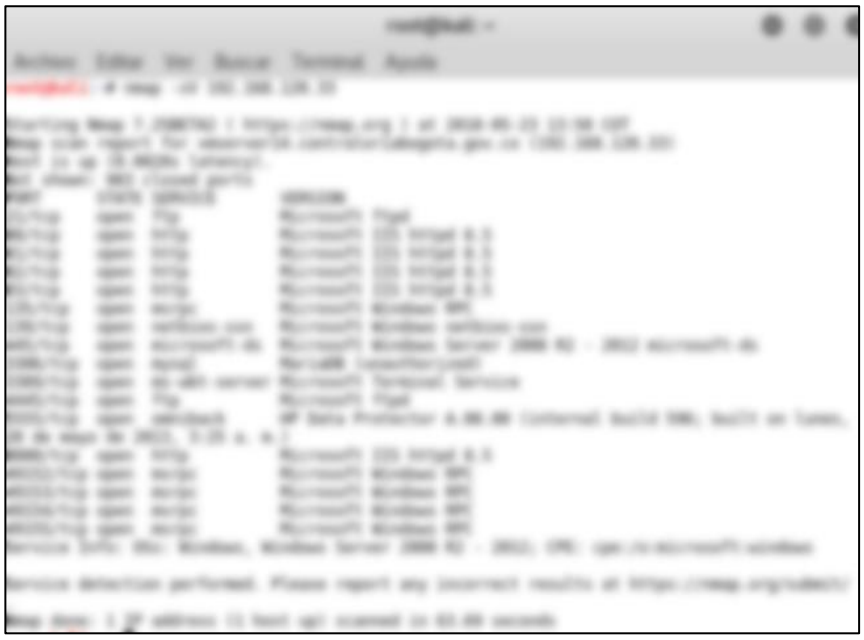
Ilustración 40. Zenmap - PREFIS - Detalle del Servidor

Fuente propia

Nmap –Sv

El parámetro “-sV” de nmap permite la detección de versión. Después de revelar los puertos TCP y UDP mediante escaneo, nmap sondea estos puertos para determinar que está funcionando sobre ellos. Nmap pretende determinar información como el protocolo del servicio, nombre del host, nombre de la aplicación, número de versión, y tipo de dispositivo.

Ilustración 41. Zenmap –sV – contraloriabogota.gov.co



Fuente propia

Ilustración 42. Zenmap –sV – SIVICOF

Fuente propia

Ilustración 43. Zenmap –sV – PREFIS

Fuente propia

4.3. ENUMERACIÓN DE VULNERABILIDADES

Está fase consiste en evidenciar las posibles fallas en los sistemas y aplicaciones que podrían ser usadas por un atacante, se extrae información más detallada sobre lo descubierto en la fase anterior, en esta se evalúa la calidad y utilidad de la información recopilada.

- Diseñar y planificar la ejecución del ataque, seleccionando las herramientas apropiadas para explotar una posible vulnerabilidad.
- Evaluar las amenazas, vulnerabilidades, y riesgos evidenciados en las fases anteriores.
- Elaborar un informe que entregue las recomendaciones a seguir para evitar la materialización de las posibles amenazas.

4.3.1 Reconocimiento

De acuerdo con la información recolectada en las fases anteriores, se realiza la siguiente clasificación:

4.3.1.1 Dominios:

Los dominios asociados a “contraloriabogota.gov.co” son:

Contraloriabogota.gov.co –
Sigespro.contraloriabogota.gov.co –
- Sivicof.contraloriabogota.gov.co -
- Pqr.contraloriabogota.gov.co - ,

4.3.1.2 Ubicación:

El servicio lo presta ETB ubicado en Bogotá D.C.

4.3.1.3 Puertos vulnerables:

De la recolección pasiva se encontraron abiertos los puertos:

De la recolección activa al interior de la Contraloría los puertos: 21, 80, 81, 82, 83, 135, 139, 445, 3306, 3389, 4445, 5555, 8080, 49152, 49152-55.

4.3.1.4 Sistemas operativos:

La herramienta who.is, encontró que los servidores están montados sobre Windows server 2012 R2, Nmap encontró Linux y Windows y FOCA, hosts que utilizan Windows 7 y equipos con Windows XP y un Servidor Apache con PHP.

4.3.1.5 Empleados que trabajan en la Contraloría de Bogotá:

Se encontraron listado de direcciones de 20 funcionarios.

4.3.1.6 Protocolos

Se evidencia el uso de HTTP y FTP, que son considerados inseguros.

4.3.2 Resumen de vulnerabilidades

Se detectaron catorce vulnerabilidades que deben ser tratadas en fases siguientes:

Tabla 4. Resumen vulnerabilidades

Categoría	Tipo de vulnerabilidad	Acción de la vulnerabilidad

Análisis Nessus

Tabla 5. Análisis Nessus

Categoría	Tipo de vulnerabilidad / Ataque	Acción de la vulnerabilidad

Continuación Tabla 5. Análisis Nessus

La aplicación realiza la siguiente aclaración: tenga en cuenta que Nessus no ha probado estos problemas, sino que se ha basado únicamente en el número de versión auto informado de la aplicación.

Las vulnerabilidades anteriormente descritas están basadas en las fases de recolección pasiva y activa de la información y serán utilizadas para el diseño de los ataques.

4.4. DISEÑO DE ATAQUES Y EXPLOTACIÓN

A continuación, se relacionan algunos ataques que se podrían ejecutar de acuerdo con su categoría:

Tabla 6. Diseño de Ataques y Explotación

Categoría	Tipo de ataque	Herramienta
FTP Bounce attack	FTP Brute force Attack FTP_login	Metasploit Nmap Armitage
Spoofing	DNS spoofing	Ettercap -g Yersnian Hamster Cain y Abel
Puertos abiertos 21, 25, 80.	Conexión remota – exploit	Metasploit Armitage
Información confidencial	Acceso a información privilegiada.	Metasploit Jhon Armitage
Sistemas operativos obsoletos	Exploits dirigidos a Windows XP	Metasploit Armitage.
Listado de correos de funcionarios	Ingeniería social	Maltego U3-PWN
Listado de usuarios	Ataque a contraseñas	Jhon Medusa Ncrack

4.5. INFORME TÉCNICO

El presente documento tiene el propósito de dar a conocer a la Dirección de las Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá. D.C., el informe detallado de las pruebas de vulnerabilidad realizadas en la fase de recolección de la información al sistema de información de la Entidad, posibles vulnerabilidades encontradas y su tratamiento.

Recolección Pasiva de Información: El objetivo es conseguir la mayor cantidad de información posible del objetivo de forma indirecta, es decir conectado desde fuera de la red de la Contraloría de Bogotá.

4.5.1 Foca:

Permite generar información de un dominio web, y extraer información valiosa como: Dominios, Usuarios, Servidores y Metadatos.

Información encontrada: nombres de Usuario, nombres de Servidores e IPS Públicas, Dominios, Servidores de Correo, Metadatos de documentos y sistemas operativos usados.

Vulnerabilidad asociada: acceso a información, y mediante el uso de los datos obtenidos y junto a técnicas de ingeniería social se pueden realizar otros ataques.

Riesgos: ingeniería Social, ataques a contraseñas mediante fuerza bruta, perdida de la privacidad y confidencialidad de la Información, ataques de denegación de servicios DDoS.

Tratamiento:

- Sensibilización y Capacitación a los usuarios en temas de la Seguridad de la Información

- Revisión de los documentos que se suban a los repositorios web en el sentido de proteger la información privada y sensible que no debe estar al alcance de todos

- Políticas de Contraseñas Seguras.

4.5.2. Who is

Realiza la búsqueda de datos públicos de un dominio.

Información encontrada: cuentas de correo institucional de algunos usuarios como: direcciones, teléfonos, correos electrónicos, proveedor del servicio Internet

Vulnerabilidad asociada: acceso a información, y mediante el uso de los datos obtenidos y junto a técnicas de ingeniería social se pueden realizar otros ataques.

Riesgos: ingeniería Social, ataques a contraseñas mediante fuerza bruta, perdida de la privacidad y confidencialidad de la Información, ataques de denegación de servicios DDoS.

Tratamiento: sensibilización y capacitación a los usuarios en temas de la Seguridad de la Información, evitar configuraciones por defecto en los dispositivos de red, políticas de Contraseñas Seguras

4.5.3 Google Gathering

Técnica que utiliza las diferentes formas de realizar búsquedas para acceder al índice de directorios “padre” del Sitio Web y la extracción de los metadatos de los documentos alojados en el portal de la Contraloría de Bogotá.

