UNIVERSIDAD DE CUENCA

Facultad de Ingeniería

Maestría en Gestión Estratégica
de Tecnologías de la Información

Método conciso para test de penetración en sistemas informáticos de empresas pequeñas privadas y públicas

Trabajo de titulación previo a la obtención del título de Magíster en Gestión Estratégica de Tecnologías de la Información

Autor: **Ing. Martín Fernando González Palomeque**

CI: 0301588091

mfgp_87@hotmail.com

Director: **Ing. Diego Arturo Ponce Vásquez, PhD.**

CI: 0101822609

Cuenca - Ecuador

12-abril-2022

Resumen

En este trabajo de titulación se desarrolla un método conciso para la ejecución de pruebas de penetración en infraestructuras tecnológicas de pequeñas empresas privadas o públicas, suministrando las herramientas adecuadas y estableciendo los procesos necesarios para su implementación. Se examinaron conceptos básicos de ciber seguridad y contramedidas a ataques informáticos, y se profundizó en algunas metodologías relevantes para la ejecución de pruebas de penetración, como base para el diseño posterior del método propuesto. Con la aplicación del caso de estudio se comprobó que la herramienta diseñada es efectiva, útil, y provee resultados de manera rápida, a la vez que optimiza el uso de recursos, lo que se traduce en ahorros significativos para las empresas. Finalmente, los resultados hacen evidente la falta de profesionales del área de seguridad informática, y sugieren una falta de conciencia por parte de las empresas pequeñas en esta temática y en los riesgos asociados a ataques informáticos.

Palabras clave: Ciberseguridad. Seguridad de la información. Metodología para pruebas de intrusión. Ciberseguridad en empresas pequeñas.

Abstract

This study develops a brief method for the execution of penetration tests in modest technological infrastructures, providing the appropriate tools and establishing the necessary processes for its implementation in small, private and public organizations. Basic concepts of cybersecurity and countermeasures to computer attacks were examined, and relevant methodologies for penetration testing were delved, as a basis for the subsequent design of the proposed instrument. With the application of the case study, the designed tool was verified to be effective, useful, and quick to provide results while optimizing the use of resources, which translates into significant savings for companies. Finally, the results show the lack of professionals in the cyber security area, and also a lack of awareness by small companies on this topic, and the associated risks with cyberattacks.

Keywords: Cybersecurity. Information security. Penetration testing methodology. Cybersecurity in small companies.

Índice de contenido

Índice de figuras

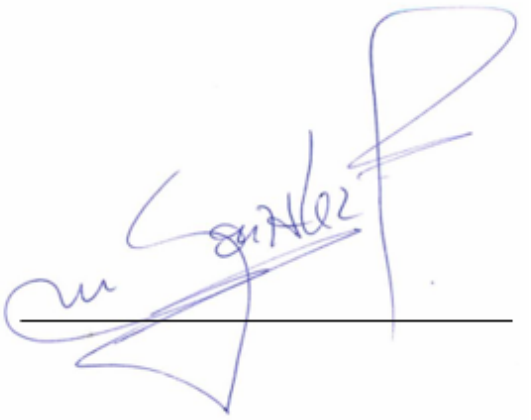
Índice de tablas

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

Yo, Martín Fernando González Palomeque, en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación "Método conciso para test de penetración en sistemas informáticos de empresas pequeñas, privadas y públicas", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 12 de Abril de 2022



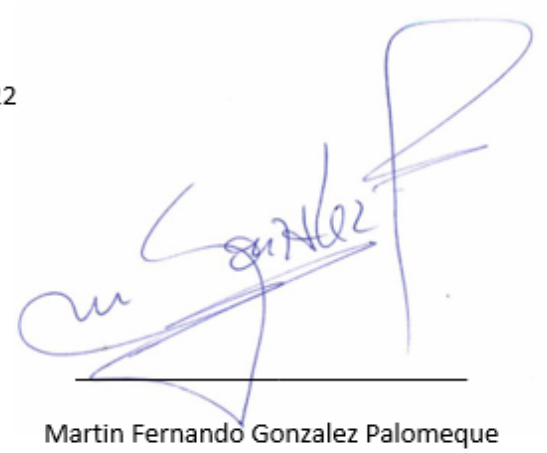
Martín Fernando González Palomeque

C.I: 0301588091

Cláusula de propiedad intelectual

Yo, Martin Fernando Gonzalez Palomeque, autor del trabajo de titulación "Método conciso para test de penetración en sistemas informáticos de empresas pequeñas privadas y públicas", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 12 de Abril de 2022



Martin Fernando Gonzalez Palomeque

C.I: 030158809-1

Agradecimientos

Al Ing. Diego Ponce, director de este trabajo de titulación, por su disposición y apoyo en el desarrollo de este trabajo.

A mi colega Ing. Rafael Palacios, por su apoyo desinteresado en la elaboración del método propuesto en el presente trabajo.

A la Universidad de Cuenca y a sus docentes del programa de master, por sus valiosos conocimientos y el aporte directo mi formación académica y profesional.

A mi esposa Patricia por ser siempre el apoyo en todos los aspectos de mi vida.

Dedicatoria

A mi esposa, mi fortaleza, el pilar y apoyo incondicional de mi hogar.

A mis hijas, mi razón de ser, mi motivación, mi mundo.

A mis padres, por sus enseñanzas, lecciones diarias y formarme en buenos valores. Por ellos es que estoy aquí hoy.

A él, que siempre vio mi mejor versión, porque siempre creyó en mí. Fuimos los 2 contra el mundo.

Capítulo I
Introducción

1.1 Antecedentes

El uso de la tecnología en los procesos de negocio, trae consigo beneficios para las empresas que no se podrían obtener de otra manera. La información se ha vuelto un activo crítico para la operación y crecimiento de todas las empresas (Santiago & Allende, 2017), y gracias a los avances tecnológicos, ésta puede encontrarse de manera digital y en distintos medios y lugares. Esto ha generado una tecno dependencia por parte de la mayoría de ellas. Por ello es necesario advertir en este punto que, la automatización e hiperconectividad de sus procesos implica riesgos asociados y vulnerabilidades, originados generalmente dentro de su propia infraestructura tecnológica, que, además, al encontrarse constantemente interconectados, exponen sus activos digitales a una gran cantidad de amenazas (Santiago & Allende, 2017).

Las amenazas tecnológicas son parte de nuestra vida diaria como individuos y dentro de nuestras organizaciones, sin embargo, es en estas últimas a donde están dirigidos en su gran mayoría los ataques informáticos (Israel, 2020), y es precisamente en donde debemos tener especial cuidado. Se vuelve necesario la implementación de políticas y herramientas que ayuden a cubrir las fallas de seguridad y a proteger los activos digitales (Santo Orcero, 2018).

El escenario actual es desalentador. En la última década, el número de ataques informáticos ha incrementado exponencialmente, así como también lo ha hecho en forma y sofisticación. Un ciber atacante puede fácilmente ocasionar daños incalculables a una empresa sin perder el anonimato, y para esto solo necesita un computador y una conexión a internet. El bajo costo y riesgo en la perpetración de estos ataques son factores clave en el crecimiento en este tipo de delitos.

El problema va un tanto más allá. Según el *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*, de los 32 países que fueron analizados, un tercio no cuenta con un marco legal sobre los delitos informáticos, 12 han aprobado una estrategia nacional de ciberseguridad, 10 países han creado organismos para la gestión de la ciberseguridad y tan solo 5 se han adherido a la convención de Budapest que facilita la cooperación internacional en la lucha contra el cibercrimen. Esto, sumado a la brecha de 600.000 profesionales en el área de la ciberseguridad, han ocasionado que la lucha contra el cibercrimen en la región, tenga un avance muy conservador.

La ciberseguridad es un tópico todavía pendiente para muchas empresas. La mayoría desconoce su estado actual en este tema, y menos realiza auditorias o comprobaciones de seguridad de forma periódica. Esta realidad predispone un escenario óptimo para la ejecución de agentes maliciosos que están en constante búsqueda de vulnerabilidades a través de diversas infraestructuras tecnológicas. La materialización de estas vulnerabilidades, significan perdidas que rondan la cifra de los 50.000 millones de dólares por año, solo para América Latina (Gonzalez, 2019).

Como es evidente, nos falta mucho camino por recorrer en este tema. En el Ecuador como en otros países de la región, la seguridad informática no tiene la relevancia que se merece por parte de las empresas y organizaciones, el problema principal es el presupuesto que asignan a la ciberseguridad (Vargas Borbúa et al., 2017), el escenario se complica para las empresas pequeñas e instituciones públicas. El presupuesto con el que disponen, la tramitología requerida y el costo de contratar servicios de esta naturaleza dificultan la materialización de la implementación de políticas de seguridad y exponen a las organizaciones a agentes maliciosos y consecuentemente a la interrupción de sus procesos y servicios.

Existe variedad de soluciones basadas en hardware y software, entrenamiento para el personal, políticas, metodologías, estándares y marcos de trabajo con el fin de hacer frente a las amenazas tecnológicas, que acechan nuestro día a día y en todos los aspectos de nuestra vida. Entre las más utilizadas se encuentran, la implementación de metodologías para la ejecución de pruebas de penetración, las que consisten en analizar una infraestructura en busca de vulnerabilidades, proponer medidas y mitigar riesgos, con un enfoque externo. Más adelante profundizaremos en algunas de ellas.

1.2 Justificación

Los ataques informáticos están a la orden del día. Basta con revisar el mapa en vivo de ataques informáticos en la web de Kaspersky (*MAP | Kaspersky Cyberthreat Real-Time Map*, s/f), para darnos cuenta que los ciberataques suceden por miles y a cada segundo, no discriminan país o región, si es una persona o una empresa, si esta última es grande o es pequeña.

El afirmar que las empresas pequeñas no son de interés para los ciberatacantes es una falacia. Si bien es cierto, el comprometer la infraestructura tecnológica de una corporación o multinacional puede traer consigo mayores beneficios económicos, atacar una empresa pequeña resulta mucho más fácil y es de igual manera rentable, aunque a una menor escala. Considerando que, son las empresas grandes las que generalmente cuentan con políticas,

infraestructura y personal dedicado a evitar o minimizar el impacto que tienen las amenazas cibernéticas, el uso de tiempo y recursos necesarios para un ataque es muy superior a los requeridos para comprometer una empresa pequeña, donde habitualmente, llevados de la falsa creencia de que no van a ser objeto de ataques, obvian la implementación de controles de seguridad muchas veces básicos, y dejan expuestos sus activos digitales, que de ser comprometidos, podrían llevar tranquilamente a la quiebra a estas empresas, por poner un ejemplo, el robo de patentes.

La variedad de formas en las que un atacante puede comprometer nuestros activos digitales, es abrumadora y lo menos que podemos hacer como dueños de casa, es asegurar puertas y ventanas. Si a este peligro latente, le sumamos la brecha de 600 mil profesionales en el área de ciberseguridad para la región de Latinoamérica y el Caribe, el problema se complica de sobremanera.

1.3 Objetivos

En base a lo anterior, el estudio propondrá un método que sea asertivo y rápido de ejecutar, utilizando un mínimo de recursos, nos permita conocer el estado actual de nuestra infraestructura tecnológica en temas de seguridad, los riesgos asociados a los activos digitales, sirva como punto de partida para exámenes más profundos como auditorias de seguridad y nos permita llevar la seguridad de nuestra empresa a niveles aceptables, al mismo tiempo que establecemos una cultura de seguridad en las empresas, sin importar su tamaño.

Capítulo II

Marco Teórico

En un mundo híper conectado, las ciber amenazas pueden venir de cualquier lugar y en cualquier forma. Los ciber criminales, muchas veces económicamente motivados, ingenian constantemente nuevas formas de vulnerar sistemas y exponer o robar información para su propio beneficio. El virus informático ha evolucionado a un abanico de amenazas más sofisticadas que resulta difícil muchas de las veces, etiquetarlas o clasificarlas (Choo, 2011), de la misma forma, la rama de la ciberseguridad se ha visto siempre en la necesidad de seguirle el paso.

La seguridad de la información, seguridad informática y ciberseguridad son temas bastante amplios y que están estrechamente relacionados. En el presente capitulo revisaremos algunos temas relevantes que nos ayudaran a comprender de mejor manera el estudio, y profundizaremos en las metodologías de pentest que se consideran más importantes, ya que son la base para el desarrollo de este estudio.

2.1 Seguridad de la Información

De una forma simplista, la seguridad de la información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información (Tabla 1). De una manera más profunda, la seguridad de la información es un proceso, una actividad continua que trata de identificar los riesgos relacionados a los recursos tecnológicos, gestionar esos riesgos (los cuales pueden o no ser de naturaleza tecnológica) y llevarlos a niveles aceptables.

Tabla 1. Características de la información. Fuente: (Samonas & Coss, 2014)

Concepto	Descripción	Característica
Confidencialidad	Se refiere al hecho de que la información o los activos digitales deberán ser accesibles únicamente por las personas autorizadas	Una persona sin autorización accede o toma ventaja de la información almacenada en un computador
Integridad	Mantener la información o activos digitales en la misma forma en la que fueron generados, sin haber sido alterados o modificados por personas no autorizadas	Una falta a la integridad es la modificación no autorizada de información; una persona cambia o altera la información almacenada en un equipo
Disponibilidad	Es la capacidad de la información o recursos digitales de permanecer accesibles cada que un usuario autorizado así lo requiera	Una falta a la Disponibilidad podría considerarse cuando un usuario no autorizado puede bloquear el acceso a los recursos digitales a usuarios autorizados

2.1.1 Seguridad informática

Es necesario saber diferenciar el concepto de seguridad de la información del de seguridad informática. Si bien a primera vista pueden parecer bastante similares, en la práctica se vuelven notables sus diferencias:

De acuerdo a Figueroa-Suárez et al., (2018), la seguridad informática se encarga de la parte operacional, el método, la implementación práctica de la protección de la información a través de actividades, herramientas, controles, que actúan de manera activa en una organización y su infraestructura.

La seguridad de la información es de orden metodológico, está más orientada a la estrategia, es la que se encarga de establecer las pautas, políticas o normas a seguir con el fin de proteger los activos digitales.

Otra diferencia importante es que la seguridad informática se limita a una infraestructura tecnológica, mientras que la seguridad de la información se expande a toda una organización (infraestructura física en general, personas, procesos, etc.). Por ejemplo: Establecer claves de acceso a los equipos de cómputo se puede considerar una práctica tanto de seguridad informática como de seguridad de la información. Implementar cerraduras inteligentes con lectores biométricos se puede considerar una práctica de seguridad de la información y no de la seguridad informática.

2.1.2 Hacking y ciberseguridad

La cultura *hacker* nace en el MIT (Massachusetts Institute of Technology) a principios de la década de los sesenta. La palabra *"hack"* en ese entonces significaba una solución simple y elegante a un problema. De ahí que, con el tiempo, el termino *hacker* se empezó a asociar con programadores informáticos, para quienes un "*hack"* era una hazaña en el campo de la programación (*Breve historia de los "hackers" y sus andanzas*, 2011).

Con la llegada del ARPANET a principios de la década de los 70 y la creciente popularidad de las computadoras, los entendidos (hackers) en los sistemas informáticos y lenguajes de programación comenzaron a poner a prueba estos sistemas para descubrir sus capacidades. Además, pasaron de ser individuos aislados a ser una tribu interconectada que compartía información y experiencias en los famosos *bulletin boards* (precursores de los foros en internet). No paso mucho tiempo para que cruzaran la barrera legal. Para la década de los 80 el termino hacker se asociaba casi exclusivamente con actividades delictivas (Guillen Zafra, 2017).

De manera simultánea, los gobiernos, principalmente de Estados Unidos y Reino Unido comenzaron a reclutar personas con un nivel técnico elevado con el fin de poner a prueba sus sistemas y corregir errores antes de que fueran explotados.

Desde la creación del primer virus informático, las amenazas tecnológicas han evolucionado en las últimas décadas. La información y los activos digitales almacenados en sistemas financieros y empresariales han sido continuamente el blanco de *hackers* de sombrero negro quienes son siempre muy creativos a la hora de elaborar un ataque.

En consecuencia, la ciberseguridad nace de la necesidad de las empresas de proteger sus activos digitales de agentes maliciosos. Dicho de otro modo, la ciberseguridad no es más que el estudio, desarrollo y practica de las contramedidas a cualquier forma de ataque informático.

2.1.3 Tipos de hackers

Existe una gran variedad de tipos de *hackers*, los cuales se clasifican en mayor medida por sus intereses y modo de operación, tal como se ve en la tabla 1. Se utilizará la terminología en inglés, ya que es ampliamente reconocida en el mundo de la ciberseguridad.

Tabla 2. Tipos de hackers. Fuente: (Ec Council, 2020)

Tipo	Descripción
Black Hats	Hackers con habilidades computacionales extraordinarias. Usan esas habilidades para ingresar de manera no autorizada a sistemas con fines delictivos como robar datos personales, contraseñas, información financiera o perjudicar o comprometer los sistemas. También se les conoce como crackers
White Hats	Se dedican a testear sistemas con el fin de conocer de forma anticipada las vulnerabilidades del mismo, antes de que puedan ser explotadas. Generalmente trabajan en empresas de seguridad y testean sistemas siempre con la autorización de sus propietarios. También se les conoce como pen testers o hackers éticos
Gray Hats	Es una especie de combinación de los anteriores. Generalmente vulneran sistemas sin autorización, pero lo hacen con buena intención y no para beneficio personal. Por ejemplo, filtran información relevante sobre una empresa que utiliza prácticas no éticas para el público en general
Suicide Hackers	Su intención es la de causar el mayor daño posible a una infraestructura tecnológica por una “causa”. No les importa que los atrapen o que puedan ir a la cárcel
Script Kiddies	Son hackers sin habilidad, aunque con conocimiento en la materia, que utilizan herramientas desarrolladas por hackers verdaderos para perpetrar sus ataques
Cyber Terrorist	Sus ataques están motivados por creencias políticas o religiosas. Expertos en una gran gama de habilidades, buscan generar miedo advirtiendo ataques a gran escala de redes computacionales

State Sponsored Hackers	Son contratados por gobiernos para penetrar sistemas, obtener información secreta o perjudicar los sistemas de información de otros gobiernos
Hacktivist	Buscan socializar o generar conciencia de su agenda política o social, generalmente deshabilitando sitios web o vulnerando sistemas informáticos gubernamentales o corporativos como una forma de protesta

2.1.4 Fases del Hacking

En la seguridad de la información, el término *"Hacking"* se refiere a explotar vulnerabilidades en una infraestructura tecnológica. Generalmente consiste en 5 fases. No es necesario seguirlos al pie de la letra, sin embargo, el realizarlo trae consigo mejores resultados.

- **Reconocimiento**

Se lo conoce también como *Footprinting*. Consiste en recolectar la mayor cantidad de información acerca del objetivo, la cual servirá para planificar las fases posteriores. La información a recolectar acerca del objetivo puede incluir: clientes, personal, redes y sistemas. Las técnicas de reconocimiento pueden ser activas o pasivas y pueden incluir ingeniería social, Google *hacking*, *whois*, *network mapping*, entre otras.

- **Escaneo**

Es la fase previa a la intrusión. En esta etapa y con la información recolectada en la fase anterior, el atacante escanea una red de datos por información específica como maquinas activas, estado de los puertos, topologías de red, tipo de dispositivo, detalles del sistema operativo, entre otras. Las herramientas utilizadas en esta fase pueden ser: *port scanners*, *vulnerability scanners, network mappers,* etc.

- **Obtener Acceso**

Como su nombre lo indica, consiste en que el atacante obtiene acceso a un host objetivo al explotar alguna vulnerabilidad descubierta en la fase previa. Tan pronto como obtiene acceso, el atacante intenta escalar los privilegios en el host para poseer control total del sistema. Para esto se utilizan técnicas como *password cracking*, *buffer overflows, session hijacking* (secuestro de sesión), etc.

- **Mantener Acceso**

Una vez que se escala privilegios en un host objetivo, el atacante requiere mantener ese acceso y sus privilegios para utilizarlos a voluntad. Habitualmente en esta fase se limpia la evidencia del acceso no autorizado, se instala un *backdoor* o un troyano para ingresar nuevamente, y un *rootkit* para ganar acceso a nivel de sistema. De aquí, que el atacante

puede subir, descargar o manipular información del sistema, aplicaciones o configuración, robar información confidencial o contraseñas, o también puede utilizar el host para perpetrar ataques futuros.

- **Eliminar rastros**

Son las actividades que el atacante realiza con el fin de esconder sus actos maliciosos. En esta fase es común permanecer cautelosamente en control del host objetivo y eliminar la evidencia que podría perjudicarlos legalmente. Se utilizan herramientas como *PsTools, Netcat* o troyanos para eliminar sus huellas y sobrescribir los logs de las aplicaciones o sistemas.

2.1.5 Ethical Hacking

Es la práctica de utilizar herramientas y conocimientos de *hacking* para ayudar a las empresas y gobiernos a descubrir vulnerabilidades y mejorar la seguridad de sus sistemas y redes computacionales. Hackers éticos o *White Hats* son contratados por las organizaciones para realizar ataques autorizados y controlados a sus infraestructuras evitando causar daños a sus activos.

El ethical hacking consiste en 5 fases:

Fase 1: Reconocimiento

Fase 2: Escaneo

Fase 3: Obtener acceso

Fase 4: Mantener acceso

Fase 5: Limpiar huellas

- **Alcance y limitaciones**

El *hacking* ético es una herramienta esencial y de soporte para la gestión de riesgos, auditorias de seguridad y mejores prácticas dentro de la seguridad de los sistemas de información. Permite identificar riesgos y gestionarlos de acuerdo a un plan, sin embargo, está limitado a los requerimientos del contratante. Para esto es importante definir de manera específica, lo que puede o no hacer, acceder o vulnerar el pentester, considerar acuerdos de confidencialidad, y establecerlo en un contrato de trabajo. Ningún trabajo de *pentest* o *hacking* ético puede empezar sin un documento legal firmado entre las partes y sin antes comprender bien las implicaciones legales del acceso no autorizado a un sistema informático. De la misma forma el pentester debe realizar su trabajo de forma profesional y no exceder lo establecido en el alcance.

Dependiendo del enfoque, hay varios tipos de test preestablecidos, cada uno con sus requerimientos y finalidad.

- **Red Team (Equipo Rojo)**

Se basa en la seguridad ofensiva. Un equipo de profesionales expertos en atacar sistemas y vulnerar defensas ponen a prueba la seguridad de un sistema al encontrar vulnerabilidades y explotarlas.

- **Blue Team (Equipo Azul)**

Son responsables de asegurar la infraestructura, sistemas y activos digitales de las empresas, contra los ataques externos (Diogenes & Ozkaya, 2018). Conjuntamente con el equipo rojo *(red team)* simulan ataques para probar la efectividad de sus medidas de seguridad, por lo que su enfoque holístico provee mejores soluciones de seguridad a las empresas.

- **Pentest**

Es evaluar la seguridad de un sistema o infraestructura por medio de un ataque autorizado. Se utilizan métodos de *hacking* con el fin de encontrar vulnerabilidades y explotarlas de la misma forma que lo haría un atacante real con el fin de proponer medidas correctivas (Guillen Zafra, 2017). Existen 3 tipos principales de pentest: *Black Box, White Box* y *Grey Box* (ver tabla 2).

Tabla 3. Tipos de pentest. Fuente: (Guillen Zafra, 2017)

Tipo	Características
Black Box	El pentester toma el rol de un atacante externo, sin información previa de la organización sobre la que está trabajando. En este enfoque, la empresa quiere poner a prueba la efectividad de las barreras de seguridad entre su red interna y el internet
White Box	La organización entrega información acerca de su infraestructura al pentester como rangos de IPs, sistemas, topologías de red, etc. La finalidad es facilitar la fase de recolección de información al pentester y enfocarse en la intrusión y la búsqueda de vulnerabilidades
Gray Box	Es una combinación de los anteriores. El pentester recibe información orientativa y asume el rol de un usuario sin privilegios dentro de la organización con el fin de evaluar la capacidad de escalar privilegios y el daño potencial que podría ejercer en la empresa

2.2 Contramedidas a ciberataques

Existen varios métodos y contramedidas que podemos implementar en nuestra organización con el fin de contrarrestar el impacto de ataques informáticos y malware, a continuación, vamos a ver los más comunes.

2.2.1 Antimalware

Aunque hay una ligera diferencia, englobaremos en esta categoría, también a los antivirus y *antispyware*. Este tipo de programas examinan los archivos de un dispositivo y los comparan con una base de firmas que actualizan constantemente. También monitorean los procesos en ejecución y detectan comportamientos sospechosos.

2.2.2 Sistemas de detección de intrusos (IDS)

Son soluciones basadas en hardware o software y sirven para detectar trafico inusual en una red de datos y emitir alertas cuando existen intentos de acceso no autorizado a los recursos. Esto lo hacen a través de monitoreo y análisis de tráfico de red y eventos del sistema.

William Stallings & Brown (2014) clasifican a los IDS en tres tipos:

- HIDS (IDS basados en host): monitorea los procesos y eventos que ocurren en un host en particular.
- NIDS (IDS basados en red): Monitorea el tráfico de red y analiza segmentos y dispositivos para identificar actividad sospechosa.
- IDS distribuidos o híbridos: Combinan funciones de los anteriores en una solución central que identifica y responde a intrusiones de forma más efectiva.

Una forma avanzada de un IDS es un *honeypot.* Un *honeypot* es un sistema señuelo, por lo que está diseñado para alejar a un atacante potencial de un activo o sistema critico (William Stallings & Brown, 2014). Pueden simular desde un equipo aislado hasta toda una infraestructura de red con todos sus servicios, por lo que son muy complejos de mantener. Ayudan a detectar y prevenir ataques, recopilan información a través de logs e incluso pueden registrar las pulsaciones de teclado del atacante (Ec Council, 2020).

2.2.3 Sistemas de prevención de intrusos (IPS)

Son extensiones de los IDS ya que de forma adicional poseen la capacidad de bloquear actividad o trafico malicioso. Al igual que los IDS, se clasifican en IPS basados en red, basados en host y distribuidos. Identifican comportamientos maliciosos a través de detección de anomalías y responden bloqueando los paquetes dentro de un perímetro o un equipo de la red (William Stallings & Brown, 2014).

2.2.4 Firewall

Son sistemas basados en hardware o software y se utilizan para prevenir accesos no autorizados de otras redes. Están integrados con varios servicios y tecnologías que

incrementan su eficiencia y sus capacidades, como *Proxys*, NAT y VPN. Generalmente se ubican entre la red privada y el internet y filtran todos los paquetes tanto de entrada como de salida, bloqueando aquellos que no concuerdan con los criterios de seguridad especificados (Ec Council, 2020). En este sentido, un firewall puede ser considerado un IPS ya que bloquea el trafico dentro de una red de acuerdo a las reglas de control de acceso implementadas. Un IPS dedicado se diferencia al ser capaz de utilizar algoritmos y técnicas avanzadas de detección de patrones y comportamiento malicioso.

