UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Análisis de vulnerabilidades y pruebas de penetración a la infraestructura tecnológica de empresas

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Eduardo Lagos Flores

ASESOR DE INFORME

M.I. Aurelio Sánchez Vaca

Ciudad Universitaria, Cd. Mx., 2018

Agradecimientos

A mis padres Estela Flores y J. Eduardo Lagos por todo el esfuerzo y sacrificio que realizaron para que yo pudiese cumplir mis metas; así mismo por todo el apoyo, tiempo y amor incondicional que me han brindado a lo largo de mi vida y formación académica, esto es por ustedes.

A mis hermanos: Misael Lagos y Carlos Lagos, por su apoyo y cariño incondicional en cualquier circunstancia. Porque más que hermanos son como mis mejores amigos.

A mi abuelita Antonieta Reyes, que es mi segunda madre. Por cuidarme, apoyarme y enseñarme a luchar hasta el final, gracias.

Al amor de mi vida, Abril García, por motivarme e impulsarme a ser mejor cada día. Por creer y confiar en mí, convirtiendo tu sonrisa en mi motor.

A mi asesor, M.I. Aurelio Sánchez Vaca, por su tiempo, interés y apoyo brindado para la elaboración y culminación de éste reporte. Cuyos consejos y recomendaciones enriquecieron este proyecto.

A White Hat Consultores, por permitirme formar parte de su equipo y darme la oportunidad de seguir desarrollándome profesionalmente en la seguridad informática.

A la Universidad Nacional Autónoma de México, a la Facultad de Ingeniería y al UNAM-CERT por brindarme una formación académica; una parte fundamental en mi desarrollo profesional.

Contenido

Índice de Figuras

Índice de Tablas

Introducción

Con el paso del tiempo, las empresas han adoptado el uso de las tecnologías de la información y comunicaciones (TIC) para la automatización de sus operaciones. Estas infraestructuras de TIC están compuestas por equipos de red, telefonía VoIP, equipos de cómputo personal, servidores de bases de datos, servidores web, entre otros.

Uno de los activos más valiosos para las empresas es la información, misma que es capturada, almacenada, procesada y transmitida por todo el sistema compuesto por los recursos humanos y recursos tecnológicos que interactúan entre sí para satisfacer las necesidades del negocio.

De manera paralela al desarrollo y crecimiento la infraestructura tecnológica, han surgido nuevas amenazas y ataques que ponen en riesgo la información y los activos tecnológicos de las empresas. Las amenazas pueden ir desde agentes humanos como empleados inconformes, crackers, hacktivistas, entre otros; hasta agentes lógicos como cualquier variante de malware, errores de configuración de servicios o errores de programación.

De acuerdo con el sitio de noticias y análisis WeliveSecurity, durante el año 2017 creció el número de incidentes de ciberseguridad y se estima que el espectro de ciberataques seguirá expandiéndose.

Cualquier interrupción o alteración no deseada en el buen funcionamiento de los elementos que forman a un sistema informático podrían generar consecuencias de alto impacto, desde la perdida de altas sumas monetarias, divulgación de información sensible, fraudes, afectación a la imagen corporativa y sanciones impuestas por las respectivas entidades regulatorias.

La seguridad informática es la disciplina que tiene como objetivo proteger y garantizar la integridad, confidencialidad y disponibilidad de la información que reside en un sistema informático, de las amenazas a las que se encuentran expuestos y reducir los riesgos hasta alcanzar un nivel aceptable.

Por lo anterior, es de vital importancia que las organizaciones conozcan las debilidades que posee su infraestructura tecnológica, de manera que le permita implementar las medidas correctivas necesarias para reducir el riesgo de ser víctima de las amenazas inherentes.

Para lograr esto, las empresas buscan el apoyo de profesionales para la realización de Servicios de Auditoría de Seguridad, cuyo objetivo es evaluar la seguridad de las infraestructuras informáticas y controles de seguridad para la detección de debilidades y problemáticas de seguridad, que podrían ocasionar afectaciones proceso de negocio.

En específico, el servicio de Pruebas de Penetración simula el accionar y comportamiento de un atacante, ya sea un cracker, un empleado descontento, entre otros; y se realiza con el objetivo de identificar el impacto que podría causar un atacante en caso de explotar vulnerabilidades asociadas a los activos de TI de una Organización.

Este tipo de pruebas se hacen con el permiso otorgado por el dueño de los activos a evaluar y bajo acuerdos de confidencialidad (NDA) para evitar la divulgación de la información obtenida durante las pruebas.

Objetivo

Aplicar los conocimientos y capacidades analíticas obtenidas a lo largo de mi formación académica en la carrera de Ingeniería en Computación, para la resolución de problemas y búsqueda de áreas de oportunidad de mejora, en el ámbito de la seguridad informática.

Este informe contiene un resumen de mis actividades realizadas como consultor y líder de seguridad ofensiva, durante el proyecto *Servicio de análisis de vulnerabilidades y pruebas de penetración* realizado a una empresa líder a nivel nacional, en el campo de la manufactura de carne y alimentos, y cuyo objetivo es la búsqueda de brechas de seguridad que afectan a su infraestructura de TI.

Capítulo 1. Descripción de la empresa

White Hat Consultores es una empresa de consultoría con alta especialización en Servicios de Seguridad de la Información, Ciberseguridad, Análisis de Vulnerabilidades y Pruebas de Penetración, con especial presencia en los mercados de Gobierno, Financiero y de Telecomunicaciones. Es una empresa de gran especialidad en el ramo de Seguridad de la Información, con más de 9 años de experiencia, manteniendo una fuerte presencia en los sectores más regulados como son APF y Financiero.

El equipo de consultores que pertenece a esta empresa ha adquirido una gran experiencia y calidad mediante la participación sistemática en proyectos en diversas entidades y con certificaciones muy especializadas de la industria y competitivas en el ámbito de la seguridad ofensiva.

El nombre de la empresa proviene de la clasificación que se tiene de los hackers, en donde los White Hat hackers son personas con grandes conocimientos sobre tecnología, seguridad y pentest, pero que tienen como objetivo ayudar a las empresas a proteger sus activos y sistemas de TI.

1.1. Misión

Proveer a las organizaciones y a las personas de soluciones de administración de riesgo y servicios avanzados de ciberseguridad, para proveer libertad en un entorno de riesgo digital, así como la optimización y eficiencia en la operación.

1.2. Visión

Ser la empresa especialista líder en servicios de alta especialización de ciberseguridad, integrando las mejores prácticas a nivel internacional y entregando soluciones de valor al negocio de nuestros clientes.

1.3. Historia

Un conjunto de socios conformó el 27 de febrero de 2009 el grupo central de White Hat Consultores, orientando a la seguridad como un enfoque sistémico de Personas, Tecnología y procesos que deben ser articulados alrededor del negocio.

White Hat Consultores S.A. de C.V. se creó con la convicción de que la Seguridad no es un problema Tecnológico, sino que se requiere de un enfoque de la Gestión del Riesgo. WHC se especializa en servicios de alto valor agregado en proyectos complejos y retadores, abarcando todas las áreas de Seguridad, Gestión del Riesgo y Administración de Servicios de TI alineados a ITIL.

1.4. Organigrama

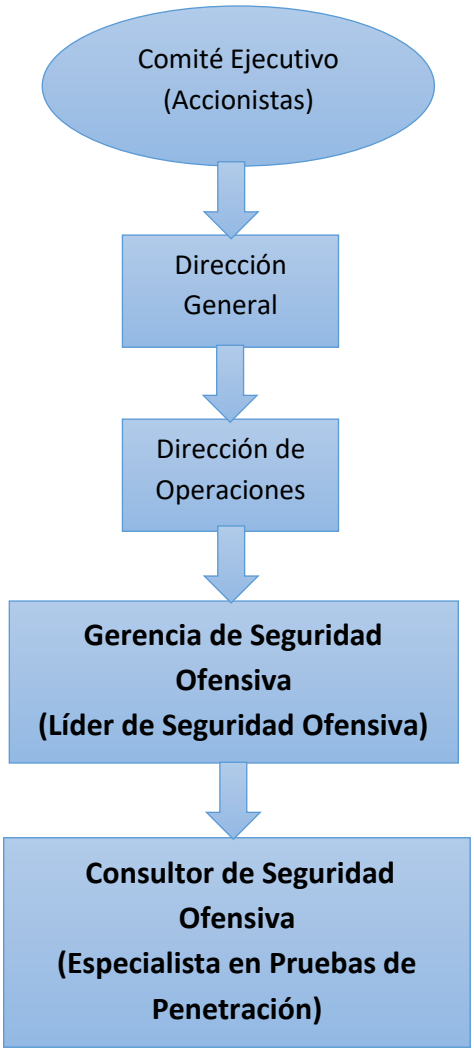


Figura 1.1 Organigrama de consultoría en WHC.

1.5. Descripción del Área

En la empresa se cuentan con un Área de Seguridad Ofensiva, la cual se encarga de realizar los servicios de Análisis de Vulnerabilidades y Pruebas de Penetración.

Análisis de Vulnerabilidades

Es el conjunto de pruebas de seguridad, en donde un especialista ejecuta técnicas y herramientas especializadas para la detección de fallas, malas configuraciones y vulnerabilidades asociadas a los servicios y activos de TI de una organización. Este servicio se realiza con el enfoque defensivo, de manera que no se realiza la explotación de las vulnerabilidades encontradas en los activos analizados, a diferencia del servicio de Pentest.

Como conclusión del servicio se entrega un reporte a nivel técnico y ejecutivo que contiene la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado, el escenario de riesgo (posibles consecuencias) y las respectivas recomendaciones para la mitigación del hallazgo de seguridad.

Pruebas de Penetración

También conocido como Pentest, es un conjunto de pruebas de seguridad, en donde un profesional de la seguridad ejecuta ataques reales y técnicas especializadas para la detección y explotación de vulnerabilidades que poseen los activos de TI de una organización. En este servicio el consultor toma el rol de un atacante real que busca explotar y aprovecharse de las vulnerabilidades detectadas para penetrar los sistemas y obtener información de carácter confidencial para la organización.

Al finalizar la ejecución de las pruebas, se entrega un reporte a nivel técnico y ejecutivo que contiene la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado, el escenario de riesgo (posibles consecuencias), las respectivas recomendaciones para la mitigación del hallazgo de seguridad y una evidencia de la explotación de la vulnerabilidad.

1.6. Descripción del Puesto

Al finalizar mis estudios, en la Facultad de Ingeniería, ingresé a la novena generación del Plan de Becarios de Seguridad Informática del UNAM-CERT, el cuál concluí de manera satisfactoria después de 14 meses. En este plan de formación recibí una capacitación especializada en materia de seguridad de la información, específicamente en los siguientes módulos:

I. Seguridad en redes y Sistemas Operativos
II. Seguridad en sistemas
III. Respuesta Incidentes
IV. Análisis de vulnerabilidades y hacking ético
V. Gestión de Proyectos

Los conocimientos y capacidades adquiridas durante mi formación académica me permitieron ingresar en el área de Seguridad Ofensiva de White Hat Consultores. Durante mi estancia en la empresa, he desempeñado el puesto de Líder de Seguridad Ofensiva y Consultor de Seguridad Ofensiva.

Consultor de Seguridad Ofensiva

El objetivo del puesto de Consultor es el de ejecutar las pruebas técnicas durante los servicios de Análisis de vulnerabilidades y Pruebas de Penetración. Entre las funciones y responsabilidades establecidas para el puesto de Consultor se encuentran:

a) Apoyar en la ejecución de las pruebas de penetración y el análisis de vulnerabilidades a los activos de TI.
b) Apoyar en la ejecución de las pruebas técnicas, tales como: descubrimiento de activos, escaneo de servicios, análisis y validación de vulnerabilidades.
c) Apoyar en la investigación de mecanismos de explotación de las vulnerabilidades identificadas durante el servicio de Pruebas de Penetración.
d) Apoyar en la generación de reportes y recomendaciones para la mitigación de hallazgos.
e) Investigar y desarrollar nuevas técnicas de detección, explotación de vulnerabilidades y evasión de controles de seguridad.

Líder de Área de Seguridad Ofensiva

El puesto de Líder tiene como objetivo planificar, dirigir, ejecutar y entregar el servicio de análisis de vulnerabilidades y pruebas de penetración. Adicionalmente, es la figura responsable por la ejecución satisfactoria de las pruebas técnicas y el desempeño del equipo de consultores que forman parte del área.

Las funciones y responsabilidades establecidas para el puesto de Líder de Seguridad Ofensiva son las siguientes:

a) Planeación de las fases que comprenderán los servicios de Análisis de vulnerabilidades y Pruebas de Penetración de acuerdo a los requerimientos cada cliente.
b) Coordinar y ejecutar las pruebas técnicas, tales como: descubrimiento de activos, escaneo de servicios, análisis y validación de vulnerabilidades.
c) Investigación de mecanismos de explotación de las vulnerabilidades identificadas durante el servicio de Pruebas de Penetración.
d) Coordinar y ejecutar la explotación de las vulnerabilidades identificadas durante el servicio de Pruebas de Penetración.
e) Dirigir, contribuir y analizar el análisis de riesgos asociado a los activos evaluados dentro durante el servicio.
f) Coordinar y revisar la generación de reportes y recomendaciones para la mitigación de los hallazgos de seguridad.
g) Entrega de resultados a nivel gerencial y técnico con los clientes.
h) Investigar y desarrollar nuevas técnicas de detección, explotación de vulnerabilidades y evasión de controles de seguridad.
i) Capacitar al equipo de consultores respecto al surgimiento de nuevas amenazas, metodologías de análisis, herramientas, eventos a nivel mundial, cualidades técnicas y noticias relacionadas al área.

Capítulo 2. Marco Teórico

En esta sección se presenta, de manera general, algunos temas y conceptos necesarios para el entendimiento del presente reporte y de mi participación en el proyecto.

2.1. Tipos de Pruebas de Penetración

Las Pruebas de Penetración pueden clasificarse dependiendo de la información proporcionada por el cliente hacia el equipo de consultores de seguridad ofensiva. A continuación, se describen los tres tipos de auditorías:

Pruebas de Penetración de Caja Negra

En este tipo de auditoría el equipo de consultores no recibe ningún tipo de información sobre los sistemas informáticos y activos pertenecientes a la infraestructura de TI de la organización. En este caso, el equipo de consultores sólo recibe el nombre de la institución, por lo que se trabaja con la información que se puede recolectar a través de medios públicos. Este tipo de pruebas simula el ataque de un cracker, por lo que permite medir el alcance e impacto que tendría un evento real.

Pruebas de Penetración de Caja Blanca

Este enfoque de auditoría se utiliza cuando el cliente necesita realizar un análisis de seguridad a profundidad en los sistemas informáticos. Para que esto suceda, el cliente comparte la mayor cantidad de información posible, de manera que el equipo consultor pueda trabajar directamente sobre los activos a analizar y reduciendo el tiempo de las fases previas a la identificación y explotación de las vulnerabilidades.

En este tipo de auditoría, el equipo consultor recibe información con mayor detalle sobre los activos y servicios de la infraestructura tecnológica, tal como: versiones de los servicios que se ejecutan, listas de los sistemas operativos instalados en los servidores, código fuente de aplicaciones, entre otros.

Pruebas de Penetración de Caja Gris

Este tipo de auditoría es una combinación de los tipos anteriores, en dónde el cliente entrega cierta información, pero no toda al equipo de consultores, tal como: segmentos de red, direcciones IP de servidores pertenecientes a la infraestructura de TI, diagramas con la topología de la organización, entre otros.

Otra manera de clasificar el tipo de pruebas es respecto al lugar desde el que el equipo de consultores realiza la ejecución de las mismas:

Pruebas de Penetración Externas

Las pruebas son realizadas por el equipo de consultores desde cualquier punto fuera de la infraestructura de TI. El objetivo de este tipo de pruebas es simular el accionar de un atacante remoto hacia los activos tecnológicos de la infraestructura de TI, que se encuentran expuestos en Internet (véase Figura 2.1).

Este tipo de pruebas permite valorar la visibilidad que tiene el atacante externo y el impacto que asociado a la explotación de las vulnerabilidades detectadas. Este tipo de pruebas son realizadas desde las oficinas de la consultoría.