Información encontrada: nombres y cargos de los funcionarios, documento de gestión y de trabajo de la Contraloría.

Vulnerabilidad asociada: acceso a información, y mediante el uso de los datos obtenidos y junto a técnicas de ingeniería social se pueden realizar otros ataques.

Riesgos: Ingeniería Social, ataques a contraseñas mediante el uso de fuerza bruta, perdida de la privacidad y confidencialidad de la Información

Tratamiento: sensibilización y capacitación a los usuarios en temas de la Seguridad de la Información, restringir la información privada y sensible, definiendo roles para las personas que necesiten acceder a esta, recortar o difuminar información personal y sensible.

4.5.4 Robtex.com

Aproximación de la infraestructura Global de la red y datos del prestador de servicio Internet.

Información encontrada: Nombres y cargos de los funcionarios, documento de gestión y de trabajo de la Contraloría.

Vulnerabilidad asociada: acceso a información, y mediante el uso de los datos obtenidos y junto a técnicas de ingeniería social se pueden realizar otros ataques.

Riesgos: ataques de Denegación de Servicios DDoS

Tratamiento: implementación y configuración de mecanismos de seguridad a nivel perimetral como Firewall e IDS/IPS, evitar configuraciones por defecto, mantener actualizadas las reglas de seguridad en los dispositivos de red.

4.4.5 Nmap

Escaneo de red, gracias a sus filtros permite detectar puertos abiertos, sistemas operativos y servicios activos.

Información encontrada: Puertos abiertos, descubrimiento de servidores, equipos, servicios y sistemas operativos

Vulnerabilidad asociada: Uso de protocolos inseguro ftp/21, uso de protocolo inseguro smtp/25, uso de protocolo inseguro http/80

Riesgos: el uso de protocolos inseguros de comunicación (no cifrados) permiten que un atacante realice diferente tipo exploits.

Tratamiento: uso de protocolos seguro como: sftp, smtps, https, bloquear cualquier PING que provenga desde Internet.

4.4.6 Theharvester

permite recolectar información de manera pasiva de datos cómo: emails, subdominios, puertos, hosts, funcionarios, entre otros

Información encontrada: cuentas de correos de funcionarios de la Contraloría, servidores e IP asociadas-

Vulnerabilidad asociada: acceso a la información.

Riesgos: acceso a información, y mediante el uso de los datos obtenidos y junto a técnicas de ingeniería social se pueden realizar otros ataques.

Tratamiento: sensibilización y capacitación a los usuarios en temas de la Seguridad de la información, evitar configuraciones por defecto en los dispositivos de red, implementar políticas de contraseñas seguras.

4.4.6 Nessus (versión prueba)

Permite realizar escaneo de vulnerabilidades de la infraestructura de red, protocolos, aplicaciones, etc.

Información encontrada: vulnerabilidades relacionadas con el servidor web Apache y Php.

Vulnerabilidad asociada: uso de versiones desactualizadas de Apache y PHP

Riesgos: ataques de tipo Craffted request que abre la posibilidad a un ataque DDoS y exploits.

Tratamiento: actualizar a las últimas versiones estables.

Recolección Activa de Información: El objetivo es recolectar la mayor cantidad de información posible del objetivo de forma directa, es decir conectado a la misma red de la Contraloría de Bogotá.

4.4.6. DNSenum

El propósito de DNSenum es capturar toda la información que sea posible sobre un dominio.

Información encontrada: servidores de dominio, Tres (3) con sus nombres de e IP

Vulnerabilidad asociada: acceso a la información

Riesgos: suplantación de Identidad por DNS Spoofing

Tratamiento: implementación y configuración de mecanismos de seguridad a nivel Perimetral como Firewall e IDS/IPS, mantener actualizadas las reglas de seguridad de los dispositivos de red, los sistemas operativos y el antivirus.

4.5.7 Nmap

Herramienta Open Source utilizada para la exploración de redes y auditorías de seguridad

Información encontrada: puertos abiertos como: 21/tcp ftp, 80/tcp http, 135/tcp msrpc

Vulnerabilidad asociada: uso de protocolos inseguro ftp/21, protocolo inseguro http/80 y protocolo inseguro msrpc/135.

Riesgos: el uso de protocolos inseguros de comunicación (no cifrados) permiten que un atacante pueda visualizar la información sensible que se transfiere por la red, explotación puerto 135 con Metaexploit.

Tratamiento: uso de protocolos seguros como: sftp, smtps, https cerrar puertos que no estén en uso.

4.5.8 Nmap -O

Información encontrada: sistemas operativos usados en la Contraloría de Bogotá.

Vulnerabilidad asociada: acceso a la información

Riesgos: explotación de las vulnerabilidades conocidas de un Sistema Operativo, mediante el uso de exploits.

Tratamiento: mantener actualizados los parches de seguridad ofrecidos por el fabricante

5. DISCUSIÓN DE RESULTADOS

La investigación tuvo como objetivo realizar un estudio de penetración en las fases de recolección (activa y pasiva) de información y análisis de vulnerabilidades, para el sistema de información de la Contraloría de Bogotá, D.C, y en particular a los aplicativos Prefis y Sivicof. Se ejecutaron una serie de pruebas de penetración para recolectar de forma pasiva y activa la mayor información posible del sistema de información de la Contraloría de Bogotá. D.C., con el propósito de analizar y detectar las posibles vulnerabilidades asociadas.

Así mismo, para una fase posterior, se dejaron diseñadas y planificadas la ejecución de ataques, para explotar una posible vulnerabilidad y así poder comprobar si efectivamente existe o no un riesgo de seguridad. También se realizó un informe técnico de las pruebas realizadas, herramientas utilizada para su obtención, información obtenida mediante ellas, posible vulnerabilidad asociada, riesgo inherente y posible tratamiento.

De los resultados obtenidos en la investigación, se puede afirmar que en un sistema de información pueden existir fallas de seguridad que permiten que un atacante pueda obtener información valiosa del sistema para diseñar, planificar y ejecutar una actividad maliciosa que pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

Como lo afirman en su investigación Luis Alcides Mendaño y María Elena Hurtado Saldoval; Un estudio sirve para detectar que existen fallas en la seguridad perimetral de la Organización que permiten obtener información relevante del sistema, identificar servicios, acceder al sistema por medio de usuarios y contraseñas por defecto, etc. En forma general el estudio permitió medir el nivel de seguridad del sistema, detectar las vulnerabilidades y poder realizar las recomendaciones para mitigar los riesgos encontrados.

También en su investigación, Daniel Iván Quirumbay Yagual, concluye que el estudio realizado permitió detectar las vulnerabilidades a la arquitectura tecnológica del Centro de procesamiento de Datos Municipal, medir el nivel de seguridad y aplicar las medidas preventivas y correctivas para prevenir y mitigar los riesgos.

Así mismo, Andrés Fernando Castañeda Suárez, como fue lo pretendido con su investigación; argumenta sobre la necesidad creciente del desarrollo de pruebas de Ethical Hacking, que permitan controlar y verificar el estado de las diferentes redes,

que cubra desde las conexiones WAN hasta las redes LAN, ya que las amenazas que se ciernen sobre estás son mayores y cada vez más sofisticadas.

Por otro lado, los resultados obtenidos en la investigación se pueden tomar como base para diseñar y planificar las siguientes fases de un estudio completo de Ethical Hacking, que permitan evaluar y medir el nivel de seguridad actual de la Contraloría de Bogotá. D.C., con el propósito de implementar las medidas necesarias para mitigar y contrarrestar los riesgos informáticos a los que se encuentra expuesta.

La búsqueda de tener un sistema seguro es un proceso en continua evolución, porque cada día los atacantes se idean nuevas formas, técnicas y herramientas para aprovecharse de las fallas y vulnerabilidades de seguridad de los sistemas de información de las organizaciones.

6. CONCLUSIONES

La información que gestionan los sistemas Sivicof y Prefis de la Contraloría de Bogotá. D.C., son de vital importancia para esta Entidad, ya que son la base de las actuaciones de auditoria que ejerce el Estado en el desarrollo de la misión de vigilancia fiscal sobre los sujetos de control. Por tanto, es responsabilidad de la Contraloría de Bogotá D.C., garantizar la integridad, confidencialidad y disponibilidad de esta información.