2.2.5 Evaluación y manejo del riesgo

Es el proceso de identificar, evaluar, responder a los riesgos y sus potenciales efectos. Implementar controles y planes de mejora con el fin de reducir y mantener los riesgos en niveles aceptables. Comprende actividades como: identificación de riesgos potenciales, identificar el impacto de los riesgos potenciales, establecer prioridades (dependiendo el impacto), comprender y analizar los riesgos, controlar los riesgos y mitigar sus efectos, socializar al personal las estrategias y planes para el manejo de los riesgos, etc.

2.2.6 Principios de la seguridad informática

Son un conjunto de reglas básicas basadas en mejores prácticas, que, aunque no sean sencillas de implementar, incrementan de manera considerable los niveles de seguridad de una organización.

- **Principio de mínimos privilegios**

Se refiere a asignar a cada usuario, los privilegios y permisos básicos o necesarios para ejecutar sus funciones. Esto puede aplicarse tanto a infraestructuras tecnológicas como físicas. Por ejemplo: Un usuario de contabilidad no tendría por qué tener acceso a la base de datos de clientes, ni tampoco acceso físico al data center.

- **Principio “secure by default”**

Este principio está de cierta forma, ligado al anterior. Se refiere a que se debe bloquear los accesos digitales y físicos de la organización de manera predeterminada (bloquear puertos, protocolos, hardware, software, accesos físicos, etc.), y únicamente habilitarlos cuando se lo requiera o lo establezca la política. Tanto este principio como el anterior tienen la desventaja de que aumentan considerablemente la carga laboral del equipo de soporte técnico debido a los permisos que requiere el usuario para realizar sus actividades. Lo importante en ese sentido, es encontrar un equilibrio entre el nivel de seguridad requerido y el desempeño de los equipos o la fluidez en las actividades del personal.

- **Principio de compartimentación**

La base de la compartimentación es la idea de que mientras menos personas conocen los detalles de una tarea, equipo, misión, etc., el riesgo de que dicha información sea comprometida o caiga en manos incorrectas es menor.

Este principio se aplica en la seguridad informática de varias formas. En infraestructuras tecnológicas, por ejemplo, se suelen realizar segmentación de redes de acuerdo a unidades departamentales o procesos, creación de VLANs, VPNs y DMZ (zonas desmilitarizadas).

- **Principio de defensa en profundidad**

Es una estrategia de seguridad que consiste en implementar varias capas de protección a través de un sistema de información. Es una estrategia mucho más eficiente que otras soluciones ya que si un atacante ha atravesado una capa, los administradores tienen tiempo para implementar contramedidas que ayuden a contrarrestar el ataque o minimizar el impacto en las capas inferiores (Ec Council, 2020). Las capas que constituyen la defensa en profundidad son las siguientes:

- Políticas y procedimientos de seguridad

Establecer reglas y obligaciones con enfoque en la seguridad de la información. Debe comunicarse y ser entendible para todo el personal de una organización.

- Seguridad física y del entorno

Consiste en implementar mecanismos de vigilancia y control de acceso físico a las instalaciones de la organización.

- Defensa perimetral

Es el punto de contacto de la red interna de la organización con redes externas no confiables. Aquí es necesario implementar soluciones *firewall* de cualquier tipo y asegurar los accesos remotos a la red.

- Defensa de red

Se debe monitorear constantemente el tráfico que fluye por la red para detectar y prevenir ataques oportunamente. En este punto son útiles sistemas de detección y prevención de intrusiones.

- Defensa de equipos

Mantener los sistemas actualizados, con soluciones antivirus, e implementar medidas de seguridad básicas como claves de usuario, usuarios con privilegios limitados y restricción de navegación por internet.

- Defensa de aplicaciones

Utilizar metodologías de desarrollo de aplicaciones seguras, implementar mecanismos de autenticación y autorización a las aplicaciones.

- Defensa de datos

Usar mecanismos de encriptación de datos y copias de seguridad.

➢ **Principio de escalamiento de la autorización**

Está ligado al principio de seguro por defecto, el objetivo es llevar un control de acceso adecuado de los recursos de la organización, especialmente a aquellos considerados críticos. En estos casos, el acceso a activos críticos requiere el conocimiento y autorización expresa de un superior.

➢ **Principio de registro o seguimiento (accounting)**

Consiste en llevar un registro de la actividad del usuario (actividad en línea, uso de aplicaciones, ejecución de comandos, etc.) dentro de la organización. De esta forma se cohíbe al usuario a realizar acciones maliciosas, o de ser el caso, el seguimiento de cualquier incidente permite fácilmente encontrar al responsable. El monitoreo debe ser transparente al usuario y se lo puede gestionar con soluciones IDS.

2.2.7 Pruebas de Intrusión (Penetration Testing)

Según Santo Orcero (2018), una prueba de penetración o prueba de intrusión es un "procedimiento de auditoría de seguridad activa en el que con autorización del propietario de un sistema de información, el auditor de seguridad analiza el susodicho sistema buscando de forma proactiva agujeros de seguridad vulnerables".

Es necesario aclarar también, que las pruebas de intrusión no solo están enfocadas a equipos de cómputo únicamente, sino a sistemas de información concretos, en los que intervienen no solo los activos tecnológicos, sino el personal y los procedimientos de la empresa,

De Manera general, el pentest o prueba de intrusión consta de 2 fases macro o 2 etapas:

- Fase pasiva: Consiste principalmente en la recolección de datos e información acerca del objetivo, además de todas las actividades en las que no existe todavía una interacción directa con el mismo.

- Fase activa: Con la información obtenida en la fase previa, el *ethical hacker* o *pentester* simula un ataque hacia la infraestructura del objetivo.

El objetivo de la prueba de intrusión es el de verificar la efectividad de los controles de seguridad implementados, además de descubrir vulnerabilidades en la infraestructura de una organización que quizás pasaron desapercibidas, finalmente, el informe sirve de punto de partida para la elaboración de planes de acción y de mejora de los controles, la subsanación de vulnerabilidades y la mitigación de riesgos, incrementando de esta forma, los niveles de seguridad de la organización.

Herramientas tales como Kali Linux provee utilitarios completos para la ejecución de pruebas de intrusión, además de que brinda descripciones detalladas sobre como ejecutar las pruebas y el uso de las herramientas.

2.2.8 Frameworks, estándares, normas y metodologías

Además de las contramedidas que hemos revisado, de naturaleza técnica y no técnica, existen otras herramientas como marcos de trabajo y estándares, que, al ser implementados en una organización, permiten no solo incrementar los niveles de seguridad, sino mejorar de manera considerable el gobierno de TI de una empresa.

Un ***framework*** o marco de trabajo es un conjunto de criterios y prácticas que se han estandarizado para servir como referencia en la resolución de problemas similares futuros.

Un **estándar** es un conjunto de reglas o requisitos mínimos aceptables que debe cumplir un proceso con el fin de asegurar la calidad del servicio o producto final.

Una **norma** es una guía o lineamiento que se nos impone con el fin de ordenar un comportamiento o modo de operación.

En resumen, estas metodologías, a manera de plantilla, nos proveen de herramientas útiles a la hora de establecer procedimientos y controles que podemos personalizar de acuerdo a las necesidades de cada organización. De esta forma, simplificamos y estandarizamos procesos, aumentamos niveles de eficiencia, minimizamos errores, etc.

La norma ISO 27001, el CSF (*Cybersecurity Framework*) de la NIST y el CEH (*Certified Ethical Hacker*) del EC-Council son algunos de los ejemplos que están orientados a la seguridad de la información y a las auditorias de seguridad. En los siguientes apartados profundizaremos algunos de ellos para entenderlos de mejor manera.

2.3 CEH (Certified Ethical Hacker)

Si no deseas que los hackers invadan tu red, primero debes invadir su mente (Ec Council, 2020). Lo dice el EC-Council en la última versión de su programa *Certified Ethical Hacker*. CEH es un programa de profesionalización y certificación que valida los conocimientos y habilidades de los profesionales en la disciplina de seguridad de infraestructuras de red. Difiere de otras certificaciones de seguridad enfocándose en una perspectiva externa ya que, a decir de ellos, enseña a "pensar como *hackers*". El programa se encuentra disponible en más de 145 países y cuenta con más de 950 centros de entrenamiento autorizado.

En su última versión (v11), el EC-Council evalúa los conocimientos y habilidades de sus participantes en 20 temas de estudio, que van desde conceptos básicos de seguridad y redes de datos, análisis y evaluación, vulnerabilidades y tipos de ataques, contramedidas, herramientas, programas, procedimientos, metodología, legislación en temas de seguridad y ética, etc.

Por temas de alcance del presente estudio, vamos a revisar los capítulos que comprenden la metodología de *pentest* o *ethical hacking*, propuesta por el EC-Council en el programa CEH en su última versión.

2.3.1 Footprinting o reconocimiento

Es el primer paso que se sigue en el proceso de evaluación de un objetivo. Es la fase preparatoria del proceso de hacking ético y consiste en recolectar la mayor información posible sobre el objetivo con el fin de planificar y facilitar las fases posteriores.

2.3.1.1 Tipos de footprinting

- **Reconocimiento pasivo**

Consiste en recolectar información del objetivo a través de actividades que no involucran una interacción directa con el target por lo que es técnicamente más difícil y demorada que el reconocimiento activo, aunque permite al atacante pasar desapercibido. Algunas actividades del reconocimiento pasivo consisten en buscar información del objetivo y/o sus empleados en motores de búsqueda y redes sociales, google *hacking*, bolsas de empleos foros y demás.

- **Reconocimiento activo**

Por otra parte, el reconocimiento activo consiste en recolectar información a través de interacción directa con el objetivo. Si bien esta actividad puede resultar más útil que la anterior, el objetivo podría reconocer la actividad ya que interactuamos de manera abierta con su red de datos. Las actividades de reconocimiento activo pueden ser *whois lookups*, extraer información de DNS, *traceroute* análisis, ingeniería social, entre otras.

2.3.1.2 Información obtenida

El ejecutar *footprinting* en distintos niveles de red, nos provee de información importante y que nos puede servir para varios ataques que podemos ejecutar en las fases posteriores. La información más importante que podemos obtener es:

- Información de la organización
  - Detalle de los empleados (nombres, contactos, dirección, cargos).
  - Direcciones y número de teléfono de la organización.
  - Socios de la organización.
  - Antecedentes de la organización.
  - Tecnologías que utilizan.
  - Documentos legales, patentes, artículos de prensa y otros.
- Información de red
  - Dominios y subdominios.
  - Rangos de direcciones IP.
  - Topologías de red, routers y firewalls de confianza.
  - Registros Whois.
- Información de los sistemas
  - Sistemas operativos de los host y servidores.
  - Localización del data center y servidores.
  - Direcciones públicas de correo electrónico.
  - Nombres de usuario, contraseñas, etc.

2.3.1.3 Metodología de footprinting

Es el proceso que se sigue para recolectar la mayor cantidad de información posible sobre un objetivo, desde todas las fuentes disponibles y utilizando varias técnicas, las cuales pueden ser:

- A través de motores de búsqueda.
- A través de servicios web.
- A través de redes sociales.

- A través de sitios web.
- A través de correo electrónico.
- A través de Whois.
- A través de DNS.
- A través de la red.
- A través de ingeniería social.

2.3.1.4 Herramientas

Existen muchas herramientas que pueden hacer de la fase de reconocimiento, una actividad fácilmente ejecutable y que nos permiten obtener diferentes tipos de información sobre un objetivo, de varias fuentes. Entre algunas de las más importantes tenemos: Maltego, Recon-ng, FOCA, OSR Framework, Recon-dog, entre otras.

2.3.1.5 Contramedidas

Algunas acciones que podemos tomar para prevenir o contrarrestar los peligros de la fase de reconocimiento son:

- Desarrollar políticas de seguridad de la información para regular la información que pueden o no divulgar los empleados.
- Restringir el acceso a las redes sociales desde la red de la organización.
- Concientizar a los empleados sobre amenazas de seguridad de la información a través de entrenamientos y talleres para evitar ataques de ingeniería social y otros.
- Configurar los servidores para evitar fugas de información.
- Evitar revelar información crítica en notas de prensa, reportes anuales, catálogos, etc.
- Limitar y controlar la información publicada en sitios web.
- Usar técnicas de footprinting para descubrir y remover información sensible que se encuentre publicada en la web.
- Utilizar servicios de registro de dominio anónimos.

2.3.2 Escaneo de redes

La fase de escaneo es una forma extendida de la fase de reconocimiento, ya que todavía consiste en recolectar información y no hay una intrusión como tal a los sistemas del objetivo. En esta fase el atacante debe determinar que hosts se encuentran activos e inactivos con el

fin de reducir el tiempo de ejecución de la fase, y encontrar un punto de entrada hacia la infraestructura del objetivo. En otros términos, es una serie de procedimientos ejecutados para identificar hosts, puertos y servicios en una red.

2.3.2.1 Tipos de escaneo

- **Escaneo de puertos**

Es el proceso de examinar el estado de los puertos y los servicios que se encuentran en ejecución en un equipo. Consiste en el envío de secuencias de mensajes a un bloque de puertos específicos y analizar sus respuestas, las que nos dan información sobre el estado de los puertos y los servicios que pueden estar ejecutándose en un host. Este tipo de escaneo nos provee información relacionada al sistema operativo y a las aplicaciones que utiliza el objetivo.

- **Escaneo de redes**

Es el procedimiento por el cual se identifican los hosts activos en una red. A través de este escaneo podemos obtener un listado de hosts y direcciones IP activas.

- **Escaneo de vulnerabilidades**

Consiste en examinar un sistema por vulnerabilidades conocidas y, por lo tanto, si puede ser explotado. Un escáner de vulnerabilidades consta de un motor de búsqueda de vulnerabilidades y un catálogo con el cual compara los recursos escaneados.

2.3.2.2 Objetivos de la fase de escaneo

Algunos de los objetivos de la fase de escaneo son:

- Obtener una lista de los hosts activos, direcciones IP y puertos abiertos.
- Descubrir los sistemas operativos y arquitecturas que utiliza el objetivo. Esto también se conoce como "*fingerprinting"*.
- Descubrir los servicios que están en ejecución en el sistema objetivo.
- Identificar las aplicaciones que se encuentran en ejecución en un host, y su versión respectiva.
- Identificar las vulnerabilidades presentes en cualquiera de los hosts objetivo.

2.3.2.3 Metodología de la fase de escaneo

Generalmente la fase de escaneo sigue la siguiente secuencia:

- Identificación de host (activos, rangos de IP).

- Identificación de puertos y servicios (abiertos, en escucha y ejecución).
- Identificación de sistemas operativos o *fingerprinting* (OS, arquitectura, versión)

2.3.2.4 Herramientas

Algunas herramientas útiles para esta fase son: NMAP, Metasploit framework, NetScanTools Pro, Hping2/Hping3, ipscaner, fing y network, estos 3 últimos para dispositivos móviles

2.3.2.5 Contramedidas

Algunas contramedidas útiles en esta fase son:

- Utilizar IDS e IPS.
- Monitorear el tráfico ICMP.
- Configurar los firewalls para detectar y prevenir *ping sweeps*.
- Ejecutar herramientas de escaneo de puertos para comprobar la existencia de puertos disponibles, así como también la efectividad de los *firewalls*.
- Mantener el *firmware* de los equipos de red actualizados.
- Deshabilitar o modificar los banners de los sistemas.
- Ocultar las extensiones de las páginas web.

2.3.3 Enumeración

Una vez que tenemos una vista general de la red, sus equipos y servicios, lo siguiente es extraer nombres de usuarios, de equipos y grupos, tablas de ruteo, recursos de red y compartidos. En esta fase, el atacante establece una conexión activa con el sistema y envía consultas directas para obtener más información. La información recolectada en esta fase permite identificar vulnerabilidades y explotarlas de una manera adecuada. Las técnicas de enumeración funcionan en un ambiente de intranet.

A continuación, algunos puertos y servicios relevantes a enumerar:

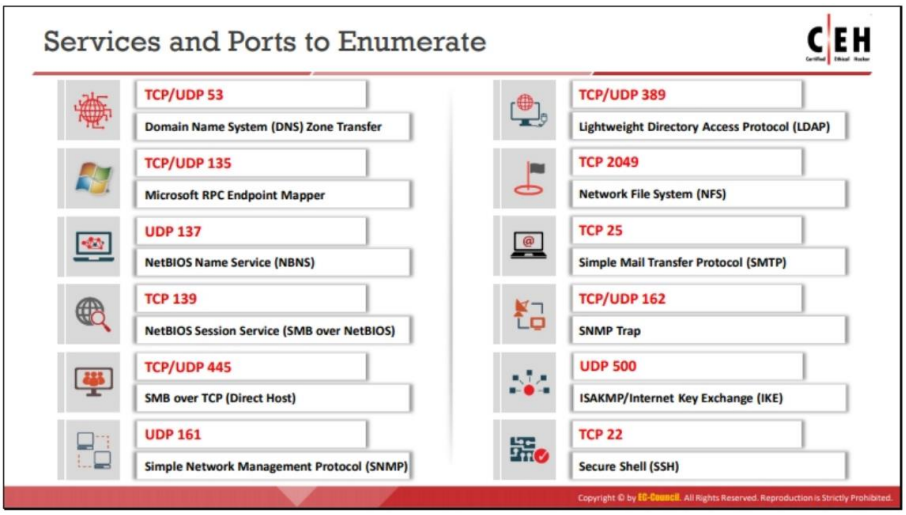


Figura 1. Puertos comunes. Fuente: CEH V.11

2.3.3.1 Tipos de enumeración

- **Enumeración de NETBIOS**

Netbios es un protocolo para la comunicación entre aplicaciones a través de la red. Para esto, establece las sesiones y mantiene activas las conexiones. Cuando de sistemas Windows se trata, lo primero que debemos hacer es la enumeración Netbios, ya que extrae una cantidad considerable de información relevante de la red del objetivo. Es un protocolo antiguo e inseguro ya que se encuentra en ejecución aun sin estar en uso.

Con la enumeración de Netbios podemos obtener:

- El listado de equipos que pertenecen a un dominio.
- Una lista de los recursos compartidos en un equipo de una red.
- Políticas y contraseñas.
- Un atacante también podría leer o escribir a un sistema remoto e incluso lanzar un ataque DOS.

Algunas de las herramientas más útiles en este tipo de enumeración son: NetBIOS Enumerator, Nmap, PsTools y Net View.

- **Enumeración SNMP**

SNMP (simple network management protocol) es un protocolo que permite a los administradores de red, administrar dispositivos de forma remota. El protocolo maneja una base de información de administración (MIB) que contiene descripción detallada de todos los dispositivos administrables como routers, switches, equipos, etc., además de recursos

compartidos y de red. La enumeración SNMP aprovecha las configuraciones por defecto de este protocolo para poder acceder a la MIB.

Herramientas utilizadas en este caso: Snmpcheck, SoftPerfect Network Scanner, OpUtils, Network Performance Monitor, PRTG Network Monitor y Engineer's Toolset.

- **Enumeración LDAP**

LDAP (Lightweight Directory Access Protocol) es un protocolo que gestiona la comunicación y la transferencia de datos entre los recursos de una red. LDAP puede acceder a servicios de directorio como *Active Directory* u otros y organiza la información en un orden lógico y jerárquico. Un atacante puede de forma anónima, realizar consultas al directorio LDAP por información sensible como nombres de usuario, direcciones, nombres de servidores y demás, que pueden ser aprovechados para la ejecución de ataques. Las herramientas comúnmente usadas en este tipo de enumeración son: Softerra LDAP Administrator, LDAP Admin Tool, LDAP Account Manager, LDAP Search, entre otras.

- **Enumeración NTP y NFS**

Network Time Protocol (NTP) sincroniza las configuraciones de hora en los dispositivos de una red. Network File System (NFS) es un sistema de archivos que permite a los usuarios acceder, visualizar, almacenar y actualizar archivos sobre un servidor remoto. Ambos protocolos almacenan listas de direcciones IP, información de host y sistemas operativos de sus clientes, NFS además almacena información sobre los recursos que comparte cada cliente. La Enumeración NTP y NFS utiliza varias técnicas para acceder a esas listas.

Entre las técnicas y herramientas útiles para este caso, encontramos: comandos de enumeración NTP, PRTG Network Monitor, Nmap, Wireshark y NTP Server Scanner para NTP, y, RPCScan y SuperEnum para NFS.

- **Enumeración SMTP y DNS**

Simple Mail Transfer Protocol (SMPT) es un protocolo simple para la transferencia de correos electrónicos. Ya que los servidores SMTP responden de manera distinta que los que trabajan con IMAP o POP3, los usuarios validos en un servidor SMTP pueden ser identificados. Utilizando técnicas de enumeración SMTP, un atacante puede fácilmente obtener listas validas de usuarios, direcciones de destino, etc. Las herramientas más comunes para este tipo de enumeración son NetScanTools Pro y smtp-user-enum.

Domain Name System (DNS) se usa principalmente para traducir las direcciones IP de internet en sus nombres de dominio respectivos. Entre las técnicas principales para la enumeración DNS están:

- Enumeración DNS por zonas de transferencia: Un atacante envía una solicitud de zone-transfer al servidor DNS, haciéndose pasar por un cliente. Si la opción está habilitada, el servidor DNS enviara de respuesta una porción de su base de datos como zona al atacante. Esta zona puede contener gran cantidad de información sobre las redes dentro de la zona del DNS. Las herramientas a utilizarse en este tipo de enumeración son: comando dig, comando nslookup y DNSRecon.
- DNS Cache Snooping: Un atacante realiza una consulta al servidor DNS por un registro de cache especifico. Este registro no puede ayudar a revelar información como el propietario del servidor DNS, su proveedor del servicio, el fabricante. Con esta información, el atacante puede aplicar métodos de ingeniería social en el objetivo. Las herramientas utilizadas para realizar este tipo de ataque son: comando dig, DNS Snoop Dog y DNSRecon.
- DNSSEC Zone Walking: es una técnica de enumeración DNS en la que el atacante intenta obtener registros internos de una Zona DNS si la zona no está configurada apropiadamente. La información obtenida por medio de este método ayuda al atacante a construir un mapa de la red. Se utilizan herramientas como: LDNS, DNSRecon, nsec3map, nsec3walker y DNSwalk.

➢ **Otras técnicas de enumeración**

Las anteriores expuestas, son las más comunes, sin embargo, existen varias técnicas de enumeración de las cuales vamos a dar algunos ejemplos:

- Enumeración IPsec
- Enumeración VoIP
- Enumeración Telnet
- Enumeración SSH user
- Enumeración FTP
- Enumeración SMB

2.3.3.2 Contramedidas

- Cambiar los valores por defecto de los dispositivos que utilizan SNMP.

- Utilizar los protocolos actualizados (en su última versión).
- Deshabilitar DNS zone transfer para host desconocidos.
- Utilizar servicios de registro DNS que permitan ocultar la información sensible.
- Configurar los servidores SMTP para ignorar los correos dirigidos a recipientes desconocidos.
- Utilizar SSL o STARTTLS en servidores LSAP para encriptar la transmisión de datos.
- Deshabilitar el protocolo SMB en servidores web y DNS.
- Deshabilitar los puertos TCP 139 y 445 que son utilizados por SMB.
- Implementar permisos apropiados de lectura y escritura en servidores NFS.
- Bloquear a través de firewall el puerto 2049 utilizado por NFS.
- Implementar SFTP o FTPS para encriptar el trafico FTP de la red.
- Asegurarse que la subida de archivos sin restricción en el servidor FTP, no está permitida.
- Restringir el acceso por IP o nombre de dominio al servidor FTP.

2.3.4 Análisis de vulnerabilidades

El análisis de vulnerabilidades consiste en la búsqueda de debilidades de seguridad en un sistema informático, la calificación de esas vulnerabilidades según la severidad, y las acciones a seguir para mitigar o remediar esas vulnerabilidades.

2.3.4.1 Clasificación de las vulnerabilidades

Las vulnerabilidades tienen una clasificación muy variada, la cual, generalmente depende de su origen y naturaleza (ver tabla 3).

Tabla 4. Clasificación de las vulnerabilidades. Fuente: (Ec Council, 2020)

Tipo	Descripción
Mala Configuración	Es la más común, y es generalmente causada por errores humanos intencionados o no intencionados. Las fallas en la configuración son comunes en servidores web, aplicaciones, bases de datos y redes
Instalaciones por defecto	Ocurre cuando se prioriza la usabilidad antes que la seguridad en la instalación de hardware o software. El no cambiar las configuraciones por defecto en el primer uso, facilita la tarea de un atacante para ingresar a un sistema sin autorización
	Son vulnerabilidades comunes de software que ocurren por errores de código que permiten a un atacante sobrepasar el tamaño asignado del

Buffer overflows	buffer hacia bloques de memoria contiguos en donde puede ejecutar instrucciones para obtener privilegios en el host objetivo
Servidores sin parches	Generalmente, los parches corrigen fallas de seguridad existentes en los sistemas. Al utilizar servidores sin los últimos parches o actualizaciones, comprometemos la seguridad e integridad de toda la información en el sistema y la red
Fallas de diseño	Aplican para todo tipo de dispositivo y sistema. Encriptación y validación incorrecta de los datos dejan fallas en la funcionalidad de un sistema los cuales pueden ser explotados por un atacante
Fallas en los sistemas operativos	La instalación de aplicaciones desconocidas, el no actualizar los sistemas operativos que utilizamos, aumenta el riesgo de infección de malware y ataques informáticos
Fallas en las aplicaciones	Las aplicaciones defectuosas representan una falla de seguridad. Es por esto que los desarrolladores deben conocer y considerar las vulnerabilidades de seguridad comunes a la hora de desarrollar aplicaciones
Servicios abiertos	Servicios y puertos abiertos de forma innecesaria pueden ser la entrada de ataques DOS o de otro tipo
Contraseñas por defecto	Los fabricantes establecen claves por defecto para la configuración inicial de sus dispositivos. Es necesario actualizar estas claves con claves fuertes ya que, de lo contrario, nuestros dispositivos son vulnerables a accesos no autorizados

2.3.4.2 Metodología del análisis y evaluación de vulnerabilidades

La evaluación de vulnerabilidades sigue la siguiente lógica:

1. Examinar y evaluar la seguridad física.
2. Buscar por fallas en las configuraciones y errores humanos.
3. Ejecutar herramientas de análisis de vulnerabilidades.
4. Seleccionar el tipo de escaneo de acuerdo a la organización y los requerimientos.
5. Identificar y priorizar vulnerabilidades.
6. Identificar falsos positivos y falsos negativos.
7. Relacionar los resultados con el contexto tecnológico y de negocio.
8. Realizar recolección OSINT de datos y validar con las vulnerabilidades encontradas.
9. Crear un reporte del escaneo de vulnerabilidades.