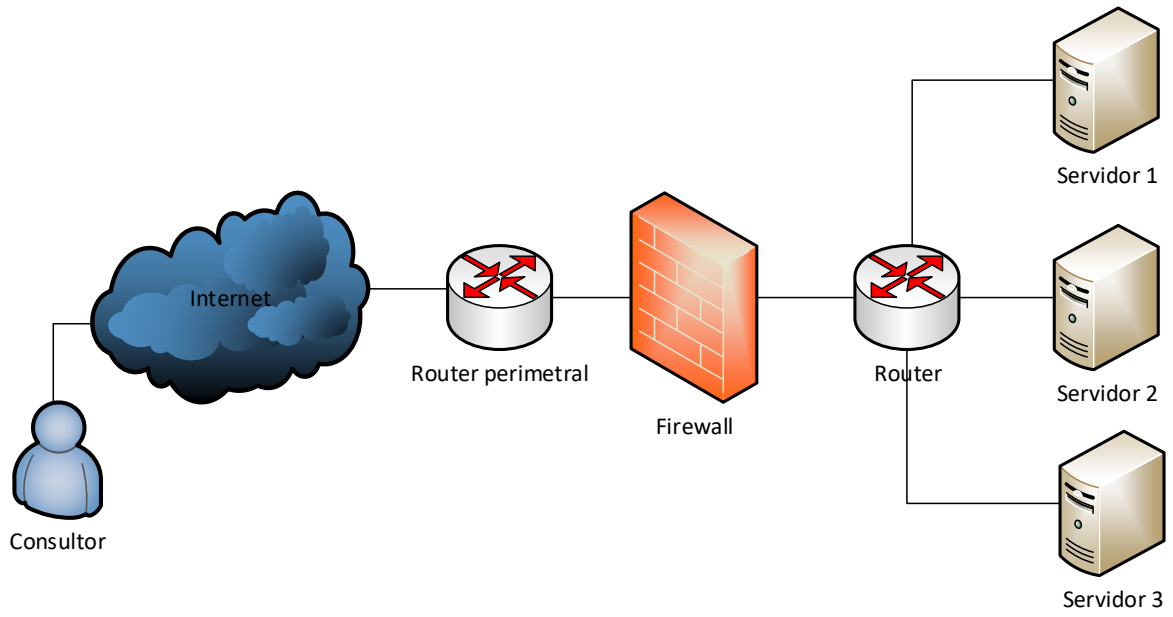


Figura 2.1 Pruebas Externas

Pruebas de Penetración Internas

El objetivo de estas pruebas es el de medir el daño que podría causar un atacante que se encuentre dentro de la red interna. Para llevar a cabo las pruebas internas, el equipo de consultores se sitúa en una estación de trabajo de la organización a evaluar y se le suministra acceso a la red interna (véase Figura 2.2). Dependiendo de las necesidades del cliente y del servicio, se podría modelar un atacante interno que posee acceso a la red de usuarios administrativos, a la red de servidores de desarrollo, red de servidores de producción, entre otros.

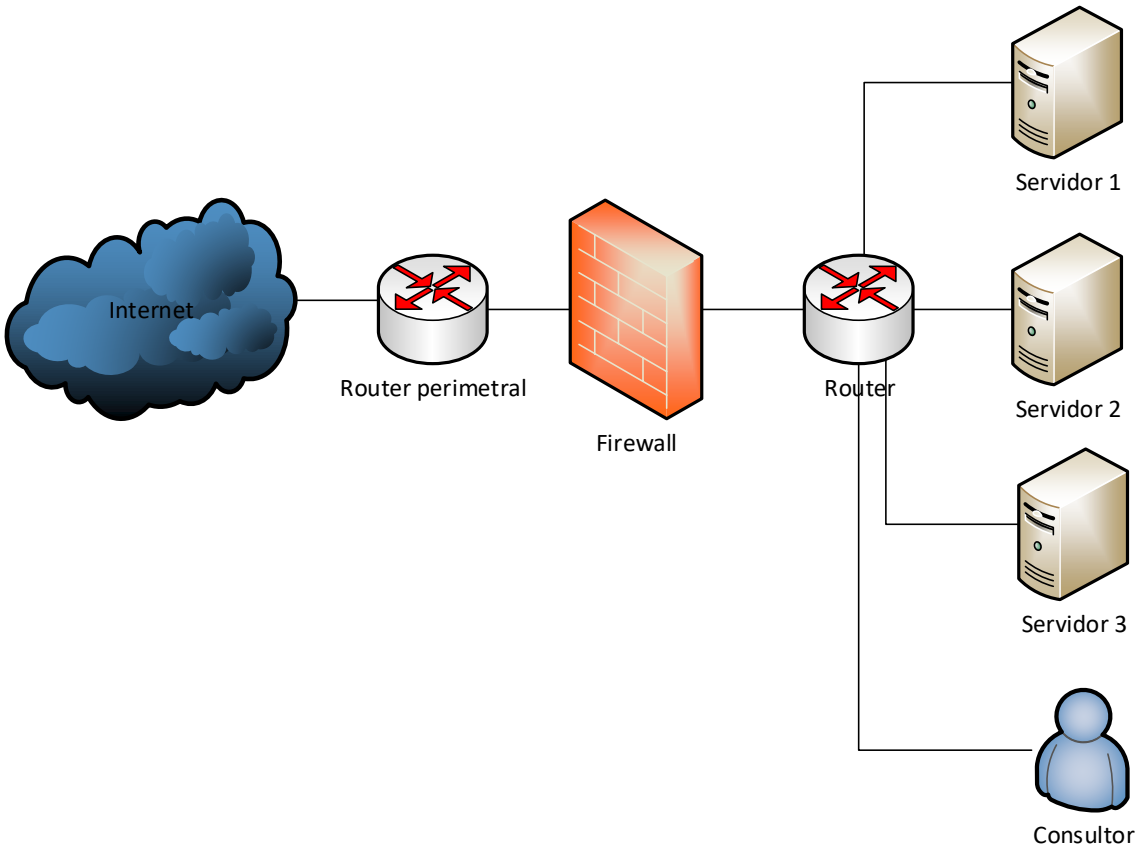


Figura 3.2 Pruebas Internas

Generalmente, las pruebas internas son las que obtienen mayores hallazgos de seguridad, además de que sirven para evaluar el accionar, la efectividad y el tiempo de reacción ante el manejo de incidentes por parte del personal que integre el equipo de seguridad defensiva y respuesta a incidentes.

2.2. Metodología

Para que el equipo de consultores pudiese realizar cada una de las pruebas técnicas, que compone al servicio, se contemplaron una serie de etapas necesarias. Como marco de referencia, se utilizó la metodología establecida en el proyecto PTES, que funge como estándar en el campo de las pruebas de seguridad.

PTES

El proyecto PTES (Penetration Testing Execution Standard) surgió a principios del año 2009, por un conjunto de profesionales de la seguridad. Este estándar se encuentra en la versión 1.0 y fue diseñado para ofrecer a las empresas y proveedores de servicios un lenguaje y enfoque común para realizar pruebas de penetración. Esta metodología consta de siete fases, como se muestra en la siguiente imagen (Figura 2.3).

Figura 4.3 Metodología PTES

Pre-engagement Interactions

Esta fase refiere a las interacciones previas a la ejecución de las pruebas técnicas. El equipo de consultores deberá entrevistarse con el cliente para entender las necesidades específicas del servicio y acordar las condiciones en las que se ejecutarán las pruebas: que tipo y enfoque de pruebas se realizará, los horarios establecidos y la duración de las pruebas.

Otro de los aspectos importantes a definir es el del alcance de la prueba, en dónde se establece que activos pueden ser considerados a evaluar y el nivel de profundidad de las pruebas. El nivel de profundidad se refiere hasta que instancias se permite escalar el ataque el equipo de consultores y el tipo de pruebas deben ser excluidas debido a su peligrosidad (DoS).

Un documento importante que se debe definir en esta etapa es el Acuerdo de Confidencialidad o NDA (Non-Disclosure Agreenment), el cuál es necesario para proteger la privacidad de la información y hallazgos obtenidos durante la ejecución de las pruebas de penetración.

Intelligence Gathering

Es la primera fase de las pruebas técnicas, se basa en la búsqueda y recolección de la mayor cantidad de información posible sobre el objetivo, por lo que puede que sea la etapa que mayor tiempo demande. Esta etapa podría dividirse en dos: reconocimiento pasivo y reconocimiento activo.

El reconocimiento pasivo se realiza para obtener información del objetivo sin tener un contacto directo con el cliente y sus activos. En este enfoque de búsqueda de información, el equipo de consultores recolecta información de sitios públicos de internet, archivos expuestos y sus metadatos, GHDB, redes sociales y servicios que brinden detalles técnicos (DNS, Whois, entre otros.).

Por otro lado, el reconocimiento activo se realiza cuando el equipo de consultores interactúa de manera directa con los activos y servicios de la infraestructura objetivo. En esta etapa, el equipo de consultores se apoya de la ejecución de herramientas que interactúen con los distintos protocolos de red y servicios, con el objetivo de descubrir: segmentos de red, direcciones IP de equipos, sistemas operativos, puertos expuestos, versiones de los servicios que se ejecutan y cuentas de usuarios.

Threat Modeling

Para realizar el modelado de amenaza, la metodología se centra en dos elementos principales: los activos y el atacante. En esta etapa se busca identificar que activos son más importantes, cuales son los grupos de riesgo (atacantes o amenazas) que existen y las capacidades o motivaciones que pudiesen tener los grupos de riesgo para causar un daño a la compañía.

Vulnerability Analysis

Es el proceso de describir fallas en los sistemas y aplicaciones, las cuales pueden ser aprovechadas por un atacante para penetra en un sistema o aplicación. Esta etapa comienza con la ejecución de herramientas, pruebas automatizadas y pruebas manuales para la detección de vulnerabilidades.

Después se continúa con la validación de los hallazgos detectados, buscando eliminar falsos positivos. Para finalizar, se realiza una investigación de las vulnerabilidades con el objetivo de conocer mayor información relacionada, como: las causas de la vulnerabilidad, si existe un exploit asociado, las consecuencias o efectos secundarios de la explotación y si cuenta con un identificador CVE-ID asociado.

CVE (Common Vulnerabilities and Exposures) es una base de datos que registra vulnerabilidades de seguridad conocidas. Cada registro contiene un identificador (CVE-ID) que tiene el siguiente formato: CVE-YYYY-NNNN, dónde YYYY es el año y NNNN es el número de la vulnerabilidad.

Explotation

Durante esta etapa, el equipo de consultores se poyará de la ejecución de exploits para aprovecharse de las vulnerabilidades previamente identificadas, con el objetivo de acceder a un sistema, evadir controles de autenticación u obtener mayor información.

Los exploits contienen un conjunto de instrucciones o carga útil, que se ejecuta después de aprovecharse de la vulnerabilidad y es conocida como payload. Entra las actividades que un payload podría hacer están: añadir usuarios en los sistemas, generar una backdoor, elevación de privilegios, obtener registros de bases de datos, desactivar servicios antivirus, entre otros.

Post Explotation

Esta fase tiene como finalidad la valoración de que tan lejos podría llegar el equipo de consultores, después del acceso al servicio o sistema (Explotación de la vulnerabilidad). Las actividades principales que componen esta fase son: mantenimiento del acceso, búsqueda de información y borrado de huellas.

La parte del mantenimiento del acceso se puede realizar a través de la instalación de backdoors, robo de credenciales o la adición de nuevos usuarios. La búsqueda de información permitiría obtener datos o documentos de carácter sensible, archivos de configuración o credenciales almacenadas en el sistema, mismas que podrían ser utilizadas en ataques denominados movimientos laterales. Los ataques de movimiento lateral permiten validar si las credenciales recuperadas son reutilizadas en otros sistemas o equipos, de manera que nos permita ampliar el alcance de la intrusión.

Para la parte del borrado de huellas, se elimina la evidencia del acceso de los archivos de registro de actividad (logs). También deben eliminarse los rastros de los usuarios y backdoors desplegados en los sistemas.

Reportes (Reporting)

Esta es la etapa más importante de la metodología ya que, a través del reporte, el equipo de consultores puede demostrar el trabajo realizado, los hallazgos de seguridad detectados y el impacto que se podría tener en caso de la explotación.

Como parte de la evidencia de la explotación y del acceso al sistema, el reporte puede contener: capturas de pantalla de inicios de sesión en servidores, credenciales obtenidas y archivos con información confidencial obtenidos.

2.3. Metodología de Pruebas Planteada

Para la ejecución de las pruebas de penetración a la empresa cliente, el equipo de consultores de Seguridad Ofensiva se basó en la metodología PTES para diseñar la metodología a utiliza durante la ejecución del servicio a la Empresa Cliente. En el siguiente diagrama (Figura 2.4) se muestran las etapas consideradas durante las pruebas:

Figura 5.4 Metodología Propuesta

Debido a que el equipo de auditoría y controles de seguridad fueron los encargados de realizar dicho proceso, en este caso, no se tomó una fase de modelado de amenazas..

Reconocimiento

En esta fase se busca la recolección de la mayor cantidad de información a través de medios públicos y servicios expuestos que no interactúen de manera directa con la organización a evaluar, tales como sitios públicos de internet, redes sociales y GHDB. También se hace la identificación de dominios, subdominios, segmentos de red y servicios de correo.

Escaneo

Una vez identificados los activos pertenecientes a la organización y que se encuentren dentro del alcance, el equipo de consultores realiza la ejecución de técnicas y herramientas que permitan identificar activos expuestos, tales como: servidores, sistemas operativos, puertos, versiones de servicios, aplicaciones web, portales de autenticación, entre otros.

También, durante esta etapa, se realizará el escaneo y análisis de vulnerabilidades asociadas a los activos encontrados, la validación de los hallazgos y la investigación de las vulnerabilidades.

Explotación

Después de haber eliminado los falsos positivos, haber encontrado información asociada a los mecanismos de explotación de las vulnerabilidades detectadas, se analiza la posibilidad de la explotación de cada hallazgo, con el objetivo de evitar alteraciones e interrupciones no deseadas en los activos evaluados (DoS, BSOD).

Al finalizar la evaluación anterior, el equipo de consultores realiza la ejecución de las exploits para aprovecharse de las vulnerabilidades previamente detectadas y que no representen un riesgo de afectación a la disponibilidad de los servicios.

Post Explotación

Esta etapa fue definida para buscar escalar los ataques, aprovechando el acceso logrado a los sistemas y servicios, tal como un atacante lo haría. Algunas de las técnicas y ataques ejecutadas en esta etapa son: generación de backdoors, ataques de movimiento lateral, búsqueda de información sensible, recuperación de credenciales, compromiso de la infraestructura de Active Directory, acceso a los sistemas SCADA.

Al finalizar el escalamiento del ataque, se realiza el proceso de borrado de backdoors y herramientas desplegadas en los sistemas y servidores comprometidos, así como la eliminación de usuarios añadidos.

Generación de Reporte

Debido a la importancia del reporte, se definió esta etapa para la generación de los reportes técnico y ejecutivo. El reporte técnico contiene información sobre el alcance de las pruebas, los activos que se evaluaron, la metodología empleada, los detalles técnicos de hallazgos de seguridad, recomendaciones de para la mitigación de las vulnerabilidades, la evidencia de la intrusión y las conclusiones.

Mientras que el reporte ejecutivo contiene un breve resumen, evitando utilizar lenguaje técnico, sobre los activos evaluados, los hallazgos más relevantes de seguridad, evidencias de intrusión y conclusiones.

2.4. Herramientas

En esta sección describo de manera general, las principales herramientas utilizadas por el equipo de Seguridad Ofensiva durante la ejecución de las pruebas técnicas.

Vmware

Es un software que permite ejecutar distintos equipos virtuales en una máquina física y de manera independiente al sistema operativo nativo. La virtualización es utilizada cuando se requiere desplegar un ambiente de pruebas o ejecutar varios sistemas operativos independientes y sólo se cuenta con una máquina física.

Existen distintas versiones de esta herramienta, sin embargo, durante la ejecución del proyecto se utilizó la versión vmware Workstation 14 Pro (véase Figura 2.5), debido a que brinda mayores funciones como: ejecución de varias máquinas virtuales, creación de snapshots, simulación de redes virtuales, entre otras.

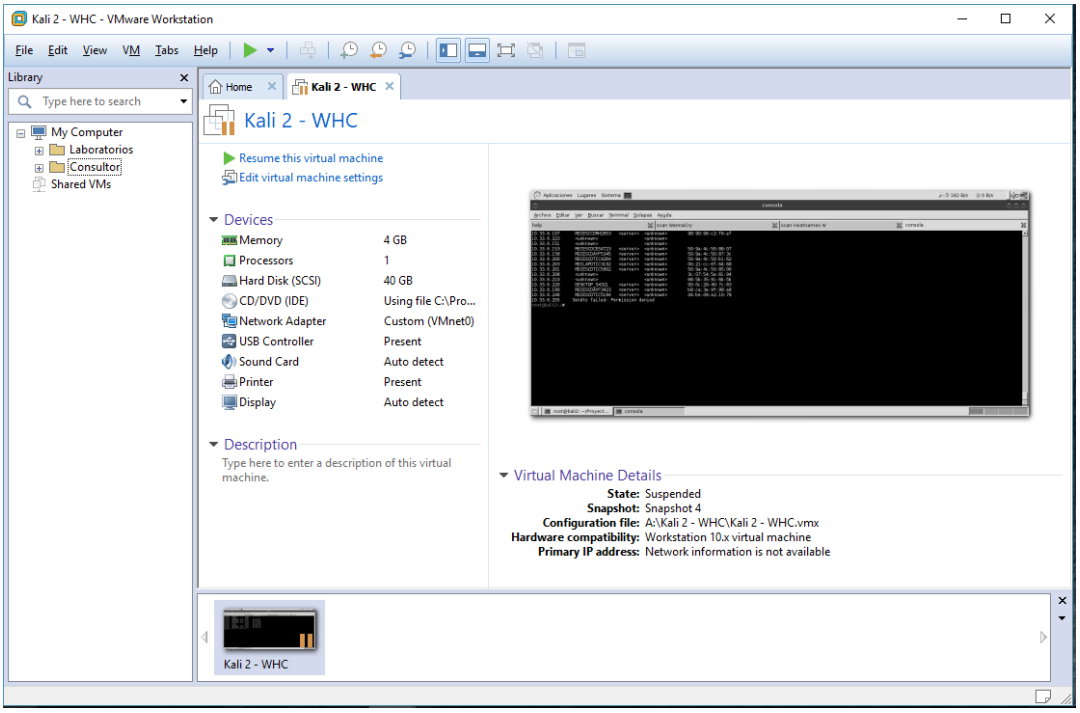


Figura 6.5 vmware Workstation Pro

Kali Linux

Es una distribución basada en el sistema operativo Debian GNU/Linux que cuenta con una suite de más de 600 herramientas preinstaladas para la auditoría de seguridad. Entra las herramientas que vienen preinstaladas podemos encontrar: escáneres de red, herramientas de enumeración de servicios, herramientas realizar análisis de vulnerabilidades, herramientas para realizar ataques a procesos de autenticación, frameworks para la generación de exploits, entre otras (véase Figura 2.6).