La fase de recolección de información de forma pasiva y activa de información por medio de herramientas de penetración, permitió develar información importante del sistema: IP, cuentas de correo institucional, dominios, metadatos de ficheros, nombres de servidores, puertos y servicios abiertos, protocolos utilizados, versiones de software utilizados, entre otros más. La fase de recolección de información es de vital relevancia, ya que es la que provee la información inicial para perfilar el objetivo y de esta forma poder diseñar, planificar y desarrollar el ataque.

Del análisis de la información recogida, se permite establecer que la Contraloría de Bogotá. D.C., evidencia algunas posibles vulnerabilidades que pueden poner en riesgo la seguridad del sistema de información: Uso de protocolos no cifrados, puertos abiertos 21, 25, 80 que son potencialmente vulnerables, visualización plana de documentos posiblemente de carácter confidencial, versiones de software que están plenamente identificadas como vulnerables, entre otras.

Se debe establecer de forma precisa cuales de las posibles vulnerabilidades enumeradas, son realmente una falla de seguridad y que puedan poner en riesgo al sistema de información. Para esto, es necesario realizar el diseño y ejecución de ataques que exploten las vulnerabilidades de seguridad encontradas con el propósito de lograr tener acceso al sistema y de esta forma comprobar si una posible vulnerabilidad es realmente un hueco de seguridad.

El presente trabajo permitió detectar que existen posibles vulnerabilidades que pueden ser aprovechadas y explotadas, y por ende pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

A partir del resultado de las pruebas de vulnerabilidad realizadas en la fase de recolección de información, se hace necesario realizar un estudio completo de Ethical Hacking, que verifique y compruebe las vulnerabilidades encontradas ya que esto estaba fuera del alcance del proyecto. La anterior recomendación se debe tomar como una oportunidad para fortalecer la seguridad del sistema de información de la Contraloría de Bogotá. D.C., partiendo de la base que en el Marco del Sistema de Gestión de la Seguridad de la Información (SGSI), el mejoramiento continuo es un componente importante, en el cual las pruebas de penetración son un mecanismo vital para mejorar cada vez más el nivel de seguridad del sistema.

7. RECOMENDACIONES

En el marco de la Ley 1712 de 2014, por medio de la cual se crea la “Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional”, y en concordancia con los artículos 4° y 5°, todas las entidades del estado deben permitir el acceso de toda persona a la información pública en posesión o bajo el control de los sujetos obligados, incluyendo la de los funcionarios y contratistas al servicio de la misma.

En el numeral (c) del Artículo 9°, se establece que todas las entidades deben publicar “Un directorio que incluya el cargo, direcciones de correo electrónico y teléfono del despacho de los empleados y funcionarios y las escalas salariales correspondientes a las categorías de todos los servidores que trabajan en el sujeto obligado, de conformidad con el formato de información de servidores públicos y contratistas;”, en este sentido, un atacante tiene el acceso al nombre de los funcionarios, correo institucional y teléfono, facilitándole un posible diseño y ejecución de un ataque utilizando técnicas de ingeniería social con el propósito de obtener información confidencial del sistema que permita tener acceso al mismo.

Por lo anterior, se recomienda que la entidad desarrolle o fortalezca estrategias de concientización y capacitación a todos los funcionarios de la Contraloría de Bogotá, acerca de la cultura de la seguridad de la información, que les permita desarrollar habilidades para detectar en un determinado momento que pueden a ser víctimas de un posible ataque informático, o que les permita analizar a priori que la acción que pretende realizar puede poner en riesgo el sistema de información de la entidad.

Por otro lado, se recomienda que la entidad revise la necesidad de tener puertos abiertos corriendo servicios con protocolos de comunicación inseguros como los detectados en las pruebas realizados en la fase de recolección de información, y que pueden ser altamente vulnerable a ataques informáticos, como por ejemplo:

Tabla 7. Puertos vulnerables.

PORT/PROTOCOLO	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
81/tcp	open	http
135/tcp	open	msrpc

El uso de protocolos inseguros permite que un atacante pueda ver el tráfico que pasa en la red por medio de un sniffer, entendiéndose por tráfico todos los datos, documentos, credenciales y demás tipo de información que pueden ser de carácter público o privado, el cual debe ser resguardado por la entidad. Tal como se evidencio en la fase de recolección de información pasiva con el uso de un sniffer (WireShark), con la cual se pudo capturar las credenciales de acceso de un usuario al sistema de información Sivicof, así mismo, cualquier aplicativo que se implemente sobre la página y que tenga acceso por medio de alguna credencial, podrá ser víctima de este tipo de ataque.

Por lo anterior, se recomienda en este sentido el uso de protocolos seguros como IPSec en la capa de red o protocolos como HTTPS, SSH, SMTPS, SFTP en la capa de aplicación, que garanticen una comunicación y transferencia de información segura. Estos protocolos seguros además de proveer los mecanismos de envío o entrega de información cifran la información que transfieren y de esta forma garantizan la autenticidad, confidencialidad e integridad de los datos que fluyen en la red.

También se recomienda mantener actualizados los sistemas operacionales y los parches de seguridad ofrecidos por el fabricante, de igual forma, se deben tener correctamente configurados los dispositivos de seguridad de red y actualizadas las reglas que implementan la misma seguridad.

8. BIBLIOGRAFÍA

ACUERDO 519 de diciembre de 2012 Normas sobre la organización de la Contraloría de Bogotá D.C., {En línea} {Consultado enero 2018} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51049).

ALBORS, Josep 09 de octubre de 2014 ¿sabes qué es un exploit y cómo funciona? En línea} {Consultado mayo 2018} disponible en: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/).

ANTONUCCI Domenic. The Cyber Risk Handbook – Creating and Measuring Effective Cybersecurity Capabilities, 2017 – EE. UU., WILEY, pag: 2-4, "Introduction. Toward an Effectively Cyber Risk-Managed Organization" {En línea} {Consultado mayo 2018} disponible en: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119309741.

Broad, James; Bindner, Andrew. Edition: 1st ed. Hacking with Kali: Practical Penetration Testing Techniques. Amsterdam Syngress. 2014. eBook., .,{En línea} {Consultado enero 2018} disponible en: Base de datos: eBook Collection (EBSCOhost). {Consultado febrero 2018}.

BROTHERSTON, Lee – BERLIN, Amanda. Defensive Security Handbook - Best Practices for Securing Infrastructure, 2017 firts edition – EE. UU., OREILLY,{Consultado mayo 2018} disponible en: pag: 149-169, "Chapter 5. User Education".

Christopher Hadnagy. Social Engineering – The Art of Human Hacking. Wiley Publishing, Inc. Indianapolis. 2011. Cap 2, P 47-85, {En línea} {Consultado enero 2018} disponible en: https://www.wiley.com/en-us/Social+Engineering%3A+The+Art+of+Human+Hacking-p-9780470639535.

Common Vulnerabilites and Exposures 2018 {En líena} {Consultado enero 2018}. Disponible en: https://cve.mitre.org/data/downloads/index.html.

David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni. Metasploit The Penetration Tester's Guide. San Francisco. 2011. Cap 2, P 7-14. {En línea} {Consultado enero 2018} disponible en: https://repo.zenk-security.com/Metasploit/MetasploitThe%20Penetration%20Tester%20s%20Guide. pdf.

DECRETO LEY 1421 del 21 de julio 1993 Régimen especial para el Distrito Capital, {En línea} {Consultado enero 2018} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1507.

de Parada, Yolanda Gallardo. Moreno Garzón, Adonay. (1999). RECOLECCIÓN DE LA INFORMACIÓN. Bogotá: ICFES. {En línea} {Consultado enero 2018} disponible

en:http://www.unilibrebaq.edu.co/unilibrebaq/images/ceul/mod3recoleccioninform.pdf.

Escrivá Gascó, Gema. Romero Serrano, Rosa María. Ramada, David Jorge. (2013) Seguridad Informática. Editorial Macmillan Iberia, S.A. Pág. 8-10, ProQuest ebrary. {En línea} {Consultado enero 2018} disponible en: http://www.parcir.com/products/300607-seguridad-informatica.html.

Exploit Database. 2018 {en línea} {Consultado enero 2018} Disponible en: https://www.exploit-db.com/google-hacking- database/.

HALSEY, Mike. Windows Virus and Malware Troubleshooting, 2017 firts edition – EE. UU., APRESS, pag: 18-38, “Chapter 1. Diffent Types of Malware {En línea} {Consultado enero 2018} disponible en: https://www.apress.com/us/book/9781484226063.