2.3.4.3 Métodos de análisis y evaluación de vulnerabilidades.

- Análisis y evaluación Activa: Utiliza escáneres de red para encontrar equipos, servicios y vulnerabilidades.
- Análisis y evaluación Pasiva: Utiliza *sniffers* de red para descubrir sistemas, redes, y vulnerabilidades.
- Análisis y evaluación Externa: Evalúa las vulnerabilidades de la red desde la perspectiva de un hacker, o que son accesibles desde la parte externa de la red.
- Análisis y evaluación Interna: Escanea la infraestructura interna de la red para descubrir *exploits* y vulnerabilidades.
- Análisis y evaluación Basada en Host: Realiza una comprobación de los hosts de la red a nivel de configuraciones en busca de fallas.
- Análisis y evaluación Basada en Red: Determina y evalúa las fallas presentes en la red de una organización.
- Análisis y evaluación de Aplicaciones: Realiza un análisis de las aplicaciones presentes en una infraestructura en busca de fallos en la configuración, uso de versiones inseguras y vulnerabilidades conocidas.
- Análisis y evaluación de Bases de Datos: Comprueba los motores de bases de datos en busca de información expuesta o vulnerabilidades de tipo inyección.

Existen otros tipos de análisis y evaluación de vulnerabilidades cada uno con su orientación y enfoque, como inalámbrica, distribuida, acreditada, no acreditada, manual y automática.

2.3.4.4 Herramientas para el análisis y evaluación de vulnerabilidades

Algunas herramientas útiles en esta fase son: Qualys Vulnerability Management, Nessus Profesional, GFI LanGuard, Open VAS, Nikto, entre otras.

2.3.4.5 Contramedidas

Como contramedidas tenemos las soluciones basadas en productos, que se encuentran en el apartado anterior, y las soluciones basadas en servicios, que consisten en contratar equipos de auditoria o empresas de seguridad especializadas en este tipo de actividad.

2.3.4.6 Reporte del análisis de vulnerabilidades

Al finalizar esta fase es siempre importante realizar un reporte de las amenazas encontradas. Herramientas como Nessus, GFI LanGuard y otras, contienen módulos para la elaboración de reportes, los cuales son personalizables a diferentes formatos. El reporte es relevante para la organización ya que revela sus debilidades, anticipa ataques y sugiere la toma de

contramedidas. Las vulnerabilidades se clasifican por su nivel de severidad en Alta, Media y Baja.

El reporte de vulnerabilidades debe por lo menos incluir la siguiente información:

- Información del método de escaneo (Herramienta utilizada, versión y puertos a escanear)
- Información del, o los objetivos (nombre de host, dirección, sistema operativo y fecha en la que se escaneo el host)
- Servicios (los servicios escaneados, nombre y número de puerto)
- Clasificación del test.

De la misma forma, las vulnerabilidades encontradas, deben reportarse con la siguiente información:

- Nombre de la vulnerabilidad y el ID en la CVE.
- Fecha de descubrimiento.
- La calificación que consta en la base de datos CVE.
- Una descripción detallada de la vulnerabilidad.
- El impacto de la vulnerabilidad.
- Detalles sobre el equipo afectado.
- Detalles para el control de la vulnerabilidad como parches, correcciones de configuración o puertos a ser bloqueados.
- De ser posible, una prueba de concepto de la vulnerabilidad en el sistema.

2.3.5 System Hacking

Con toda la información recolectada en las fases anteriores, el atacante procede a la fase más importante, y en algunos casos la última: la vulneración del sistema. El comprometer la seguridad de un sistema le permite a un atacante alcanzar sus objetivos.

La metodología de esta fase, sigue los siguientes pasos:

2.3.5.1 Obtener acceso

En esta fase, el atacante primero debe obtener el acceso a un sistema objetivo, para hacerlo, se apoya de algunas técnicas existentes:

- **Password cracking**

Es el proceso de recuperar una contraseña desde los datos transmitidos por un sistema o que se almacenan en el mismo. Una contraseña puede recuperarse de varias formas (ver tabla 4), simplemente adivinando por suposición o utilizando herramientas de software que automatizan este proceso.

Tabla 5. Tipos de password attack. Fuente: (Ec Council, 2020)

Tipo	Descripción
Ataque no técnico	El ataque no precisa de herramientas tecnológicas (ingeniería social, *shoulder surfing, dumpster diving*)
Ataque activo y en línea	requiere de interacción directa con el equipo de la víctima (diccionario, fuerza bruta, *hash injection*, malware, etc)
Ataque pasivo y en línea	El atacante trata de recuperar una clave sin interactuar con el equipo de la víctima (*Wire sniffing, Man-in-the-middle attack*, etc)
Ataque fuera de línea	El atacante copia el archivo que contiene una clave y ejecuta *password cracking* en otro lugar (*rainbow table attack, distributed network attack*)

Algunas herramientas útiles para *password cracking* son: L0phtCrack, ophcrack, *Rainbowcrack*, entre otras.

- **Explotar vulnerabilidades**

Un atacante debe primero descubrir una vulnerabilidad en un sistema para luego desarrollar un *exploit*, que, al ejecutarlo, le permita el acceso a un host objetivo. Ahora, esto involucra todo un proceso, que vamos a revisar a continuación:

1. Identificar la vulnerabilidad.
2. Determinar el riesgo asociado con la vulnerabilidad.
3. Determinar la capacidad de la vulnerabilidad.
4. Desarrollar el *exploit*.
5. Seleccionar el método para la entrega (local o remoto).
6. Generar y entregar el *payload*.
7. Obtener acceso remoto.

Para explotar vulnerabilidades, un atacante puede ejecutar *buffer overflow* en cualquiera de sus métodos o también acudir a uno de los varios sitios web o bases de datos de vulnerabilidades y *exploits* en internet, en donde puede descargar o desarrollar *exploits* y

ejecutarlos en un objetivo. Algunos sitios conocidos son: Exploit Database, Security Focus, VulDB y MITRE CVE.

- **Ingeniería social**

El factor humano continúa siendo el eslabón más débil en la cadena de la ciberseguridad (Greavu Serban & Serban, 2014). Es ahí donde se enfoca la ingeniería social. Esta disciplina no técnica, pretende manipular a las personas a través de métodos de persuasión, de modo que revelen información importante acerca de su objetivo. Las medidas de protección técnicas no son efectivas contra este tipo de ataques (Krombholz et al., 2015).

Entre los métodos más comunes de ingeniería social se encuentran el *phishing, spam, baiting*, *tailgating, dumpster diving y shoulder surfing*, entre otros.

2.3.5.2 Escalar privilegios

Es la segunda etapa en la fase de *system hacking*. Con las claves obtenidas en la etapa anterior, el atacante intenta elevar sus privilegios en el sistema objetivo.

A través de un ataque de elevación de privilegios, el atacante puede tomar ventaja de fallas de diseño, errores de programación, *bugs*, y fallas de configuración en el sistema operativo y las aplicaciones para ganar privilegios de administrador, lo que le dará acceso a ver, modificar, eliminar información sensible, o instalar malware en el sistema.

La elevación de privilegios se divide en 2 tipos:

- **Horizontal**

Se refiere a obtener los mismos privilegios que ya han sido obtenidos, asumiendo el rol de otro usuario con el mismo nivel de privilegios. El objetivo es acceder a la información y recursos de otro usuario, por ejemplo: los datos de su cuenta bancaria.

- **Vertical**

El atacante intenta ganar privilegios mayores a los que posee actualmente con el fin de poder acceder a información crítica o ejecutar algún tipo de malware.

- **Métodos y herramientas**

Existen varias formas de escalar privilegios en un sistema, como explotar vulnerabilidades (que podemos encontrar en una de las bases que revisamos anteriormente) o utilizar herramientas. Algunas herramientas importantes para esta actividad son: BeRoot, linpostextp, entre otras.

2.3.5.3 Mantener acceso

Una vez que se ha obtenido acceso al sistema y escalado los privilegios, el atacante intenta mantener el acceso y sus privilegios del sistema, para futura explotación del mismo o para perpetrar ataques a otros sistemas en la red. En esta fase un atacante puede hacer 2 cosas:

- **Ejecutar aplicaciones**

Los atacantes ejecutan varios tipos de malware de manera remota como *spyware* y *keylogger* a fin de poder robar información como nombres de usuario y contraseñas, o instalar *back doors*.

Existen varias herramientas para la ejecución remota de aplicaciones, que ayudan a los atacantes a instalar, ejecutar, eliminar o modificar los recursos dentro de un sistema objetivo. Algunas importantes son: RemoteExec, PsExec y Pupy.

En el caso de los *key loggers*, existen soluciones de hardware como pendrives que almacenan todas las pulsaciones de teclado en un archivo de texto dentro del mismo. También hay soluciones de software importantes como Spyrix Keylogger Free, REFOG Personal Monitor, Elite keylogger, entre otros.

El spyware es otro tipo de malware comúnmente usado en esta etapa. Algunas soluciones útiles son: SpyAgent, PowerSpy, NetVizor, Spy Voice Recorder, Free2X Webcam Recorder, Phone Spy, mSpy para dispositivos con GPS, entre otros.

- **Ocultar archivos**

El paso siguiente que un atacante realiza en esta fase, es ocultar los archivos o los programas maliciosos que ejecuta, para evitar que aplicaciones de protección como antivirus, antispyware y otras, adviertan de su presencia y pongan en riesgo toda la operación.

De entre las herramientas más importantes para ocultar la actividad maliciosa de un atacante se encuentran:

- *Rootkits*
- *NTFS Streams*
- Esteganografía

2.3.5.4 Eliminación de rastros

Como instancia final, el atacante debe remover toda evidencia de su actividad maliciosa en el sistema comprometido, aun si decidiera seguir explotándolo, de tal manera que pueda permanecer encubierto y evitar ser rastreado.

En esta fase, es tarea del atacante, hacer que el sistema aparente el no haber estado comprometido por actividad maliciosa. Para esto, debe devolver los logs, archivos de configuración y demás, a su estado previo al ataque.

Técnicas utilizadas para eliminar rastros:

- Deshabilitar la auditoria: El atacante deshabilita las capacidades de auditoria del equipo comprometido.
- Limpiar los logs: El atacante limpia o elimina las entradas correspondientes a sus actividades.
- Cubrir los rastros en la red: El atacante utiliza técnicas como reverse HTTP shells, reverse ICMP tunnels, DNS tunneling y otras para cubrir sus rastros en la red.
- Cubrir los rastros en el sistema operativo: Utilizar NTFS streams para esconder archivos y actividad maliciosa en el host comprometido.
- Eliminar archivos: Utilizar herramientas como Cipher.exe para eliminar datos y prevenir su futura recuperación.
- Deshabilitar funcionalidades de Windows: tales como timestamp, hibernación, memoria virtual y puntos de restauración para cubrir sus rastros.

Algunas herramientas útiles a la hora de eliminar los rastros son: CCleaner, DBAN, Privacy Eraser, Wipe, ClearProg, entre otras.

Como se evidenció, el trabajo completo de un atacante no es solo comprometer el sistema de manera exitosa, sino también eliminar sus rastros y cualquier evidencia que pudiera servir para rastrearlo y perjudicarlo en un futuro.

2.4 PTES (Penetration Testing Execution Standard)

Es una metodología para el desarrollo de pruebas de intrusión, desarrollada por un grupo de practicantes y profesionales de todas las áreas (Finanzas, proveedores de servicios, fabricantes, etc.) en el año 2009.

El estándar está orientado a servir de línea base, tanto para proveedores de servicio involucrados en este tipo de actividades, así como también a empresas que requieren contratar este tipo de servicios. Se diferencia de otras metodologías en que se enfoca en identificar el "riesgo de negocio" asociado con una vulnerabilidad.

Consiste de 7 fases que tratan de cubrir todo lo relacionado a las pruebas de intrusión, desde las interacciones previas al compromiso, en donde se define el alcance y los temas legales, hasta la explotación y reporte del test, en donde se captura todo el proceso de un modo que provea valor técnico y de negocio para el cliente.

Por ultimo. Ya que el estándar PTES no provee lineamiento técnico para la ejecución del test, han elaborado una guía técnica con recomendaciones, que se encuentra disponible en su sitio web.

Las fases del PTES son:

2.4.1 Interacciones previas al compromiso

Sin duda la fase más subestimada dentro del proceso de una prueba de penetración, cuando en realidad debería ser la más importante. La prueba de esto es que, muy poco se ha dedicado dentro de la literatura a esta fase. Las interacciones previas al compromiso tienen el potencial de causar varios problemas de alcance, insatisfacción en los clientes, e incluso problemas legales, si no son abordadas adecuadamente.

Esta fase pone especial esfuerzo en definir el alcance y establecer una estructura de costos. Ambos tienen que ser muy específicos en cuanto a las actividades que se van a realizar. Además, el PTES recomienda basar los costos de las actividades en trabajo realizado. Es importante también en esta fase, que el cliente tenga claro que es lo que necesita ser testeado, y que es lo que espera del test. De allí, que es necesaria la intervención del pentester o consultor, quien servirá de guía en lo que, muy probablemente, sea terreno desconocido para el cliente.

Las consideraciones del PTES para esta fase son:

- Definir métricas para estimar el tiempo.
- Establecer una reunión para definir el alcance (lo más específico posible).

- Proveer al cliente de una tarifa por hora para el caso de actividades que no constan en el alcance.
- Los cuestionarios que facilita el PTES pueden ayudar al pentester a resolver varias dudas sobre lo que cliente espera obtener del pentest.
- Aumento descontrolado del alcance.
- Reglas del compromiso (*Rules of engagement,* determinar las reglas bajo las que se va a ejecutar el test).
- Especificar fechas de inicio y fin.
- Especificar horarios para ejecución de las actividades.
- Especificar rangos de IP y dominios.
- ISP, Servicios en la nube y de terceros (se debe pedir autorización a los propietarios de los servicios para la ejecución del test, en el caso de *ISPs,* pueden bloquear el tráfico malicioso cuando el test está en ejecución).
- Comunicación de la información (periodicidad para la entrega de reportes y en que formatos).
- Términos para el pago (fechas y condiciones).

Solo luego de haber llegado a un entendimiento con el cliente, elaborado todos los documentos, y se cuenta con la autorización legal para ello, procedemos con la siguiente fase.

2.4.2 Recolección de información

Esta fase corresponde con la de reconocimiento en el proceso genérico de un pentest. Como se vio anteriormente, consiste en recolectar la mayor cantidad de información posible sobre un objetivo, con el fin de aumentar los vectores de ataque que podrían usarse en fases posteriores. Una técnica comúnmente utilizada en esta fase es *OSINT*, que consiste en recolectar información de fuentes públicamente abiertas.

El PTES clasifica las fuentes de recolección de información en 3 niveles, y para hacerlo, considera variables como tiempo, esfuerzo y actividades requeridas. De allí tenemos:

- Nivel 1: Esfuerzo mínimo. La información en este nivel puede ser obtenida por una herramienta automatizada.

- Nivel 2: Esfuerzo medio: La información se obtiene de la misma forma que el nivel 1 y un análisis básico con un buen entendimiento del negocio.
- Nivel 3: Esfuerzo alto: Se aplican las técnicas de los niveles 1 y 2, y se realiza un análisis más profundo. Se establecen relaciones del negocio y se obtiene información más pulida.

Consideraciones del PTES para esta fase:

- Identificación profunda del objetivo (investigar por empresas más pequeñas propiedad del objetivo y otros dominios de nivel superior que podrían haber quedado fuera del alcance, para reconsideración).
- Basarse siempre en las reglas del compromiso para mantenerse enfocado y evitar contratiempos.
- La duración del tiempo.
- El objetivo del test.
- Inteligencia de fuentes abiertas (*OSINT*).

Por su parte, basándose en la experiencia de todos sus miembros, el PTES provee en su sitio web, una vasta colección de fuentes y métodos para recopilar información, clasificadas y calificadas de acuerdo a los niveles previamente analizados, con el fin de facilitar la labor de un auditor. Entre algunas de las fuentes tenemos, infraestructura física, tecnológica, de la organización, financiera, etc.

2.4.3 Modelado de amenazas

“El análisis de modelo de amenazas (TMA) es un análisis que ayuda a determinar los riesgos de seguridad que pueden acaecer en un producto, aplicación, red o entorno, así como la forma en la que se aparecen los ataques. El objetivo consiste en determinar cuáles son las amenazas que requieren mitigación y los modos de hacerlo.” (Microsoft, s/f)

En otras palabras, se trata de anticipar cualquier tipo de ataque, considerando el valor de los activos para los atacantes, cuanto les costaría llegar a comprometerlos, bajo qué circunstancias podrían hacerlo y el impacto que tendría la perdida de esos activos.

Para esto, el estándar se centra en 2 elementos tradicionales del modelado de amenazas: activos y atacantes. Los activos a su vez, se clasifican en Activos de negocio y Procesos de negocio. En este sentido, el modelado de amenazas resulta beneficioso no solo para la

auditoria en sí, sino para la organización, ya que le permite reconocer el valor de sus activos, y priorizarlos.

Martí & Lloret (2016), afirman que el PTES no especifica una metodología para el modelado de amenazas, únicamente indica que debe ser consistente y repetible para futuros test. Sin embargo, existen varias metodologías especificas disponibles en la web como el *Security Development Lifecycle* o el OSSTMM.

- **Proceso del modelado de amenazas de alto nivel**

1. Recopilar información relevante.
2. Identificar y categorizar activos, primarios y secundarios.
3. Identificar y categorizar amenazas y grupos de riesgo
4. Emparejar los activos con los grupos de riesgo.

- **Análisis de los activos de negocio**

Los activos de negocio son aquellos activos que pueden resultar de gran valor para un atacante. Es necesario analizar la documentación conjuntamente con el personal de la organización para poder identificarlos.

Se consideran activos de negocio la información de los productos (patentes, etc.), información financiera, información sobre el personal y sobretodo información sobre la infraestructura de los sistemas, redes, aplicaciones y demás datos técnicos.

- **Análisis de los procesos de negocio**

Se consideran procesos de negocio, aquellos que añaden valor al conocimiento o materias primas de una organización, transformándolas en bienes o servicios. Con esto en cuenta, los procesos y los activos de negocio forman cadenas de valor, las que debemos conocer, para comprender en qué forma nos puede perjudicar un determinado grupo de riesgo.

- **Clasificación de los grupos de riesgo**

Al identificar los grupos de riesgo, es necesario clasificarlos en internos y externos. El PTES provee la siguiente tabla:

*Tabla 6. Grupos de riesgo PTES. Fuente: (*The Penetration Testing Execution Standard*, s/f)*

Internos	Externos
Empleados	Socios empresariales
Dirección (ejecutiva o gerencia)	Competidores
Administradores (red, sistemas o servidores)	Contratistas

Desarrolladores	Proveedores
Ingenieros	Estados nacionales
Técnicos	Crimen organizado
Contratistas	Hacktivistas
Comunidad de usuarios en general	Script kiddies
Soporte remoto	

Luego que se ha identificado el grupo de riesgo, debemos considerar la capacidad de dicho grupo en términos de conocimientos, acceso a herramientas y motivos por los que quisiera perjudicar a la organización, a fin de crear un modelo que refleje la posibilidad de un ataque exitoso de su parte (Martí & Lloret, 2016) y establecer estrategias sobre como mitigarlos.

2.4.4 Análisis de vulnerabilidades

Recapitulando, una vulnerabilidad es una debilidad de un recurso tecnológico que lo expone a un ataque o acceso no autorizado, y a su vez, atenta contra la confidencialidad, integridad y disponibilidad del mismo.

El PTES considera 3 etapas para el análisis de vulnerabilidades:

2.4.4.1 Pruebas

El proceso de pruebas consiste en buscar errores en sistemas o aplicaciones que pudieran ser aprovechadas por un atacante, como fallas de configuración o errores en el diseño de aplicaciones.

La prueba de vulnerabilidades puede dividirse en activa (interacción necesaria con el objetivo) y pasiva (sin interacción con el objetivo). De la misma forma, la interacción puede ser automática (con el uso de herramientas) o manual.

Existen varios tipos de herramientas automatizadas con distintos enfoques en cuanto a la tecnología a la que se orientan y al tipo de prueba que ejecutan. Algunas de ellas como NMAP, OpenVAS, NESSUS, Wireshark, Yersinia, y Burp Suite son verdaderamente útiles.

2.4.4.2 Validación

El proceso de validación consiste en establecer correlaciones entre los resultados que arrojan las herramientas utilizadas. Se clasifica en correlación específica, y correlación categórica:

- **Correlación específica.**

Hace referencia a una vulnerabilidad concreta, ya sea un error conocido en un software o una vulnerabilidad indexada en una base de datos (CVE, OSVDB, etc.).

- **Correlación categórica.**

Se relaciona con estructuras categóricas que permiten agrupar elementos por macro factores, como tipos de vulnerabilidades, errores de configuración, etc. Un ejemplo sería agrupar todos los equipos encontrados con contraseñas por defecto, en el grupo de complejidad de las contraseñas dentro de la NIST 800-53 (IA-5) (*The Penetration Testing Execution Standard*, s/f).

Por último, es necesario considerar todos los vectores de ataque, para lo que se recomienda la elaboración de árboles de ataque, los que además de servirnos de guía para la fase siguiente, nos serán de gran utilidad para la fase de reporte (Martí & Lloret, 2016).

2.4.4.3 Investigación

Luego que se ha descubierto una vulnerabilidad, es necesario identificarla con exactitud y estimar la posibilidad de ocurrencia y el daño potencial dentro del alcance del test. Existen varias herramientas que nos facilitan la labor de investigación, como las bases de datos de vulnerabilidades, las guías de fortificación, sitios web y foros especializados. También debemos revisar los equipos y sistemas en busca de fallas de configuración, contraseñas y configuraciones por defecto. En algunos casos resultarán ser vulnerabilidades conocidas, y en otros casos podrán ser errores humanos como fallas de configuración, contraseñas por defecto, entre otras.

El objetivo de esta fase es priorizar las vulnerabilidades encontradas según su gravedad y organizarlas en un árbol de ataque que nos servirá en la fase de explotación (Martí & Lloret, 2016).

2.4.5 Explotación

Esta fase se enfoca en establecer acceso a un sistema o recurso pasando por alto sus seguridades, por lo que su objetivo principal es encontrar una entrada a la infraestructura de la organización e identificar sus activos de mayor valor. Si la fase anterior se ejecutó de manera adecuada, esta fase deberá estar bien planificada y ejecutarse sin problemas.

Al ejecutar un *exploit*, es necesario considerar varios factores como las seguridades y contramedidas (firewalls, IDS, IPS, medidas preventivas, etc) que se han implementado en la organización para prevenir este tipo de ataques. Por lo que, si queremos continuar inadvertidos, debemos considerar métodos alternativos de explotación. En el mejor de los casos, deberíamos haber enumerado (técnicas de enumeración) a priori, las contramedidas y seguridades.

Dicho esto, es fácil darse cuenta la cantidad de escenarios posibles para un ataque. Cada organización posee distintas tecnologías, sistemas, hardware, políticas de seguridad y utiliza

distintas contramedidas. Cada caso es distinto. Por tal motivo y con el objeto de ser exitosos en esta fase, es necesario desarrollar una estrategia a la medida, basada en cada escenario.

La intención de un pentest es simular un ataque real, por consiguiente, no se busca explotar todas las vulnerabilidades encontradas, ya que resultaría ruidoso y alertaría al equipo de seguridad. Este enfoque es útil al final de la prueba de penetración ya que nos permite comprobar la capacidad de respuesta del equipo de seguridad. En la mayoría de los casos, la fase de explotación se orienta en la acumulación de investigación especifica de un objetivo (*The Penetration Testing Execution Standard*, s/f).

Una herramienta esencial para esta fase es *Metasploit Framework*, aunque también podemos ayudarnos de herramientas similares, bases de datos de vulnerabilidades o servicios de acceso remoto como SSH o VNC.

Finalmente, debemos ser muy cautelosos a la hora de ejecutar un *exploit*, sobre todo si es descargado de internet, ya que podría hacer más de lo que dice hacer. Sin querer, podríamos estar provocando daños irreparables en los equipos y sistemas de una organización por lo que se recomienda primero, realizar pruebas de los *exploits* descargados, en un ambiente controlado (Martí & Lloret, 2016).

2.4.6 Post Explotación

La fase de post explotación consiste en valorar el equipo comprometido, basándose en la criticidad de la información contenida dentro de este, y la utilidad del equipo para comprometer los recursos de red más adelante. Los métodos descritos en esta fase están diseñados para ayudar al auditor a identificar información sensible, ajustes de configuración, y relaciones con los recursos de red que nos podrían ser útiles para mejorar el método de intrusión y la calidad del test.

2.4.6.1 Reglas de compromiso (Rules of engagement)

Las reglas del compromiso son específicas de esta fase y están diseñadas para asegurarse que los sistemas del cliente no están sujetos a riesgos innecesarios por las acciones del auditor. Como línea base, nos provee las siguientes recomendaciones:

- **Proteger al cliente**

1. A menos que se haya acordado previamente, no se modificaran servicios que el cliente considere “críticos” para su infraestructura. La única justificación válida para la modificación de los servicios, será para demostrar al cliente, en que forma un atacante

podría escalar privilegios, obtener acceso a información específica, o causar denegación de servicio.

2. Todas las modificaciones en las configuraciones de los sistemas deben ser documentados. Finalizado el test o el propósito del cambio, los mismos deben ser devueltos a la normalidad y se deberá entregar una lista al cliente con todos los cambios restituidos y con aquellos que no se pudieron devolver a su estado normal.
3. Se debe mantener una lista con todas las acciones tomadas a los sistemas comprometidos. Esta lista debe incluir, la información del equipo, la acción y el tiempo en que incurrió la acción. La lista deberá ser entregada al final del test a manera de apéndice.
4. Toda la información (privada o personal) obtenida en el test, será utilizada para conseguir más permisos y ejecutar acciones relacionadas con el test, únicamente si:
   a) La Política de Uso Aceptable del cliente establece que todos los sistemas y la información contenida dentro de los mismos son propiedad del cliente.
   b) La Política de Uso Aceptable establece que todo equipo conectado a la red del cliente se considera con consentimiento de ser analizado.
   c) El cliente tiene confirmación que todos sus empleados han leído y comprendido la Política de Uso Aceptable.
5. Ninguna de las contraseñas obtenidas será incluida en el reporte final, con el fin de resguardar la confidencialidad e integridad de la información y los sistemas.
6. Cualquier método, herramienta o dispositivo utilizado por el auditor que pudiera alterar la operación normal de los sistemas, no podrá ser implementado sin el consentimiento previo del cliente.
7. La información recolectada y que se almacena en el equipo utilizado por el auditor, debe ser encriptada.
8. La información sensible, presentada en el reporte, debe ser enmascarada a través de métodos que impidan su recuperación.
9. Toda la información recopilada en la prueba será destruida, posterior a la aceptación del cliente del reporte final. El método y las pruebas de la destrucción serán entregados al cliente.

10. Si la recopilación de datos está restringida por la ley de alguna forma, el auditor únicamente proveerá prueba de acceso a esa información.
11. No se compartirá ningún tipo de información ni se utilizará servicios de terceros para *password cracking*, sin el consentimiento previo del cliente.
12. Si al ejecutar la prueba, se encuentra evidencia de que los sistemas del cliente han sido comprometidos previamente, la evidencia respectiva será entregada de manera inmediata al cliente, quien determinará las acciones siguientes.
13. Ningún log será eliminado, saneado o modificado a menos que así lo haya solicitado el cliente. De serlo, se realizarán copias de seguridad de los logs, previo a cualquier cambio.