Este proyecto de código abierto fue fundado y es mantenido por el equipo de Offensive Security. Para la ejecución de las herramientas y ataques, se instaló el sistema operativo Kali Linux sobre una máquina virtual.

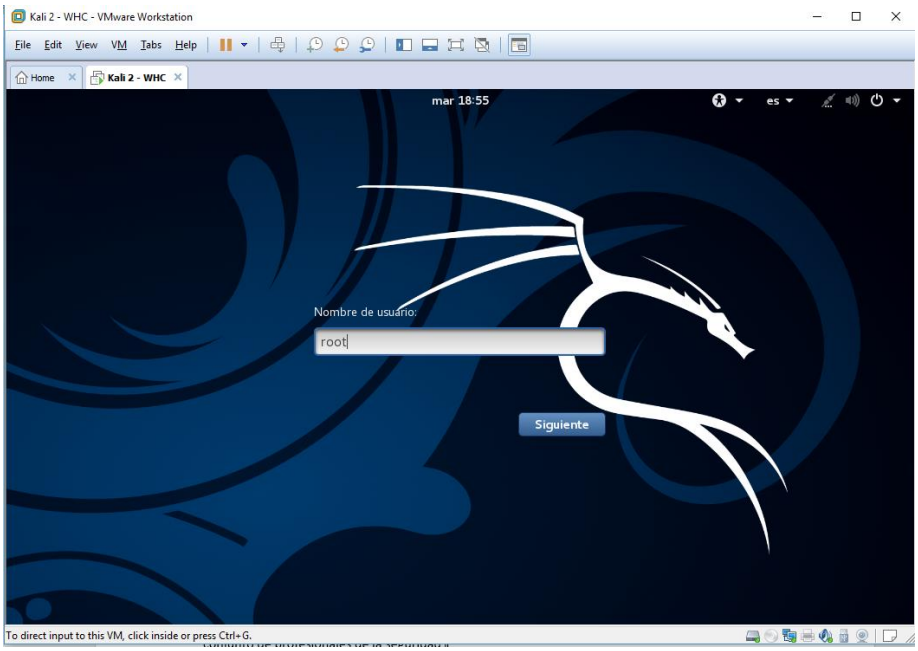


Figura 7.6 Kali Linux

Whois

Es una base de datos pública, que contiene los datos personales y de contacto de los titulares de dominios registrados en Internet ante una IANA (Internet Assigned Numbers Authority). La IANA es la entidad encargada de administrar los nombres de dominios, direcciones IP asignadas, entre otros datos técnicos.

Entre los datos que se pueden obtener a través de una consulta Whois son: Nombre de dominio, datos del contacto administrador, segmentos de red asociados, servidores DNS, fecha de registro, entre otros. La base de datos Whois puede ser consultada a través del cliente que se encuentra instalado en la suite de herramientas de Kali Linux o vía web.

En la siguiente imagen (Figura 2.7) se muestran los datos de contacto del sitio google.com, recuperados a través de la consulta WHOIS.

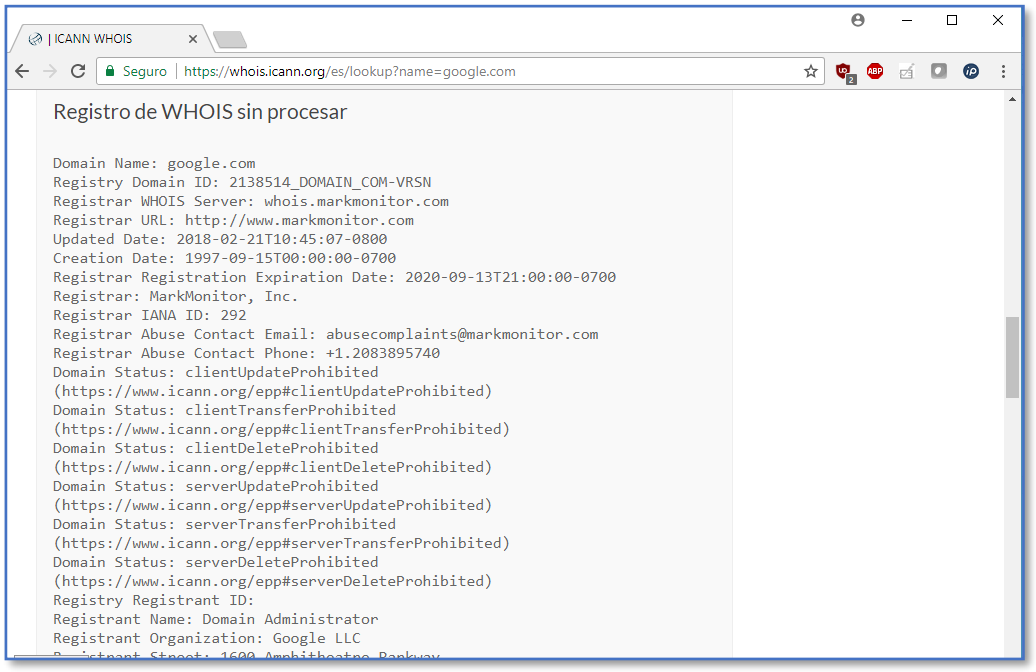


Figura 8.7 Consulta WHOIS

GHDB

Google es el motor de búsqueda más utilizado en la actualidad, por lo que cuenta con la mayor cantidad de páginas indexadas. Google soporta distintos operadores avanzados para realizar búsquedas más específicas.

Google Hacking Database es un gran compendio de combinaciones de operadores de búsqueda, también llamados *google Dorks*, utilizados para obtener información valiosa para los atacantes o consultores de seguridad, tal como archivos de configuración, usuarios y contraseñas almacenados en archivos expuestos a internet, cámaras de seguridad accesibles desde internet, respaldos de bases de datos, archivos con información de los servicios instalados, entre otros datos.

A continuación, se muestra parte del compendio de GHDB, que se encuentra en el sitio web ExploitDataBase (Véase Figura 2.8).

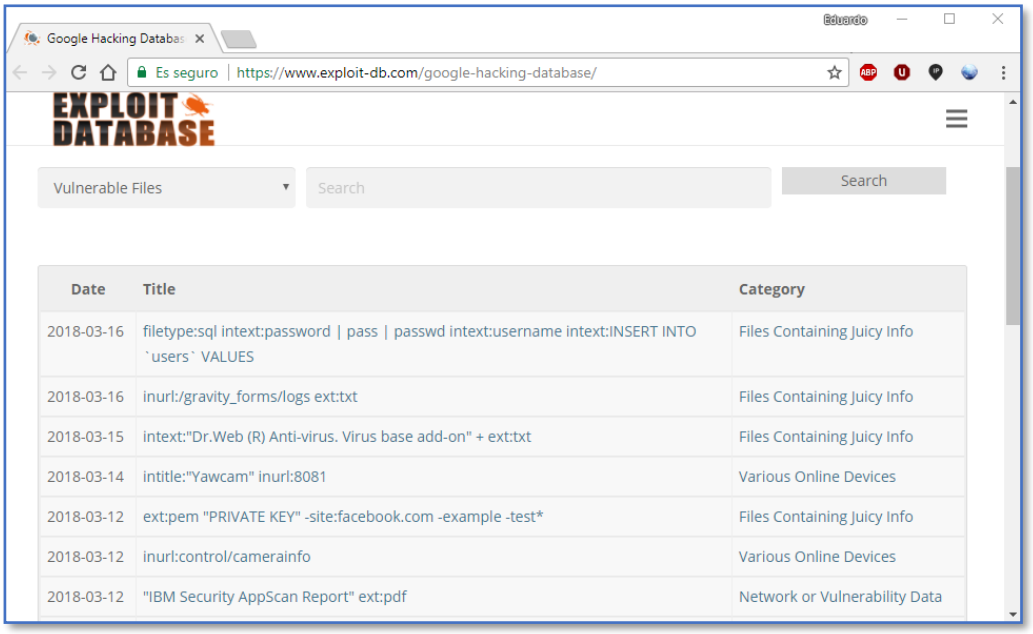


Figura 9.8 google Dorks

En la siguiente tabla 2.1 se describe el funcionamiento y un ejemplo de algunos operadores de búsqueda avanzada de Google.

Tabla 2.1 Operadores de búsqueda de avanzada de Google

Operador	Funcionamiento	Ejemplo
site	Operador utilizado para buscar recursos asociados a un sitio web.	site:dominiocliente.com
inurl	Operador utilizado para buscar una cadena en específico dentro de una URL.	inurl:login
intitle	Operador utilizado para buscar recursos que contengan una cadena de texto específica en el título.	intitle:”main page”
filetype	Operador utilizado para buscar archivos o recursos de acuerdo a su extensión, por ejemplo archivos de texto (.txt), documentos (.doc), entre otros.	filetype:txt credenciales
related	Operador utilizado para buscar sitios web relacionados a un dominio en específico.	related:dominiocliente.com
intext	Operador utilizado para buscar recursos que contengan una cadena en específico dentro del mismo recurso, excepto en el título, en la URL y en los enlaces	intext: mysql_connect password

Nmap

Esta herramienta toma su nombre de Network Mapper y es de código abierto, utilizada para el descubrimiento de redes y las auditorías de seguridad. Esta herramienta nos permite: identificar equipos en una red, conocer el estado de los puertos TCP o UDP, identificar las versiones de los servicios que se ejecutan en un equipo e identificar el sistema operativo de los equipos en una red (véase Figura 2.9).

También cuenta con la funcionalidad NSE (Nmap Scripting Engine), la cual permite la escritura ejecución de scripts para automatizar una gran variedad de tareas. La ejecución de estos scripts permite realizar las siguientes actividades: escaneo de vulnerabilidades, auditoría de procesos de autenticación, identificación de malware, explotación de vulnerabilidades, entre otras.

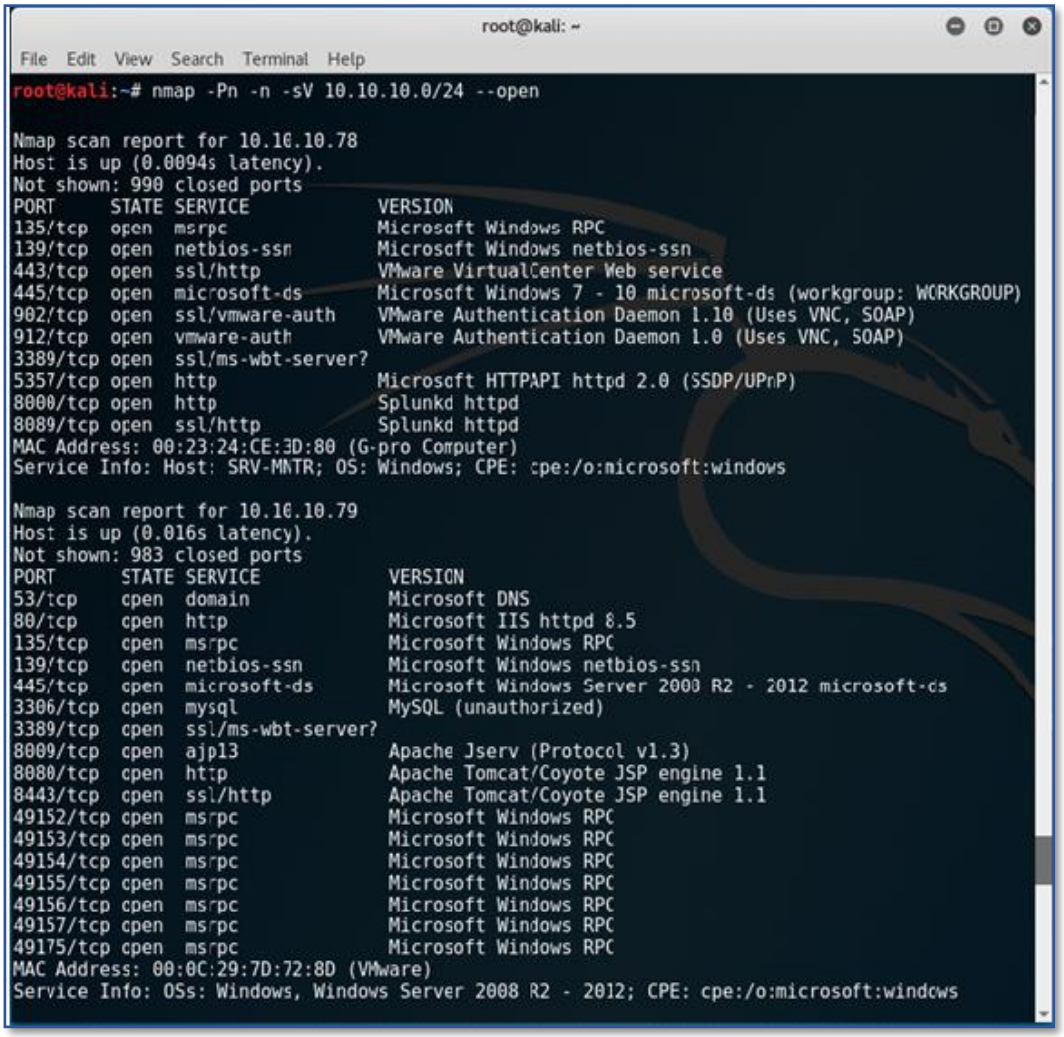


Figura 10.9 Escaneo de Servicios y Versiones con NMAP

Nessus

Esta herramienta es utilizada para el diagnóstico de vulnerabilidades, detección de errores de configuración y de malware que se pudiesen encontrar alojados en los dispositivos de una red (véase Figura 2.10). Cuenta con una amplia gama de plugins (más de 90,000) para realizar auditorías de seguridad. Para la ejecución del servicio fue utilizada la versión de Professional, que es de licenciamiento, debido a que ofrece más funcionalidades, tales como: ejecución de distintos escaneos de manera paralela, actualización diaria de nuevos plugins y su diseño para uso comercial.

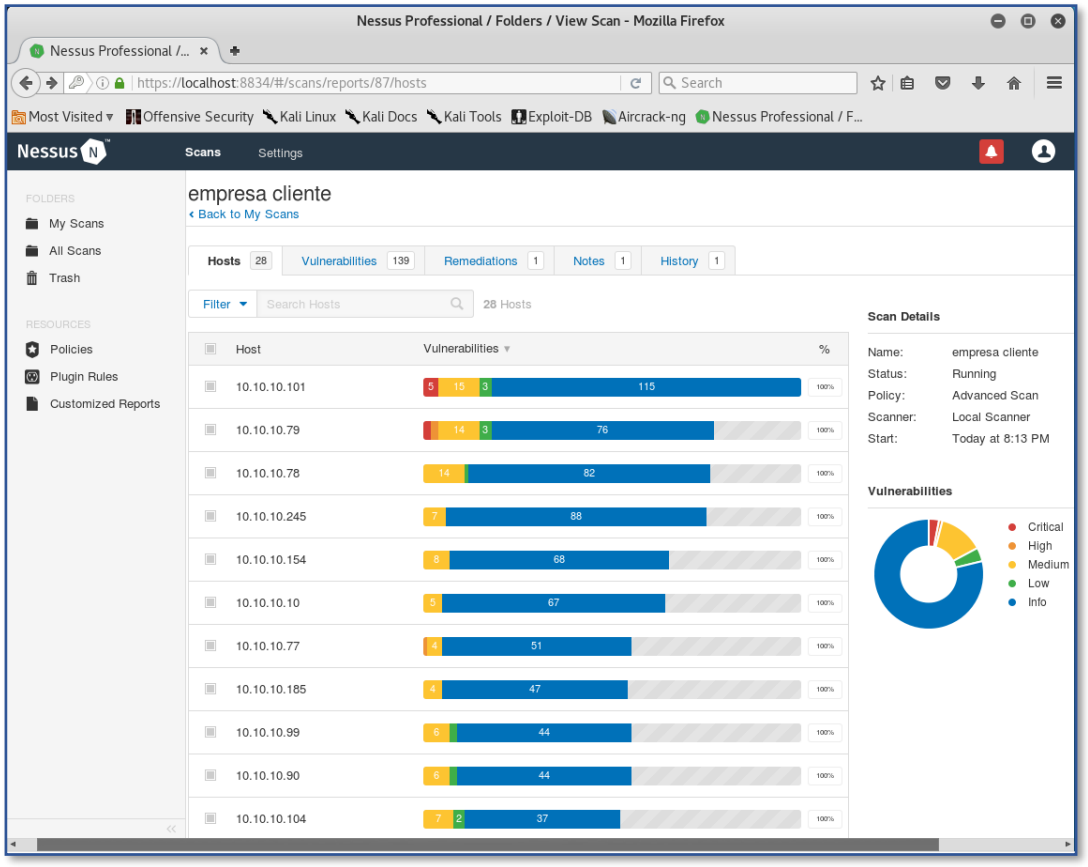


Figura 11.10 Escaneo de Vulnerabilidad con Nessus

Para categorizar las vulnerabilidades, Nessus tiene cinco categorías: Informativas, Bajas, Medias, Altas y Críticas. Al final nos permite obtener detalles de cada hallazgo de seguridad, tales como: CVE-id asociado, detalle de la vulnerabilidad, recomendación para mitigación, entre otros.