Kali By Ofensive Security. 2018 {En línea} {Consultado enero 2018} Disponible en: https://www.kali.org/.

Martí Talón, Rafael Manuel. (2016). Tesis: Desarrollo e implementación práctica de un PENTEST. Gandia: Universidad Politécnica de Valencia. Pág. 3. {En línea} {Consultado enero 2018}, disponible en: https://riunet.upv.es/bitstream/handle/10251/70164/MART%C3%8D%20-%20Desarrollo%20e%20implementaci%C3%B3n%20pr%C3%A1ctica%20de%20un%20PENTEST.pdf?sequence=2.

MENDOZA PALACIOS. Rudy. Monografías.com. Investigación cualitativa y cuantitativa – diferencias y limitaciones 2006, {En línea} {Consultado enero 2018}, disponible en: http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa.shtml.

Michael T. Simpson, Kent Backman, James E. Corley. Hands-On Ethical Hacking and Network Defense. Boston. 2011. Cap 10, P 263-300.

Nessus escáner de Vulnerabilidades 2018. {En línea} {Consultado enero 2018} disponible en:http://es-la.tenable.com/.

Nmap Free Security Scanner 2018 {En línea} {Consultado enero 2018} disponible en: https://nmap.org/.

Oday Security [IN] Security In Networks 2017. {En línea} {Consultado enero 2018} disponible en: http://www.0daysecurity.com/penetration-testing/discovery-and-probing.html.

Paredes Flores, Carlos Iván. (2009). Hacking. El Cid Editor | apuntes. Pág. 7 -9, {En línea} {Consultado enero 2018} disponible en: https://es.calameo.com/books/000632775865d9d85e1c2 .

Penetration Testing Execution Standard 2018. {En línea} {Consultado enero 2018} disponible en: http://www.pentest-standard.org/index.php/FAQ.

Plan Estratégico Contraloría de Bogotá. D.C 2016, {En línea} {Consultado enero 2018} disponible en: http://www.contraloriabogota.gov.co/sites/default/files/documentos/PEI_2016-2020.pdf.

Proyecto de Acuerdo No. 037 de 2013, {En línea} {Consultado enero 2018} disponible en: disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661.

Sean Philp. CEH Certified Ethical Hacker v8 – Study Guide, 2014 v8 – EE. UU., CEH, pag: 89-93, “Chapter 1 – Security Testing, {En línea} {Consultado enero 2018} disponible en: Methodology” https://underc0de.org/foro/hacking/t28645/.

Thomas Wilhelm. Edition: 2st ed. Professional Penetration Testing; Creating and Learning in a Hacking Lab. Burlington : Syngress. 2013. Cap 2, P 11-31. {En línea} {Consultado enero 2018} disponible en: eBook., Base de datos: eBook Collection (EBSCOhost).

Tori, Carlos. (2008) Hacking Ético. Rosario Argentina. El Autor, Pág. 13-16. {En línea} {Consultado enero 2018} disponible en: https://www.maestrodelacomputacion.net/libro-gratuito-de-hacking-etico-en-espanol/.

9. ANEXOS

9.1. SOLICITUD PERMISO DE TRABAJO

Ilustración 44. Solicitud permiso de trabajo

Bogotá, D.C. Marzo 14 de 2017

Doctor
RODRIGO HERNAN REY LOPEZ
Director Dirección de Tecnologías de la Información y las Comunicaciones
Contraloría de Bogotá, D.C.
Ciudad

Ref: Solicitud permiso trabajo de grado.

Respetado Doctor.

Queremos comentarle que en el momento estamos cursando el primer semestre del programa de Especialización en Seguridad Informática, de la Universidad Nacional Abierta y a Distancia -UNAD-, en la modalidad virtual. Que para acceder al título de Especialistas, la Universidad permite que podamos presentar un Proyecto Aplicado, el cual consiste en un trabajo orientado a la solución de problemas locales, regionales o nacionales, partiendo del conocimiento específico del programa que se cursa.

Por lo anterior, y con el propósito también de contribuir desde nuestro crecimiento profesional al cumplimiento de la misión de la Entidad, solicitamos muy respetuosamente nos permita realizar el proyecto de grado anteriormente mencionado, aplicado al Sistema para el Seguimiento y Control de Procesos de Responsabilidad Fiscal -PREFIS-, el cual consideramos que es uno de los sistemas de Información más importantes en los que se apoya la gestión de la Entidad.

El objetivo principal del proyecto consiste en realizar un análisis de riesgos y algunas pruebas de vulnerabilidades, tanto de la base de datos como de los aplicativos que acceden al sistema de información -PREFIS-, y determinar las vulnerabilidades y los riesgos asociados al sistema de información, para de esta forma recomendar los controles más adecuados para mitigarlos. En otras palabras, pretendemos coadyuvar para que el sistema de información -PREFIS-, sea un sistema más seguro, y que la información en este sistema cumpla con los principios de integridad, confidencialidad, disponibilidad y autenticidad.

Agradecemos de antemano la atención a la presente, y quedamos atentos a sus comentarios

Cordialmente.

Fuente: propia

9.2. AUTORIZACIÓN TRABAJO

Ilustración 45. Autorización trabajo

Gmail — Lenin Herrera <leninher@gmail.com>

RV: Solicitud permiso trabajo de grado
1 mensaje

Lenin Herrera Moncada <lherrera@contraloriabogota.gov.co> 28 de marzo de 2017, 16:55
Para: "leninher@gmail.com" <leninher@gmail.com>

De: Rodrigo Hernan Rey Lopez
Enviado el: lunes, 27 de marzo de 2017 17:19
Para: Lenin Herrera Moncada <lherrera@contraloriabogota.gov.co>; Osbaldo Cortes <ocortes@contraloriabogota.gov.co>
CC: Claudia Patricia Martinez Jaramillo <cmartinez@contraloriabogota.gov.co>; Maria Angelica Zamora Bautista <mzamora@contraloriabogota.gov.co>
Asunto: RE: Solicitud permiso trabajo de grado
Importancia: Alta

Cordial saludo;

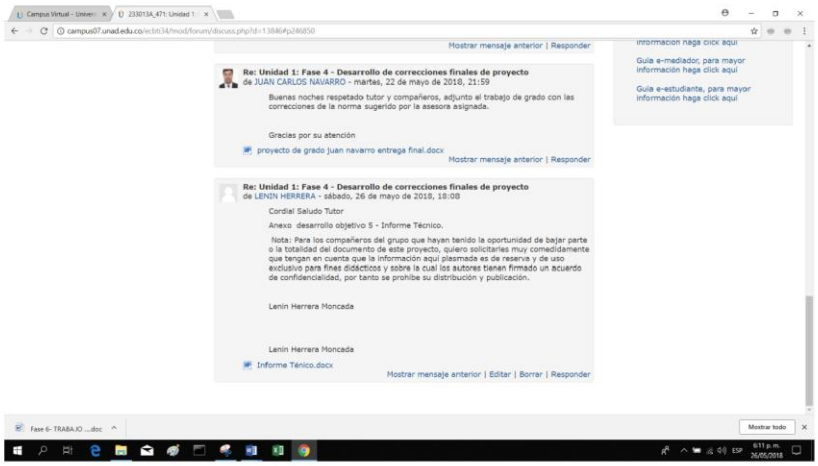
Analizando la solicitud interpuesta, me permito considerar viable que se efectué este proyecto de grado sobre el aplicativo PREFIS; sin embargo cómo se maneja información sensible de los proceso de Responsabilidad Fiscal se deberá suscribir un acuerdo de confidencialidad para el caso.

Cordialmente;

Fuente: propia

9.3. COMUNICACIÓN DE ACUERDO DE CONFIDENCIALIDAD EN EL GRUPO DE TRABAJO DEL PROYECTO

Ilustración 46. . Comunicación de acuerdo



Fuente: propia

9.4. ANÁLISIS BIBLIOGRÁFICO

9.4.1. Hacking with Kali : Practical Penetration Testing Techniques

Autor: Broad, James. Bindner, Andrew

Contenido: los autores de este libro pretenden dar a conocer las fases que se deben seguir cuando se quiere realizar un estudio de Ethical Hacking. Para tal propósito los autores basan su enseñanza utilizando el sistema Kali Linux, sistema operacional que está diseñado para evaluar la seguridad de un sistema informático. Este documento inicia explicando como descargar e instalar el sistema Kali Linux, así como también enseña a configurarlo y personalizarlo al ambiente donde se va a correr. Después de esto y a través de las siguientes secciones del libro se detallan las actividades o pasos que se deben realizar en las diferentes fases o ciclo de vida de un estudio de Ethical Hacking y que en su orden son: reconocimiento, escaneo, explotación, mantener acceso y reportes. En cada fase mencionada, el documento enumera, explica y visualiza las herramientas que provee Kali Linux para realizar una determinada actividad o lograr un objetivo. Por último y de gran importancia y utilidad para el lector, al final del libro en el Apéndice B, presenta una tabla que muestra todas las herramientas que provee Kali Linux ordenadas de acuerdo a la utilidad que presta.