- **Proteger al equipo auditor**

1. Asegúrate que, en el contrato de trabajo, las acciones y métodos aplicados a los sistemas objeto de la prueba, son en nombre y en representación del cliente.
2. Solicita una copia de la Política de seguridad o Política de uso aceptable de la empresa, previo a la ejecución del test. Asegúrate que la política cubre la propiedad y derechos de la información, uso personal de equipos y almacenamiento de información de los empleados.
3. Encripta los drives y equipos que contienen información sobre el cliente.
4. Discute y establece con el cliente, el procedimiento a seguir en el caso de encontrar evidencia de ataques previos o sistemas previamente comprometidos por parte de terceros.
5. Revisa regulaciones y restricciones existentes sobre la captura y almacenamiento de datos (y demás actividades a ejecutarse), dentro del marco legislativo que rige sobre la organización.

2.4.6.2 Análisis de la infraestructura

Un equipo comprometido contiene información valiosa que nos puede servir para identificar configuraciones de la red, protocolos que utilizan y los servicios q consumen. Lo que debemos revisar en este punto son:

- **Configuraciones de red**

Interfaces, dirección IP, sub red, puertas de enlace. Esta información nos puede a su vez, servir de apoyo para identificar protocolos de ruteo, servidores DNS, servidores proxy, entradas ARP, etc.

- **Servicios de red**

Es necesario identificar los servicios de red que consume y ofrece el host comprometido. De esta forma podríamos descubrir servicios que no fueron detectados en la etapa de escaneo, y establecer relaciones con otros recursos de red que podrían resultar relevantes. También es necesario examinar conexiones VPN, servicios de directorio y los vecinos disponibles.

2.4.6.3 Expoliación

Esta actividad se refiere a obtener información de diversas fuentes, que pudiera resultar relevante para el test. El PTES considera fuentes de información crítica, las siguientes: programas instalados, servicios instalados, recursos compartidos, servidores de base de datos, servidores de directorio, autoridades certificadoras configuradas en el equipo, servidores DHCP, virtualización, mensajería, sistemas de respaldo, capturas de trafico de red, de pantalla y pulsaciones de teclado, información de usuario, configuraciones del sistema, políticas de seguridad, etc.

2.4.6.4 Intrusión profunda

Consiste en utilizar el sistema comprometido para enumerar y obtener acceso en otros sistemas del cliente. Esto se puede lograr a través de lo que se conoce como *footprinting* interno, para lo que podríamos ejecutar herramientas locales o cargadas en el host, ARP *scans*, *pig sweep*, enumeración interna de servicios, ataques de fuerza bruta, ejecución de *exploits*. También podríamos utilizar el host comprometido como *proxy* o VPN para la red interna, ejecutar *port forwarding* o *exploits* de manera remota. Las acciones tomadas en esta actividad dependerán de los requerimientos del test y los riesgos asociados.

2.4.6.5 Limpieza

Una vez concluido el test, es necesario hacer un saneamiento de los sistemas de la siguiente manera:

- Remover todos lo ejecutables, *scripts* y temporales de los hosts comprometidos. De ser posible, utilizar herramientas de eliminación segura de archivos.
- Devolver a su estado original, los parámetros de configuración del sistema y las aplicaciones en el caso que hayan sido modificadas durante el test.
- Remover los *backdoor* y *rootkits* instalados.

- Eliminar los usuarios creados en los sistemas durante el test.

2.4.7 Reportes

Aunque es altamente recomendable que cada equipo auditor o pentester desarrolle su propio formato de reporte con información personalizada de acuerdo a cada prueba realizada, esta fase provee criterios básicos que permitan presentar un trabajo entendible y de valor para el cliente. Para esto, el PTES desglosa el reporte final en 2 documentos:

- **Resumen ejecutivo**

Describe los objetivos específicos y los hallazgos del test en un nivel alto. Está dirigido a quienes están a cargo de la visión y la estrategia de la organización y del programa de seguridad, por lo que no debería contener muchos detalles técnicos, sino más bien enfocarse en como los problemas encontrados pueden afectar el negocio. También es una buena práctica incluir referencias al reporte técnico por si se requiere ahondar en detalles.

El PTES recomienda incluir en el resumen ejecutivo, siempre que sea posible, los siguientes:

1. Antecedentes

Presenta el propósito general del test, al igual que los objetivos relacionados al riesgo, contramedidas y a la ejecución del test. Los cambios también se incluyen en esta sección.

2. Situación general

Descripción general de la efectividad de la ejecución del test, y la habilidad del equipo de auditoria para conseguir los objetivos planteados en las fases iniciales. Se puede incluir una descripción general y breve de las faltas identificadas y el posible impacto al negocio.

3. Perfil de riesgo

En esta sección se identificará, describirá y explicará la calificación, perfil o ranking general del riesgo obtenido en el test. El método de calificación será definido entre el cliente y el equipo auditor, en la primera fase del test.

4. Hallazgos generales

Esta sesión presentara una sinopsis de los problemas encontrados durante el test en un formato básico y estadístico. Índices de efectividad y métricas de todo tipo, que se hayan definido en la primera fase del test, pueden incluirse en esta sección.

5. Recomendaciones

Esta sección deberá proveer un alto nivel de entendimiento del proceso requerido para resolver los riesgos identificados, así como también un nivel general del esfuerzo necesario para implementar la solución sugerida.

6. Hoja de ruta estratégica

Para la hoja de ruta es necesario elaborar un plan de remediación de los problemas encontrados, asignarles un peso o prioridad basándose en el impacto potencial y el objetivo del negocio. Para esto es necesario tomar de referencia la matriz de riesgos elaborada en la fase de modelado de amenazas. La hoja de ruta es una guía a seguir, ya que desglosa los objetivos en actividades y estima tiempos de cumplimiento.

- **Reporte Técnico**

Comunica los detalles técnicos del test y todos los aspectos acordados como indicadores clave de éxito en la primera fase del test. El PTES recomienda las siguientes secciones:

1. Introducción

Sirve de referencia específica para todos los recursos involucrados y el alcance técnico del test. Se orienta a ser un inventario inicial de:

- Personal involucrado en el test (equipo auditor y del cliente).
- Información de contacto.
- Activos involucrados en el test.
- Objetivos del test.
- Alcance del test.
- Enfoque.
- Estructura de calificación de amenazas.

2. Recolección de información

Lista la información (pública y privada) encontrada y los métodos utilizados en la fase de recolección de información. Los resultados deben presentarse en 4 categorías:

- Inteligencia pasiva.
- Inteligencia activa.
- Inteligencia corporativa.
- Inteligencia personal.

3. Evaluación de vulnerabilidades

Describe las vulnerabilidades encontradas, el método utilizado, y su clasificación. La información en esta sección debe incluir:

- Nivel de clasificación de las vulnerabilidades.
- Vulnerabilidades técnicas.
    - Capa OSI.
    - Encontradas por escáner.
    - Identificadas manualmente.
    - Exposición general.
- Vulnerabilidades lógicas.
    - No OSI.
    - Tipo de vulnerabilidad.
    - Como y donde se encontró.
    - Exposición.
- Resumen de resultados.

4. Confirmación de explotación

Describe de forma detallada el proceso realizado para explotar las vulnerabilidades encontradas previamente, y el nivel de acceso obtenido en el objetivo. También debe contener lo siguiente:

- Línea de tiempo de explotación.
- Objetivo seleccionado para explotación.
- Actividades realizadas para explotación.
    - Ataque directo.
        - Objetivos explotados sin éxito.
        - Objetivos explotados con éxito.
            - Información del host.
            - Ataques realizados.

- Ataques exitosos.
- Niveles de accesos concedidos (vía de escalamiento).
- Remediación.
  - Enlace de referencia a la sección de vulnerabilidades.
  - Técnicas adicionales de mitigación.
  - Sugerencias para compensar el control.

- Ataque indirecto.
  - Phishing.
    - Detalles y línea de tiempo del ataque.
    - Objetivos identificados.
    - proporción éxito / fracaso.
    - Niveles de acceso obtenidos.
  - Lado del cliente
    - Detalles y línea de tiempo del ataque.
    - Objetivos identificados.
    - proporción éxito / fracaso.
    - Niveles de acceso obtenidos.
  - Lado del navegador
    - Detalles y línea de tiempo del ataque.
    - Objetivos identificados.
    - proporción éxito / fracaso.
    - Niveles de acceso obtenidos.

5. Post explotación

Es una de las secciones más importantes ya que se enfoca en asociar las vulnerabilidades y su capacidad de explotación, con el riesgo real de negocio. Algunas formas de evidenciarlo son a través de capturas de pantalla y recuperación de contenido enriquecido. A continuación, algunos ejemplos de lo que se debe presentar en esta sección:

- Vía de escalamiento de privilegios.
    - Técnicas usadas.
- Adquisición de la información crítica definida por el cliente.
- Valor de la información.
- Acceso a los sistemas Core de negocio.
- Acceso a conjuntos de datos protegidos.
- Sistemas accedidos, información adicional.
- Habilidad de persistencia.
- Habilidad de exfiltración.
- Efectividad de las contramedidas.
    - Capacidad de detección.
    - Firewall / WAF / IDS / IPS
    - Humano.
    - Prevención de perdida de información (DLP).
    - Log
- Respuesta y efectividad.

6. Exposición y riesgo

Se combinan los resultados de la sección anterior con la valoración de los riesgos, criticidad de la información, valoración corporativa, y el impacto del negocio derivado de la primera fase, con el fin de proveer al cliente una visión de negocio (monetizar) de las vulnerabilidades encontradas y priorizarlas según sus objetivos. El PTES sugiere cubrir los riesgos de la siguiente forma:

- Evaluar la frecuencia de los incidentes.
    - Frecuencia probable del evento.
    - Estimar la capacidad de la amenaza (fase 3).
    - Estimar la efectividad de los controles (fase 6).
    - Vulnerabilidad compuesta (fase 5).
    - Nivel de destrezas requerido.

    - Nivel de acceso requerido.
- Estimar la magnitud de las perdidas por incidente.
    - Perdida primaria.
    - Perdida secundaria.
    - Análisis de la causa raíz del riesgo.
        - La causa raíz no es un parche.
        - Identificar procesos fallidos.
- Riesgo derivado.
    - Amenaza.
    - Vulnerabilidad
    - Superposición (Overlap).

7. Conclusiones

Se realiza una revisión general del test. Se debe incluir las partes más importantes y destacar las mejoras en cuanto a la postura de seguridad del cliente.

2.5 OSSTMM (The Open Source Security Testing Methodology Manual)

Es una metodología para la ejecución de pruebas de seguridad orientada a la medición de la seguridad en un nivel operacional. Como metodología, está diseñada para ser consistente, repetible y adaptable a cualquier tipo de auditoria (*ethical hacking*, evaluación de riesgo, etc.). Provee especificaciones detalladas para la ejecución de pruebas de seguridad sobre los llamados "canales operacionales" que incluyen Humano, Físico, Inalámbrico, Telecomunicaciones y Redes de datos, además de las instrucciones para la elaboración de métricas derivadas (ISECOM, 2010).

Fue creado por el ISECOM (Instituto para la seguridad y metodologías abiertas) en el año 2001 conjuntamente con la colaboración de más de 150 profesionales en seguridad y contempla, además, el cumplimiento de otras normas como ISO, NIST, ITIL, etc., por lo que lo convierte en un manual completo en el campo de las pruebas de penetración (Valdez Alvarado, 2013).

El ISECOM ofrece certificación y acreditación de las pruebas realizadas, que sirven como evidencia de facto de la ejecución de la prueba y responsabilizan al analista a cargo de su ejecución, entre otros. Para esto es necesario cumplir los requerimientos para la elaboración del reporte establecidos en el manual y enviarlos al ISECOM para su evaluación.

2.5.1 Definir el test

El ISECOM establece 7 pasos para definir el test de una manera adecuada.

1. Definir lo que se quiere proteger (activos). Se probarán los controles (mecanismos de protección de los activos) para identificar limitaciones.
2. Identificar la zona de compromiso (el área alrededor de los activos, mecanismos de protección, procesos, servicios).
3. Definir todo lo necesario para mantener los activos en estado operativo y que se encuentran fuera del área de compromiso. Esto puede incluir procesos, protocolos, recursos, contratos, socios comerciales, etc., y factores en los cuales no se pude influir como electricidad, agua, legislación, regulaciones, etc.
4. Identificar los vectores de prueba, al definir las diferentes interacciones dentro del alcance (por ejemplo, de adentro hacia afuera, de afuera hacia adentro, del departamento A al departamento B, etc.).
5. Identificar los recursos necesarios para la ejecución de las pruebas en cada vector y canal.

6. Determinar la información que quieres obtener del test (definir el tipo de test).
7. Asegurar que la definición del test está en cumplimiento con las reglas del compromiso.

2.5.2 Alcance

Se debe considerar como alcance a todos los posibles ambientes de seguridad operacional, por cada interacción con cualquier activo (ISECOM, 2010). Dicho en otras palabras, es necesario considerar todos los recursos tecnológicos y sus relaciones con otros activos dentro y fuera de una organización, desde un punto de vista operacional. Sin embargo, en la práctica, el alcance está determinado por la experticia del auditor, la disponibilidad de recursos y los requerimientos del cliente.

2.5.3 Canales

El alcance también considera los medios específicos con los que se interactúa con los activos. OSSTMM los llama canales y su clasificación se describe en la tabla 6.

Tabla 7. Canales OSSTMM. Fuente: (ISECOM, 2010)

Canal	Descripción
Humano	Es parte de la seguridad física (PHYSSEC) y comprende el elemento humano de las telecomunicaciones en donde la interacción es física o psicológica
Físico	También es parte de la seguridad física y comprende los elementos tangibles de la seguridad y que requieren interacción a través de esfuerzo físico
Inalámbrico	Es parte de la seguridad del espectro (SPECSEC) y comprende las señales electrónicas y emanaciones que tienen lugar en el espectro electromagnético
Telecomunicaciones	Es parte de la seguridad de las comunicaciones (COMSEC) y comprende las redes de telecomunicaciones digitales o analógicas
Redes de datos	También es parte de la seguridad de las comunicaciones y comprende todos los sistemas electrónicos y redes de datos

.

2.5.4 Tipos de test

OSSTMM define 6 tipos comunes de test que dependen de la cantidad de información inicial del objetivo con la que cuenta el auditor, o de las expectativas del cliente.

- **Blind (Ciego)**

El auditor empieza la auditoria sin ningún conocimiento sobre el objetivo o sus defensas. El objetivo conoce de antemano los detalles de la auditoria. El éxito de esta auditoria depende mucho del auditor, de sus conocimientos y experiencia.

- **Double blind**

El auditor comienza el test sin ninguna información sobre el objetivo o sus defensas. El objetivo no es notificado sobre el alcance, los canales o vectores de la prueba. Este tipo de prueba examina las habilidades del auditor, y la preparación del objetivo a distintas variables de agitación.

- **Caja gris**

El auditor inicia la prueba con conocimiento total sobre los canales, pero con conocimiento limitado del objetivo, sus defensas y activos. El objetivo conoce de antemano todos los detalles relativos a la prueba.

- **Doble caja gris**

El auditor inicia la prueba con conocimiento total sobre los canales, pero con conocimiento limitado del objetivo, sus defensas y activos. El objetivo conoce de antemano el alcance y los tiempos, pero no los canales ni vectores de ataque relativos a la prueba.

- **Combinado (Tándem)**

El auditor y el objetivo están preparados para la prueba con conocimiento total de los detalles relativos a la misma. Se enfoca en poner a prueba las protecciones y controles del objetivo de manera exhaustiva, sin embargo, no examina la preparación del objetivo a distintas variables de agitación.

- **Reversa**

El auditor inicia la prueba con total conocimiento de los detalles de seguridad operacional y los procesos del objetivo. El objetivo desconoce que, como y cuando el auditor ejecutara la prueba. El objetivo es probar el nivel de respuesta del objetivo a distintas variables y vectores de agitación.

2.5.5 Reglas del compromiso (Rules of engagement - ROE)

Definen las guías operacionales de prácticas aceptables dentro de la ejecución del test. La metodología provee varias recomendaciones para la elaboración de las ROE, clasificadas en 7 ejes principales que servirán de soporte para ejecutar de manera adecuada el test y evitar complicaciones futuras. Estos 7 ejes son:

- Ventas y marketing.
- Evaluación y estimación de la entrega.
- Contratos y negociaciones.
- Definición del alcance.
- Planificación del test.
- Ejecución del proceso.
- Reporte.

2.5.6 Métricas

OSSTMM utiliza el RAV (valor de evaluación de riesgo) como métrica de seguridad operacional. El RAV es una escala de medida de la superficie de ataque, de la cantidad e interacciones no controladas con el objetivo y se obtiene del balance cuantitativo entre las operaciones, limitaciones y controles. El RAV no provee información sobre si un objetivo podría ser atacado como lo haría el análisis de riesgo, más, sirve para conocer en que parte podría ser atacado, contra que ataques puede defenderse, y que tanto daño puede causar (ISECOM, 2010).

En esta escala, un RAV de 100 representa un balance perfecto, menos de 100, la falta de controles, y más de 100, más controles de los necesarios, lo cual añade interacciones y complejidad innecesaria en el proceso (Sierra, 2018).

El ISECOM ha provisto en su página web una herramienta basada en una hoja de cálculo prediseñada, para la elaboración de RAVs de manera fácil y rápida, en la cual únicamente, se debe ingresar los datos respectivos y la herramienta hará los cálculos de manera automática.

2.5.7 Fases

La metodología se basa en el proceso de 4 puntos, el cual descompone cualquier tipo de prueba, de inicio a fin. Las fases a su vez están compuestas por módulos específicos que en conjunto conforman la metodología, que veremos más adelante.

1. Inducción

Consiste en el análisis del entorno de la organización. La metodología clasifica la información obtenida en esta fase de la siguiente forma:

- Revisión de la postura: Consiste en la cultura, reglas, normativa, regulaciones, legislación y política que aplica sobre el objetivo, conocer el alcance y que test son requeridos.
- Logística: Consiste en identificar las restricciones del alcance y sus interacciones, con el fin de minimizar errores e incrementar la eficiencia.
- Verificación de detección activa: La verificación de la práctica y la amplitud de detección de interacciones.

2. Interacción

Conocer el alcance en función de las interacciones con los objetivos y con los activos. Consiste en interactuar con el objetivo, obtener repuestas y analizarlas.

- Auditoria de visibilidad: Identificar los objetivos existentes y cómo interactúan dentro del alcance.
- Verificación de acceso: Identificar los puntos de acceso a la organización y la autenticación utilizada.
- Verificación de confianza: Conocer las relaciones entre los objetivos para evaluar la importancia de las interacciones.
- Verificación de control: Identificar los controles establecidos a los procesos, su vigencia y relevancia.

3. Investigación

Consiste en identificar las emanaciones del objetivo o las marcas que deja a través de las interacciones dentro de su ambiente. Se lo realiza a través de:

- Verificación del proceso: Conocer el proceso, como trabaja y sus controles.
- Verificación de la configuración: Explora las condiciones por defecto bajo las que regularmente opera un objetivo, con el fin de entender la justificación de negocio y el razonamiento sobre los objetivos.
- Validación de la propiedad: Conocer el estado de la organización sobre los derechos de propiedad, el uso ilegal o sin licencia de propiedad intelectual o aplicaciones dentro del objetivo.
- Revisión de la segregación: Conocer los derechos de privacidad que aplican sobre la información personal recuperada en las pruebas.

- Verificación de la exposición: Descubrir la información disponible sobre el objetivo y sus activos desde fuentes públicas.
- Exploración de inteligencia competitiva: Identificar procesos u objetivos que puedan ser más valiosos que los activos a los cuales protegen.

4. Intervención

Consiste en intervenir en los recursos que consume el objetivo desde su ambiente con el fin de provocar cambios en su comportamiento.

- Verificación de cuarentena: Determina la efectividad de los controles de autenticación en términos de listas de cuarentena.
- Auditoria de privilegios: Determina la efectividad de los controles de autorización en términos de roles.
- Continuidad del servicio: Determina la efectividad de los controles de continuidad a través de la verificación de denegación de servicio.
- Encuesta final: Conocer que partes de la auditoria proporcionaron evidencia confiable y usable.

2.5.8 Una metodología

Al juntar todos los procesos descritos en cada una de las fases, obtenemos lo que se conoce como “Una Metodología”. Esto es un conjunto de procesos y actividades que son aplicables a todas las pruebas de seguridad, sea el objetivo una persona, un sistema, una ubicación, etc., (Sierra, 2018). La metodología está representada en el siguiente flujo:

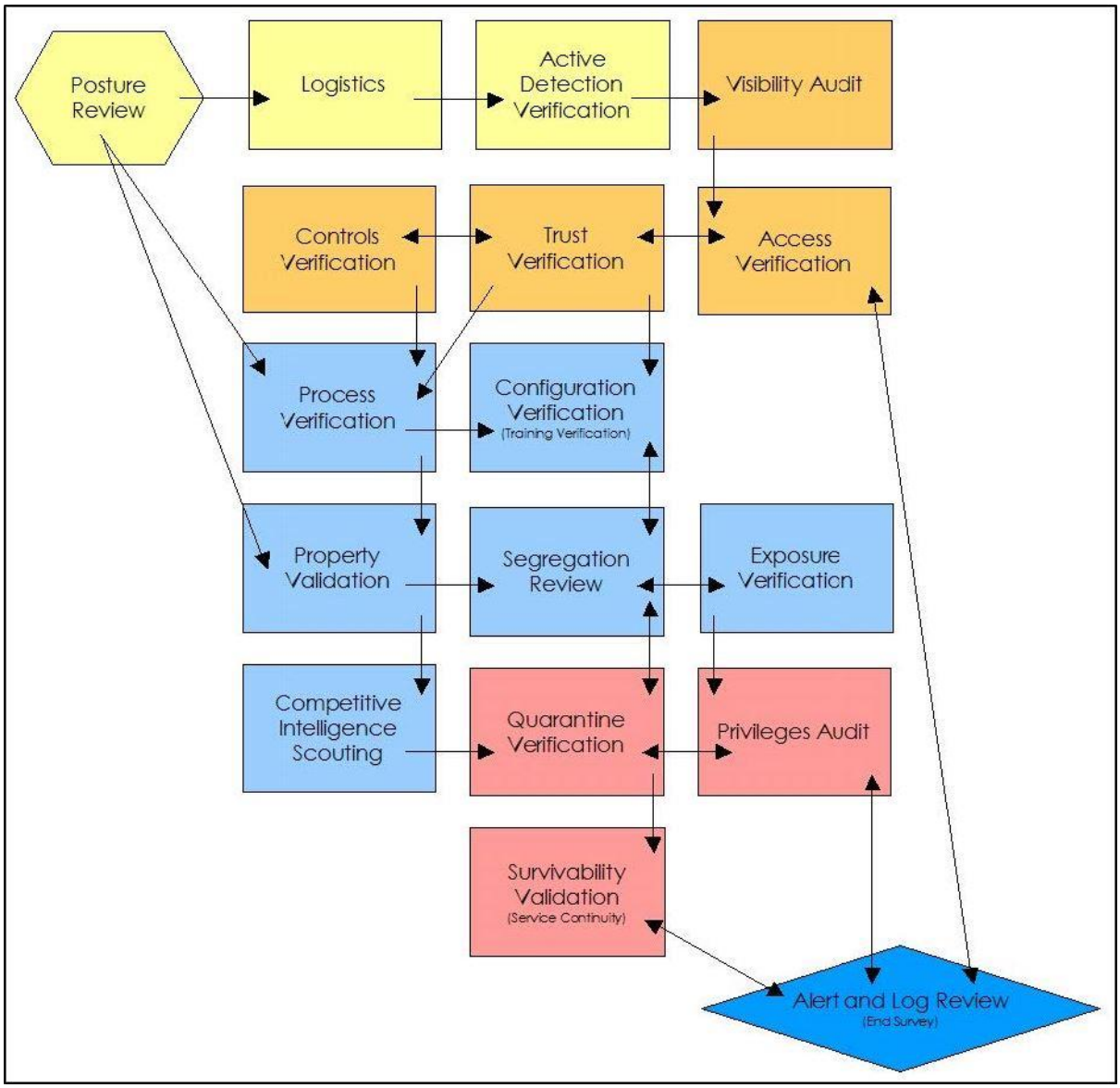


Figura 2. Una Metodología. Fuente: OSSTMM

OSSTMM establece el cumplimiento de este flujo para la ejecución de las pruebas de cada uno de los canales según el alcance del test, y provee consideraciones, fuentes, técnicas y herramientas relevantes para facilitar la labor del auditor.

2.5.9 Pruebas de seguridad

El objetivo general de las pruebas es definir el estado actual de las seguridades en cada uno de los canales y analizar las brechas entre lo actual y el estándar requerido por la organización.

- **Humano**

Requiere la participación y la interacción de las personas con los activos y su objetivo principal es valorar la conciencia de seguridad del personal y medir la brecha entre la situación actual y el estándar sugerido por la empresa (Sierra, 2018).

- **Físico**

El objetivo es poner a prueba las seguridades en las barreras físicas y lógicas de la organización, así como también el personal en custodia de los activos y su interacción con las barreras

- **Inalámbrico**

Consiste en validar los accesos a los activos a través de la interceptación y análisis de señales inalámbricas dentro del espectro electromagnético.

- **Telecomunicaciones**

Su objetivo es poner a prueba las barreras lógicas de la organización dentro de los límites de las telecomunicaciones sobre medios cableados.

- **Redes de datos**

Consiste en poner a prueba las medidas operacionales de las redes de datos para salvaguardar la información y los activos. Se involucra los sistemas computacionales, dispositivos electrónicos y las redes de datos establecidos en el alcance (ISECOM, 2010).

2.5.10 Reportes con STAR (Security Test Audit Report)

STAR es el reporte de auditoría del test de seguridad. Provee un resumen ejecutivo de alta precisión ya que su particular enfoque permite contrastar lo que se ha testeado con lo que no se ha testeado.

El ISECOM provee una plantilla que debe ser llenada en su totalidad y enviada al ISECOM en el caso de solicitar la certificación del test. La plantilla funciona a manera de cuestionario en donde se plasma la ejecución del test siguiendo el flujo de la metodología de ejecución de las fases, y además provee información relevante como los valores de seguridad operacional, controles y limitaciones.

Capítulo III

Diseño del método

Luego de revisar las metodologías descritas en los capítulos anteriores y obtener un amplio entendimiento de su orientación, forma de operar e implementar, es necesario en este punto, y previo al desarrollo del método propuesto, tener varias consideraciones que nos servirán de base para elaborar una herramienta adecuada y útil para su aplicación.