Metasploit

Es un framework de explotación de vulnerabilidades de seguridad, es utilizado para el desarrollo y ejecución de exploits y payloads. Metasploit está escrito en el lenguaje de programación Ruby y contiene una suite de herramientas que permiten realizar pruebas sobre vulnerabilidades, enumeración de redes, ejecución de ataques, evasión de controles de seguridad y evasión de servicios de detección.

Existen distintas ediciones de Metasploit, sin embargo, para el proyecto se utilizó la versión gratuita, que se encuentra instalada en la suite de Kali Linux (véase Figura 2.11).

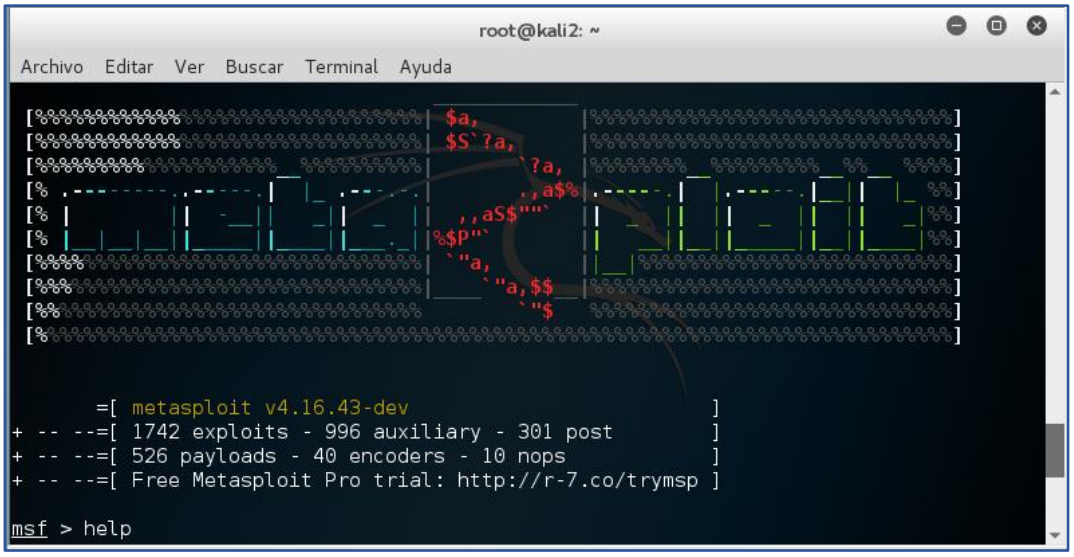


Figura 12 metasploit

SQLmap

Es una herramienta desarrollada en Python y de código abierto, que permite la automatización de procesos de detección y explotación de vulnerabilidades del tipo de inyección de comandos SQL en aplicaciones web (véase Figura 2.12). Esta herramienta cuenta con funciones de detección de versión de servidores de datos, enumeración de usuarios y roles, extracción de datos, ejecución de comandos de sistema, evasión de sistemas de detección y firewalls de aplicación, entre otros.

SQLmap interactúa con los parámetros que se envían durante una petición Web, ya sea del tipo POST o GET, para detectar errores de filtrado en entradas de cadenas e identificar si el sitio web analizado es vulnerable a inyección de comandos de sql.

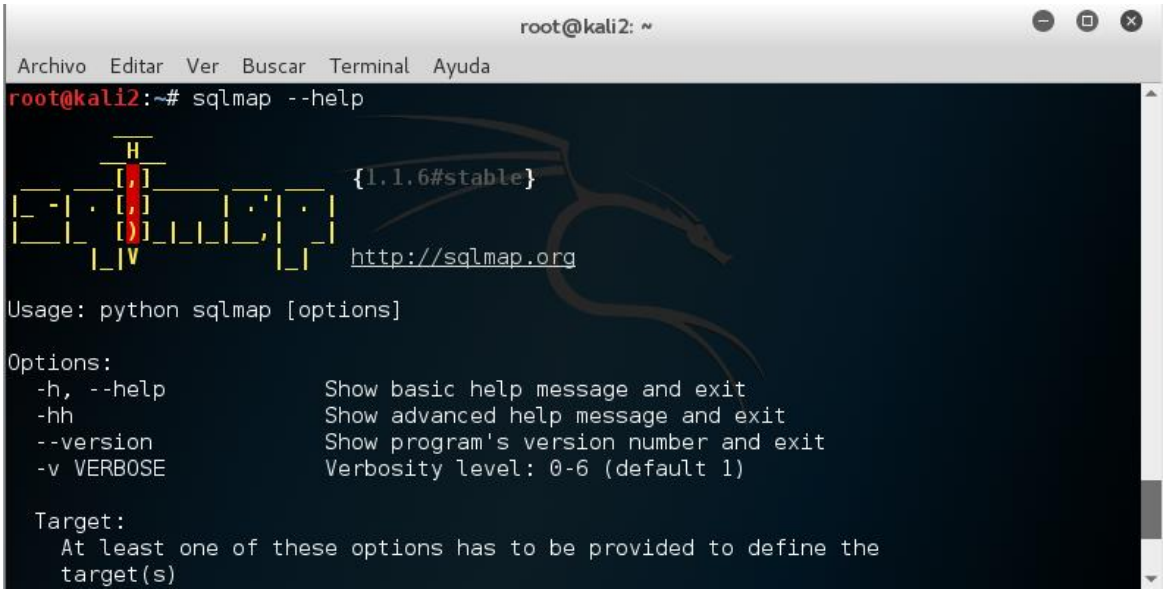


Figura 13.12 Sqlmap

2.5. Servicios Críticos

Uno de los aspectos que se deben considerar durante la ejecución del servicio de pruebas de penetración son los servicios críticos. Estos servicios son un proceso primordial para la compañía a evaluar, por lo que una afectación en dichos servicios podría representar la interrupción de la operación, pérdidas monetarias y hasta el desencadenamiento de situaciones peligrosas. A continuación, describiré algunos de estos servicios.

Active Directory

Es un servicio de directorio de estructura jerárquica, implementado por Microsoft y que permite simplificar la gestión centralizada de los objetos en una red, tales como: usuarios, grupos de usuarios, equipos, políticas de seguridad, entre otros. El servicio de Active Directory se basa en los protocolos LDAP, Kerberos, DNS, DHCP, entre otros.

Para lograr una gestión simplificada, Active Directory se base en un dominio, que es el conjunto de usuarios, equipos, grupos y recursos que se encuentran dentro de una misma base de datos jerárquica. La base de datos de un dominio se almacena en un servidor llamado Controlador de Dominio y, dependiendo de la arquitectura y necesidades del negocio, pueden desplegarse más de un controlador (Véase figura 2.13).

Entre las ventajas de la implementación de un servicio de Active Directory se mencionan las siguientes:

- ✓ Permite tener un control de acceso de los usuarios pertenecientes al dominio, a través de la gestión de permisos, políticas de credenciales, entre otros.
- ✓ Permite la aplicación de políticas para el control de los objetos y recursos de pertenecientes a un dominio, tales como políticas de contraseñas, políticas de software, entre otros.
- ✓ Permite la creación de unidades organizacionales para facilitar la administración de los objetos de dominio.
- ✓ Permite la replicación de la base de datos entre los Controladores de Dominio que formen parte de la infraestructura de Active Directory.
- ✓ Permite la implementación y gestión de servicios, tales como DHCP, DNS, IIS, entre otros.

Debido a que este servicio está diseñado para tener un control sobre de todos los objetos y servicios pertenecientes a un dominio, es considerado como un punto clave en el proceso de auditoría de seguridad. El equipo de consultores realiza pruebas para la detección de brechas de seguridad que permitan a una amenaza escalar privilegios de usuario Administrador de dominio.

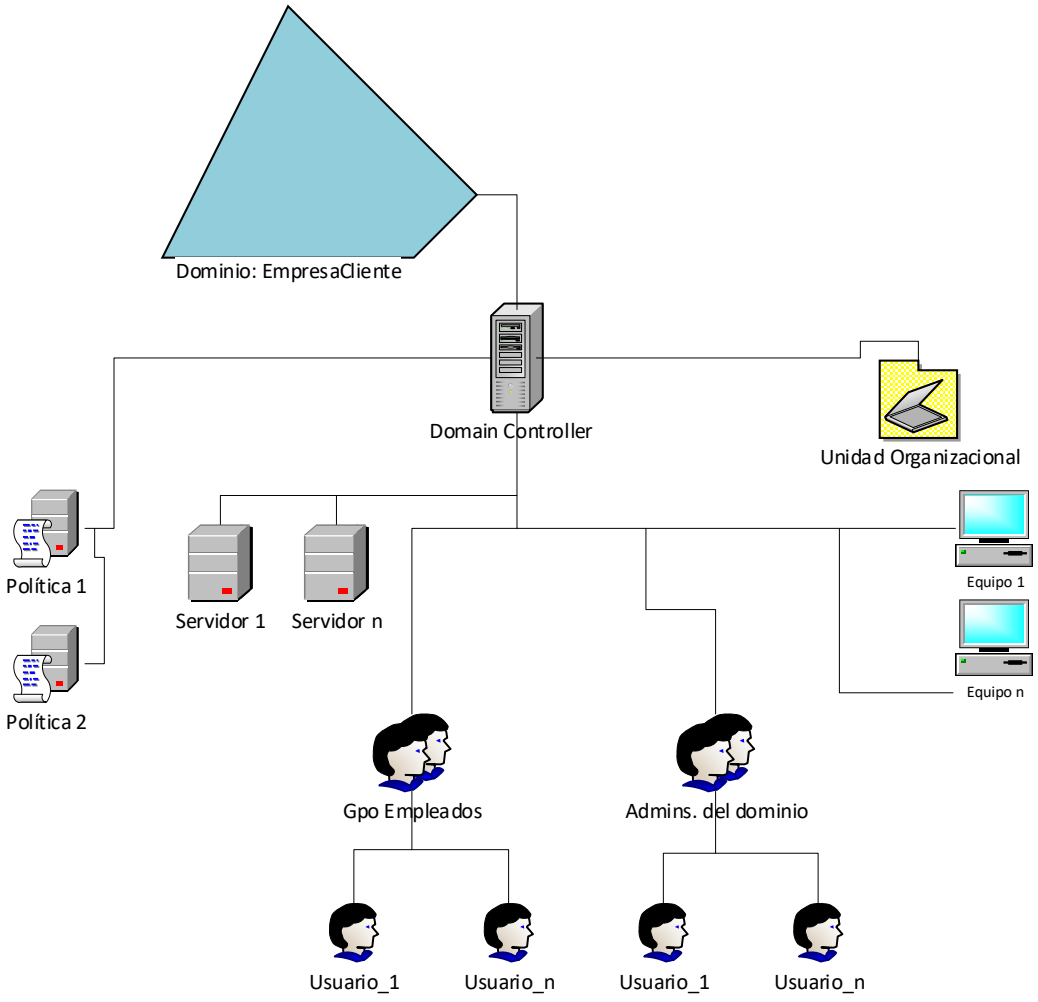
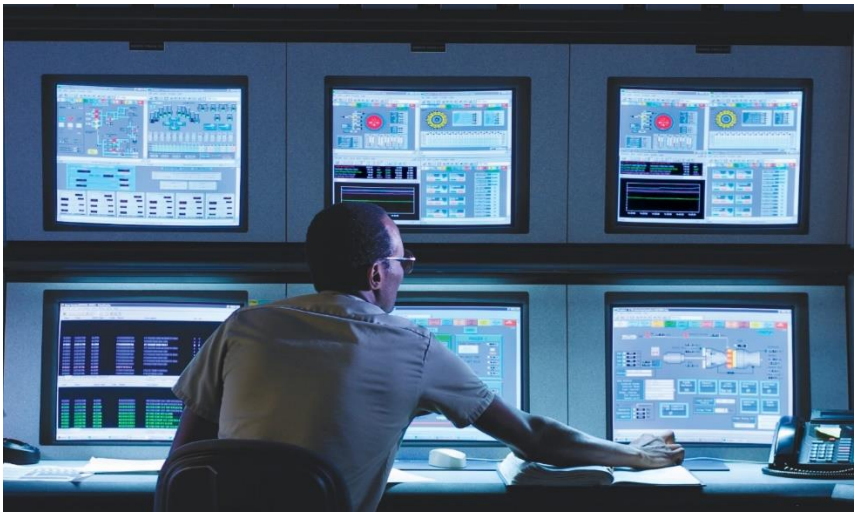


Figura 14.13 Arquitectura de Active Directory

Sistemas SCADA

Los sistemas SCADA o Sistemas de Supervisión, Control y Adquisición de Datos son aplicaciones utilizadas pata el control y supervisión de procesos industriales en infraestructuras críticas (véase Figura 2.14). Los sistemas SCADA utilizan sensores para la recolección de datos en tiempo real, sobre los parámetros de rendimiento y estabilidad a manera de detectar si los valores del proceso industrial están dentro de los niveles de tolerancia.

Debido a la criticidad de los procesos que supervisan y controlan, los sistemas SCADA son considerados como sistemas críticos ya que cualquier incidente, alteración o error podría ocasionar desde daños importantes a la infraestructura industrial, perdidas monetarias o hasta poner en riesgo a la sociedad y el entorno.



(http://proyesco.com/sistemas-de-control,2018)

Figura 15.14 Ejemplo Sistema SCADA

Capítulo 3. Servicio de Análisis de Vulnerabilidades y Pruebas de Penetración a la Infraestructura Tecnológica de la Empresa Cliente

En este capítulo describiré las actividades que llevé a cabo, junto con el equipo de consultores del área de Seguridad Ofensiva de WHC, durante el servicio de pruebas de seguridad a activos tecnológicos de una destacada compañía líder en el desarrollo de la agroindustria mexicana.

3.1. Antecedentes

Justificación del Proyecto

Como lo mencioné en la Introducción, en la actualidad todas las empresas se apoyan en el uso de las tecnologías y los sistemas informáticos para la automatización y gestión de cada uno de los recursos que componen los distintos procesos operacionales. En muchos de los casos y dependiendo del giro, las empresas cuentan con infraestructuras críticas, encargadas de suministrar servicios esenciales para el funcionamiento de la economía y de la sociedad. Una afectación al servicio de estas infraestructuras críticas podría desembocar en grandes pérdidas monetarias, retrasos en la entrega de los servicios y sanciones por incumplimiento de contratos o por entidades regulatorias.

Por tal motivo, una empresa líder a nivel nacional, en el ramo de los alimentos, que a partir de ahora haré referencia como *la Empresa Cliente*, solicitó que se realizara el proyecto: *Servicio de análisis de vulnerabilidades y pruebas de penetración*, con el objetivo de encontrar brechas de seguridad, relacionadas a su infraestructura tecnológica, que deban ser atendidas para reducir el riesgo asociado.

La Empresa Cliente

La Empresa Cliente fue fundada en la década de los 80’s y actualmente es una de las principales productoras y distribuidoras de carnes frías, lácteos, carnes rojas y otros productos cárnicos, contando con cobertura nacional e internacional. La compañía cuenta con un complejo industrial en el estado de Chihuahua, además de poseer una red nacional de centros de distribución que le permite tener presencia en los 32 estados de la República Mexicana.

El éxito de esta compañía le ha permitido generar más de 10,000 empleos en todo el país y cotizar en la Bolsa Mexicana de Valores Debido al crecimiento industrial que ha tenido, desde su fundación y hasta el día de hoy, la compañía busca de manera continua el mejoramiento de sus procesos, con el objetivo de mantener las más altas de normas de calidad en cada uno de los productos que comercializan.