Conclusión: un profesional en Seguridad Informática que tiene como función garantizar la seguridad de la información en una organización, debe estar continuamente evaluando la seguridad de esta y para tal fin debe realizar actividades de Ethical Hacking apoyándose en metodologías y herramientas orientadas y diseñadas para tal fin. En este sentido este libro es una guía no solo teórica sino practica para el desarrollo del proyecto.

9.4.2. Professional Penetration Testing; Creating and Learning in a Hacking Lab

Autor: Thomas Wilhelm

Contenido: El autor en capitulo Segundo “Ethics and Hacking” de su libro, aclara que la diferencia entre un Black Hacker y un White Hacker no es la “ética” sino el

“permiso”. Un White Hacker es la persona que efectúa un estudio de seguridad donde previamente se ha efectuado un acuerdo y se le ha otorgado el debido permiso para hacerlo. Mientras el Black Hacker es el individuo que accede a un sistema de información de forma abusiva y sin autorización. El autor hace referencia al Hacker Adrián Lamo, que logro infiltrase en los sistemas de varias compañías americanas con el propósito mostrarles las vulnerabilidades de sus sistemas, pero siempre actuó con “buena” intención resguardando y protegiendo la información a la que pudo tener acceso. A pesar de esa buena conducta ética, Lamo fue condenado por la justicia americana por haber penetrado los sistemas de información sin el permiso debido. Thomas Wilhelm, recalca que debe existir un compromiso total por parte de las personas que se dedican a la seguridad informática para cumplir la conducta ética de manera personal, pero también tienen la obligación de promoverla a nivel colectivo del gremio. Las leyes que los gobiernos expiden al respecto son de gran ayuda, pero si no son apoyadas por la comunidad no logran su objetivo completamente. En este sentido en Colombia se implementó la Ley 1273 de 2009, “por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", con el propósito de identificar y penalizar los delitos informáticos. Según el autor, el concepto de ético pude diferir de un país a otro y dependen directamente de las leyes que legislan al respecto, es por esta razón que lo que puede ser delito en un país puede no serlo en otro. Pero lo cierto es que sea en uno u otro país, la razón principal que motiva una práctica delictiva informática es el dinero.

El autor define a un Black Hat Hackers como aquellas personas que realizan acciones de ataques con el objetivo de penetrar sin autorización a un sistema de información generalmente para realizar actividades maliciosas, no siguen ninguna regla o contrato. Los White Hat Hackers son los que acceden a un sistema de información con el debido permiso y con el objetivo de evaluar la seguridad de este, detectado las vulnerabilidades del sistema para poder corregirlas. Estos últimos hackers son contratados por las compañías, capacitados en las técnicas modernas de penetración que utilizan delincuentes informáticos y le son asignados grandes recursos de tecnología, desarrollo y para investigación. El autor hace referencia a que las certificaciones de seguridad de la información que existen actualmente, como puede ser la certificación CISSP o SANS entre muchas otras, implementan dentro de su contenido las reglas o requisitos que deben tener sus miembros para poder certificasen. Entre sus principios rectores de ética se resalta la honestidad,

integridad y confidencialidad. Existen Universidades y organizaciones que han orientado esfuerzos con el ánimo de perfeccionar los modelos éticos dentro de la seguridad de la información como, por ejemplo: The Information System Security Association (ISSA), The Internet Activities Board (IAB), The Institute of Electrical and Electronics Engineers (IEEE).

Conclusión: el concepto de Ethical Hacking se refiere directamente a la acción de evaluar la seguridad de un sistema de información, para esto se realizan ataques de penetración al sistema objetivo con el fin de obtener acceso al mismo. Pero estos ataques se realizan con pleno permiso o autorización por parte de la organización y con el propósito de encontrar las vulnerabilidades de seguridad del sistema y poder corregirlas. Es el término “permiso” lo que diferencia a un White Hacker con un Black Hacker y no el término “ético”, porque lo ético puede diferir de un lugar a otro por ejemplo por las leyes que lo rigen.

9.4.3. Metasploit The Penetration Tester’s Guide

Autor: David Kennedy, Jim O’Gorman, Devon Kearns, Mati Aharoni

Contenido: a través del todo el capítulo 2 de este libro los autores adentran al lector en el entendimiento y compresión sobre el framework o entorno de pruebas de penetración denominado Metaesploit (MSF), entorno Open Source diseñado y desarrollado para explotar las vulnerabilidades encontradas en un sistema, con el objeto de tomar control de este o realizar una acción en particular. Los autores identifican y definen los siguientes conceptos claves para la mejor compresión del proceso de explotación y la forma como trabaja Metaesploit. Un exploit es el medio que permite explotar o sacar provecho a una vulnerabilidad descubierta; Payload es el código que se pretende ejecutar; Shellcode se define como la secuencia de instrucciones que se ejecutan y que están contenidas en el Payload; Módulo es un componente o programa que realiza una tarea particular en la tarea de explotación, ejemplo el modulo para inyectar código SQL. La interfaz más relevante de este framework está diseñada para correr en modo consola y en ambiente propio, de ahí su nombre “MSFconsole”, donde todos los llamados a los módulos o al shellcode se realizan a través de instrucciones digitadas en la línea de comando. Pero también Metaesploit provee otras interfaces como MSFCli, que también está orientada a consola con la diferencia que los comandos ejecutados en esta interfaz se ejecutan

en la consola del sistema operacional que le permite que la salida de una instrucción msfcli pueda ser recogida por un comando del sistema para fines determinados. Otra interfaz que los autores mencionan se denomina “Armitage”, a diferencia de las dos anteriores es un interfaz gráfica y poderosa. Por otra parte, los autores describen en este capítulo y en forma general los componentes o utilidades más relevantes que proporciona Metaesploit y para mencionar son: MSFpayload que permite generar código ejecutable para realizar exploit en lenguajes como Ruby, JavaScript, C y Paython entre otras; MSFencode, componente que permite que los payload no sean detectados por los sistemas IDS o programas antivirus de forma que se puedan ejecutar de manera correcta.

Conclusión: una forma de probar que una vulnerabilidad encontrada en un sistema informático se pueda considerar realmente como un riesgo de seguridad, es mediante la explotación de esta. Para este propósito fue desarrollado el Framework Metaesploit. Herramienta Open Source, que proporciona varias interfaces que se adecuan a la necesidades del usuario y que ya viene de manera preinstalada en los más importantes sistemas operativos orientados a seguridad como Kali Linux, BackBox, Network Security Tolking, Parrot y BackTrack entre otros.

9.4.4. Hands-On Ethical Hacking and Network Defense

Autor: Michael T. Simpson, Kent Backman, James E. Corley

Contenido: Los autores de este documento y más específicamente en el capítulo 10 titulado “Attacks Hacking Web Servers” en español Ataques Hacking a Servidores Web, tratan este tema en tres tópicos. En el primero, se describen los componentes de una aplicación Web, en el segundo tópico explican las vulnerabilidades de estas aplicaciones y en tercer lugar describen las estrategias, técnicas y herramientas que generalmente son utilizadas para realizar ataques a los servidores web. Un entorno o ambiente Web está conformado por la aplicación, que es la página Web, el componente servidor web como Apache, IIS y por último el componente que soporta a los dos anteriores que es el sistema operativo. Cada uno de estos componente vistos de forma independientes tienen asociados sus propias vulnerabilidades, pero vistos como un conjunto en un ambiente web, el riesgo se maximiza. Retomando los temas centrales de este capítulo, los autores definen que:

1. Los componentes de una aplicación web son: HTML que es la base generalmente utilizada por una página web, a la cual se pueden añadir componentes tipo ASP, JavaScript, PHP y de acceso a datos para hacer aplicaciones dinámicas; Formularios Web, donde están los input de entrada de datos que son enviadas al servidor web; Common Gateway Interface (CGI), este componente es el que presenta o pasa los datos envidos por el servidor web a un browser o navegador, estos CGI pueden estar escritos en diferentes tipos de lenguajes como Perl, C/C++, Visual Basic entre otros; Active Server Pages (ASP) que permite mostrar páginas en código HTML a medida que se van solicitando, lo que posibilita la creación de sitios dinámicos, este entorno solo es compatible con un servidor web IIS en sistemas Windows, en sistemas Linux el servidor web recomendado es Apache que generalmente ya viene preinstalado; Scripting Languages es el código utilizado para desarrollar las páginas web, ejemplo php, Java, Javascript, VBScript; Connecting to Databases, componente que permite al servidor web acceder a la información almacenada en una base de datos mediante una conexión Open Database Connectivity (ODBC) utilizando una interfaz de programación ActiveX Data Objects (ADO).