3.1 Consideraciones importantes

El método está orientado a empresas pequeñas, privadas y públicas, por lo que debe ser de cierta forma genérico, adaptable y repetible. Se enfoca a servir de instantánea, en cuanto a las fallas de seguridad existentes en la infraestructura tecnológica de una organización. Debe ser relativamente fácil de ejecutar y proveer resultados de manera rápida.

Basándonos en el párrafo anterior, se considera importante desarrollar un método práctico orientado al análisis de red (*network assessment*), basado en un test de caja blanca (de esta forma se aligera la fase de *footprinting)* y la utilización de herramientas automatizadas, con el fin de facilitar la labor del auditor y acortar los tiempos de ejecución de las fases.

3.2 Clasificación del objetivo

Debido a la variedad de tipos y tamaños de empresas, no es posible desarrollar un método genérico que sea altamente efectivo para todas ellas. El método propuesto es, de hecho, aplicable para cualquier infraestructura tecnológica, sin embargo, en una escala macro, existen varias otras consideraciones que requieren de soluciones a la medida y que ofrezcan altos niveles de fiabilidad en sus resultados.

El método propuesto en el presente trabajo ofrece obtener el mejor provecho en 2 tipos de empresas:

3.2.1 Empresas pequeñas

Chávez Cruz et al., (2018) recopilan varias clasificaciones para el tamaño de las empresas en su estudio, coincidiendo todas en los criterios de evaluación utilizados y con resultados similares. En éste, una empresa pequeña está constituida por lo siguiente:

- Número de empleados: entre 11 a 49
- Volumen de ventas: Entre $100.000 a $1.000.000 (anualmente)
- Activos Totales: Entre $100.000 a $1.000.000

Dependiendo de la naturaleza del negocio de la organización, algunas empresas contarán con una dirección de tecnología o personal técnico capaz de ejecutar el método propuesto. Para aquellas empresas que no cuenten con profesionales en el ámbito de la tecnología, el presente trabajo servirá de línea base, y guía para la contratación de un profesional que implemente el método desarrollado, a una fracción del valor económico de este tipo de servicios.

3.2.2 Instituciones publicas

La *Constitución del Ecuador (2008)*, en el artículo 225, numeral 3, describe una entidad del sector público como “Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.”

En este sentido, existe también una gran variedad en el tamaño y tipo de una entidad de gobierno. En el Ecuador como en la mayoría de países de Latinoamérica, las entidades públicas operan con una oficina central y varias oficinas a lo largo del territorio nacional, en conjunto y de manera articulada. Es en las oficinas centrales generalmente en donde se encuentran las coordinaciones nacionales y se emiten resoluciones y reglamentos que deben ser cumplidos y ejecutados por las oficinas territoriales, por lo que existe mayor concentración de empleados e infraestructuras físicas y tecnológicas más amplias y sofisticadas.

El método propuesto está optimizado para aquellas oficinas territoriales, así como también para gobiernos autónomos descentralizados y empresas públicas que disponen de infraestructuras más modestas y un número menor de empleados que una oficina central.

3.3 Análisis comparativo de las metodologías

Con el fin de desarrollar una herramienta útil para cada aplicación, vamos a proceder a realizar una comparación entre las metodologías previamente analizadas, seleccionando las técnicas y herramientas que resultan relevantes en cada una de ellas y que puedan aportar al desarrollo del método propuesto, considerando siempre su enfoque en la ejecución práctica.

Para ello se ha hecho uso del método de estudio de similitud entre modelos y estándares (MSSS) (Gasca Hurtado, 2010), el cual establece el siguiente flujo (figura 3) para la comparación entre distintos estándares y modelos:

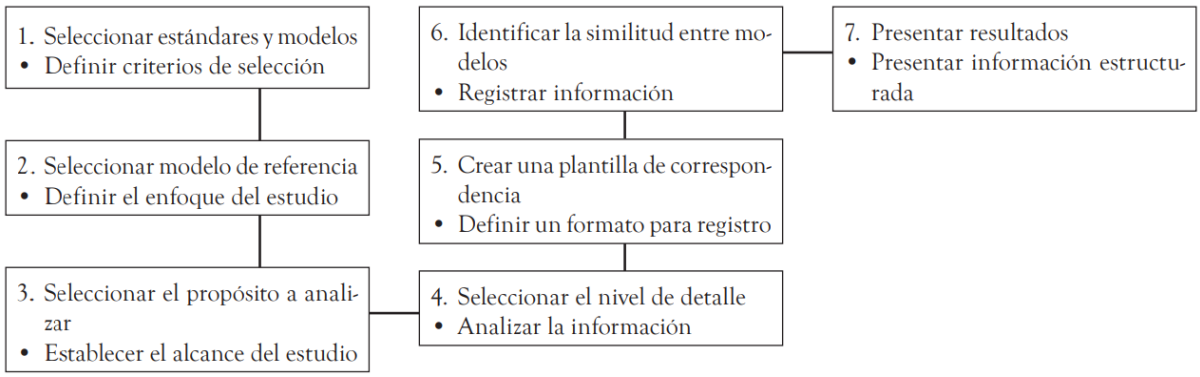


Figura 3. Flujo metodología MSSS. Fuente: (Gasca Hurtado, 2010)

El análisis del MSSS se lleva a cabo a partir de 3 aspectos:

- Alcance o enfoque de la aplicación del modelo o estándar.
- Filosofía o principios básicos y parámetros del modelo o estándar.
- Estructura de los pasos o fases que componen el modelo o estándar.

Siguiendo el método y el flujo mencionado, y considerando los aspectos establecidos por el MSSS, se ha elaborado la siguiente tabla (tabla 8):

Tabla 8. Resumen de las metodologías seleccionadas. Fuente: Autor

Metodología	Alcance	Filosofía	Estructura
CEH	Enfoque práctico y orientado al profesional	Se orienta en proveer el conocimiento, las herramientas, la práctica y la experiencia para la ejecución de pruebas de penetración, con una óptica externa o de un atacante.	1. Footprinting 2. Escaneo 3. Enumeración 4. Análisis de vulnerabilidades 5. System Hacking
PTES	Para proveedores de servicio y empresas que requieren contratar este tipo de servicios. Cubre aspectos técnicos y no técnicos relacionados a la ejecución de pruebas de penetración	Se centra en proporcionar un valor de negocio a los riesgos y vulnerabilidades asociados a los activos digitales de una organización	1. Interacciones previas al compromiso 2. Recolección de información 3. Modelado de amenazas 4. Análisis de vulnerabilidades 5. Explotación 6. Post explotación 7. Reportes

OSSTMM	Se enfoca en analizar las superficies de ataque de una organización, los controles implementados, la eficacia de los controles, y realiza un análisis de brecha entre la situación actual y la deseada	Está orientada a la medición de la seguridad en un nivel operacional, y está diseñada para ser repetible y adaptable a cualquier tipo de auditoria	1. Inducción 2. Interacción 3. Investigación 4. Intervención

En base al enfoque y orientación del método a desarrollar, se procede a realizar una comparación de las características de las metodologías seleccionadas. Los resultados se muestran en la tabla 9.

Tabla 9. Comparación de características de las metodologías seleccionadas. Fuente: Autor

Metodología	CEH	PTES	OSSTMM
Provee una guía técnica de aplicación	X		
Provee las herramientas para su aplicación	X	X	
Con un enfoque especifico en la practica	X		
Contempla todos los pasos del proceso genérico del ethical hacking	X	X	
Cubre aspectos no técnicos relacionados al test		X	X

Finalmente, se realiza un análisis de las metodologías seleccionadas, con un enfoque especifico en la ejecución práctica, y se resaltan sus objetivos y sus carencias como se demuestran en la tabla 10.

Tabla 10. Comparación de metodologías con enfoque en la ejecución práctica. Fuente: Autor

Metodología	Enfoque	Objetivos	Relación con la ejecución practica y carencias
CEH	Metodología de ethical hacking	La formación y acreditación de profesionales y especialistas en seguridad informática y ethical hacking, en la aplicación de las mismas técnicas y herramientas de un atacante	Es una metodología 100% practica, provee las herramientas y métodos para la implementación de pruebas de penetración y contempla todas las fases del proceso genérico de ethical hacking. No contempla aspectos no técnicos relacionados con pruebas de penetración
PTES	Metodología de pruebas de penetración	Cubrir todos los aspectos relacionados a la ejecución de pruebas de penetración (técnicos y no técnicos), analizar los riesgos y	Contiene una guía técnica y las herramientas para su ejecución. Su implementación va más allá de la práctica por lo que le incrementa complejidad. Contempla todas las fases del proceso genérico de ethical

		traducirlos a un lenguaje de negocio	hacking. No provee lineamientos técnicos de como ejecutar pruebas de penetración
OSSTMM	Metodología de auditorías de seguridad	Proveer una metodología científica que permita verificar y medir los controles de seguridad de una organización, y presentar métricas en base a hechos derivados de la ejecución de las pruebas	Provee varios tipos de test para la ejecución de las pruebas o auditorias de seguridad, también provee técnicas para la ejecución de los test en cada uno de los canales. No provee las herramientas para la ejecución de las pruebas y no contempla las fases del proceso genérico de ethical hacking

La implementación del método MSSS permitió determinar, gracias al análisis de las características de los modelos seleccionados, que la Metodología *Certified Ethical Hacker* es la que más se orienta a la ejecución práctica, por lo que la herramienta desarrollada estará alineada en su mayoría a esta metodología.

Se considera también importante, incluir una fase preliminar de planificación en la que se establezcan los acuerdos y reglas necesarios para la ejecución del test, y en donde se coordinen los esfuerzos para que el beneficio sea el máximo posible y en ambas direcciones. Para esto, vamos a tomar la fase “Interacciones previas al compromiso” de la metodología PTES que provee técnicas y herramientas de gestión y planificación, que serán de utilidad tanto para el diseño del método como para su implementación.

Por último, el tipo de test establecido en el método propuesto se asemejará al test doble gris de la metodología OSSTMM por su orientación al análisis de vulnerabilidades.

3.4 Resumen de las metodologías analizadas

No cabe duda de que cada metodología revisada es relevante y útil, y sus distintos enfoques aportan un valor único en cada implementación. Mientras que el CEH con un enfoque práctico se orienta al profesional, en proveerle el conocimiento y las herramientas para la ejecución de pruebas de penetración con una óptica externa o de un atacante, el PTES se centra en proporcionar un valor de negocio a los riesgos y vulnerabilidades asociados a los activos digitales de una organización, también considera aspectos relacionados a la logística, para la ejecución del test dentro de un marco legal y un ambiente seguro tanto para el cliente como para el auditor. Finalmente, la metodología OSSTMM se enfoca en analizar las superficies de ataque de una organización, los controles implementados, la eficacia de los controles, y realiza un análisis de brecha entre la situación actual y la deseada.

A fin de obtener un mayor beneficio en la contratación de servicios de seguridad, es necesario que la empresa u organización entienda, primeramente, que es lo que espera del servicio, y luego, que conozca ciertos parámetros dentro de este tipo de servicios, como los mencionados en el párrafo anterior. Solo de esta forma, se tomará una decisión acertada y de acuerdo a sus necesidades.

3.5 Fases establecidas

Gracias al análisis comparativo realizado en el apartado 3.3, hemos podido sintetizar el proceso genérico de ethical hacking para adaptarlo a nuestro modelo, incluyendo actividades de naturaleza no técnica, pero necesarias para asegurar un servicio conforme a las necesidades del cliente o beneficiario. De esta forma, se ha estructurado nuestro modelo con la siguiente disposición:

Fase 1: Criterios para la ejecución del test.

Fase 2: Escaneo.

Fase 3: Análisis de vulnerabilidades.

Fase 4: Explotación.

Fase 5: Reporte.

A un nivel general, la tabla 11 presenta las características más importantes de la herramienta desarrollada, a la vez que justifica las decisiones de diseño con el propósito de darle sentido al método.

Tabla 11. Características generales del método propuesto. Fuente: Autor

Fases	Objetivo	Actividades	Metodología Base	Justificación
1. Criterios para la ejecución del test	Recolectar la información necesaria para planificar las fases posteriores y organizar los recursos disponibles, con el fin de garantizar fluidez en la ejecución del test y prevenir inconvenientes	A través de reuniones con el beneficiario o su representante se debe definir: Rangos de IP, dominios, puertos, Fechas de inicio, fin, horarios de ejecución y honorarios de ser el caso.	Se basa en la fase de "Interacciones previas al compromiso" del PTES	Aunque el método propuesto está orientado a la ejecución práctica, se ha integrado esta fase por considerarse de gran valor, al proporcionar cierto grado de seguridad tanto para el beneficiario como para el equipo auditor, estableciendo reglas claras y límites para la ejecución de las fases posteriores. Esta fase, aunque corta, previene posibles futuras controversias como desbordamiento del alcance, insatisfacción del cliente o beneficiario, etc.
2. Escaneo	La búsqueda de vulnerabilidades y vías de acceso a la infraestructura tecnológica del objetivo a través de la interacción con herramientas automatizadas	Escaneo de red Escaneo de puertos Escaneo de vulnerabilidades Elaborar un diagrama de red	Se basa en las fases de "Escaneo de redes" y "Enumeración" de la metodología CEH	Ya que el método propuesto se basa en un test de caja blanca (o un test doble caja gris según el OSSTMM), el equipo auditor cuenta con toda la información sobre la infraestructura de la organización, siendo necesario únicamente realizar un escaneo automatizado de la misma. Se ha combinado la fase de Enumeración junto con la fase de escaneo de redes del CEH, ya que la orientación, el alcance de cierta forma genérico del test, y las herramientas utilizadas, permiten realizar la enumeración de manera simultánea al escaneo.
3. Análisis de Vulnerabilidades	Aumentar la probabilidad de una explotación exitosa al analizar las vulnerabilidades encontradas, priorizarlas	Correlación específica y correlación categórica de vulnerabilidades	Se basa en la fase de "Análisis de vulnerabilidades" de la metodología PTES	Las herramientas utilizadas para el escaneo de vulnerabilidades, devuelven en la mayoría de los casos, vulnerabilidades conocidas, por lo que, el proceso de validación (de la fase Análisis de Vulnerabilidades del PTES), a través de correlación

	por nivel de severidad y posibilidad de explotación. Buscar y analizar los métodos de explotación.			especifica (y categórica en ciertos casos), resulta más que suficiente para encontrar métodos de explotación.
4. Explotación	Obtener evidencia de una explotación exitosa de un host, dentro de la infraestructura del objetivo.	Búsqueda, selección y ejecución de payloads y exploits en un host vulnerable	Se basa en la fase de "System hacking" de la metodología CEH	La consecución de una explotación exitosa a un host dentro de la infraestructura del objetivo, resulta de suma importancia, ya que provee evidencia "tangible" de que una organización es vulnerable, y ayuda al beneficiario a interiorizar el peligro y los riesgos de un ataque real
5. Reporte	Presentar los resultados del test de una manera entendible y cuantificable	Generar reportes de herramientas utilizadas, Elaborar reporte final	Se basa en la fase "Reporte" de la metodología PTES	Es necesario un entregable con información relevante y entendible, que provea una visión holística de la situación en temas de seguridad de la información, y que sirva de soporte para la elaboración de hojas de ruta y planes de acción para subsanar las vulnerabilidades encontradas. Podría considerarse la fase más importante del método, ya que, sin este documento, el beneficiario no tendría conocimiento del estado de su infraestructura, por lo que, la ejecución del test habría sido en vano.

De forma visual y simplificada, nuestro método estaría representado como se muestra en la figura 4.

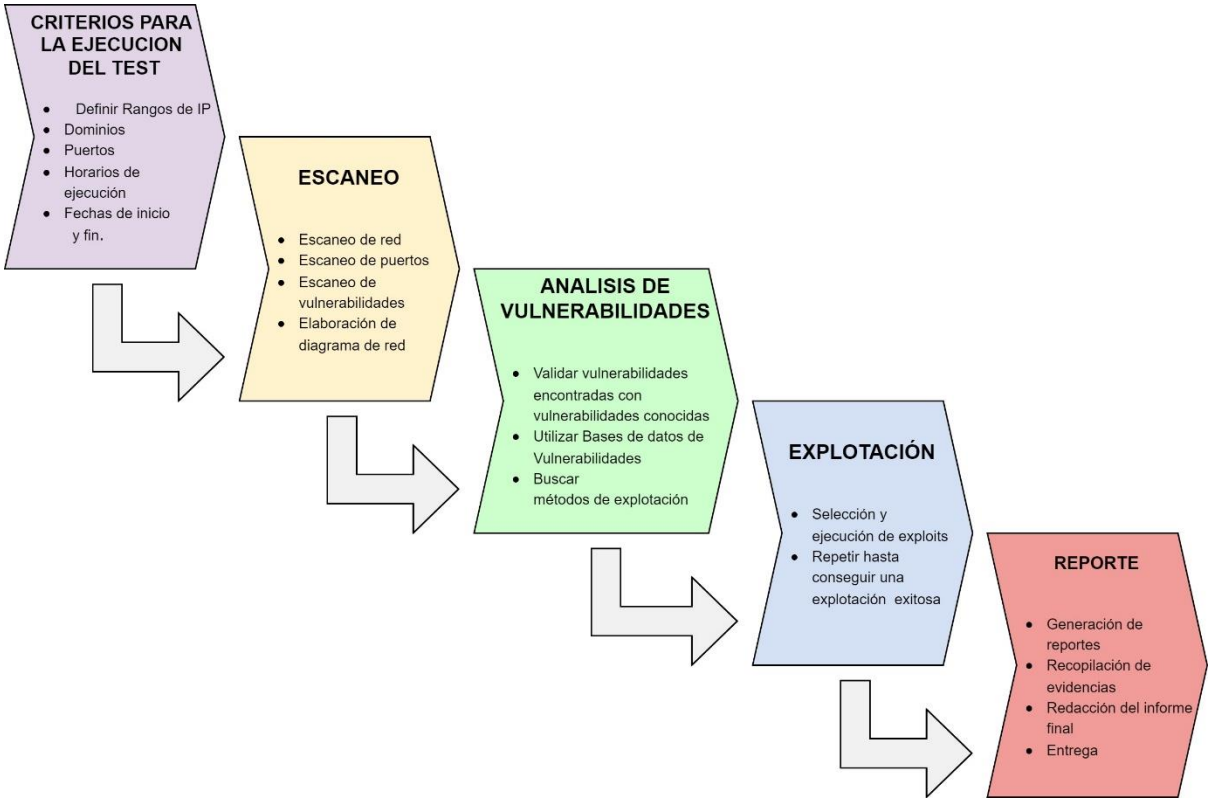


Figura 4. Diagrama del método de pentest propuesto. Fuente: Autor

A continuación, profundizaremos en cada una de las fases, desarrollando el "como" en cada una de ellas, y facilitando el conocimiento necesario para su correcta ejecución.

3.5.1 Criterios para la ejecución del test

Si bien el método propuesto en el presente trabajo tiene una orientación práctica, resulta necesario acordar con el cliente o beneficiario, ciertos aspectos del test, con el fin de garantizar una logística adecuada que resulte beneficiosa para el auditor y ayude a prevenir inconvenientes en la operación normal de la empresa.

Esta fase se basa en la fase de "Interacciones previas al compromiso" del PTES y consta de las actividades previas a la ejecución del test (el CEH no considera tales actividades). Tiene como finalidad delimitar los aspectos técnicos del test, establecer tiempos y horarios de ejecución y organizar todas las actividades y recursos necesarios para la correcta ejecución del test.

Los criterios considerados de relevancia para esta fase son:

- Rangos de IP: Ya que nuestro método se basa en un test de caja blanca, es necesario conocer de antemano, la porción de la infraestructura y las respectivas direcciones IP que van a ponerse a prueba.
- Dominios: De igual forma, es necesario conocer, que dominios van a ser testeados o están dentro del alcance de la ejecución de la prueba.
- Puertos: Es recomendable realizar un escaneo de todos los puertos, y en la mayoría de los casos sucede de esta manera, sin embargo, habrá casos en los que el beneficiario requiera únicamente que ciertos puertos sean testeados.
- Horarios para la ejecución: Es muy importante considerar en que horarios se van a ejecutar las pruebas, pueden ser, pasado el horario laboral, con el fin de evitar inconvenientes en la operación normal de la infraestructura o la empresa, o también se puede requerir la ejecución de las pruebas en un horario laboral, con el fin de verificar el nivel de respuesta de la infraestructura, dispositivos de seguridad y el departamento de TI.
- Fechas de inicio, fin y entregables: Para que exista una planificación adecuada, es necesario definir fechas de inicio y fin de las pruebas, además de fechas de entrega de los informes finales, esto evitará que la ejecución de las pruebas, no se prolongue más de lo que debería.
- Honorarios: En el caso de contratar una prueba de intrusión con un proveedor externo, es necesario definir los honorarios para la ejecución de las pruebas, el costo por actividad, por hora y/o por asesoramiento.
- Restricciones y exclusiones: De la misma forma en la que establecemos los criterios anteriores, es necesario definir que esta fuera del alcance, por ejemplo, direcciones IP específicas que no se desea testear (por ejemplo, un servidor de base de datos), puertos, días festivos o fechas en los que no podrán ejecutarse las pruebas, etc.

Estos criterios pueden establecerse en una o varias reuniones con el beneficiario y el equipo de TI de la empresa, en las que también se podrán elaborar y legalizar contratos de trabajo, acuerdos de confidencialidad y demás documentos que puedan servir de respaldo para evitar futuras controversias.

3.5.2 Escaneo

Una vez tomadas las consideraciones necesarias para la ejecución del test, el siguiente paso en el método es el escaneo. Ya que nos estamos basando en un test de caja blanca, nos

hemos evitado la fase de *footprinting*, o simplemente, la misma se encuentra implícita en la fase anterior.

El escaneo se basa en las fases de “Escaneo de redes” y “Enumeración” de la metodología CEH. Se han combinado en una sola fase, ya que la orientación y alcance del método propuesto permite realizar las dos actividades al mismo tiempo, y el CEH provee las herramientas y la metodología para llevarlo a la práctica.

La metodología para esta fase consta de 2 etapas:

- **Escaneo de red y puertos**

Con el uso de herramientas automatizadas, vamos a realizar lo siguiente:

- Un barrido de red (*pingsweep*) para descubrir los hosts que se encuentran activos. Con la herramienta nmap, el comando utilizado seria el siguiente:

  nmap -Pn (rango de IP)

- Escaneo de puertos en los hosts que se encuentran activos. Con la herramienta nmap, el comando utilizado seria el siguiente:

  nmap -A -T4 –p (puertos abiertos encontrados en el paso anterior) (IP host activo)

  Este comando realiza la enumeración al mismo tiempo, ya que obtiene nombres de host, servicios ejecutados, sistemas operativos y versiones, información que nos será de utilidad para las fases posteriores.

- Elaborar un diagrama de la red nos ayuda a facilitar el trabajo ya que nos da un rápido acceso a los hallazgos. Se puede utilizar herramientas en línea como draw.io o de escritorio como Visio de Microsoft.

- Documentar la ejecución de los comandos y los hallazgos. Se puede utilizar aplicaciones como *cherry tree, one note* o simplemente un procesador de texto.

- **Escaneo de vulnerabilidades**

Las herramientas a utilizarse en esta fase son Nessus y Openvas. Nessus es una herramienta muy completa y fácil de usar, pero su versión gratuita tiene un límite de 16 hosts, por esta razón vamos a utilizar también Openvas, que además nos servirá para contrastar los resultados. La metodología es la siguiente:

- Una vez instalada y configurada la herramienta procedemos a crear un nuevo Scan o Tarea.

- Seleccionamos la opción *Basic Network Scan* para Nessus y *Task Wizard* para OpenVAS.
- Configuramos como objetivos, los hosts descubiertos en el escaneo de red.
- Establecemos el escaneo para todos los puertos TCP y dejamos el resto de configuraciones por defecto en ambas herramientas.
- Damos inicio al test.

Desde esta fase y en adelante, se recomienda como plataforma de trabajo, hacer uso de distribuciones de Linux optimizadas para la ejecución de pruebas de penetración y auditorias de seguridad como Kali Linux o Parrot OS, ya que vienen pre configuradas con herramientas y recursos destinados a facilitar este tipo de actividades.

3.5.3 Análisis de vulnerabilidades

Luego de culminar la fase de escaneo, es necesario hacer un análisis de las vulnerabilidades encontradas. Esta fase se basa en el proceso de Validación de la fase de “Análisis de vulnerabilidades” de la metodología PTES, y consta únicamente de la ejecución del proceso a través de los métodos de “Correlación Especifica” en su mayoría, y “Correlación Categórica” cuando la correlación especifica no ha tenido éxito. Con las herramientas utilizadas, procedemos a hacer lo siguiente:

- Ingresamos a los resultados de la prueba y ordenamos las vulnerabilidades encontradas por criticidad.
- En este punto, podemos buscar las vulnerabilidades conocidas, utilizando su id de CVE en alguna base de datos, o podemos hacer una búsqueda de manera manual, en base a los puertos, servicios y versiones encontrados en la fase anterior. En este paso podemos utilizar Bases de Datos de CVE como exploit-db.com, cve.mitre.org, vuldb.com, o utilizar herramientas como *searchsploit* o *metasploit framework* que vienen incluidas en Kali Linux.
- Una vez identificada la forma de explotación, es necesario considerar en este punto, el sistema operativo y la versión del host objetivo, así como también la versión del servicio que éste ejecuta y que se encuentra vulnerable. Esta información es relevante para seleccionar el *payload* adecuado y aumentar la probabilidad de una explotación exitosa.
- Encontrados el o los *payloads*, procederemos a la fase de explotación.

Nota: Ya que la ejecución de *payloads* es riesgosa y puede perjudicar la correcta operación del host o la red, se recomienda realizar la fase de explotación hasta haber alcanzado la explotación exitosa de un solo objetivo, lo que nos bastara como prueba de concepto, y no sin antes tener la autorización de la dirección o gerencia de la empresa.

3.5.4 Explotación

En esta fase pondremos a prueba los *payloads* para los *exploits* encontrados. Se recomienda empezar con las vulnerabilidades de criticidad alta y en los equipos de mayor impacto en la organización (siempre que se encuentren dentro del alcance) a fin de proveer evidencia de los riesgos existentes y el impacto del negocio en caso de que un host se vea comprometido.

Ya que se debe evitar a toda costa la interrupción de los servicios y procurar la operación normal de la empresa, se recomienda utilizar *payloads* únicamente para la obtención de *Shell* remotos, para otros casos se debe considerar solicitar la autorización al administrador de la red o la empresa.

Esta fase se basa en el proceso de “Explotar vulnerabilidades” dentro de la fase de “System Hacking” de la metodología CEH, al tener una orientación práctica, y utilizaremos la herramienta *Metasploit Framework* recomendada por el PTES.

Utilizando la herramienta seleccionada podemos realizar búsquedas, consultas y encontrar información relacionada a cada *exploit* como, para que sirve, los parámetros necesarios para su ejecución, los sistemas y versiones susceptibles, etc. Es relativamente fácil de usar, basta con ejecutar en la terminal de Kali Linux el comando *msfconsole* para acceder a la herramienta. Con el comando *search* podemos buscar entre varios tipos de *exploit*, el comando *use* nos permite seleccionarlos, y el comando *info* provee información relevante como utilidad y parámetros admitidos. Finalmente, los comandos *run* o *exploit* nos permiten ejecutarlos.