Para lograr lo anterior, la Empresa Cliente se ha apoyado en la implementación de la tecnología para la automatización de procesos industriales críticos, como el procesamiento de carnes y otros alimentos, centro de empaque, centro de almacenamiento y centro de distribución, logrando mejorar la productividad en un 60% y reduciendo los costos energéticos en un 30%.

La Empresa Cliente está conformada por tres complejos principales, los cuales residen en un estado al norte de la República Mexicana. (véase Figura 3.1)

- Complejo Industrial: Está conformado por las plantas de corte de carnes, planta de embutidos, planta de productos madurados y la planta de empaquetamiento.
- Centro de Almacenamiento y distribución: Está conformado por grandes bodegas que cuentan con sistema de refrigeración y son operados por una infraestructura automatizada (sistema robótico), que permite mantener un proceso más eficiente de almacenamiento.
- Oficinas centrales: En este complejo residen todos los procesos administrativos de la empresa, tales como: Área de Mercadotecnia, Área de Administración y Contabilidad, Área de Ventas, Área de TI, Contraloría Interna, entre otros.

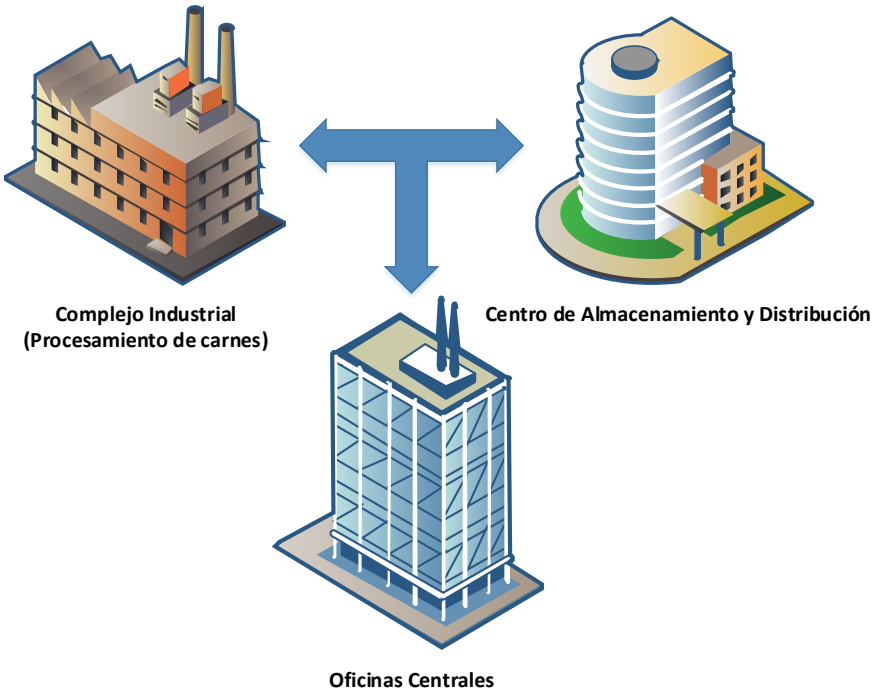


Figura 16 Complejos de la empresa cliente

3.2 Definición del Alcance

Durante la etapa de planeación del proyecto, entre WHC y la Empresa Cliente, se acordó que el servicio estaría compuesto de dos fases principales, la primera es el diagnóstico de seguridad, desde un punto externo y con el enfoque de caja negra, a la infraestructura de TI expuesta. Mientras que la segunda fase es el diagnóstico de seguridad, desde un punto interno y con el enfoque de caja negra, a la infraestructura de TI expuesta.

Esto quiere decir, que en la primera fase se modela como amenaza a un atacante externo, tal como un cracker, y son realizadas desde las oficinas de WHC en la Ciudad de México. En tanto que, para la segunda fase se modela como amenaza a un atacante interno, tal como un empleado descontento o un atacante externo que ha obtenido acceso a la red interna, y son realizadas por el equipo de consultores desde la red interna en las oficinas centrales de la Empresa Cliente, localizadas en un estado al norte del país.

En ambas fases el alcance de las pruebas será un enfoque muestral, es decir, serán contemplados dentro de las pruebas técnicas los activos que puedan ser identificados por parte del equipo de consultores y que pertenezcan a la infraestructura de la Empresa Cliente.

En la siguiente tabla (Tabla 3.1) se muestran los criterios de aceptación del servicio, acordados por parte de WHC y la Empresa Cliente para la ejecución del servicio de auditoría de seguridad.

Se estableció que cada una de las fases de pruebas técnicas tendría una duración de 10 días hábiles y se tendría un periodo de 5 días hábiles para la generación de los reportes ejecutivo y técnico, por parte del equipo de consultores.

Tabla 1.1 Requerimientos para la ejecución del servicio

Servicio	Criterio de aceptación	Duración	Horario	No. de recursos	Entregable
Externo Caja Negra	Servicio de Pruebas de Penetración y Análisis de Vulnerabilidades desde internet a cualquier componente de la infraestructura de la Empresa Cliente sin previo conocimiento de la arquitectura e infraestructura TI de la Compañía.	2 Semanas	Horario de WHC 10:00 – 17:00 hrs	1 Líder 2 Consultores	Reporte Técnico de Fase Externa
Interno Caja Negra	Servicio de Pruebas de Penetración y Análisis de Vulnerabilidades desde la intranet a cualquier componente de la infraestructura de la Empresa Cliente sin previo conocimiento de la arquitectura e infraestructura TI de la Compañía.	2 Semanas	Horario de Cliente 9:00 – 17:00 hrs	1 Líder 2 Consultores	Reporte Técnico de Fase Interna

También se acordó que sólo el área de contraloría, de la Empresa Cliente, sería informada de la realización de las pruebas de seguridad, esto es con el motivo de evitar que el personal encargado de los activos tecnológicos evaluados realice cambios que alteren los resultados parciales de las pruebas.

3.3 Plan de trabajo

Una vez acordados los criterios de aceptación, el equipo de Administración de Proyectos de WHC generó el plan de trabajo y calendarizó cada una de las actividades que forman parte del servicio, respetando los tiempos que se acordaron para cada fase.

A continuación, se muestran las fechas establecidas para cada fase y actividad (véase Tabla 3.2).

Tabla 2.2 Calendario de Actividades

	Ta: Mc	Nombre de tarea	Dural	Start	Finish	Predecessors
1		**Servicio de análisis de vulnerabilidades y pruebas de penetración**	**44 days**	**Mon 07-08-17**	**Thu 05-10-17**	
2		**Pruebas Externas - Caja Negra**	**10 days**	**Mon 07-08-17**	**Fri 18-08-17**	
3		Descubrimiento	2 days	Mon 07-08-17	Tue 08-08-17	
4		Escaneos de servicios y vulnerabilidades	3 days	Wed 09-08-17	Fri 11-08-17	3
5		Explotación de vulnerabilidades	3 days	Mon 14-08-17	Wed 16-08-17	4
6		Post Explotación	2 days	Thu 17-08-17	Fri 18-08-17	5
7		**Pruebas Internas - Caja Negra**	**10 days**	**Fri 01-09-17**	**Thu 14-09-17**	**2**
8		Descubrimiento	2 days	Fri 01-09-17	Mon 04-09-17	6
9		Escaneos de servicios y vulnerabilidades	3 days	Tue 05-09-17	Thu 07-09-17	8
10		Explotación de vulnerabilidades	3 days	Fri 08-09-17	Tue 12-09-17	9
11		Post Explotación	2 days	Wed 13-09-17	Thu 14-09-17	10
12		**Reportes**	**15 days**	**Fri 15-09-17**	**Thu 05-10-17**	**2,7**
13		Generación de Reportes: Ejecutivo y Técnico	5 days	Fri 15-09-17	Thu 21-09-17	11
14		Entrega de reportes: Ejecutivo y Técnico	1 day	Fri 22-09-17	Fri 22-09-17	13
15		Validación por Empresa Cliente	5 days	Mon 25-09-17	Fri 29-09-17	14
16		Atención de comentarios	3 days	Mon 02-10-17	Wed 04-10-17	15
17		Liberación de entregables finales	1 day	Thu 05-10-17	Thu 05-10-17	16

Al finalizar la calendarización de las actividades, se obtuvo que el proyecto tendría una duración de 44 días hábiles, arrancando el lunes 07 de agosto con la primera fase de las pruebas técnicas y terminando el Jueves 05 de Octubre con la liberación de los entregables finales.

En la siguiente imagen (Figura 3.2) se muestra el diagrama de Gantt resultante del plan de trabajo:

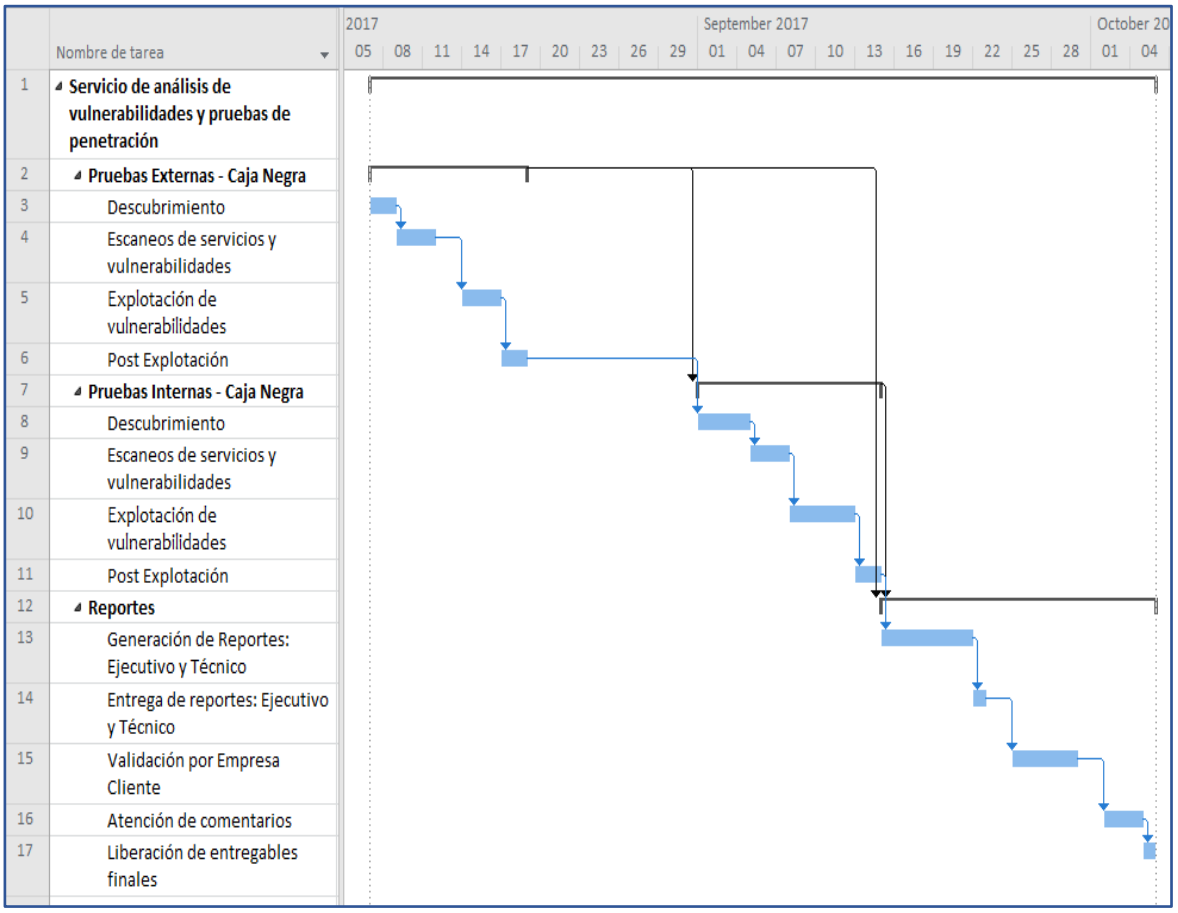


Figura 17 Diagrama de Gantt del Proyecto

3.4 Pruebas Externas

Las pruebas externas fueron realizadas por el equipo compuesto por un líder de equipo y dos consultores de seguridad. Yo desempeñé el rol de líder de equipo, sin embargo, también colaboré con actividades de consultor de seguridad con el objetivo de validar la ejecución cada tarea.

Como líder del equipo de consultores, consideré que las pruebas técnicas se enfocarían en evaluar los principales servicios de seguridad de los activos y sistemas evaluados. Los servicios de seguridad contemplados son:

- Confidencialidad: Servicio de seguridad de la información que garantiza que la información sólo debe ser accesible o revelada a individuos, entidades o procesos autorizados.
- Integridad: Servicio de seguridad de la información que garantiza que la información debe mantener su plenitud y exactitud, es decir, no debe sufrir modificaciones no autorizadas.
- Disponibilidad: Servicio de seguridad de la información que garantiza que la información debe estar accesible cuando un individuo, entidad o proceso autorizado lo requiera.

Siguiendo la metodología planteada, el equipo de consultores comenzó con las pruebas técnicas correspondientes a la etapa de *Reconocimiento*, logrando la identificación de activos expuestos a Internet (véase Tabla 3.3).

Tabla 3.3 Pruebas Externas - Reconocimiento

Activos	Cantidad
Dominios principales asociados a la empresa cliente	6
Servidores, dispositivos de red y seguridad	55
Aplicaciones Web	24
Segmentos de red asociados	3

En la etapa de *Escaneo* se realizó la identificación puertos abiertos y servicios que se ejecutan. Estos datos obtenidos fueron utilizados para realizar el escaneo de vulnerabilidades en los activos identificados, así como la investigación de los distintos vectores de explotación asociados a cada hallazgo. Los hallazgos resultantes se contabilizaron y se agruparon por categorías (véase Tabla 3.4):

Tabla 4.4 Pruebas Externas - Escaneo

ID	Hallazgos	Cantidad
1	Vulnerabilidades de SQL Injection	1
2	Vulnerabilidades de XSS	2
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	4
4	Sistemas Operativos sin Soporte	6

Partiendo de la previa identificación de vulnerabilidades y la investigación de los posibles vectores, se comenzó con la etapa de *Explotación*. Cada posible mecanismo de explotación identificado y que calificara como no disruptivo (que no causa afectaciones al activo evaluado) fue ejecutado con las respectivas medidas de seguridad.

En el caso del hallazgo *Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes* se identificó la existencia de un exploit que podría causar un ataque de denegación de servicios (DoS) por lo que esta prueba fue omitida, sin embargo, se incluyó en reporte el hallazgo de seguridad y el posible impacto en caso de su explotación.

Por otro lado, las *Vulnerabilidades de XSS* permiten a un atacante externo aprovecharse del aplicativo web afectado para desplegar ventanas emergentes de alerta (de JavaScript) en el navegador de la víctima, por lo que esta vulnerabilidad permitiría realizar campañas de phishing o redirecciones a sitios web maliciosos. A continuación, se muestran los resultados obtenidos durante la etapa de *Explotación* en las pruebas externas (véase Tabla 3.5).

Tabla 5.5 Pruebas Externas - Explotación

ID	Hallazgos	Posibles mecanismos de explotación	Explotación exitosa	Activos vulnerados
1	Vulnerabilidades de SQL Injection	1	Si	1/1
2	Vulnerabilidades de XSS	2	Si	2/2
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	2	Si	1/4
4	Sistemas Operativos sin Soporte	N/A	N/A	N/A

La etapa final, *Post-Explotación*, comenzó con la investigación sobre qué acciones se podrían llevar a cabo después de lograr aprovecharse de las vulnerabilidades previamente explotadas. Debido al alcance y tiempos establecidos, se identificó que los hallazgos de *SQL Injection* y *Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes* permiten escalar los ataques.

En el caso de la vulnerabilidad de *SQL Injection*, el equipo de consultores fue capaz de evadir el control de autenticación de la página web, sustraer registros de las bases de datos almacenadas en el servidor, entre otras acciones. Por otro lado, uno de los hallazgos pertenecientes a la categoría de *Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes* permitió al equipo de consultores realizar las siguientes actividades: ejecución de comandos de sistema en el servidor afectado, recuperación de credenciales de los usuarios pertenecientes al servidor afectado, entre otras.

En la siguiente tabla (Tabla 3.6) se muestran los resultados obtenidos al finalizar la ejecución de las técnicas durante la etapa de *Post -Explotación*:

Tabla 6.6 Pruebas Externas – Post Explotación

Hallazgos	Acciones de Post-Explotación
Vulnerabilidades de SQL Injection	• Evasión del control de autenticación. • Extracción de registros en las bases de datos. • Creación de usuario en el servicio de base de datos.
Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	• Ejecución de comandos a nivel de sistema operativo. • Creación de usuario con privilegios del grupo de Administración en el servidor. • Recuperación de contraseñas de otros usuarios pertenecientes al servidor. • Instalación de backdoors a nivel local (Equipo).

En el caso de la vulnerabilidad de XSS no fue necesario realizar una campaña de phishing para demostrar los riesgos asociados, por lo que bastó con la demostración de la explotación del hallazgo de seguridad.