2. Las vulnerabilidades de las páginas están directamente relacionadas con la seguridad que exista en la red, en las aplicaciones y en el mismo sistema donde están alojadas. Por otro lado muchos sistemas de seguridad implementados de tipo IDS y otros, no detectan el contenido del tráfico en los protocolos HTTP, por esta razón se puede afirmar que los controles que se implementen en el nivel de red (IDS/IPS, Firewall, etc.) no son suficientes para no recibir ataques a nivel de las aplicaciones web, que puedan poner en riesgo el sitio, permitir acceder a las bases de datos, inyectar código SQL, obtener acceso a cuentas de usuario, implantación de malware, elevación de privilegios entre muchas otras acciones delictivas. Según la OWASP (Open Web Application Security Project), organismo sin ánimo de lucro, que tiene como fin descubrir las vulnerabilidades en las aplicaciones web y recomendar los controles adecuados, las aplicaciones web pueden estar expuestas entre otras mas a las siguientes vulnerabilidades: Cross-site scripting (XSS) que es la ejecución de un script en los formularios de entrada en el navegador; Injection flaws, que consiste en colocar código malicioso para que sea ejecutado por el servidor; Malicious file execution, consiste en incrustar archivos con contenido malicioso; Unsecured direct object reference, vulnerabilidad producida cuando la información devuelta por el servidor y mostrada por la URL del cliente, contiene

referencias a objetos del sistema como directorio, bases de datos, etc.; Cross-site request forgery (CSRF) o falsificación de peticiones. Esta vulnerabilidad que puede darse cuando se realizan peticiones maliciosas a través de un navegador que previamente ha sido autenticado.

Estas son algunas de las vulnerabilidades asociadas a las páginas web que los autores describen y que pueden poner en riesgo la seguridad de un sistema de información. Ante esta situación la OWASP desarrolló el proyecto WebGoat, que tiene como objetivo principal, el de ayudar a los profesionales en seguridad a aprender y entender como se deben realizar pruebas de vulnerabilidad en páginas web.

3. Por último en este capítulo y después de identificar las vulnerabilidades presentes en las aplicaciones web, los autores se centran en describir las herramientas que se usan en Ethical Hacking para poder explotarlas. Es evidente que estas mismas herramientas son las utilizadas por un atacante. A continuación se mencionan algunas de ellas y se describen su función principal. Cgiscan, esta herramienta permite realizar escanear o buscar sitios Web que puedan ser explotados por medio de script CGI; Wapiti, es un escáner que examina un sitio Web para atacar vulnerabilidades de tipo PHP, XSS, JSP, SQL, y manejo de archivos básicamente; Wfetch, es una herramienta Microsoft, que permite evaluar el estado de seguridad de un servidor Web, e intenta acceder al sistemas y lograra la autenticación empleando diferentes estrategias.

Se resalta que los autores de este libro no solo se preocuparon por escribir la parte conceptual y teórica de las vulnerabilidades en las aplicaciones web y de las herramientas utilizadas en Ethical hacking para explotarlas, sino que también involucran la parte práctica a través de todo el documento, permitiendo una mejor compresión y análisis en este tema.

Conclusión: todas las organizaciones que exponen su información a través de aplicaciones web deben tener muy claro que estas tienen asociados varias vulnerabilidades que pueden poner en riesgo no solo el sitio web como tal, sino todo el sistema de información. Y en este sentido el responsable de la seguridad informática de la organización debe estar constantemente evaluando la seguridad de las aplicaciones web, para lo cual debe apoyarse en herramientas diseñadas y orientadas para probar y atacar las vulnerabilidades en estos aplicativos. También

debe estar actualizándose en las nuevas técnicas, estrategias y herramientas que se están siendo utilizadas para atacar estas aplicaciones, OWSAP es una muy buena fuente de información y de obtención de conocimiento en este tema.

9.4.5 Social Engineering – The Art of Human Hacking

Autor: Christopher Hadnagy

Contenido: El autor, a través de este capítulo pretende que el lector conozca, entienda y ponga en práctica las estrategias, técnicas y herramientas de ingeniera social que se utilizan para realizar recolección de información en el marco de Ethical Hacking.

Se dice que en el proceso de recolección, toda dato es importante y puede ser muy relevante para conducir que la etapa de recolección de información sea exitosa. Pero para lograr que la recopilación de información sea adecuada y eficaz, el Ingeniero Social debe saber el cómo puede recolectar información, que fuentes existen para realizarlo, que puede deducir de la información recogida para orientar sus estrategias y cómo clasificar y analizar la información para ser usada en las siguientes etapas del pentester. También el ingeniero social debe contener y aprovechar las cualidades que tiene un buen vendedor, debe saber comprender e interactuar con las redes sociales, ya que estas son una excelente fuente de información, donde las personas fácilmente están dejando datos confidenciales que pueden ser útiles en la recolección y fácilmente explotables. El ingeniero social cuando establece una conversación en búsqueda de información está pensando en la relevancia que tienen esos datos dentro y fuera de la plática, en cuanto más información valiosa se extraiga, más probabilidad de éxito se asegura.

El autor a continuación discute cómo recopilar información, luego pasa a mencionar las fuentes utilizadas para recolectar información y por último enseña como Ingeniero Social une y utiliza estos recursos.

Recolección de Información: En un proceso de recolección se debe tratar de obtener información como: datos del sitio web del cliente, datos generales, datos de empleados, sitios de redes sociales asociados a ellos y aficiones entre otros,

imágenes, y cualquier otra información que sea vinculante a la organización. Una buena forma de empezar con el proceso de recolección es la de construir un fichero o utilizar un servidor de recolección de información, para ir almacenando y clasificando la información que se vaya recogiendo. Entre las herramientas que son útiles para la este propósito y que vienen preinstaladas en sistemas operacionales como BackTrack, se mencionan BasKet "http://basket.kde.org/" y Dradis "http://dradisframework.org". Basket funciona como un Bloc de notas, pero es más que Bloc de notas, es fácil de usar y su interfaz es bastante funcional. Basket permite almacenar y organizar la información recogida. Puede copiar y pegar datos, incluir imágenes de capturas de pantalla, también puede interactuar con programas ofimáticos o de manipulación de gráficos y otras más funcionalidades. En el análisis de la información, Basket permite catalogarla por diferentes tipos de datos como datos generales, datos de redes sociales, etc. También Basket permite almacenar imágenes y georreferenciarlos con aplicativos como Google Maps o Google Earth. Dradis es otra herramienta utilizada para almacenar y organizar la información recogida, funciona en ambiente web con la url "https: // localhost:3004".

El autor enfatiza que un ingeniero social debe planificar, preparar y pensar en qué información pretende obtener y cómo la va a ser. También asegura que hay que tener cierta malicia a la hora de obtenerla y analizarla. Cuando "la víctima" utiliza diferentes redes sociales, se debe encontrar los vínculos que los puede unir y armar un conjunto de información con el que se puede crear un perfil completo. Un ingeniero social no debe desechar ningún tipo de dato por irrelevante que parezca, debe analizarla, referenciarla y asociarla al conjunto de la información.