En base a los comandos mencionados, procederemos a buscar los *payloads* y *exploits*, según los resultados de la fase de escaneo, seleccionar el adecuado, configurarlo y ejecutarlo. Ya que en la práctica no resulta tan sencillo, deberemos repetir este procedimiento, intentando con cada vulnerabilidad encontrada, hasta conseguir una explotación exitosa.

Tan pronto como hayamos obtenido un *Shell* remoto en un equipo, resultado de la ejecución de un *payload*, debemos verificar el usuario y el nivel de privilegios alcanzado. Se pueden utilizar los comandos *whoami, hostname* y *dir* en Windows, y *whoami, host* y *ls* en Linux. Es importante realizar capturas de pantalla como evidencia de lo conseguido.

Todas las capturas de pantalla, archivos y evidencia de la ejecución del test, generados durante todas sus fases, serán incluidas como anexo al reporte final.

3.5.5 Reporte

Esta fase consiste en la presentación de los resultados de la ejecución de la prueba de penetración. Se basa en la fase de “Reportes” de la metodología PTES, con la diferencia que ésta engloba los 2 reportes recomendados por el PTES, en uno solo. Recopila la información adquirida a lo largo de la implementación a modo de resumen ejecutivo, para un fácil entendimiento, a la vez que incorpora los elementos fundamentales y hallazgos obtenidos en cada una de las fases con una óptica de narrativa, con el fin de proveer una línea de tiempo que ayude a comprender de principio a fin el proceso ejecutado, para finalmente proveer un criterio del auditor sobre la situación general de la infraestructura analizada. Los reportes generados de la ejecución de las herramientas utilizadas, alimentarán el apéndice y servirán para el tratamiento de cada vulnerabilidad encontrada y para la elaboración de hojas de ruta, planes de acción, prevención y mitigación de riesgos.

La metodología para la fase, sería la siguiente:

- Las herramientas Nessus y OpenVAS contienen módulos para la generación de reportes, muy útiles y personalizables. Se recomienda filtrar las vulnerabilidades altas y críticas para la generación del reporte, ya que son de mayor relevancia para la empresa y para el test, además de que permite una presentación más limpia y de fácil entendimiento. El resto de configuraciones, es mejor dejarlas por defecto.
- Es posible generar un reporte con todas las vulnerabilidades encontradas, ya que en este se encuentran las recomendaciones a seguir con el fin de eliminar o mitigar dichas vulnerabilidades. El mismo se entregaría a la Dirección de Tecnologías para la elaboración de un plan de acción y gestión de las amenazas encontradas.
- El reporte genérico en ambos casos (Nessus y OpenVAS) provee información técnica muy relevante y da una clara idea del riesgo de negocio asociado, por lo que la personalización del mismo queda a consideración del auditor.
- Para la elaboración del reporte final, se recomienda incluir como mínimo, los siguientes puntos:
    - Portada: datos del auditor / compañía de seguridad, datos de la empresa auditada, fechas, etc.
    - Índice.

- Resumen ejecutivo: hallazgos más relevantes y conclusión del auditor.
- Metodología utilizada: por ejemplo, caja blanca con orientación al *host assessment.*
- Narrativa del test: acciones realizadas y hallazgos encontrados
- Conclusiones y recomendaciones.
- Apéndice: Reportes generados de las herramientas utilizadas, resultados de la ejecución de los comandos, evidencia completa de hallazgos, logs, etc.

3.6 Flujo

A fin de obtener una mejor comprensión del método y tener una herramienta visual que facilite la ejecución del mismo, se ha diseñado el siguiente diagrama (figura 5):

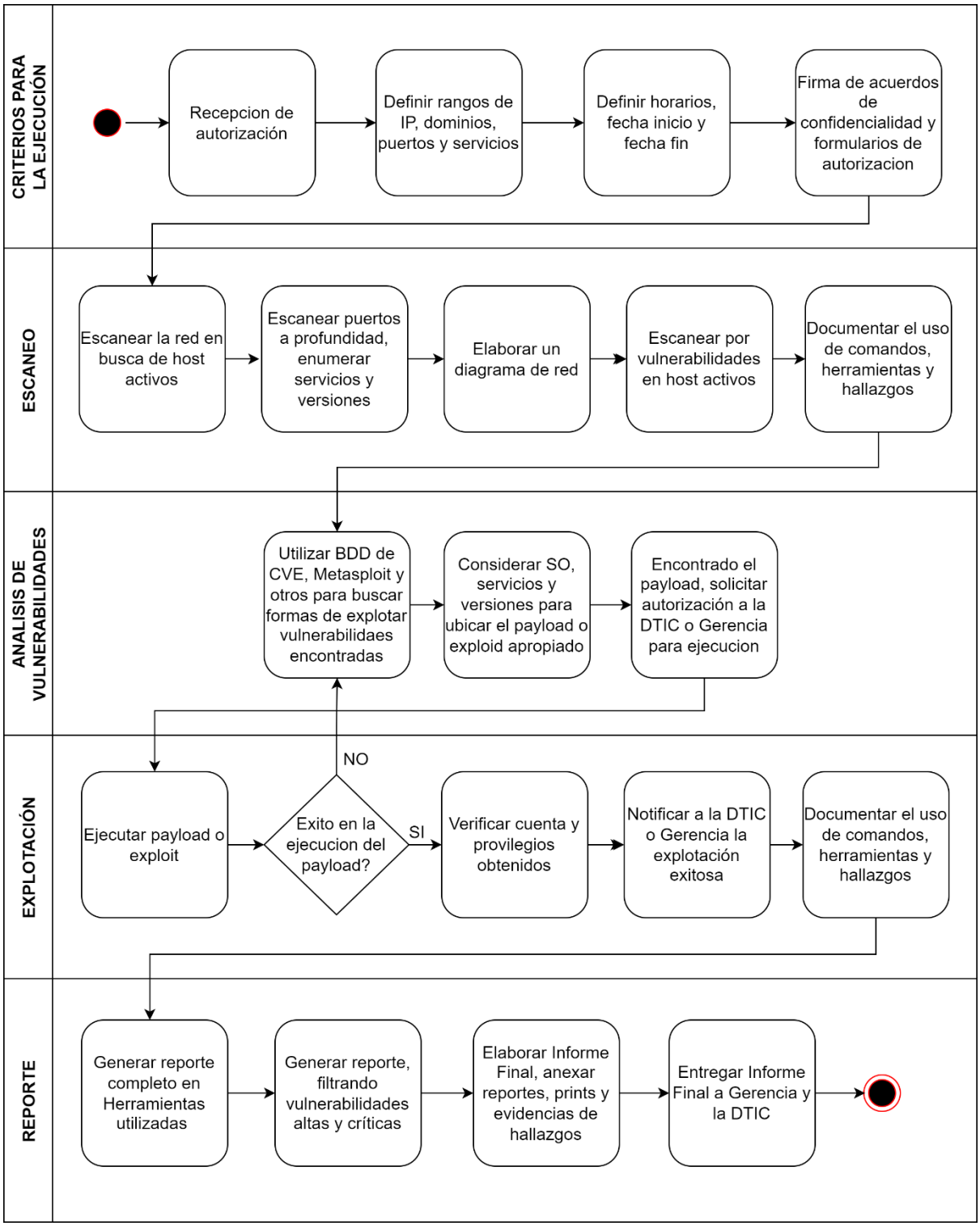


Figura 5. Diagrama de Flujo. Fuente: Autor.

Capítulo IV

Aplicación del caso de estudio

En el presente capítulo pondremos en práctica lo desarrollado en el capítulo anterior, como prueba de concepto y de utilidad del método. Empezaremos conociendo el objetivo, para luego ir desglosando cada fase, aplicando las herramientas seleccionadas y evidenciando los hallazgos. Finalmente se intentará plasmar información relevante para la organización, tanto técnica como de negocio, en el reporte final. Cabe mencionar que la información de carácter sensible, obtenida como resultado de la ejecución de comandos y herramientas, ha sido enmascarada, con el fin de preservar la anonimidad de la organización objetivo, evitar poner en riesgo su infraestructura y dar cumplimiento al acuerdo de confidencialidad.

4.1 Antecedentes del target

La organización en la que se va a aplicar el método desarrollado, es una institución pública ubicada en la provincia de Cañar. La misma consta de una Dirección Distrital con autonomía administrativa y financiera, pero con la coordinación de sus procesos en una oficina central, ubicada en la ciudad de Quito. Cuenta con 17 trabajadores, cada uno con un equipo de cómputo a su custodia y conectado a la red de la oficina, ya que los servicios que ofrecen, tanto para usuarios internos como externos, están basados en tecnologías de la información.

Teniendo en cuenta estas consideraciones, podemos afirmar que el target u objetivo, califica perfectamente dentro de la clasificación descrita en el capítulo anterior, por lo que, la ejecución del método es adecuada y útil en este caso.

4.2 Definición del alcance

Luego de recibir la autorización para la ejecución del método, por el representante provincial de la primera autoridad de la Institución, se ha convocado a una reunión al personal del área de TIC’s y a la Dirección Provincial con el fin de establecer los aspectos logísticos, técnicos y legales del test. Para ello se han elaborado y legalizado los siguientes documentos:

- Formulario de autorización de pentest: En este se define el alcance (Rangos de IP, horarios de ejecución, etc) y se recibe la autorización para la ejecución. Una copia se encuentra disponible en el apartado de anexos.
- Acuerdo de confidencialidad: Establece las condiciones para el uso de la información proporcionada por la organización, y para la ejecución del test. Está disponible en el apartado de anexos.

Una vez definidos estos aspectos, y recibido la autorización para el inicio del test, pasamos a la fase de escaneo.

4.3 Escaneo

Esta fase empieza al crear un enlace de red, del equipo del auditor con la red del objetivo. Para ello conectamos un cable ethernet en un punto de red disponible y verificamos la información de red. No se recomienda conexiones inalámbricas para la ejecución de las herramientas, ya que la naturaleza exhaustiva de los análisis, satura las redes inalámbricas y genera indisponibilidad en el servicio. Abrimos una terminal y ejecutamos el comando *ifconfig:*

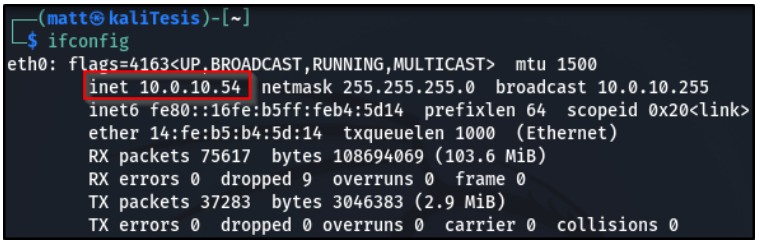


Figura 6. Ejecución de comando ifconfig. Fuente: Autor

De esta forma verificamos que nos encontramos en la sub red definida en el alcance. Es importante mencionar, que como plataforma de trabajo se ha seleccionado el sistema operativo Kali Linux.

- **Escaneo de red**

En la misma terminal, utilizamos la herramienta nmap con el siguiente comando:

nmap -Pn 10.0.10.0/24 -o /home/matt/TESIS/comando1.txt

- -Pn: evita el bloqueo de host Discovery
- -o: almacena el resultado de la ejecución del comando en un archivo de texto

```
1  nmap -Pn 10.0.10.0/24 -o /home/matt/TESIS/comando1.txt
2
3  # Nmap 7.91 scan initiated Tue Aug 10 11:43:44 2021 as: nmap -Pn -o /home/matt/TESIS/comando1.txt 10.0.10.0/24
4  Nmap scan report for 10.0.10.1
5  Host is up (0.00036s latency).
6  Not shown: 997 closed ports
7  PORT     STATE SERVICE
8  53/tcp   open  domain
9  1723/tcp open  pptp
10 2000/tcp open  cisco-sccp
11 MAC Address: 00:0C:42:E2:48:D2 (Routerboard.com)
12
13 Nmap scan report for 10.0.10.5
14 Host is up (0.00075s latency).
15 Not shown: 995 closed ports
16 PORT     STATE SERVICE
17 99/tcp   open  metagram
18 554/tcp  open  rtsp
19 880/tcp  open  unknown
20 8000/tcp open  http-alt
21 9010/tcp open  sdr
22 MAC Address: BC:AD:28:A3:3C:A6 (Hangzhou Hikvision Digital Technology)
23
24 Nmap scan report for 10.0.10.10
25 Host is up (0.00034s latency).
26 Not shown: 999 closed ports
27 PORT   STATE SERVICE
28 22/tcp open  ssh
29 MAC Address: DC:9F:DB:98:EB:E7 (Ubiquiti Networks)
30
31 Nmap scan report for 10.0.10.12
32 Host is up (0.00031s latency).
33 Not shown: 993 filtered ports
34 PORT      STATE SERVICE
35 135/tcp   open  msrpc
36 139/tcp   open  netbios-ssn
37 445/tcp   open  microsoft-ds
38 7070/tcp  open  realserver
```

Figura 7. Escaneo de red. Fuente: Autor

Obtenemos varios hosts activos e información adicional como puertos y fabricante de la tarjeta de red. En base a esta información, podemos empezar a elaborar un diagrama de la red y realizar una búsqueda más profunda de los puertos y servicios disponibles en cada host.

- **Escaneo de puertos**

El comando anterior escanea los mil puertos comunes dentro del protocolo TCP, sin embargo, se considera necesario escanear todos los puertos dentro de este protocolo, ya que, de no hacerlo, podríamos estar omitiendo información importante tanto en temas de seguridad como para la ejecución del test. El comando queda de la siguiente forma:

nmap -T4 -p- 10.0.10.1

- -T4: utiliza una plantilla predeterminada (0: más profundo, 5: más rápido)
- -p-: selecciona todos los puertos para el análisis

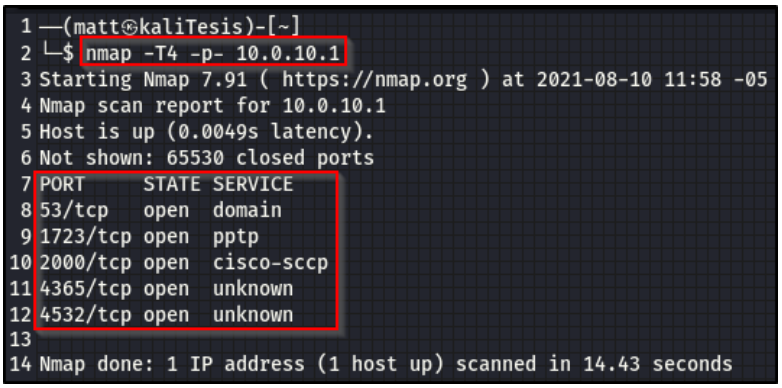


Figura 8. Escaneo de puertos. Fuente: Autor

Podemos ver que obtenemos información adicional que no obtuvimos con el comando anterior. Ahora procedemos a enumerar los puertos en busca de información adicional de cada host:

nmap -A -T4 -p80,135,139,443,445,3306,3389,5357,5800,5900,7070,49152,49154,49180,49206,49207,49318 10.0.10.16

- -A: combina detección de sistema operativo, versión, *traceroute* y otros más.
- -p: especifica el puerto, puertos o rango de puertos dentro del análisis

En algunos casos es necesario agregar el parámetro *–Pn* ya que algunos dispositivos mantienen activo el bloqueo de *host discovery*. Puede incrementar el tiempo de la ejecución del comando significativamente.

```
PORT      STATE SERVICE           VERSION
80/tcp    open  http              Apache httpd 2.2.21 ((Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1)
|_http-server-header: Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1
| http-title: Access forbidden!
|_Requested resource was http://10.0.10.16/xampp/
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2021-08-10T17:32:44+00:00; +35s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
445/tcp   open  microsoft-ds      Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: [redacted])
3306/tcp  open  mysql             MySQL (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=AZ6AZO08
| Not valid before: 2021-06-27T13:02:48
|_Not valid after:  2021-12-27T13:02:48
|_ssl-date: 2021-08-10T17:32:44+00:00; +35s from scanner time.
5357/tcp  open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5800/tcp  open  vnc-http          TightVNC (user: az6azo08; VNC TCP port: 5900)
|_http-title: TightVNC desktop [az6azo08]
```

Figura 9. Enumeración de puertos. Fuente: Autor

La herramienta nos ayuda a determinar que el host 10.0.10.16 ejecuta un sistema operativo Windows 7 Profesional SP1, basado en una arquitectura de 32 bits, su nombre de host (*AZ6AZO08*) y su grupo de trabajo. También podemos observar los servicios que se ejecutan en cada puerto activo, sus versiones, configuraciones, entre otros.

Nota: El proceso de escaneo de puertos se realizó para todos los hosts descubiertos en el escaneo de red. En razón de no saturar el presente trabajo y mantener la información de la organización, confidencial, se consideró incluir, para efectos de ilustración, el proceso con un solo host, dando continuidad y demostrando paso a paso el flujo establecido.

- **Diagrama de red**

Para elaborar el diagrama de red se ha utilizado la herramienta en línea draw.io. Se ha procedido a integrar los equipos de red encontrados, los hosts, y un equipo de grabación de video digital, esquematizando la disposición lógica de la infraestructura.

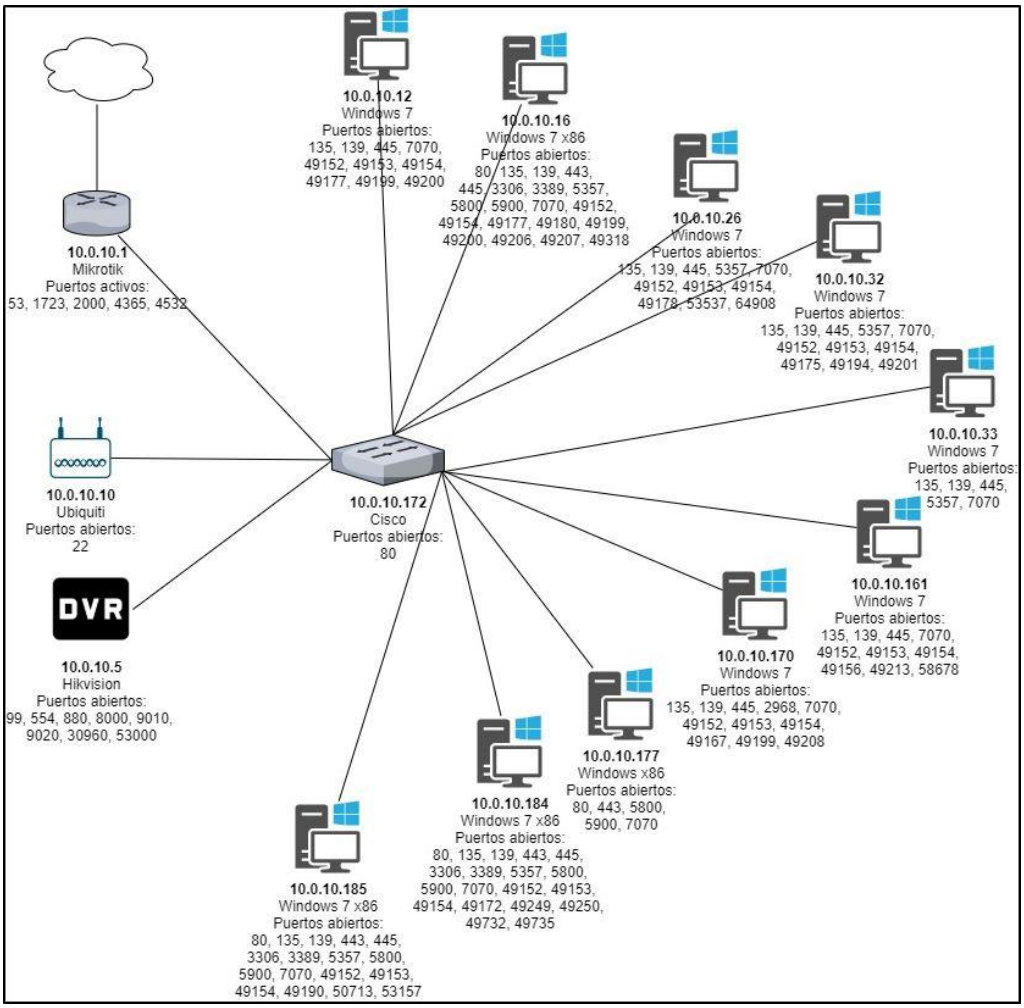


Figura 10. Diagrama de red. Fuente: Autor.

El diagrama (figura 10) nos muestra las direcciones ip, el tipo de dispositivo, el sistema operativo y los puertos activos en cada host, por lo que resulta una herramienta de consulta rápida y útil. Aunque no se lo ha hecho en este caso debido a la gran cantidad de puertos activos, se recomienda también incluir los servicios y versiones que se ejecutan en cada puerto.

- **Escaneo de vulnerabilidades**

Para el escaneo de vulnerabilidades vamos a hacer uso de las herramientas OenVAS y Nessus. La instalación y configuración inicial de las herramientas sale del alcance del presente trabajo por lo que vamos a empezar por la creación y configuración de un escáner de vulnerabilidades básico en cada una.

En el caso de Nessus, iniciamos sesión en la herramienta y seleccionamos la opción *basic network scan* dentro del apartado *new scan* y configuramos como se muestra en la figura 11.

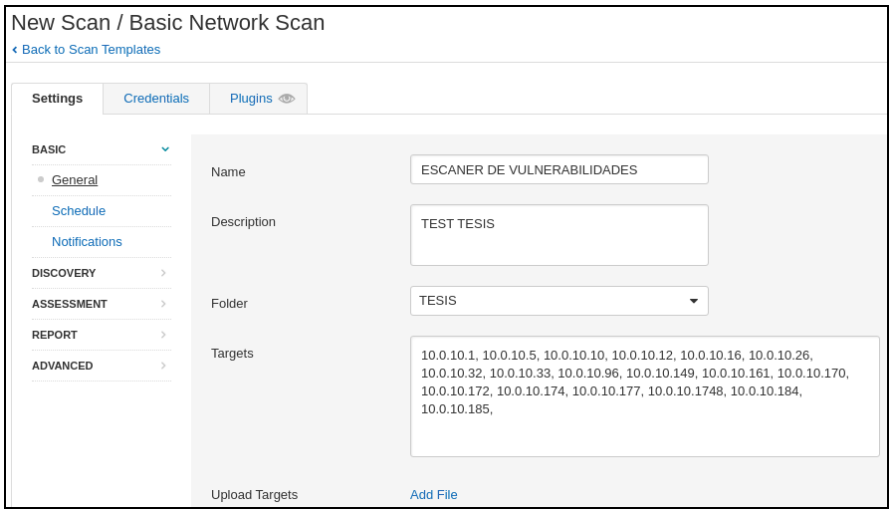


Figura 11. Configuración básica Nessus. Fuente: Autor

Le damos un nombre, una descripción, agregamos las direcciones de los hosts encontrados en el escaneo de red y seleccionamos la sección *Discovery.*

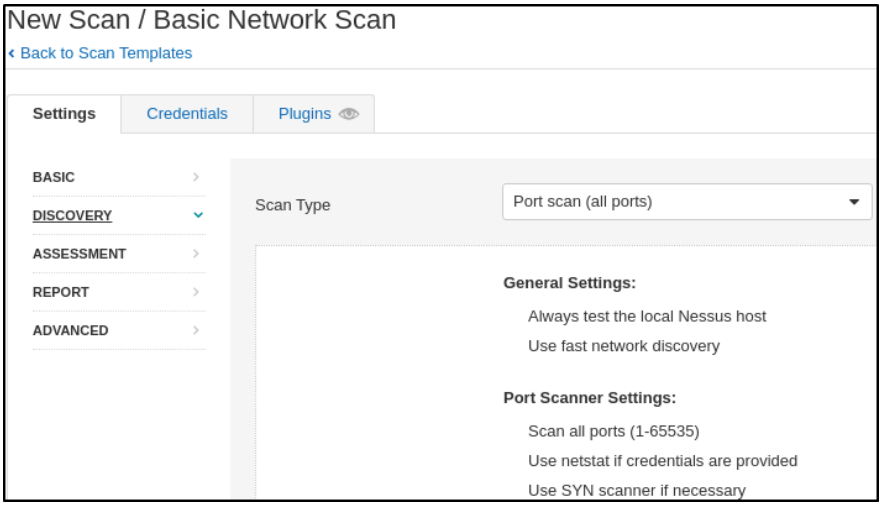


Figura 12. Configuración Discovery Nessus. Fuente: Autor.

Configuramos el escaneo para todos los puertos (figura 12) y el resto de configuraciones las dejamos por defecto, guardamos el test, y lo ejecutamos desde la sección *My scans.*

Una vez concluido el test, podemos ingresar a los resultados desde la misma sección y seleccionando el test generado, para continuar con la siguiente fase.

4.4 Análisis de vulnerabilidades

Esta fase comprende un análisis minucioso de cada vulnerabilidad encontrada. Al igual que en la fase anterior, en esta fase utilizaremos los ejemplos más representativos para demostración.

Figura 13. Resultados Nessus por host. Fuente: Autor.

Nessus nos permite mostrar los resultados de varias formas. En la figura 13, de forma visual podemos ver el número de vulnerabilidades encontradas, identificadas por severidad en cada host analizado. Al seleccionar un host, se nos muestran las vulnerabilidades encontradas en ese host en particular, clasificadas por grupo de amenaza.

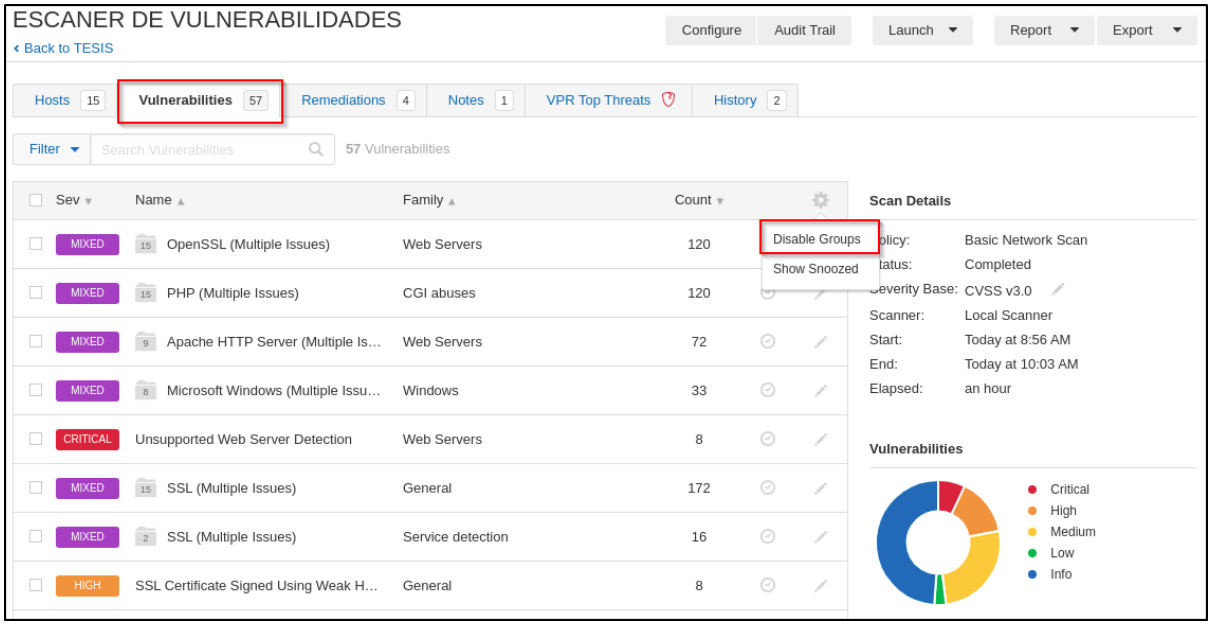


Figura 14. Resultados Nessus por grupo. Fuente: Autor.