Al finalizar las pruebas técnicas externas, se tuvo una reunión con la Empresa Cliente para dar seguimiento y mostrar los resultados finales de la fase externa.

3.5 Pruebas Internas

Durante la etapa interna, el equipo de consultores viajó a un estado al norte de la república para poder realizar las pruebas técnicas desde la red Interna, en las oficinas centrales de la Empresa Cliente. Ya establecidos en las oficinas centrales, se nos proporcionó un lugar de en el área de administración.

El equipo de consultores que viajó a las oficinas centrales estuvo compuesto por un líder de equipo y dos consultores de seguridad. Para estas pruebas, también desempeñé el rol de líder de equipo y también colaboré con actividades de consultor de seguridad con el objetivo de validar la ejecución segura de cada herramienta y técnica.

Como líder del equipo de consultores, consideré que las pruebas técnicas se enfocarían en evaluar los principales servicios de seguridad de los activos y sistemas evaluados. De igual manera al análisis externo, los servicios de seguridad contemplados en la etapa interna son la confidencialidad, integridad y disponibilidad.

Siguiendo la metodología planteada, el equipo de consultores comenzó con las pruebas técnicas correspondientes a la etapa de *Reconocimiento*, en donde se buscó la identificación de los distintos activos pertenecientes a la infraestructura interna, tales como: segmentos de red interna, servidores, equipos de cómputo, dispositivos de red, entre otros. A continuación, se muestran los resultados obtenidos al finalizar la etapa de Reconocimiento (véase Tabla 3.7).

Tabla 7.7 Pruebas Internas - Reconocimiento

Activos	Cantidad
Segmentos de red interna	22
Dispositivos de red y seguridad	15
Servidores	95
Equipos de Cómputo	980
Dispositivos VoIP	200
Dispositivos de CCTV	14
Aplicaciones Web	25

Cabe resaltar que las pruebas internas fueran realizadas con la misma visibilidad y privilegios que tendría un usuario común de la red interna, esto fue con el objetivo de estimar que tanta visibilidad tendría un atacante hacia los demás elementos de la infraestructura interna. En este caso, el equipo de consultores fue capaz de mantener conectividad con segmentos de red de producción industrial, servidores de TI, desarrollo y operación.

La etapa de *Escaneo* comenzó con la identificación de los puertos abiertos y servicios que se ejecutan en las distintas redes, a través de la ejecución de herramientas y técnicas manuales. Posteriormente se realizó la identificación de vulnerabilidades asociadas a servicios web, sistemas operativos, protocolos, servicios y procesos de autenticación. Al finalizar esta etapa se contabilizaron y agruparon las vulnerabilidades por categoría. (véase Tabla 3.8).

Tabla 8.8 Pruebas Internas - Escaneo

ID	Hallazgos	Cantidad
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	11
2	Credenciales por defecto en dispositivos de CCTV	1
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	4
4	Contraseñas débiles en dispositivos de red.	10
5	Sistemas Operativos sin Soporte	7

Cabe mencionar que, durante la ejecución de herramientas de escaneo, el equipo de consultores mantuvo las medidas necesarias para no causar una degradación del servicio de red, afectaciones a los servidores críticos (Controladores de dominio, servidores de bases de datos, entre otros) y pasar desapercibidos, tal como lo haría un atacante que busca no ser descubierto.

Adicionalmente, se mantuvo un cuidado especial durante los escaneos y pruebas técnicas realizadas al segmento de producción, con el motivo de no afectar de ninguna manera a los sistemas de control industrial (SCADA). Algunas de estas medidas tomadas fueron: ejecución de pruebas y herramientas en horarios no críticos, configuración de herramientas para reducir la cantidad de pruebas simultaneas, entre otros.

Posterior a la identificación de las vulnerabilidades, el equipo de consultores realizó la investigación sobre los posibles vectores de explotación existentes para cada hallazgo, así como las consecuencias de asociadas a su ejecución para descartar los exploits que pudiesen causar una afectación mayor, tal como denegación de servicios (DoS), eliminación de datos y usuarios, alteración al sistema operativo, cambio de configuraciones en servicios críticos, ente otros. En la siguiente tabla (Tabla 3.9) se muestran los resultados obtenidos durante la etapa de Explotación.

Tabla 9.9 Pruebas Internas - Explotación

ID	Hallazgos	Posibles mecanismos de explotación	Explotación exitosa	Activos vulnerados
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	2	Si	7/11
2	Credenciales por defecto en dispositivos de CCTV	1	Si	1/1
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	2	Si	1/4
4	Contraseñas débiles en dispositivos de red.	1	Si	10/10
5	Sistemas Operativos sin Soporte	N/A	N/A	N/A

Siguiendo la metodología, en la etapa final de *Post-Explotación* se identificó que los hallazgos de *Contraseñas débiles en dispositivos de red* permiten acceder y tener el control total de la infraestructura de red, desde apagar el servicio hasta alterar las configuraciones de las distintas redes. Por tal motivo, sólo se realizaron algunas acciones que no representaran un riesgo adicional o que causaran un comportamiento no deseado en el servicio.

En el caso de los hallazgos pertenecientes a las categorías *Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows* y *Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes*, el equipo de consultores llevó al límite las acciones que un atacante podría hacer después de la intrusión en servidores críticos. Algunas de las acciones que se realizaron fueron desde la búsqueda de información almacenada en los servidores, hasta el compromiso de la cuenta del usuario administrador del dominio (Active Directory) y el acceso a la infraestructura industrial, a través de la consola de administración de los sistemas SCADA.

Por otro lado, se identificó que el hallazgo perteneciente a la categoría de *Contraseñas débiles en dispositivos de red* permite acceder y tener el control total de la infraestructura de CCTV, desde apagar el servicio hasta alterar las configuraciones y posiciones de las cámaras de seguridad. Por tal motivo, sólo se realizaron algunas acciones que no representaran un riesgo adicional o que causaran un comportamiento no deseado en el servicio.

A continuación, se muestran las acciones que se pudieron realizar después de la explotación de las vulnerabilidades (véase Tabla 3.10).

Tabla 10.10 Pruebas Internas – Post Explotación

Hallazgos	Acciones de Post-Explotación
Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	• Ejecución de comandos a nivel de sistema operativo. • Creación de usuario con privilegios del grupo de Administración en los equipos y servidores afectados. • Recuperación de contraseñas de otros usuarios pertenecientes al servidor y al dominio de Active Directory. • Compromiso de la cuenta del usuario administrador del dominio (Active Directory). • Acceso a los Controladores de Dominio. • Acceso a todos los equipos pertenecientes al dominio (Active Directory) de la Empresa Cliente. • Instalación de Backdoor a nivel de dominio (Active Directory). • Recuperación de los hashes (contraseñas cifradas) de todos los usuarios pertenecientes al dominio (Active Directory) de la Empresa Cliente.

	• Acceso a la consola de administración del sistema de Supervisión, Control y Adquisición de Datos de procesos industriales (SCADA).
Credenciales por defecto en dispositivos de CCTV	• Acceso a la consola de administración del sistema de monitoreo de cámaras de video vigilancia. • Se puede deshabilitar el servicio proporcionado por cada cámara.
Contraseñas débiles en dispositivos de red.	• Acceso al dispositivo de red. • Recuperación de los parámetros de configuración de la infraestructura: vlans, credenciales de usuarios. • Recuperación de las contraseñas de usuarios del dispositivo.
Falta de actualizaciones de seguridad en servidores web y componentes	• Ejecución de comandos a nivel de sistema operativo. • Creación de usuario con privilegios del grupo de Administración en los equipos y servidores afectados. • Recuperación de contraseñas de otros usuarios pertenecientes al servidor y al dominio de Active Directory. • Compromiso de la cuenta del usuario administrador del dominio (Active Directory). • Acceso a los Controladores de Dominio. • Acceso a todos los equipos pertenecientes al dominio (Active Directory) de la Empresa Cliente. • Instalación de Backdoor a nivel de dominio (Active Directory). • Recuperación de los hashes (contraseñas cifradas) de todos los usuarios pertenecientes al dominio (Active Directory) de la Empresa Cliente.

Al finalizar la ejecución de las pruebas de seguridad internas, el equipo de consultores se reunió con el equipo de contraloría de la Empresa Cliente para la presentación de los hallazgos de seguridad. Durante la reunión se hizo el énfasis en la segregación de redes, debido a que el equipo de consultores fue capaz de mantener conectividad con el segmento de producción industrial, realizar ataques a equipos que residen en esa red y lograr el acceso al sistema SCADA.

3.6 Resultados

En la Figura 3.3 se muestran los hallazgos de seguridad, más relevantes, detectados por el equipo de consultores durante la etapa de pruebas externas, así como los resultados obtenidos a través de la explotación de las vulnerabilidades.

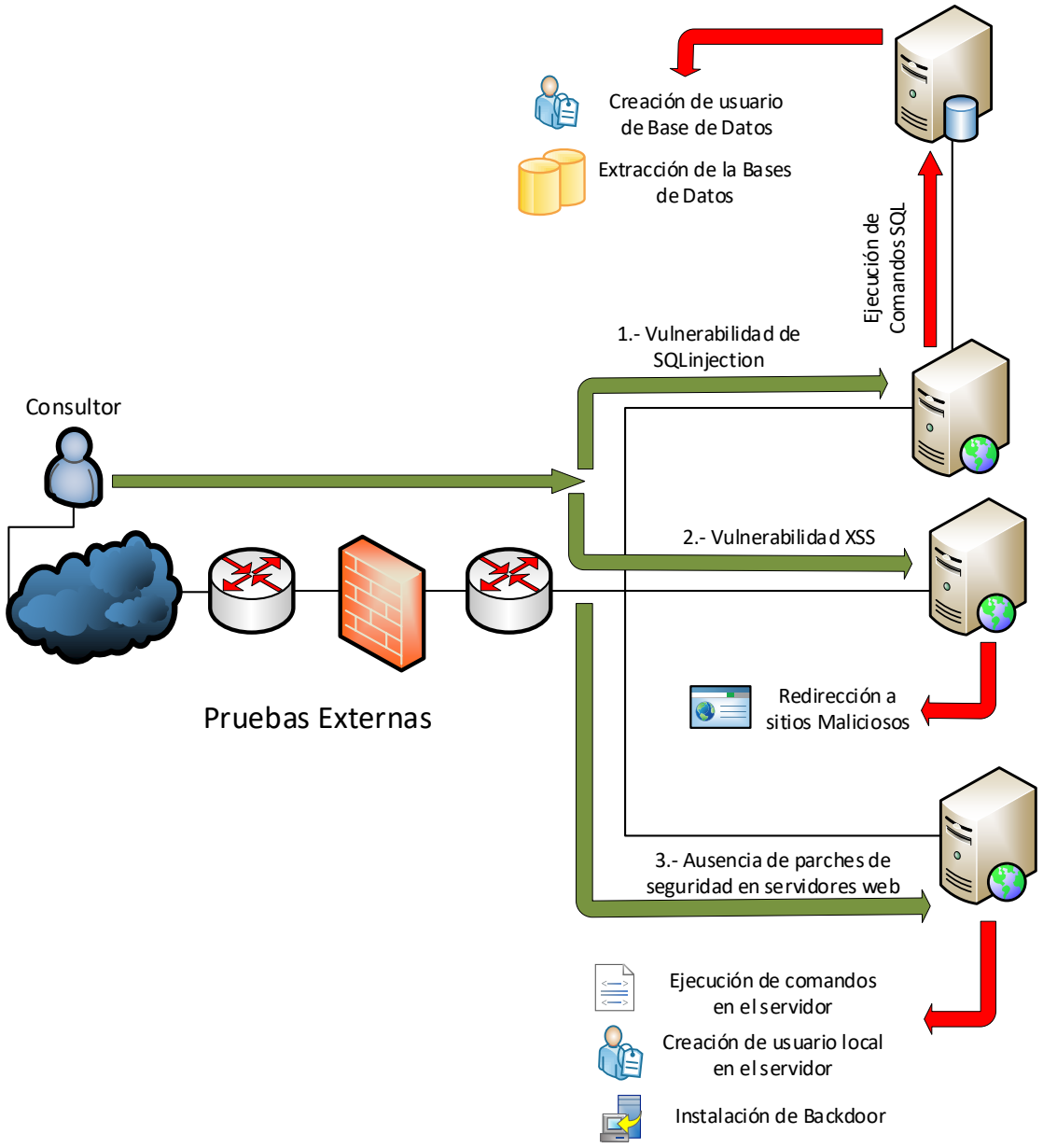


Figura 18 Resultados de Pruebas Externas

Derivado de los resultados obtenidos de la explotación de los hallazgos de seguridad externos, se identificaron los servicios de seguridad afectados (véase Tabla 3.11).

Tabla 11.11 Servicios de seguridad afectados - Externo

ID	Hallazgo de Seguridad	Resultado de Explotación	Servicios afectado
1	Vulnerabilidades de SQL Injection	➢ Creación de usuario de base de datos. ➢ Extracción de información almacenada en las Bases de Datos. ➢ Posible alteración del contenido de las Bases de Datos.	Confidencialidad Integridad Disponibilidad
2	Vulnerabilidades de XSS	➢ Posible modificación del contenido del sitio web. ➢ Re direccionamiento a sitios web maliciosos o fraudulentos (Campañas de phishing).	Integridad Disponibilidad
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	➢ Ejecución de comandos en el servidor. ➢ Creación de usuario local en el servidor. ➢ Instalación de backdoors.	Confidencialidad Integridad Disponibilidad

En el siguiente diagrama se muestran los hallazgos de seguridad, más relevantes, detectados durante la ejecución de las pruebas internas y los resultados de la explotación de dichas vulnerabilidades:

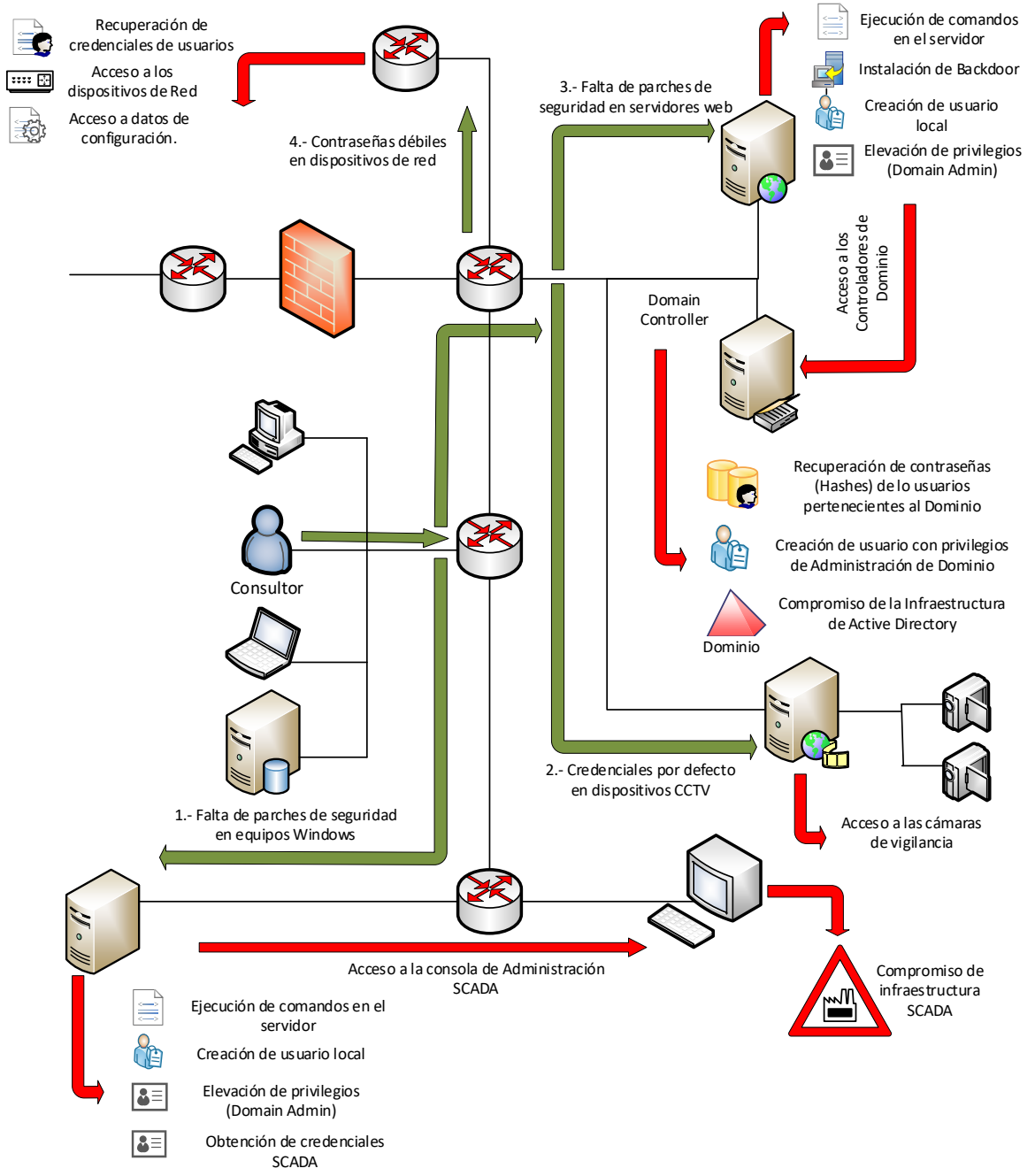


Figura 19 Resultados de Pruebas Internas

A través del análisis de los resultados obtenidos durante la explotación de los hallazgos de seguridad internos, se identificaron los servicios de seguridad afectados (véase Tabla 3.12).