Fuentes de Recolección de Información: Las principales fuentes de recolección de información son las siguientes: Sitios Web, por ejemplo, después de navegar por un sitio web corporativo, podemos obtener información de lo que hace la organización, de su estructura organización, de los productos o servicios que ofrece, ubicación geográfica, teléfonos, posiblemente nombres de contactos, teléfonos, correos, direcciones a redes sociales, etc. Toda esta información es importante para el ingeniero social, que puede relacionarla y vincularla con otras fuentes para obtener un perfil completo. Motores de Búsqueda, Un buscador es buena forma de encontrar información importante a cerca de una empresa o una persona, pero hay que saber cómo preguntarle al buscador para obtener los datos deseados. El ingeniero social, debe conocer los términos y las sintaxis que se emplean en la búsqueda y que le

pueden ayudar a localizar la información en el destino. Por ejemplo, si se quiere listar los archivos PDF que un determinado sitio web contiene, se debe escribir la siguiente cadena “site: microsoft.com filetype: pdf”. Este está relacionado con el uso de los operadores Google. Johnny Long desarrolló una lista llamada "Dorks de Google", o una cadena que se puede usar para buscar en Google. Reconocimiento Whois, con whois se puede obtener por ejemplo la dirección IP del servidor DNS, direcciones de correo electrónico entre otros datos. Servidores Públicos, Los servidores que una organización dispone para que sean accedidos públicamente también pueden ser una fuente en búsqueda de información. La forma como están configuradas estas direcciones IP públicas pueden revelar si estos servidores son alojados localmente o por lo contrario si es un servicio contratado con un proveedor. También es posible con la utilización de herramientas como NMAP, determinar puertos y servicios abiertos, sistemas operacionales utilizados, sistemas de seguridad instalado, etc. Redes Sociales - Blogs, sitios como Facebook, Twitter, LinkedIn, Blippy, MySpace y otros. La información que generalmente se pública en las redes sociales, como servicios prestados, noticias, eventos, foros, etc., y en el caso de personas, gustos, información personal y familiar, puede ser valiosa y mas cuando se relaciona con otras fuentes de información. En estos sitios es muy común que se suban imágenes o videos y que con herramientas apropiadas como Exiftool, son capaces de consultar los metadatos asociados a estos tipos de archivos y obtener información como la fecha y hora de la imagen, lugar donde se capturo la imagen GPS entre otra información. Los Cestos de Basura, no es difícil encontrar entre los cestos de basura CDs, documentos, factura, USB, hasta computadores y otros dispositivos que se pueden convertir en una excelente fuente de información. En la basura se pueden encontrar documentos completos que han pasado previamente por maquinas destructoras, pero que dejan el papel de forma que con algo de paciencia se pude reconstruir y extractar información. Software de Creación de Perfiles, para el ingeniero social es importante conocer y dominar diferente tipo de software que le ayuden en su labor. Software para generación de contraseñas potenciales como Who’s Your Daddy (WYD) y Common User Passwords Profiler (CUPP). Por ejemplo, JMJ escudriña un sitio web y puede crear una lista de contraseñas a partir de la información encontrada. Otra herramienta es Maltego que permite realizar búsquedas basadas en la web y crear un posible perfil de una organización o de una persona. Software Técnico, Software que permite la recolección de información como servicios, servidores DNS, Netbios, protocolos SMTP, protocolo SNMP entre otros.

Ingeniero Social en Acción: El Ingeniero Social debe desarrollar un modelo de comunicación para: lograr contacto con el objetivo, cautivar su interés y extraer la información requerida. También debe desarrollar uno o dos escenarios para iniciar el contacto con el objetivo. En este sentido puede enviar un correo a varios empleados de la organización que sirva de carnada, con mensajes de interés para ellos, con el propósito de establecer contacto y posiblemente poder incrustar algún tipo de artefacto en la máquina del objetivo por medio de un archivo adjunto o algún tipo de vínculo dentro del correo, que permita tomar control de esta.

Conclusión: en un proceso de Ethical Hacking, la fase de recolección de información es de vital importancia, ya que es la que provee la información inicial para perfilar el objetivo y de esta forma poder diseñar, planificar y desarrollar el ataque. El ingeniero social debe tener presente que toda información es valiosa, debe tener la capacidad de relacionar diferentes fuentes de información, debe saber donde y como buscarla, debe saber como almacenarla y categorizarla para poder hacer uso de ella en las siguientes fases y por último debe familiarizarse de los modelos, técnicas y herramientas mas usadas en la recolección de la información.

9.4.6 Defensive Security Handbook - Best Practices for Securing Infrastructure

Autor: Lee Brotherston and Amanda Berlin

Contenido: Según los autores Brotherson y Berlin, la educación y la conciencia de los usuarios a cerca de la seguridad informática de las compañías en las cuales laboran, es un punto de alto impacto, y lo argumentan con una investigación realizada por la empresa Verizon en el año 2015, en la dice que el Phishing, se ha convertido en un ataque popular, y que estos ataques han evolucionado hasta el punto de incluir la instalación de malware y que la efectividad de estos ataques alcanzan el 23% de los destinatarios, y el 11% de usuarios haciendo clic sobre archivos adjuntos y asegura el estudio que pasan solo 82 segundos antes de que una campaña de Phishing obtenga su primer clic.

Esto evidencia que los usuarios se están convirtiendo el día de hoy en un eslabón débil en la seguridad de las compañías.

Los autores argumentan que muchas de las campañas de educación organizadas por las compañías (CBTs) “Computer Based Trainings” fracasan ya que estas se convierten más en un requisito; que una respuesta real a la situación actual.

Los autores recomiendan que los planes de capacitación deben convertirse en talleres vivenciales, en el que, haciendo uso de técnicas de sensibilización y concientización, al igual que el uso de estímulos y simular escenarios de la vida real, permite aumentar las habilidades de los usuarios, y esto redunda en el refuerzo de la seguridad en las compañías.

Entre otras sugerencias los autores proponen las siguientes estrategias para que los programas de capacitación sean más efectivos:

Construir su propio programa de capacitación: cada empresa es diferentes: en este punto los autores proponen que, para realizar programas efectivos, no es necesario gastar miles de dólares en estas campañas, sino ser creativos y hacer uso de los recursos propios, utilizando ejemplos, empoderando a los empleados en papel que desempeñan en preservar la integridad de la seguridad de las empresas y como impactan las decisiones que cada uno toma.

Establecer objetivos: es importante tratarse pocos objetivos pero que estos sean realistas y que permitan ser cumplidos en el tiempo, los autores sugieren establecer uno o dos objetivos al iniciar y realizar ajustes periódicos de acuerdo con los logros obtenidos.

Establecer una línea base: es importante conocer el estado actual de la brecha en seguridad de los funcionarios y tomarla como línea de partida, lo que permitirá conocer objetivamente los avances adquiridos.

Establecer el alcance y crear reglas y pautas del programa: es importante establecer las diferentes reglas y normas, al igual que comunicarlas de manera efectiva y pertinente, es importante que las reglas estén alineadas con las políticas y cultura organizacional. La claridad y sencillez de las reglas permitirá su éxito.

Implementar y documentar un programa de simulación: es bastante útil capacitar, pero es necesario complementar estos conocimientos con escenarios simulados; como por ejemplo realizar una campaña de Phishing interna, donde los empleados

que hagan clic en el enlace ilegitimo, sean redirigidos a un sitio web que esté programado con los temas de seguridad enseñados.

Refuerzo positivo: es importante crear confianza en los empleados y en caso de que alguno de ellos sea víctima de un ataque es importante saber manejar la situación para no crear temores y así obtener la total colaboración.

Gamificación: es la ciencia que se apoya en el juego para lograr las metas, los pasos son: 1) establecer metas, 2) reglas, 3) retroalimentación y 4) la participación es voluntaria,

Definir procesos de respuesta a los incidentes: es importante que estos programas sean implementados y estén en constante actualización, ya que permiten evaluar la respuesta a los incidentes y las acciones a tomar en caso de su ocurrencia.

Definir métricas: es importante establecer sistemas de medición, partiendo de la línea base y conocer los avances obtenidos, estas métricas podrían ser:

- Emails enviados
- Emails abiertos
- Links abiertos
- Recolección de credenciales
- Reporte de intento de pishing
- Emails no reportados
- Links en sitios de entrenamiento

Conclusión: La educación es una estrategia en el esquema de seguridad muy importante, ya que proporciona una capa adicional de defensa, puede que no sea el primero, y los autores aseguran que es más efectiva la política de la zanahoria sobre el garrote, y la importancia de “asegurar el elemento humano, que es el eslabón de seguridad más débil ".

9.4.7 Windows Virus and Malware Troubleshooting

Autor: Andrew Bettany and Mike Halsey

Contenido: Diffenrent Types of Malware: en este apartado del capítulo uno (1) los autores Bettany y Halsey, introducen a los lectores en los diferentes tipos de malware que pueden afectar los PCs.