Para continuar con la implementación del método, deshabilitamos la agrupación de amenazas (ver figura 14) y ordenamos por severidad, empezando por las de categoría crítica.

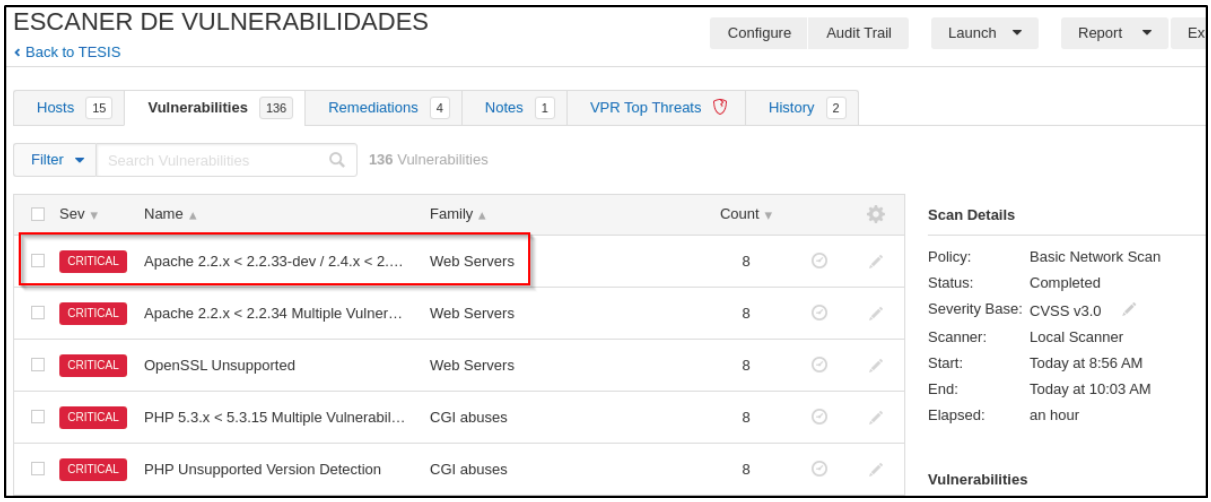


Figura 15. Resultados Nessus por nivel de riesgo. Fuente: Autor.

Accedemos a la primera vulnerabilidad en la lista (figura 15), podemos ver que es de severidad Critica.

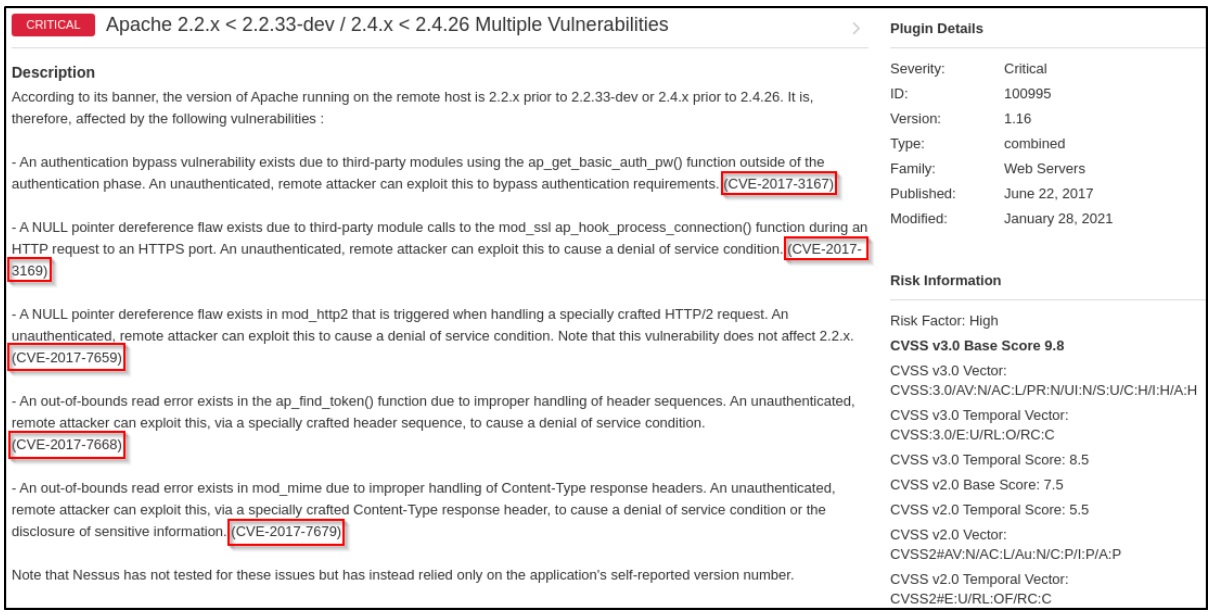


Figura 16. Nessus - Información vulnerabilidad Apache. Fuente: Autor.

La figura 16 nos muestra todas las amenazas a las que está expuesto este equipo, las mismas que podemos buscar en bases de datos o herramientas como *searchsploit* o *metasploit framework* con el fin de validar su aplicabilidad en este caso, tomando en cuenta las versiones del sistema operativo y el servicio que se encuentra vulnerable.

```
PORT      STATE SERVICE         VERSION
80/tcp    open  http            Apache httpd 2.2.21 ((Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1)
|_http-server-header: Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1
| http-title: Access forbidden!
|_Requested resource was http://10.0.10.184/xampp/
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2021-08-10T21:09:24+00:00; -6s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_IDEA_128_CBC_WITH_MD5
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: [redacted])
3306/tcp  open  mysql           MySQL 5.0.21-community-nt
| mysql-info: <
```

Figura 17. Escaneo de puertos nmap. Fuente Autor.

Continuando con el hallazgo, se procede a realizar la búsqueda respectiva de esta vulnerabilidad y se encuentran varios *exploits* en las herramientas *Metasploit Framework* y *searchsploit*, pero ninguno que se aplique a nuestras condiciones, las que podemos ver en la figura 17 (apache y mod_ssl 2.2.21, PHP 5.3.8, sistema operativo Windows). En la figura 18 podemos ver una lista de productos afectados por la vulnerabilidad conocida CVE-2017-3167, ningún sistema Windows está incluido.

- Products Affected By CVE-2017-3167

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Apache	Http Server	*	*	*	*	Version Details Vulnerabilities
2	OS	Apple	Mac Os X	*	*	*	*	Version Details Vulnerabilities
3	OS	Debian	Debian Linux	8.0	*	*	*	Version Details Vulnerabilities
4	OS	Debian	Debian Linux	9.0	*	*	*	Version Details Vulnerabilities
5	Application	Netapp	Clustered Data Ontap	-	*	*	*	Version Details Vulnerabilities
6	Application	Netapp	Oncommand Unified Manager	-	*	*	*	Version Details Vulnerabilities
7	Application	Netapp	Storagegrid	-	*	*	*	Version Details Vulnerabilities
8	Application	Oracle	Secure Global Desktop	5.3	*	*	*	Version Details Vulnerabilities
9	OS	Redhat	Enterprise Linux Desktop	6.0	*	*	*	Version Details Vulnerabilities
10	OS	Redhat	Enterprise Linux Desktop	7.0	*	*	*	Version Details Vulnerabilities
11	OS	Redhat	Enterprise Linux Eus	6.7	*	*	*	Version Details Vulnerabilities

Figura 18. Resultados CVE - productos afectados. Fuente: Autor.

Al no encontrar un exploit adecuado y siguiendo con el flujo, seleccionamos la siguiente vulnerabilidad en la lista, la cual, como se observa en la figura 19, si afecta a sistemas Windows.

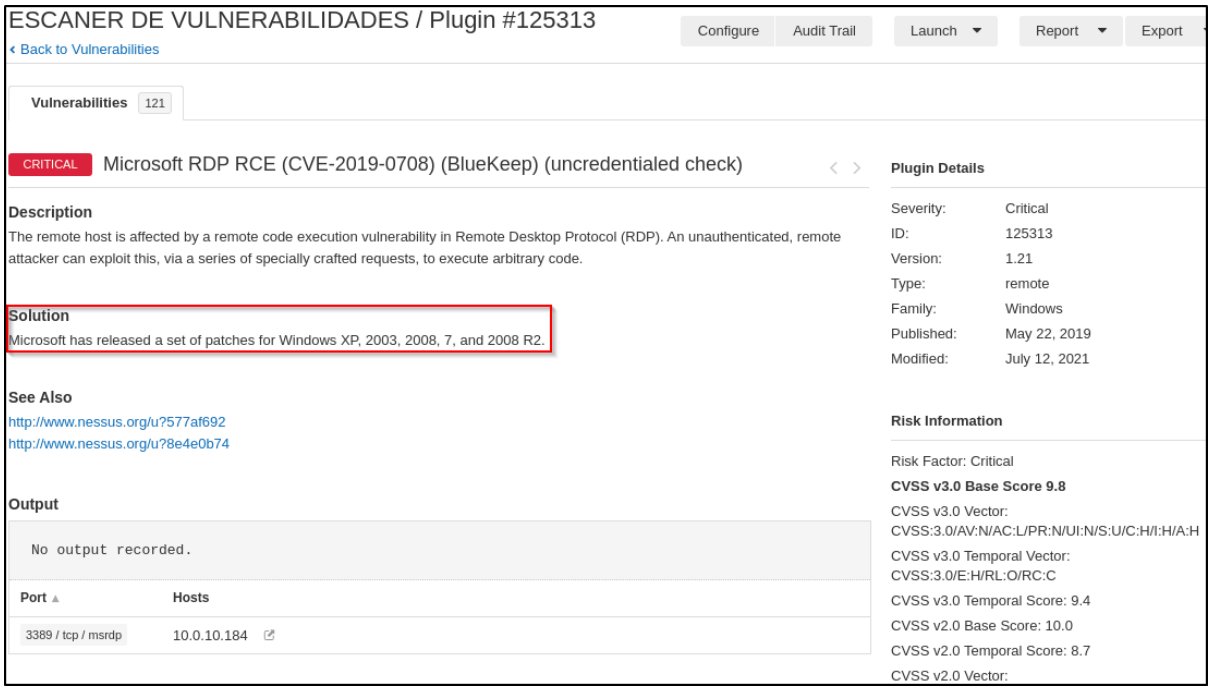


Figura 19. Nessus - Información vulnerabilidad Bluekeep. Fuente: Autor.

Haciendo una búsqueda rápida en *metasploit framework*, encontramos un auxiliar que determina si el host vulnerable, es de hecho explotable por esta vulnerabilidad. Para ello, abrimos la consola de *metasploit framework* con el comando *msfconsole,* seleccionamos el módulo adecuado, configuramos los parámetros y ejecutamos (ver figura 20).

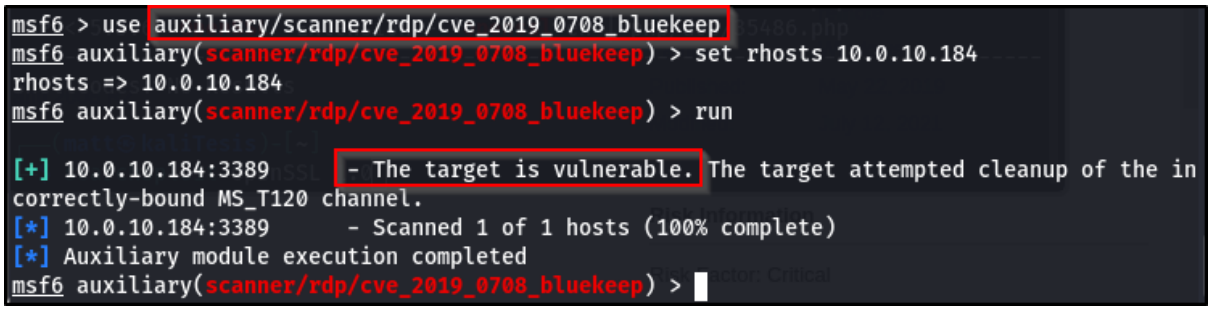


Figura 20. Metasploit Framework - ejecución de Auxiliar. Fuente: Autor.

El resultado de la prueba demuestra que el host cumple todas las condiciones para su explotación. El *exploit bluekeep* está disponible para su descarga en el sitio exploit-db.com al igual que en otras bases de datos de vulnerabilidades. Basta con descargarlo, configurar sus parámetros y ejecutarlo para ocasionar un ataque DOS al host vulnerable, razón por la que no se procedió con la explotación. Recordemos que lo que buscamos es la obtención de un *Shell* remoto y no ocasionar fallos a la operación normal de los equipos. Procedemos a documentar el importante hallazgo para incluirlo en el reporte final.

Ya que no hemos conseguido un *Shell* remoto, continuamos con la siguiente vulnerabilidad encontrada:

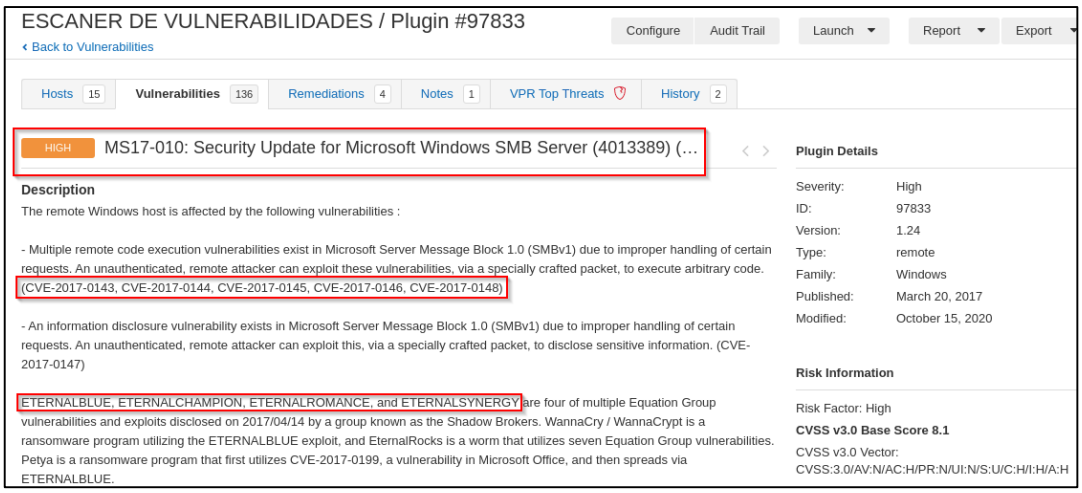


Figura 21. Nessus - Información vulnerabilidad Eternalblue 1. Fuente: Autor.

Hemos encontrado una vulnerabilidad bastante conocida dentro del protocolo SMB, esta vez, presente en el host 10.0.10.16 (figura 21).

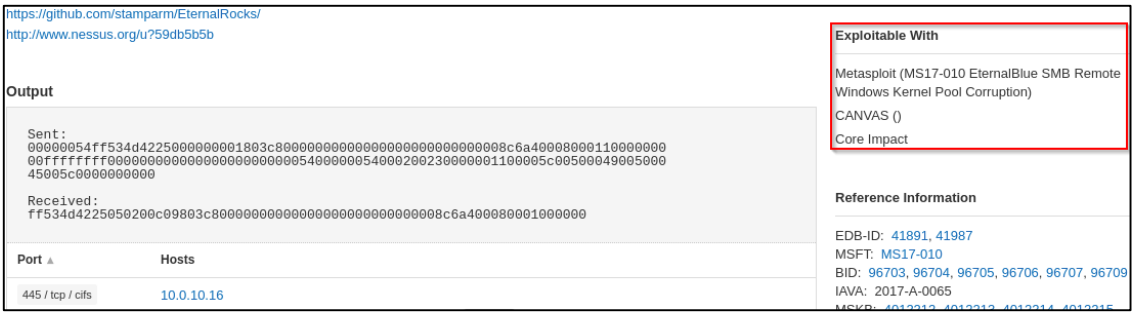


Figura 22. Nessus - Información vulnerabilidad Eternalblue 2. Fuente: Autor.

Como podemos ver en la figura 22, la herramienta Nessus nos indica que el host es explotable por la vulnerabilidad MS17-010, más conocida como *eternalblue* y que además permite la ejecución remota de código.

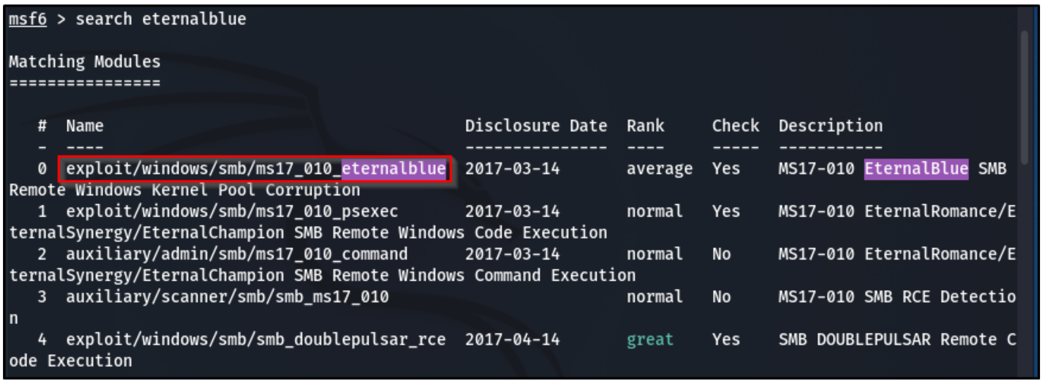


Figura 23. Metasploit Framework - Búsqueda Eternalblue. Fuente: Autor.

Procediendo a hacer el análisis respectivo en *Metasploit Framework*, encontramos el exploit *ms17_010_eternalblue* (figura 23) por lo que procedemos a la siguiente fase.

4.5 Explotación

Seleccionamos el exploit con el comando use y configuramos los parámetros necesarios para su ejecución. Podemos ver en la figura 24 que por defecto se configura el *payload reverse_tcp.*

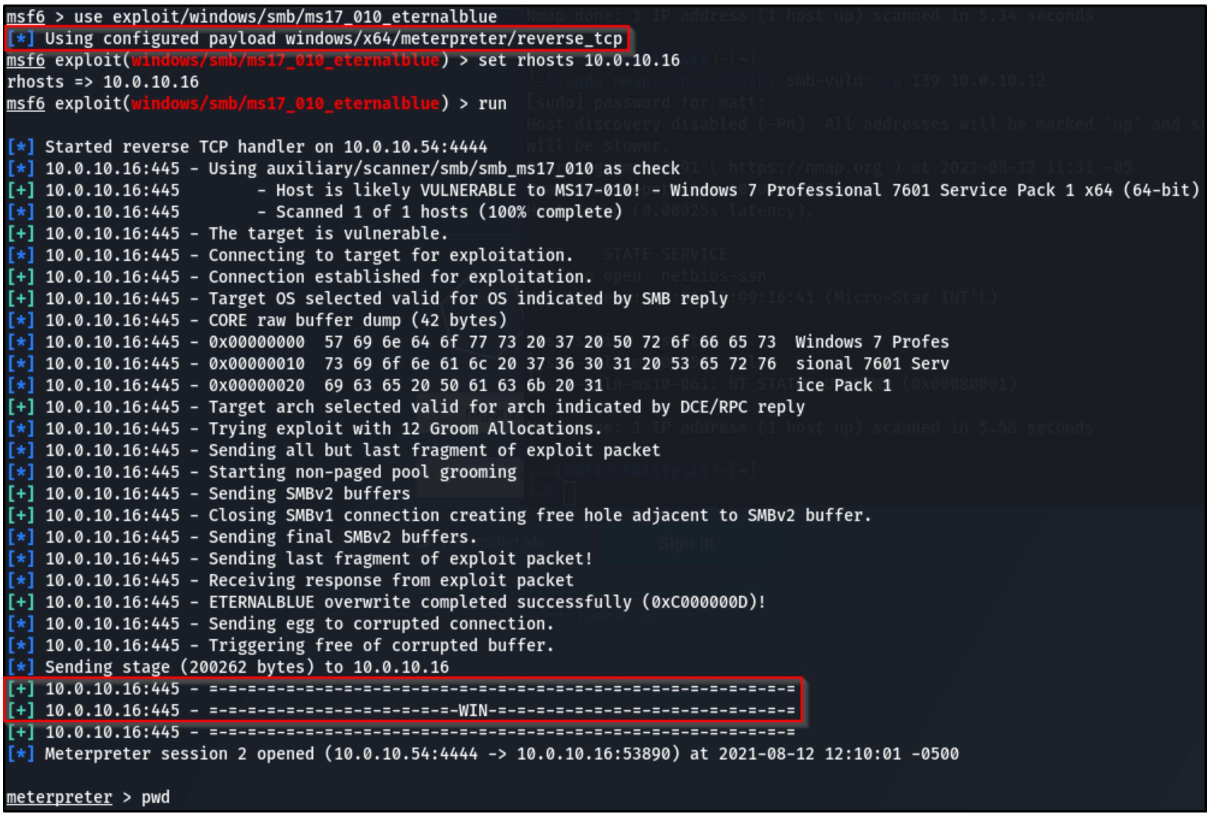


Figura 24. Metasploit Framework - Selección de Exploit. Fuente: Autor.

Dependiendo de las condiciones y sobre todo cuando el *payload* por defecto no se ejecuta con éxito, se puede cambiar el tipo de *payload.* En esta ocasión, el payload ha tenido éxito (ver figura 24) y hemos obtenido una sesión de *Meterpreter.* A continuación, se ha procedido a verificar información básica de la sesión y a obtener una sesión *Shell* normal (ver figura 25):

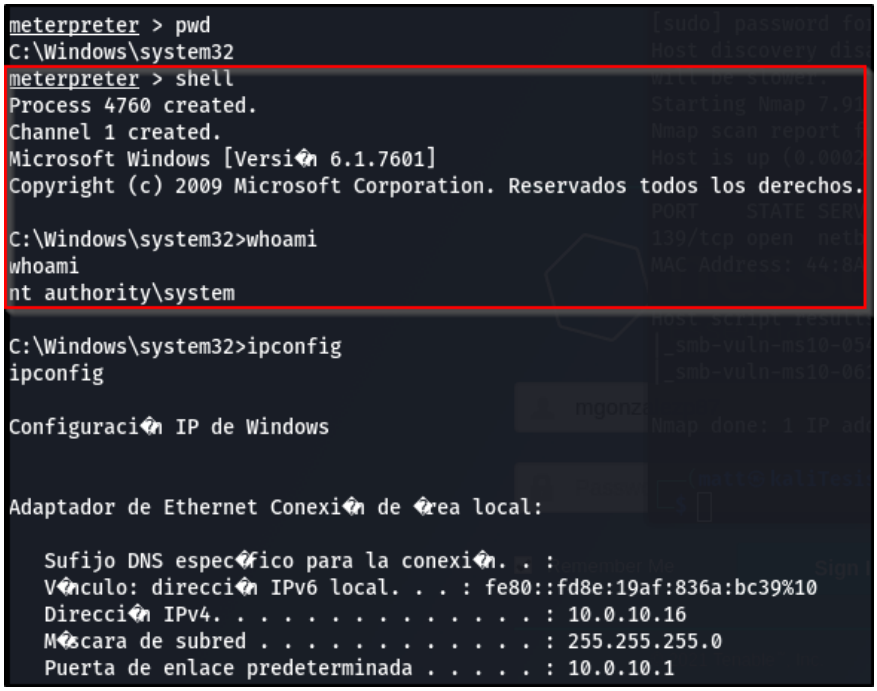


Figura 25. Metasploit Framework - Sesión de meterpreter. Fuente: Autor.

De aquí que el auditor puede crear conexiones adicionales, cambiar configuraciones y realizar actividades de post explotación y escalamiento de privilegios.

Ya que hemos conseguido una explotación exitosa, notificamos a la DTIC y Dirección y procedemos a documentar la ejecución de la fase y los hallazgos encontrados para incluirlos en el reporte final.

4.6 Reporte

El reporte final es extenso y contiene información sensible que de ser publicada podría llegar a comprometer la seguridad de la infraestructura y activos digitales de la organización, por lo que el mismo será entregado directamente a la DTIC y a la Dirección Provincial para gestión interna de la institución. Los pasos para la elaboración adecuada del reporte del test de penetración, se encuentran en el capítulo anterior.

Capítulo V

Análisis de resultados

Tras la implementación del caso de estudio, se ha podido comprobar que el método desarrollado en el presente trabajo, es útil como herramienta de pruebas de penetración. El método ha provisto las herramientas necesarias para agilizar los procesos ejecutados en cada fase, optimizando el consumo de recursos y minimizando los tiempos.

Comparado con las metodologías analizadas, el método propuesto es simple pero efectivo. Además, a diferencia de la mayoría, considera una fase de planificación, previa a la ejecución del test. La misma, a pesar de ser modesta, ha sido de gran utilidad aportando la información necesaria para proveer la planificación necesaria y garantías para la ejecución del test, en un ambiente seguro tanto para el cliente como para el auditor.

La ejecución del test de inicio a fin, desde su planificación hasta su explotación y elaboración del reporte final, ha tomado alrededor de 20 horas, proporcionando un promedio de 4 horas por fase. Este tiempo variará en cada caso, dependiendo del tamaño de la infraestructura a ser analizada y la experiencia del auditor.

Los resultados obtenidos en la ejecución de la prueba demuestran que, en la institución, la seguridad de la información no es un tema prioritario, seguramente por desconocimiento del riesgo al que están expuestos. Esperemos que el caso sea aislado y no se generalice para la mayoría de entidades del sector público.

El número de vulnerabilidades encontradas es alarmante (ver figura 26) sobre todo si se considera el tamaño de la infraestructura y el alcance del test realizado. Las amenazas de severidad Critica demuestran una infraestructura altamente vulnerable que, de ser comprometida, pondría en riesgo toda la información y la continuidad de los procesos de la institución.

Figura 26. Resultados test Nessus. Fuente: Autor.

Se pretende también con la implementación del test, el reporte sirva para la subsanación de los riesgos encontrados y se establezca una cultura de seguridad en la organización.