Tabla 12.12 Servicios de seguridad afectados - Interno

ID	Hallazgo de Seguridad	Resultado de Explotación	Servicios afectado
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	➢ Ejecución de comandos en el servidor. ➢ Creación de usuario local. ➢ Compromiso de la infraestructura de Active Directory ➢ Compromiso del servicio SCADA.	Confidencialidad Integridad Disponibilidad
2	Credenciales por defecto en dispositivos de CCTV	➢ Acceso al servicio de video vigilancia.	Confidencialidad Integridad Disponibilidad
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	➢ Ejecución de comandos en el servidor. ➢ Creación de usuario local. ➢ Compromiso de la infraestructura de Active Directory	Confidencialidad Integridad Disponibilidad
4	Contraseñas débiles en dispositivos de red.	➢ Recuperación de credenciales de usuarios de los dispositivos. ➢ Acceso a los dispositivos de red. ➢ Acceso a los datos de configuración.	Confidencialidad Integridad Disponibilidad

Generación de Reportes

Una vez finalizadas las pruebas externas e internas, el equipo de consultores regresó a las oficinas de WHC para comenzar con el análisis de los resultados, el cálculo de la severidad de los hallazgos y la elaboración de los reportes. Dando cumplimiento a los requerimientos del proyecto, el equipo de consultores generó dos tipos de reportes:

- Reporte Técnico: Documento dirigido al área técnica responsable de los activos afectados, contiene una matriz que concentra información detallada sobre los hallazgos de seguridad, los activos afectados, el escenario de riesgo, severidad del hallazgo y las respectivas acciones correctivas y de mitigación sugeridas. También incluye evidencias de la explotación de las vulnerabilidades, tales como: imágenes de la ejecución de las herramientas de escaneo, captura de pantalla de alertas y errores generados en páginas web, captura de pantalla de escritorio remoto en servidores y equipos afectados, entre otros.

- Reporte Ejecutivo: Documento dirigido a los gerentes responsables de los procesos afectados, el departamento de contraloría y la junta directiva, contiene una matriz que concentra información sobre los hallazgos de seguridad, los activos afectados, el escenario de riesgo, severidad del hallazgo y las respectivas acciones correctivas y de mitigación sugeridas. Este documento se escribe en un lenguaje no técnico, de manera que sea de fácil comprensión para el público al que va dirigido. También incluye algunas evidencias de las actividades resultantes de la explotación de las vulnerabilidades, tales como: captura de pantalla de generadas en páginas web, captura de pantalla de escritorio remoto en servidores y equipos críticos, entre otros.

Secciones de la Matriz de Hallazgos

En la siguiente tabla (Tabla 3.13) se describe cada una de las secciones que compone la matriz de hallazgos, incluida en cada uno de los reportes generados:

Tabla 13.13 Secciones de la Matriz de Hallazgos

Campo	Descripción
Hallazgo	Se describe la vulnerabilidad, debilidad o anomalía identificada.
Dispositivos afectados	En esta sección se detallan los datos necesarios para la identificación del activo afectado. Se incluye el nombre (hostname) del dispositivo afectado o el nombre del aplicativo al cual está asociada la vulnerabilidad. También se incluye la dirección IP del dispositivo y la URL del aplicativo.
Escenarios de Riesgo	En esta sección se describen los escenarios de riesgo que podrían materializarse a partir de la explotación de la vulnerabilidad en el activo. Este campo también contiene una breve explicación del posible vector de explotación.
Impacto	En esta sección se realiza una valoración sobre el impacto que tendría la explotación de la vulnerabilidad y dependiendo del daño que pudiese causar, se le asigna un valor entre 1 y 5. WHC cuenta con una metodología propia para la asignación del nivel de Impacto y se describe en la tabla “Descripción de los niveles de impacto”.
Probabilidad de ocurrencia	En esta sección se calcula la probabilidad de ocurrencia de la explotación de la vulnerabilidad. Para esto se evalúan los requerimientos necesarios para la explotación exitosa, tales como: las habilidades necesarias del atacante, la existencia de herramientas/exploits públicos, condiciones especiales, entre otros. WHC cuenta con una metodología propia para la asignación del nivel de Probabilidad y se describe en la tabla “Descripción de niveles de probabilidad”.
Severidad de la vulnerabilidad (Riesgo)	En esta sección se realiza una valoración sobre la severidad de la vulnerabilidad. Para obtener este valor se utiliza la siguiente formula: R=IP; en dónde R es el riesgo, I es el valor del impacto y P es el valor de la probabilidad de ocurrencia. Entre más alto sea el valor del riesgo, mayor debe de ser la urgencia y prioridad de atención de la vulnerabilidad.
Acciones correctivas y de mitigación sugeridas	En esta sección se presentan las acciones correctivas sugeridas y en su caso, algunos controles compensatorios que pueden ayudar a mitigar su posible explotación.

Metodología de análisis de riesgo

Como lo mencioné en la tabla anterior, WHC posee una metodología y escala propia para el cálculo y clasificación del riesgo de cada hallazgo de seguridad. A continuación, se describen los niveles de Impacto, utilizados por WHC para el cálculo de la severidad de la vulnerabilidad (véase Tabla 3.14).

Tabla 14.14 Descripción de los niveles de Impacto

Nivel	Descripción de Impacto
1	El abuso del hallazgo de seguridad puede provocar una pérdida o daño insignificante o nulo.
2	El abuso del hallazgo de seguridad puede provocar una pérdida o daño pequeño.
3	El abuso del hallazgo de seguridad puede provocar una pérdida o daño serio y el proceso de negocio puede verse afectado de forma negativa.
4	El abuso del hallazgo de seguridad puede provocar una pérdida o daño muy serio a la institución y el proceso de negocio puede fallar.
5	El abuso del hallazgo de seguridad puede provocar una pérdida monetaria, no cumplimiento regulatorio grave, daño a algún individuo o a la organización en reputación, credibilidad, afectación de marca, privacidad y puede provocar la falla del proceso de negocio.

En la siguiente tabla (Tabla 3.15), se describen los niveles de Probabilidad de ocurrencia, utilizados por WHC para el cálculo de la severidad de la vulnerabilidad:

Tabla 15.15 Descripción de niveles de probabilidad

Nivel	Descripción de Probabilidad
1	Existe una probabilidad baja de ocurrencia; la vulnerabilidad es difícil de explotarse pues requiere algunas condiciones muy especiales o las habilidades demandadas al atacante son muy altas.
2	Existe una probabilidad media de ocurrencia; la vulnerabilidad es medianamente fácil de explotarse, pues con algunas habilidades del atacante y en ciertas condiciones se podría consumar el ataque.
3	Existe una probabilidad alta de ocurrencia; la vulnerabilidad es muy fácil de explotarse porque existen herramientas automáticas o exploits públicos en la red, por lo que los atacantes pueden disponer de ellos y acceder al servicio vulnerable.

Los rangos y la clasificación de criticidad del riesgo, utilizada por el equipo de consultores de WHC se describen en la Tabla 3.16.

Tabla 16.16 Clasificación de Severidad

Valores	Nivel de Criticidad	Color
12-15	Crítica	
8-11	Alta	
4-7	Media	
1-3	Baja	

Análisis de Riesgo de los hallazgos de seguridad

Para realizar el cálculo del riesgo de los hallazgos detectados durante las pruebas externas e internas, el equipo de consultores estableció los niveles de Probabilidad e Impacto de cada hallazgo.

Hallazgos Externos

En la siguiente tabla (Tabla 3.17) se muestran los criterios analizados para el cálculo del nivel de Probabilidad de Ocurrencia de los hallazgos externos:

Tabla 17.17 Hallazgos Externos – Probabilidades de Ocurrencia

ID	Hallazgo de Seguridad	Criterio	P
1	Vulnerabilidades de SQL Injection	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas, públicas en internet (SQLmap), que permiten abusar de la vulnerabilidad.	3
2	Vulnerabilidades de XSS	Existe una probabilidad alta de ocurrencia, debido a que un atacante no requiere de altas habilidades para explotar las vulnerabilidades.	3

3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas y exploits públicos en internet (Metasploit, ExploitDB) que permiten abusar de la vulnerabilidad.	3
4	Sistemas Operativos sin Soporte	Existe una probabilidad media de ocurrencia. Actualmente no se encontraron vulnerabilidades críticas, ni herramientas o exploits que representen un alto riesgo para los activos afectados. Sin embargo, los sistemas operativos que ya no cuentan con soporte, por parte del proveedor, no contarán con una solución ante el descubrimiento de nuevas vulnerabilidades y la liberación de nuevos exploits.	2

A continuación, se muestran los criterios analizados para la valoración del Impacto, asociado a los hallazgos de seguridad externos (véase Tabla 3.18).

Tabla 18 Hallazgos Externos - Impacto

ID	Hallazgo de Seguridad	Criterio	I
1	Vulnerabilidades de SQL Injection	Un atacante podría explotar esta vulnerabilidad para realizar cualquiera de las siguientes acciones: ➢ Robo de información. ➢ Evasión de controles de autenticación. ➢ Consulta, extracción, modificación o destrucción de datos existentes en el servidor de Base de Datos. Por lo tanto, el abuso del hallazgo de seguridad puede provocar el no cumplimiento regulatorio grave (LFPDPPP), así como una afectación a la imagen y privacidad de la Empresa Cliente, por lo que puede provocar la falla del proceso de negocio.	5
2	Vulnerabilidades de XSS	Un atacante podría aprovecharse de estas vulnerabilidades para realizar las siguientes acciones: ➢ Daño a la imagen pública mediante la alteración o modificación del contenido del sitio web. ➢ Re direccionamiento a sitios web maliciosos o fraudulentos (Campañas de phishing). ➢ Instalación de software malicioso en los equipos de los visitantes del sitio web	3

		Por lo tanto, el abuso del hallazgo de seguridad puede provocar daño serio a la imagen y reputación de la Empresa Cliente, por lo que el proceso de negocio puede verse afectado de forma negativa.	
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	Un atacante podría aprovecharse de esta vulnerabilidad para realizar las siguientes acciones: ➢ Ejecución de código remoto. ➢ Robo de información. ➢ Denegación de servicio. Por lo tanto, el abuso del hallazgo de seguridad puede provocar un daño muy serio a los datos y servicios que dependen del activo afectado, por lo que se podría provocar la falla del proceso de negocio.	5
4	Sistemas Operativos sin Soporte	Actualmente no se encontraron vulnerabilidades críticas, ni herramientas o exploits que representen un alto riesgo para los activos afectados. Sin embargo, los sistemas operativos que ya no cuentan con soporte, por parte del proveedor, no contarán con una solución ante el descubrimiento de nuevas vulnerabilidades y la liberación de nuevos exploits.	4

La siguiente Tabla 3.19 contiene el proceso del cálculo y la clasificación del riesgo correspondiente a los hallazgos externos. Los resultados se muestran a continuación:

Tabla 199 Hallazgos Externos – Cálculo de Riesgos

ID	Hallazgo de Seguridad	P	I	R	Nivel	Color
1	Vulnerabilidades de SQL Injection	3	5	**15**	**Critica**	
2	Vulnerabilidades de XSS	3	3	**9**	**Alta**	
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	3	5	**15**	**Critica**	
4	Sistemas Operativos sin Soporte	2	4	**8**	**Alta**	

Hallazgos Internos

Siguiendo la metodología, se realizó el cálculo del nivel de Probabilidad de Ocurrencia e Impacto de los hallazgos internos, como se muestra en la Tabla 3.20.

Tabla 20 Hallazgos Internos – Probabilidades de Ocurrencia

ID	Hallazgo de Seguridad	Criterio	P
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas y exploits públicos en internet (Metasploit, ExploitDB) que permiten abusar de la vulnerabilidad.	3
2	Credenciales por defecto en dispositivos de CCTV	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas e información que facilita la explotación de la vulnerabilidad, además, un atacante no requiere de altas habilidades para realizar los ataques.	3
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas y exploits públicos en internet (Metasploit, ExploitDB) que permiten abusar de la vulnerabilidad.	3
4	Contraseñas débiles en dispositivos de red.	Existe una probabilidad alta de ocurrencia, debido a que existen herramientas e información que facilita la explotación de la vulnerabilidad, además, un atacante no requiere de altas habilidades para realizar los ataques.	3
5	Sistemas Operativos sin Soporte	Existe una probabilidad media de ocurrencia. Actualmente no se encontraron vulnerabilidades críticas, ni herramientas o exploits que representen un alto riesgo para los activos afectados. Sin embargo, los sistemas operativos que ya no cuentan con soporte, por parte del proveedor, no contarán con una solución ante el descubrimiento de nuevas vulnerabilidades y la liberación de nuevos exploits.	2

A continuación, se muestran los criterios analizados para la valoración del Impacto, asociado a los hallazgos de seguridad internos (véase Tabla 3.21).

Tabla 21 Hallazgos Internos - Impacto

ID	Hallazgo de Seguridad	Criterio	I
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	Un atacante podría aprovecharse de esta vulnerabilidad para realizar las siguientes acciones: ➢ Ejecución de código remoto. ➢ Comprometer la infraestructura de Active Directory ➢ Comprometer el servicio SCADA. ➢ Denegación de servicio. ➢ Robo de información Por lo tanto, el abuso del hallazgo de seguridad puede provocar un daño muy serio a los datos y servicios que dependen del activo afectado, por lo que se podría provocar la falla del proceso de negocio.	5
2	Credenciales por defecto en dispositivos de CCTV	Un atacante podría aprovecharse de estas vulnerabilidades para realizar las siguientes acciones: ➢ Consulta, modificación o alteración de parámetros de configuración del servicio. ➢ Negación de servicio ➢ Robo de información Por lo tanto, el abuso del hallazgo de seguridad puede provocar daño serio al servicio de CCTV de la Empresa Cliente, por lo que el proceso de negocio puede verse afectado de forma negativa.	3
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	Un atacante podría aprovecharse de esta vulnerabilidad para realizar las siguientes acciones: ➢ Ejecución de código remoto. ➢ Comprometer la infraestructura de Active Directory ➢ Denegación de servicio. ➢ Robo de información Por lo tanto, el abuso del hallazgo de seguridad puede provocar un daño muy serio a los datos y servicios que dependen del activo afectado, por lo que se podría provocar la falla del proceso de negocio.	5
4	Contraseñas débiles en dispositivos de red.	Un atacante podría aprovecharse de estas vulnerabilidades para realizar las siguientes acciones: ➢ Consulta, modificación o alteración de parámetros de configuración del servicio. ➢ Negación de servicio	4

		➢ Robo de información ➢ Compromiso de la infraestructura de red. Por lo tanto, el abuso del hallazgo de seguridad podría causar una pérdida o daño muy serio a la institución y el proceso de negocio puede fallar.	
5	Sistemas Operativos sin Soporte	Actualmente no se encontraron vulnerabilidades críticas, ni herramientas o exploits que representen un alto riesgo para los activos afectados. Sin embargo, los sistemas operativos que ya no cuentan con soporte, por parte del proveedor, no contarán con una solución ante el descubrimiento de nuevas vulnerabilidades y la liberación de nuevos exploits.	4

Al finalizar la obtención de los niveles de Probabilidad e Impacto de cada hallazgo, se realizó el proceso del cálculo y la clasificación del riesgo resultante. Los resultados se muestran en la Tabla 3.22.

Tabla 22 Hallazgos Internos – Cálculo de Riesgos

ID	Hallazgo de Seguridad	P	I	R	Nivel	Color
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	3	5	**15**	**Critica**	
2	Credenciales por defecto en dispositivos de CCTV	3	3	**9**	**Alta**	
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	3	5	**15**	**Critica**	
4	Contraseñas débiles en dispositivos de red.	3	5	**15**	**Alta**	
5	Sistemas Operativos sin Soporte	2	4	**8**	**Alta**	

Cabe mencionar que, conforme a la metodología empleada, el nivel de riesgo asignado a cada hallazgo es desde el punto de vista del consultor; por lo que, al finalizar la entrega de los reportes, la Empresa Cliente debe determinar el nivel de riesgo de cada vulnerabilidad conforme a su propia metodología de análisis de riesgo.

Entrega del servicio

Una vez finalizados y revisados los reportes, el equipo de consultores se reunió con el equipo responsable del servicio por parte de la Empresa Cliente, para la entrega de resultados de las pruebas de seguridad.