Virus y gusanos: estos tipos de malware derivan su nombre por no por las acciones sino por la forma en que se propagan. Los virus, por ejemplo, se esparcen de un Pc a otro por contacto o por compartir, mientras que un gusano se propagará por medio de la red, y el actuar de estos pueden ser una o más de las acciones que se describirán a continuación.

Spyware: la privacidad es según los autores “una palabra clave en la informática moderna” y la información personal de millones de usuarios circulan por las diferentes redes sociales y grandes corporaciones, que recolectan todo tipo de información. El Spyware es un malware que recopila información de la víctima sin importar si está online u offline, entre la información está usuario y clave, de diferentes sitios, bancos, cuentas, tarjetas de crédito, usando Keylogger, para enviarla posteriormente a sus creadores.

Adware: los autores lo catalogan como el más “inofensivo” de los malware, ya que su principal objeto es inundar los navegadores de ventanas emergentes que contienen publicidad no deseada, pero advierten que existen variables de este que pueden contener keylogger.

Troyano: los autores lo describen como un programa, que aparentemente es inofensivo como codecs de audio o video, pero carga en su interior un malware potencialmente peligroso en su interior, haciendo alusión al caballo que obsequiaron los griegos a los troyanos, quienes abrieron las puertas de la ciudad sin saber que en el interior de este caballo estaba un grupo de soldados, “siendo realmente un caballo griego”.

Bots: los autores advirtiendo que no es recomendable, pero que este tipo de malware se puede contratar como otros en la “Deep Web” y consiste en redes de bots (equipos infestados que actúan de acuerdo a las mandatos de sus atacantes), generalmente estas redes Botnet, son usadas para lanzar ataques DDoS (denegación de servicio distribuido) y es básicamente la sincronización de está para inundarla de peticiones un objetivo (servidor, pc, servicio, etc.) hasta hacerlo colapsar y de paso aprovechar para infectar con keylogers y backtracks.

Rootkits/Bootkits: desde Windows 8.1, Microsoft dispuso que los nuevos Pcs vendidos con este SO, deberían contar con un firmware UEFI; el cual contiene un sistema de booteo seguro.

Protección pensada contra los Rootkits y Bootkits, que como su nombre lo indica son malware que se alojan en la raíz o en la estructura de booteo del sistema operativo lo que los hace difícil de eliminar, y estando la máquina infestada este tipo de malware puede obtener el control total de su víctima.

Backdoor: los autores hacen referencia varias veces a este tipo de malware, “ya que es la carga útil” de un troyano, un bot u otro. Estas Backdoor permiten mantener el acceso remoto y en ocasiones el control remoto de la máquina infectada por parte de su atacante.

Ransomware: los autores lo describen como el “más desagradable de los malware”, cifra los archivos y documentos almacenados en el Pc víctima, para posteriormente pedir rescate generalmente en Bitcoins, y así poder obtener la llave de descifrado.

Los autores hacen referencia que este tipo de ataque ha afectado a cientos de víctimas, y que muchas de estas pagan los rescates, lo que incentiva el delito informático.

Spam (correo no deseado) y Pishing: los autores aclaran que en si estos no sol malware, pero pueden inducir a las víctimas a páginas web, que si pueden contener malware.

Conclusión: Conocer los diferentes tipos de malware que afectan los sistemas, permitirá estructurar mecanismos de defensa más sólidos y duraderos en el tiempo, es clave la educación a los usuarios, ya que ellos se convierten en la primera línea de defensa.

9.4.7 CEH Certified Ethical Hacker v8 – Study Guide

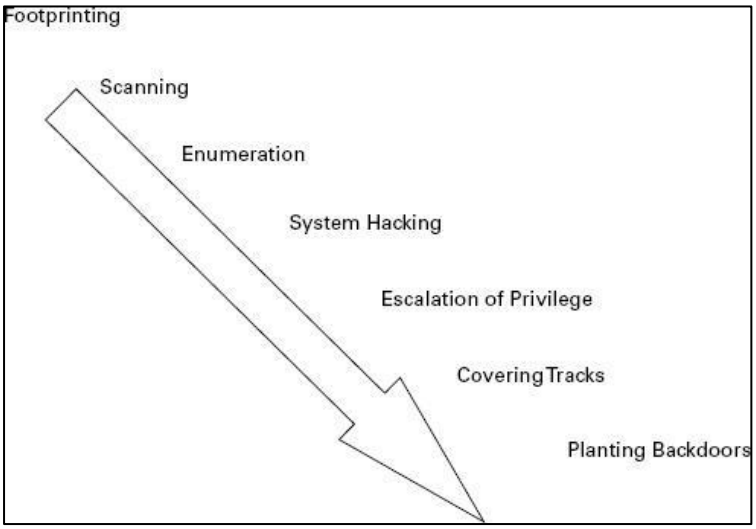
Autor: Sean Philp Oriyano

Contenido: De acuerdo con el autor una “Metodología Hacking” se refiere a los pasos que un atacante lleva a cabo para realizar un ataque a un objetivo como un

Pc conectado a una red, estos pasos no son una regla ya que de por sí, los hackers están por fuera de la ley. El autor hace referencia que la diferencia entre un “hacker y un Ethical hacker, es el código de ética suscrito”.

CEH ilustra los siguientes pasos en el proceso de Hacking:

Ilustración 47. CEH Certified Ethical Hacker v8 – Study Guide



Fuente CEH Certified Ethical Hacker v8 – Study Guide

A continuación, se describe brevemente los pasos documentados por CEH.

- Footprinting: son los diferentes métodos pasivos para obtener información, se mantiene la mínima interacción con el objetivo, evitando así alertarlo. Se usan recursos como; consultas “whois”, consultas Google, redes sociales y puestos de trabajo.
- Scanning (exploración): gracias a la información obtenida en la fase anterior se orienta el ataque de manera “más precisa” se realizan tareas de exploración de puertos, solicitudes Ping, observación de las instalaciones “una de las herramientas más usadas es Nmap”.

- Enumeration (enumeración): se extrae información más detallada sobre lo descubierto en la fase anterior, en esta se evalúa la calidad y utilidad de la información recopilada.
- System Hacking: ganar acceso al sistema, en esta fase se planifica y ejecuta un ataque, basado en l información descubierta, por ejemplo, realizar ataques de acuerdo con las cuentas de usuarios descubiertas.
- Escalation of privilege: si la fase hacking fue exitosa, se puede proceder a obtener privilegios, dependiendo del conocimiento del hacker puede cambiar entre cuentas, como pasar de la cuenta de invitado a la cuenta de administrador o “system-level Access”.
- Covering tracks (cubrir huellas) en esta fase el atacante intenta eliminar cualquier rastro de su paso por el sistema, borrar logs, dejar archivos como los encontró, lo importante es que pasé desapercibido el ataque.
- Planting bak doors: el propósito es “plantar una puerta trasera” que permite al atacante ingresar cunado quiera al sistema.

Conclusión: Las metodologías de “Ethical Hacking”, permite a las compañías obtener un panorama del estado de seguridad de sus sistemas informáticos y así poder cerrar la brecha en seguridad.

9.4.8 The Cyber Risk Handbook – Creating and Measuring Effective Cybersecurity Capabilities

Autor: Domenic Antonucci

Contenido: El autor introduce al lector sobre el “riesgo cibernético” , de cómo están creciendo en sofisticación y tamaño a un “ritmo sin precedentes” debido a los avances tecnológicos, las tecnologías emergentes (Big Data, Cloud Computing, etc.).

Este panorama representa un reto para alinear los objetivos de las organizaciones con la gestión eficaz de las amenazas.

Se enfatiza en la necesidad de un “enfoque integrado e integral para la gestión del riesgo cibernético”.

El autor argumenta acerca de la madurez y efectividad que deben tener las organizaciones, que no se pueden detener ante las amenazas, por el contrario, deben crecer y transformarse.

También enfatiza acerca de la eficiencia “hacer las cosas bien” y la eficacia “hacer las cosas correctas”, como el desafío que deben afrontar las organizaciones, que no es responsabilidad exclusiva de las directivas, sino que debe abarcarse desde una perspectiva funcional de toda la organización

Conclusión: el despertar la conciencia sobre los riesgos cibernéticos, permite a las organizaciones desarrollar diferentes estrategias que permiten mitigar estos riesgos garantizando su permanencia, sostenibilidad y crecimiento.