Durante la junta, se hizo la mención de que en los resultados únicamente se reportan los hallazgos de seguridad que tienen una mayor severidad, basándose en la probabilidad de explotación y el alto impacto que podrían causar al proceso de negocio, en caso de que una amenaza/atacante logre explotar dichas vulnerabilidades. Esto es con el motivo de enfocar el mayor esfuerzo en la mitigación de los hallazgos de seguridad que representan un mayor riesgo a la Empresa Cliente.

Al finalizar la exposición de los hallazgos de seguridad, dando cumplimiento con las normas establecidas en el contrato y los acuerdos de confidencialidad, se procedió a la destrucción de la evidencia e información obtenida, a través de la ejecución de las pruebas técnicas.

El borrado seguro se garantiza con el uso de herramientas especializadas para la eliminación de información digital, almacenada en los equipos de cómputo de cada consultor. En el caso de documentos físicos, se destruyen a través de cortadoras automáticas.

CONCLUSIONES

A medida que avanza el desarrollo de nuevas tecnologías de la información, que sirven de apoyo a los distintos procesos de negocio, surgen de manera paralela distintas amenazas. En los últimos años se reportó un incremento de incidentes de seguridad informática que han impactado a grandes compañías a nivel mundial. Por este motivo, muchas empresas adoptaron la práctica de realizar análisis de seguridad a sus infraestructuras de TI, con el objetivo de diagnosticar brechas de seguridad que pudiesen ser aprovechadas por las amenazas/atacantes.

Al finalizar el proyecto *Servicio De Análisis De Vulnerabilidades Y Pruebas De Penetración*, se identificaron hallazgos de seguridad que podrían causar una afectación a la confidencialidad, integridad y disponibilidad de la seguridad informática, y que a su vez podrían desembocar en pérdidas monetarias, sanciones por entidades regulatorias, afectación a la reputación, afectaciones a procesos industriales, entre otros. Estos hallazgos de seguridad permitieron a la Empresa Cliente desarrollar un plan para la pronta atención y mitigación de las vulnerabilidades reportadas.

Algunas de las medidas acordadas son la implementación de un sistema de aplicación de parches de seguridad críticos en los servidores y dispositivos vulnerables, migración de servidores obsoletos a sistemas operativos que cuenten con soporte vigente por parte del proveedor, implementación y mejora de reglas en dispositivos de seguridad (IDS/IPS), adopción de una metodología de revisión de código durante la publicación y desarrollo de aplicaciones, entre otras.

Es importante resaltar que estas medidas reducirán los niveles de riesgo de los hallazgos, a un nivel que será aceptable y manejable, sin embargo, al finalizar la implementación de medidas correctivas se recomienda realizar un diagnóstico para evaluar la efectividad de mitigación y calcular los niveles de riesgo resultantes (riesgo residual).

Durante mi participación en este proyecto desempeñé las labores de líder y consultor, lo que me permitió interactuar de manera directa en el proceso de planeación y ejecución de las pruebas técnicas. Para logar el objetivo de este proyecto, realicé tareas de investigación, planteamiento de una metodología a utilizar, desarrollo de herramientas (scripts), toma de decisiones, ejecución de ataques, resolución de problemas emergentes y el análisis de resultados obtenidos (Hallazgos de seguridad), de manera que hice uso de mis habilidades y capacidades en la resolución de problemas, adquiridas durante mi formación académica y experiencia laboral.

Anexos

1.1. Mapa de calor de los hallazgos Externos

En la siguiente imagen (Figura A.1) se muestra un mapa de calor con el concentrado de los hallazgos externos, en donde el ID correspondiente a los hallazgos descritos en la Tabla de Riesgos Externos (Tabla A.1).

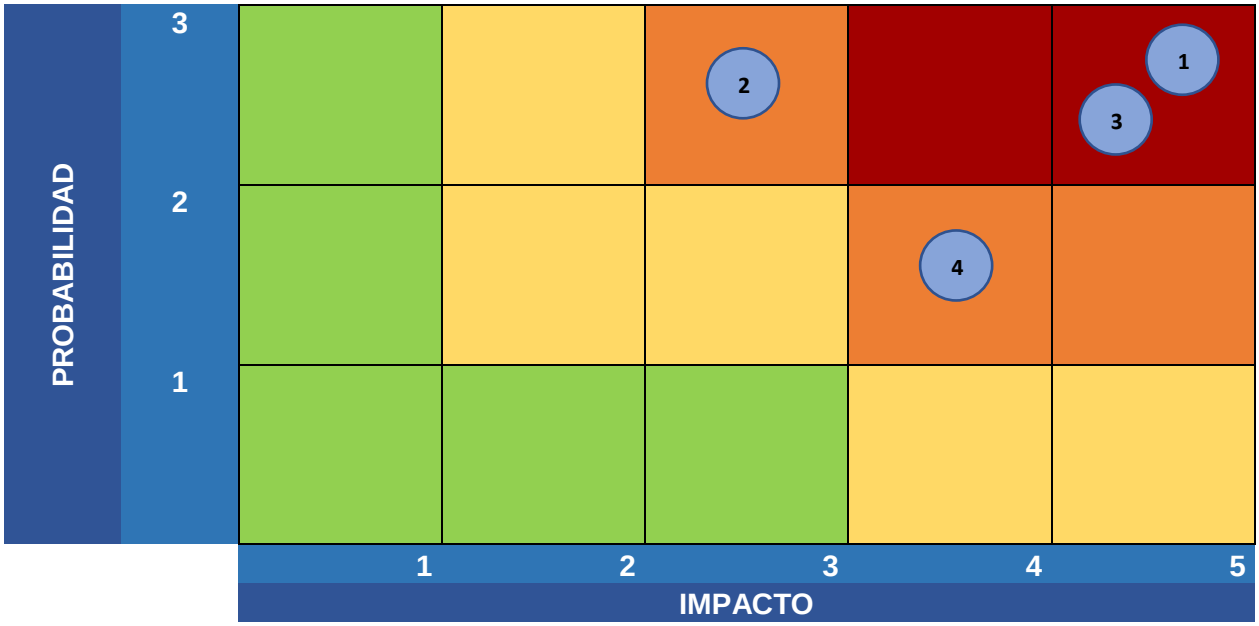


Figura 20 Mapa de Calor - Hallazgos Externos

Tabla 23 Tabla de Riesgos Externos

ID	Hallazgo de Seguridad	P	I	R	Nivel
1	Vulnerabilidades de SQLinjection	3	5	**15**	**Critica**
2	Vulnerabilidades de XSS	3	3	**9**	**Alta**
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	3	5	**15**	**Critica**
4	Sistemas Operativos sin Soporte	2	4	**8**	**Alta**

1.2. Mapa de calor de los hallazgos Internos

En la siguiente imagen (Figura A.2) se muestra un mapa de calor con el concentrado de los hallazgos externos, en donde el ID correspondiente a los hallazgos descritos en la Tabla de Riesgos Internos (Tabla A.2).

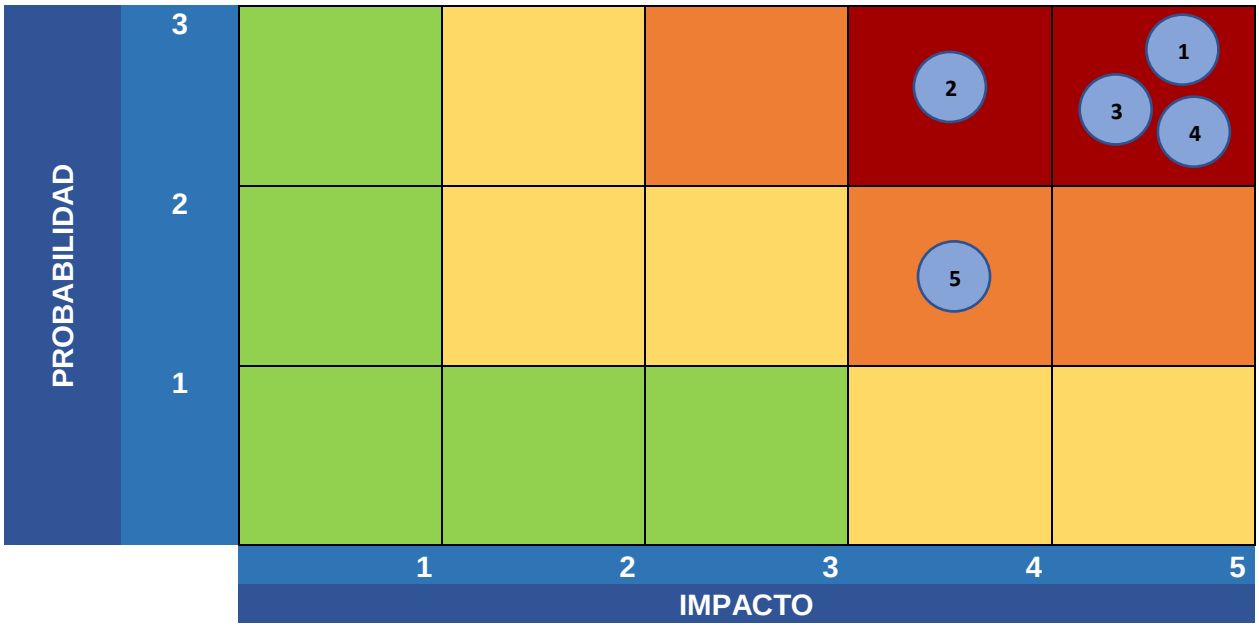


Figura 21 Mapa de Calor - Hallazgos Internos

Tabla 24 Tabla de Riesgos Internos

ID	Hallazgo de Seguridad	P	I	R	Nivel	Color
1	Vulnerabilidades asociadas a la ausencia de parches de seguridad en equipos de Windows.	3	5	**15**	**Critica**	
2	Credenciales por defecto en dispositivos de CCTV	3	3	**9**	**Alta**	
3	Vulnerabilidades asociadas a la ausencia de actualizaciones de seguridad en servidores web y componentes	3	5	**15**	**Critica**	
4	Contraseñas débiles en dispositivos de red.	3	5	**15**	**Alta**	
5	Sistemas Operativos sin Soporte	2	4	**8**	**Alta**	

Glosario

Activo: Todo aquello que represente un valor para una persona u organización; puede ser un objeto, persona, proceso o información.

Amenaza: Cualquier agente que pueda causar una afectación o incidente no deseado a un activo.

Backdoor: También conocido como Puerta Trasera, es un mecanismo que permite a un atacante evadir los controles de autenticación y acceder al sistema infectado.

Cracker: Proviene del término Criminal Hacker, se refiere a aquella persona que posee amplios conocimientos en informática y los utiliza para vulnerar algún sistema de seguridad, ya sea con fines maliciosos o por un beneficio personal.

Confidencialidad: Propiedad de la información que garantiza que la información sólo debe ser accesible o revelada a individuos, entidades o procesos autorizados.

Disponibilidad: Propiedad de la información que garantiza que la información debe estar accesible cuando un individuo, entidad o proceso autorizado lo requiera.

DoS: Del inglés Denial of Service, es un ataque que consiste en la sobrecarga de un servicio, teniendo como consecuencia que el servidor sea inaccesible.

Exploit: Es un mecanismo utilizado por un atacante para aprovecharse de una vulnerabilidad y provocar un comportamiento no deseado en el activo afectado.

Hacker: Es aquella persona que posee amplios conocimientos en el ámbito de las tecnologías de la información.

IDS: Del inglés Intrusion Detection System, es una herramienta de seguridad que se basa en el análisis de tráfico de red para la detección actividad sospechosa y genera alertas para informar la existencia de un evento.

Impacto: Es la consecuencia que tiene la materialización de una amenaza sobre un activo.

Incidente: Evento no deseado o inesperado y que puede ocasionar una afectación en la operación.

Integridad: Propiedad de la información que garantiza que la información debe mantener su plenitud y exactitud, es decir, no debe sufrir modificaciones no autorizadas.

IPS: Del inglés Intrusion Prevention System, es una herramienta de seguridad que se basa en el análisis de trafico de red para la detección de actividad sospechosa y que establece políticas de prevención y protección que se ejecutan de durante al momento de la detección del evento.

Malware: Del inglés Malicious software, es un programa diseñado para realizar un conjunto de acciones malignas.

No repudio: Servicio que garantiza que un emisor no pueda negar el envío de un mensaje y que un receptor no pueda negar la recepción de un mensaje.

Payload: Es la carga dañina liberada por un exploit, es decir, el conjunto de acciones secundarias que se realizan después de que un exploit se aprovecha de una vulnerabilidad, por ejemplo, la creación de usuarios, cambios en la configuración de un sistema, robo de contraseñas, entre otras acciones maliciosas.

Phishing: Es un ataque basado en la suplantación de identidad de una entidad, generalmente bancaria, a través del cual se busca obtener datos privados de los clientes, como contraseñas, números de cuentas.

Ransomware: Malware que tiene como principal comportamiento el secuestro de los archivos, información o la sesión en un equipo infectado que solicita una recompensa para su liberación.

Riesgo: Es la probabilidad de que una amenaza se concrete, es decir, la probabilidad de que una amenaza explote una vulnerabilidad y que cause un impacto en el activo afectado.

SQL injection: Vulnerabilidad que consiste en la inyección de comandos SQL a través de un aplicativo web, debido a la errónea validación de las entradas de datos en el aplicativo afectado.

Vulnerabilidad: Es una falla o debilidad en un activo o control y que puede ser aprovechada por una amenaza para realizar una acción no deseada.

WAF: Del inglés Web Application Firewall, es una solución que realiza funciones de filtrado HTTP y seguridad hacia una aplicación web.

Bibliografía

A continuación, se muestra la bibliografía utilizada para el desarrollo del presente reporte:

- Mendoza, M. (2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. [online] WeLiveSecurity. Recuperado de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/
- Foltýn, T. (2018). *Tendencias en seguridad 2018: el costo de nuestro mundo conectado*. [online] WeLiveSecurity. Recuperado de: https://www.welivesecurity.com/la-es/2017/12/15/tendencias-seguridad-2018/
- Reyes, A. (2011). *Ethical Hacking*. [online] Recuperado de: https://www.seguridad.unam.mx/historico/documento/index.html-id=7
- Pentest-standard.org. (2014). *The Penetration Testing Execution Standard*. [online] Recuperado de: http://www.pentest-standard.org/index.php/Main_Page
- Soriano, A. (2012). *Hacking ético: mitos y realidades* | *Revista .Seguridad Cultura de Prevención para TI, Número 12*. [online] Recuperado de: https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/Para%20PDF_12.pdf
- Cve.mitre.org. (2018). *CVE -Common Vulnerabilities and Exposures (CVE).* [online] Recuperado de: https://cve.mitre.org/
- Carozo, E. (2013). *Sistemas SCADA, consideraciones de seguridad* | *Revista. Seguridad Cultura de Prevención para TI, Número 18*. [online] Recuperado de: https://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Num18_RevistaSeguridad_0.pdf
- Bortnik, S. (2013). *Pruebas de penetración para principiantes: 5 herramientas para empezar, consideraciones de seguridad* | *Revista. Seguridad Cultura de Prevención para TI, Número 18*. [online] Recuperado de: https://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Num18_RevistaSeguridad_0.pdf
- Tovar, A., García D., González R. (2017). *WannaCry: ataque mundial y consideraciones sobre ciberseguridad* | *Revista. Seguridad Cultura de Prevención para TI, Número 29*. [online] Recuperado de: http://revista.seguridad.unam.mx/sites/default/files/rev_seguridad_29_0.pdf
- VMWare. (2018). *Workstation Pro* [online] Recuperado de: https://www.vmware.com/mx/products/workstation-pro.html
- Whois.icann.org. (2013). *Guía básica de WHOIS* | *ICANN WHOIS*. [online] Recuperado de: https://whois.icann.org/es/guía-básica-de-whois

- Arroyo, M. (2011). *SE Hacking Ético: Google Hacking – Parte 1.* [online] Hacking Ético. Recuperado de: https://hacking-etico.com/2011/07/20/se-hacking-etico-google-hacking-parte-1/
- Nmap.org. (2018*). Guía de referencia de Nmap (Página de manual)* [online] Recuperado de: https://nmap.org/man/es/index.html
- Alfaro, R. (2009). *Nmap Scripting Engine (NSE)* [online] Security Art Work. Recuperado de: https://www.securityartwork.es/2009/06/08/nmap-scripting-engine-nse/
- Tebanle. (2018). *Nessus Professional* [online] Recuperado de: https://es-la.tenable.com/products/nessus/nessus-professional
- Albors, J. (2015). *¿Sabes qué es un backdoor y en qué se diferencia de un troyano?* [online] WeLiveSecurity. Recuperado de: https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/
- de Pablos Heredero, C., López-Hermoso, J., Martín-Romo, S. y Medina, S. (2004). *Informática y comunicaciones en la empresa*. 1st ed. Madrid: ESIC, pp.33-35.
- Oncins Rodríguez, A. y Olivares Serrano, J. (2015). *Seguridad informática*. 3rd ed. Cornellá de Llobregat: ENI, pp.133-136.
- Jara, H. and Pacheco, F. (2018). *Ethical Hacking 2.0.* 1st ed. Buenos Aires: Fox Andina, pp.39-46.