La explotación fue relativamente fácil. Esto seguramente al alto número de vulnerabilidades presentes en la infraestructura. También se comprobó que la institución continúa utilizando software desatendido, como el caso del sistema operativo Windows 7. Esto quiere decir que el software utilizado ya no tiene actualizaciones de seguridad y por lo tanto es vulnerable.

Finalizando, para una adecuada implementación del método, se requiere que el auditor posea conocimientos básicos sobre ciberseguridad y *ethical hacking*, ya que, de no hacerlo, la ejecución del test resultaría compleja y muy probablemente tienda al fracaso. El presente trabajo aborda los temas necesarios para proveer un conocimiento básico y llevar a cabo una implementación exitosa del método propuesto.

Capítulo VI

Conclusiones y trabajos futuros

6.1 Conclusiones

Los resultados de la implementación del caso de estudio, nos dan una clara idea de la situación en temas de seguridad de la información, dentro de las empresas pequeñas. Se comprobó que las mismas, a pesar de que, si cuentan con soluciones basadas en software o hardware como antivirus y firewalls, éstas proporcionan un falso sentido de seguridad. Si a esto le adicionamos el desconocimiento en las amenazas externas y sus modos de operación, provoca que los responsables de infraestructuras tecnológicas pequeñas, entren en una zona de confort en la que están prácticamente a la espera de un ataque, poniendo en riesgo todos los activos digitales de su empresa. En este punto es necesario considerar a la seguridad de la información como una solución integral que abarque todos los aspectos tanto técnicos como no técnicos de una empresa, como infraestructura, personal, políticas, etc., y no como la suma de herramientas que trabajan de forma aislada.

La bibliografía revisada proporciono una óptica ampliada de la ejecución de pruebas de penetración, sus fases y las distintas metodologías entre las que se enmarca, permitiendo diferenciar cada uno de sus enfoques y obteniendo información valiosa que fue el sustento de lo propuesto en el presente trabajo.

Al igual que las metodologías analizadas, el método propuesto cubre todas las fases correspondientes a una prueba de penetración, con la diferencia de que está orientado al análisis de red, por lo que permite ser especifico en sus requerimientos, de esta manera se evita la generalización y se minimiza la ambigüedad en la comprensión de criterios por parte del auditor. También provee las herramientas para su ejecución.

En este sentido, el presente trabajo de titulación ha cumplido con los objetivos propuestos, ofreciendo una herramienta completa y sencilla en su ejecución. La aplicación del caso de estudio nos permitió comprobar su efectividad al analizar una infraestructura tecnológica, encontrar sus vulnerabilidades y darles seguimiento hasta conseguir una explotación exitosa. El reporte final nos da una idea de los riesgos a los que está expuesto la infraestructura, a la vez que compromete a la Dirección de Tecnologías a subsanar las mismas y a tomar acciones para prevenir riesgos futuros o mitigar su impacto. Todo esto, en menos de 20 horas de trabajo.

La brecha de profesionales en el área de seguridad de la información se hace tangible cuando encontramos infraestructuras tan desatendidas que demuestran el poco conocimiento de los

profesionales a cargo, y que se traduce en empresas susceptibles a todo tipo de ataques. La seguridad de la información debería ser un tema de interés para todo tipo de empresas, y la socialización de este tipo de temas a través de talleres y capacitaciones a su personal, generando una cultura de seguridad, una prioridad.

Se considera que el método propuesto puede ayudar a cubrir, de cierta forma, el déficit de profesionales de ciberseguridad, ya que es una herramienta simple, pero a la vez efectiva, requiere de pocos recursos (humanos, económicos y tiempo) y es relativamente fácil de ejecutar. Como en el caso de cualquier auditoria de seguridad, es muy importante implementarla de manera periódica, sea semestral o anual, de esta forma podemos llevar un control de la efectividad de las acciones tomadas y soluciones provistas para los riesgos encontrados. Lo más beneficioso de todo esto, es que se establece una cultura de seguridad en las empresas, sin importar su tamaño.

6.2 Trabajos futuros

Ya que el presente trabajo está orientado al análisis de red (*network assessment*), como trabajos futuros podemos considerar la creación de métodos paralelos, cambiando su orientación o enfoque, por ejemplo, se podría proponer un método de pentest orientado únicamente a páginas web (*webapp assessment*), con orientación al host (*host assessment*), o a bases de datos.

Cambiando un poco la línea de investigación, sería interesante la elaboración de un método orientado hacia las personas. En este caso se propondría un modelo para pruebas de penetración con el uso únicamente de técnicas de ingeniería social.

Bibliografía

Breve historia de los "hackers" y sus andanzas. (2011, junio 9). BBC News Mundo. https://www.bbc.com/mundo/noticias/2011/06/110609_tecnologia_breve_historia_hackers_nc

Chávez Cruz, G., Campuzano Vásquez, J., & Betancourt Gonzaga, V. (2018). Las micro, pequeñas y medianas empresas. Clasificación para su estudio en la carrera de Ingeniería en Contabilidad y Auditoría de la Universidad Técnica de Machala. *Conrado*, *14*, 247–255.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Constitución del Ecuador (2008). 218.

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity ??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing Ltd.

Ec Council. (2020). *CEH Ethical Hacking and Countermeasures v11*.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, *2*(12), 145–155. https://doi.org/10.23857/pc.v2i12.420

Gasca Hurtado, G. P. (2010). ESTUDIO DE SIMILITUD DEL PROCESO DE GESTIÓN DE RIESGOS EN PROYECTOS DE OUTSOURCING DE SOFTWARE: UTILIZACIÓN DE UN MÉTODO. *Revista Ingenierías Universidad de Medellín*, *9*(17), 12.

Gonzalez, R. (2019, junio 20). *Estiman en $87 mil 940 millones pérdidas anuales por ataques cibernéticos | La Prensa Panamá* [Periodico en linea]. La Prensa. https://www.prensa.com/economia/Estiman-millones-perdidas-anuales-ciberneticos_0_5331966763.html

Greavu Serban, V., & Serban, O. (2014). Social Engineering A General Approach. *Informatica Economica*, *18*(2/2014), 5–14. https://doi.org/10.12948/issn14531305/18.2.2014.01

Guillen Zafra, J. L. (2017). *Introducción al pentesting*. 66.

ISECOM. (2010). *OSSTMM 3*. www.isecom.org/OSSTMM.3.pdf

Israel. (2020, abril 16). *Los tipos de ciberataques a empresas más frecuentes*. Viewnext. https://www.viewnext.com/tipos-de-ciberataques-a-empresas/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

MAP | Kaspersky Cyberthreat real-time map. (s/f). MAP | Kaspersky Cyberthreat Real-Time Map. Recuperado el 14 de agosto de 2021, de https://cybermap.kaspersky.com

Martí, R., & Lloret, J. (2016). *Desarrollo e implementación práctica de un PENTEST*. https://riunet.upv.es/handle/10251/70164

Microsoft. (s/f). *Análisis del modelo de amenazas—BizTalk Server*. https://docs.microsoft.com/es-es/biztalk/core/threat-model-analysis

Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe | Publications. (s/f). Recuperado el 14 de agosto de 2020, de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Samonas, S., & Coss, D. (2014). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*. 25.

Santiago, E. J., & Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. *Tecnología y desarrollo*, *15*, 10.

Santo Orcero, D. (2018). *Pentesting con Kali: Aprende a dominar la herramienta Kali para hacer tests de penetración y auditorías activas de seguridad*.

Sierra, O. (2018). *ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LAS GUIAS DEL OSSTMM v3*. 11.

The Penetration Testing Execution Standard. (s/f). Recuperado el 6 de junio de 2020, de http://www.pentest-standard.org/index.php/Main_Page

Valdez Alvarado, A. (2013). *OSSTMM 3—ARTICULO*.

Vargas Borbúa, R., Recalde Herrera, L., & Reyes Ch., R. P. (2017). *Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa*. http://repositorio.flacsoandes.edu.ec/handle/10469/12199

Glosario

Autenticación: Es la capacidad de validar o identificar a un usuario autorizado o genuino, y su nivel de acceso a un activo digital.

Vulnerabilidad: Característica de debilidad de un recurso tecnológico que lo expone a un acceso no autorizado o a ser explotado por una amenaza.

Amenaza: Se considera amenaza a todo aquello (incidente o evento) que, de ocurrir o materializarse, causaría daños a los recursos tecnológicos de una organización.

Riesgo: Es la combinación de probabilidad de ocurrencia y el impacto (positivo o negativo), de materializarse una amenaza.

Malware: Se considera malware a todo aquel software malicioso (de ahí proviene el nombre) que instalado en un equipo trata de ganar accesos no autorizados al explotar sus vulnerabilidades. Tiene varias clasificaciones.

Virus informático: Programa o código malicioso que está diseñado para alterar el comportamiento normal de un dispositivo electrónico, por lo que su presencia suele notarse. Se propaga de equipo a equipo, adjunto a un programa legítimo y se ejecuta solo por intervención del usuario.

Worm: Se considera una subcategoría del virus ya que su comportamiento es muy similar, sin embargo, no necesita la intervención del usuario para ejecutarse ni replicarse por la red. Puede aprovechar los servicios de red del sistema anfitrión para viajar por la red sin ser detectado.

Trojan: malware que aparenta ser un programa legítimo, pero en realidad son programas destructivos que pueden llegar a robar información o instalar *backdoors* en el anfitrión.

Backdoor: malware cuya finalidad es permitir sin conocimiento del usuario, el acceso remoto de un agente malicioso y ejercer control sobre el equipo infectado.

Keylogger: Capturan y registran cada pulsación de teclado en un archivo de texto plano que luego es enviado a un tercero para su beneficio. Son una subcategoría de spyware ya que capturan información confidencial como credenciales de acceso o información financiera.

Rootkit: malware basado en un conjunto de herramientas que buscan pasar inadvertidos y conseguir privilegios de administrador en un sistema. Se utilizan para ocultar puertos abiertos, comunicaciones y la ejecución de otros tipos de malware del usuario y de herramientas de seguridad como antivirus.

Ransomware: Viene del inglés *"ransom"* que significa rescate. Malware que encripta o bloquea todo el contenido del disco duro de un equipo a modo de secuestro, y solicitan el pago de una recompensa a cambio de liberarlo.

Bots: Son programas o scripts que realizan tareas de forma automatizada y sus consecuencias son diversas. Pueden operar de manera aislada o en una red de equipos o bots (botnet) en la que un atacante puede llegar a controlar decenas de miles de computadores con la intención de ejecutar ataques de denegación de servicio, lanzar campañas a gran escala de spam u otro tipo de ciberataque.

Spyware: Malware que puede instalarse en el anfitrión por si mismos o mediante otras aplicaciones. Actúan de forma sigilosa para robar información confidencial del equipo anfitrión, recopilar datos de las aplicaciones, disco duro, historial de navegación, etc.

Adware: Es software de tipo invasivo. No intenta robar información ni mucho menos dañar el equipo anfitrión, pero invade la pantalla, aplicaciones o el navegador con publicidad, lo que es realmente molestoso. Algunos adware entran en la categoría de spyware ya que recolectan y envían información personal.

Phishing: tipo de ataque en el que el atacante intenta engañar a su objetivo a través de llamadas telefónicas o e-mail, con sitios web falsos o contestadoras de voz interactivas, simulando ser, por ejemplo, instituciones financieras y solicitando información personal.

Spam: envió indiscriminado de correo electrónico no solicitado y masivo.

Baiting: Es una sub categoría del phishing ya que se busca atraer a los usuarios con engaños y ofrecimientos como premios o cosas por el estilo. Se envían por medio de spam, sitios web maliciosos o incluso de forma física. El atacante "olvida" un pendrive en el escritorio de su víctima o en una cafetería. Al conectar el dispositivo se ejecuta código malicioso sin conocimiento de la víctima.

Tailgating: Consiste en acceder a lugares restringidos aprovechándose de gente con acceso legítimo. Por ejemplo, un atacante vestido con el uniforme de la empresa le pide a un trabajador que le sostenga la puerta. Estos ataques exponen a las empresas a robo de información, sabotaje, terrorismo, etc.

Dumpster diving: Consiste en buscar información relevante acerca del objetivo, en los contenedores de basura de la organización o de cada empleado. También se considera dumpster diving el apoderarse de tecnología desechada de las víctimas como computadores y celulares viejos o discos duros dañados para intentar extraer información de los mismos.

Shoulder surfing: Consiste en mirar por encima del hombro de la víctima mientras digita claves o información sensible.

Denegación de Servicio (DoS): Este tipo de ataque atenta contra el principio de disponibilidad, ya que busca inhabilitar el acceso a un equipo o recurso de red a sus usuarios legítimos. Es causado por eventos o acciones que eliminan la capacidad de operación de un recurso de red, por ejemplo, saturar con solicitudes un sitio web, disminuyendo el poder de procesamiento del servidor.

Cross Site Scripting (XSS): Un atacante ejecuta código JavaScript en el navegador de la víctima con la intención de robarle información sensible. Se aprovecha de ciertas vulnerabilidades presentes en algunos sitios web.

Session Hijacking (Man in the middle): El ataque de hombre en el medio consiste en que, sin autorización, un tercero se apropia de un canal de comunicación entre varios terminales. De esta forma el atacante puede interrumpir, manipular o reemplazar el tráfico del canal sin el conocimiento de las víctimas, quienes confían en que el canal de comunicación está seguro y protegido.

Sql Injection: La inyección Sql intenta tomar ventaja de los campos de entrada de un sitio web, que no han sido codificados correctamente. En este tipo de ataque, el atacante inserta una sentencia sql maliciosa en un campo de entrada, esperando acceder a la base de datos y manipular sus registros.

Exploit: Código, secuencia de comandos o software que se aprovecha de un error o vulnerabilidad presente en un sistema.

Payload: Es la carga que se ejecuta al aprovechar una vulnerabilidad explotada.

Metasploit Framework: Plataforma completa para la ejecución de test de penetración que contiene módulos para realizar varios tipos de ataques y actividades relacionadas con el pentest.

Meterpreter: payload muy potente que viene integrado con *metasploit framework*. Contiene un intérprete de línea de comandos que permite interactuar con el objetivo y realizar actividades de post explotación.

Arpanet: Red computacional creada en 1969 para la transferencia de datos de carácter militar y de investigación en los Estados unidos. Se le considera la precursora de lo que hoy se conoce como Internet.

VPN: Red privada virtual.

Proxy: Programa o dispositivo que hace de intermediario en una comunicación entre 2 puntos.

Nat: Network address translation, o traducción de direcciones de red. Protocolo que permite la interacción de redes locales con el internet, con el fin de preservar direcciones IP.

Datacenter: Centro de procesamiento de datos.

Fingerprinting: Proceso de descubrimiento del Sistema operativo y versión que utiliza un host.

Host: En informática, se refiere a cualquier dispositivo conectado a una red de datos.

OS: Sistema operativo.

ICMP: Protocolo de mensajes de control de internet. Reporta errores en la generación y envío de mensajes a través del protocolo IP.

Ping sweep: Técnica utilizada en el escaneo de red para descubrir hosts activos. También se le conoce como Barrido de direcciones IP.

Firmware: Programa básico que controla los circuitos de un dispositivo electrónico.

Active directory: Proporciona servicios de directorio en una red empresarial. Aunque tiene varias funciones, se utiliza generalmente para la gestión de equipos, usuarios y recursos de una red.

Pop 3: Protocolo para la transferencia de correo electrónico.

Imap: Protocolo para la transferencia de correo electrónico.

Sniffer de red: Aplicación que analiza y captura paquetes en tránsito dentro de una red de datos.

CVE: Common vulnerabilities and exposures. Registro que identifica las vulnerabilidades y exposiciones comunes.

Bug: Error de código en un software que ocasiona un mal funcionamiento.

ISP: Internet service provider o proveedor del servicio de internet.

NIST: National Institute of Standards and Technology. Instituto Nacional de Estándares y Tecnologías.

ITIL: Information Technology Infrastructure Library**.** Biblioteca de infraestructuras de tecnologías de la información. Conceptos y buenas prácticas para la gestión de servicios de TI.

Shell: Interprete de línea de comandos para interactuar con el anfitrión.

Anexos

Anexo 1. Formulario de autorización de Pentest

FORMULARIO DE AUTORIZACIÓN DE PENTESTING

Beneficiario:	[redacted]
Representante:	[redacted]
Cargo:	[redacted]
Fecha:	06 de agosto de 2021
Auditor:	Ing. Martin Gonzalez Palomeque

1. Información relacionada al test

El beneficiario de la prueba de penetración autoriza al Ing. Martin Gonzalez Palomeque para llevar a cabo las actividades de verificación de seguridad de los equipo(s), sistema(s) y red que se describe(n) a continuación, según las siguientes condiciones:

- **Alcance (Activos autorizados):**
  - Todos los equipos de red y de cómputo de la oficina de la [redacted] incluidos sus sistemas, dentro de su rango de direccionamiento IP interno [redacted] todos los puertos TCP, UDP y servicios activos.

- **Condiciones:**
  - Las pruebas serán internas y se realizarán desde dentro de la red del cliente utilizando una conexión cableada o inalámbrica para acceder a los activos incluidos en el alcance.
  - Se realizarán un único TEST de penetración:
    - Caja blanca.
      - Orientación: Network Assessment

- **Planificación temporal:**
  - Fecha de inicio: 10 de agosto de 2021.
  - Fecha de finalización: 13 de agosto de 2021.
  - Horario de ejecución de las pruebas: Entre las 08:00 y 16:30 horas.

- **Teléfonos de soporte y notificación en caso de caída de servicio:**
  - Beneficiario:
    - Nombre: [redacted]
    - Teléfono: [redacted]
    - Email: [redacted]
  - Auditor:
    - Nombre: Martin Gonzalez Palomeque
    - Teléfono: 0992513784
    - Email: martin.gonzalez@ucuenca.edu.ec

2. Tipos de pruebas (Pentesting)

El servicio de test de intrusión nos permite testear la fortaleza de la infraestructura IT para medir su nivel de seguridad técnico y si cumple los niveles requeridos por la política organizativa. Estos test son realizados por expertos en seguridad sobre todos los servicios expuestos a internet y aquellos que puedan accederse remotamente. Se pueden realizar dos tipos distintos de Test de Intrusión, Externo o Interno dependiendo desde dónde se realicen los ataques.

- El **Test de Intrusión Externo**: se realiza desde internet sobre la infraestructura del cliente, más concretamente, sobre aquellos dispositivos de la organización que están expuestos a internet, por ejemplo, router, firewall, servidor web, servidor de correo, DNS, etc.
- El **Test de Intrusión Interno**: se realiza desde dentro de la red del cliente desde donde pueden localizarse más problemas de seguridad que con un test externo.
- Propósito del pentest: Comprobar el estado de las vulnerabilidades que presenta la infraestructura tecnológica del beneficiario, a nivel de red.

Los tipos de test descritos, se pueden clasificar de la misma forma en tres tipos de pruebas, dependiendo su enfoque:

- **Test de Intrusión de Caja Negra**: este es un tipo de test de intrusión externo, sin información o solo con muy poca información del objetivo (solo lo que debe ser auditado). Por ejemplo, dada una web o portal publicado, intentar atacarlo desde una red externa sólo a partir de información básica disponible, desconociendo información relativa a arquitectura, usuarios, etc.
- **Test de Intrusión de Caja Gris**: este tipo de test puede ser interno o externo, poseyendo solo información limitada sobre el objetivo como, por ejemplo, credenciales de autenticación básicas.
- **Test de Intrusión de Caja Blanca**: este tipo de test es interno, accediendo a la red desde un punto de acceso y teniendo el diagrama de red, las plataformas, los servicios principales, y varios perfiles con distintas credenciales y privilegios, etc.

Dada la naturaleza de los trabajos a realizar cabe la posibilidad de que, de forma no intencionada, se produjese algún efecto colateral indeseado. Si así fuese, el Auditor lo notificaría inmediatamente al Teléfono de soporte correspondiente o se pondría a disposición del cliente para aportar la información requerida sobre las acciones realizadas.

2.1. Restricciones y conformidades

Las siguientes restricciones se aplicarán a esta autorización:

- Esta autorización estará vigente desde el 10 de agosto de 2021 hasta el 12 de agosto de 2021.

De conformidad con la concesión de esta autorización, el Beneficiario declara que:

- Es dueño de los sistemas donde se realiza la auditoria de vulnerabilidades y el suscrito tiene la autoridad adecuada para poder llevar a cabo las actividades de verificación de seguridades a nivel de red.
- Ha creado una copia de seguridad completa de todos los sistemas dentro del ámbito de las pruebas de vulnerabilidades, y se ha comprobado que el procedimiento de copia de seguridad permitirá al cliente restaurar los sistemas a su estado previo al test.
- El servicio implica necesariamente el uso de herramientas y técnicas diseñadas para detectar las vulnerabilidades de seguridad, y que es imposible identificar y eliminar todos los riesgos asociados a los activos digitales.
- El cliente se compromete a no modificar la infraestructura tecnológica durante la ejecución del test. Si esto sucediera se entenderá como un cambio de alcance, de tal modo que el pentest se dará por finalizado y se entregará el informe al cliente con los resultados obtenidos hasta ese momento.

Cualquier cambio a las limitaciones y condiciones descritas deberá realizarse por escrito y ser aceptado por ambas partes.

Para constancia de aceptación del presente documento, suscriben las partes:

Ing. Martin Gonzalez Palomeque
C.I. 0301588091
Auditor

Anexo 2. Acuerdo de Confidencialidad

[redacted]

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN PARA [redacted]

Intervienen en la celebración del presente "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN", por una parte, [redacted] con cédula de ciudadanía Nro. [redacted], en mi calidad [redacted], en adelante y para efectos del presente instrumento en representación de [redacted] en calidad de Proveedor de Información; y por otro lado el Ing. Martin Fernando Gonzalez Palomeque con cédula de ciudadanía Nro. 0301588091 en mi calidad de Auditor de Seguridad, en adelante y para efectos del presente instrumento en calidad de Receptor de la Información quienes libre y voluntariamente celebran el presente acuerdo.

Ambas partes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base a las siguientes cláusulas.

CLÁUSULA PRIMERA. - ANTECEDENTES:

El artículo 226 de la Constitución de la República del Ecuador prevé que: "Las instituciones del Estado sus organismos y dependencias, y las servidoras o servidores públicos, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";

En virtud de lo establecido en el numeral 19 del artículo 66 de la Norma Suprema se dispone: "Se reconoce y garantizará a las personas: (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley";

El artículo 178 del Código Orgánico Integral Penal establece: "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…";

El artículo 190 ibídem señala: "La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de

1

telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años(...)";

El artículo 230 del Código Orgánico Integral Penal determina: "Será sancionada con pena privativa de libertad de tres a cinco años: (...) La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (...)";

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en los artículos 2 y 44, respectivamente, reconoce ante el Estado la validez jurídica de los mensajes de datos electrónicos, así como el valor y efecto jurídicos de cualquier actividad, transacción mercantil, financiera o de servicios que se realice con los mismos por medio de redes electrónicas;

La Carta Iberoamericana de Gobierno Electrónico, en la sección 24, recomienda a los gobiernos tomar en consideración la importancia de la interoperabilidad de las comunicaciones y servicios, así como disponer las medidas necesarias, para que todas las entidades públicas, cualquiera que sea su nivel y con independencia del respeto a su autonomía, establezcan sistemas que sean interoperables;

La Ley del Sistema Nacional de Registro de Datos Públicos publicada en el Registro Oficial No. 162 de 31 de marzo de 2010, en su artículo 4, cita: "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información...";

El artículo 27 de la Ley ibídem establece: "Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos utilizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas";

Bajo este marco regulatorio, la información que se dispone en los servicios institucionales se clasifica como reservada y/o confidencial, a tal efecto se acuerda suscribir el presente "Acuerdo de Confidencialidad y No Divulgación de la Información" entre la entidad que solicita el acceso a los servicios institucionales y la entidad proveedora del servicio con la finalidad de proteger la información que se consuma cuando ésta tenga el carácter de reservada y/o confidencial.

[redacted]

Se garantizará la confidencialidad, integridad, disponibilidad, reserva y protección de los datos e información que se comparta e intercambie entre las entidades, de acuerdo a la normativa vigente.

CLÁUSULA SEGUNDA. - OBJETO:

En virtud de los antecedentes expuestos, por medio del presente instrumento el RECEPTOR DE LA INFORMACIÓN se obliga expresamente a guardar sigilo, confidencialidad y reserva sobre el contenido de toda la información generada, verbal o escrita, que se comparta entre las partes.

La información obtenida por el RECEPTOR DE LA INFORMACIÓN será utilizada para investigación científica como parte de su trabajo de titulación de Master en la Universidad de Cuenca, y sus resultados serán publicados, preservando la anonimidad del PROVEEDOR DE LA INFORMACIÓN y enmascarando o alterando la información que pudiera perjudicar de cualquier forma a [redacted].

Además, el RECEPTOR DE LA INFORMACIÓN se compromete a hacer uso de la información, únicamente para las actividades descritas en el FORMULARIO DE AUTORIZACIÓN DE PENTEST, anexo al presente documento.

CLÁUSULA TERCERA. - DERECHOS Y OBLIGACIONES:

Son deberes de quien haga las veces de **RECEPTOR DE LA INFORMACIÓN**:

1. Guardar la reserva y confidencialidad, sin el deterioro de cualquier tipo de información que se le suministre o a la cual llegare a tener acceso o conocimiento;

2. Mantener en forma estrictamente reservada y confidencial toda la información que por razón de su competencia tendrá acceso, por lo tanto, se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral, escrito, y/o tecnológico y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses de la Institución a la cual pertenece.

3. Utilizar la información suministrada por [redacted] únicamente para los fines acordados por las partes.

No realizar copia o duplicado alguno de la información mencionada en este acuerdo sin la autorización previa y escrita de la otra parte; tampoco podrán divulgar dicha información a terceras personas sin que medie igualmente la respectiva autorización previa y escrita de la otra parte. Se excluye de esta obligación la información que sea de dominio público o que sea del conocimiento previo de [redacted] sin constituir discreción de la información en los términos del presente acuerdo y, cuya revelación no cause agravio o perjuicio alguno a su titular.

3

[redacted]

CLÁUSULA CUARTA. - PATRÓN DE CONDUCTA, IMPLICACIONES DE LA RECEPCIÓN DE LA INFORMACIÓN Y RESPONSABILIDAD

Las partes actuarán con responsabilidad en el buen uso de la información, lo que supone entre otros deberes, el de limitar la divulgación autorizada al menor número de personas, y el de tomar las medidas idóneas y eficaces para evitar el tráfico y fuga indebida de la información, así como su uso por fuera de los límites de este convenio.

El incumplimiento del deber de reserva establecido en la Cláusula Cuarta de este acuerdo, constituye violación de secreto y justa causa de terminación unilateral de la relación, sin desmedro de las indemnizaciones (sólo para proveedores) legales correspondientes.

El **RECEPTOR DE LA INFORMACIÓN** reconoce que la información confidencial a la que se refiere el presente acuerdo posee una valoración en imagen institucional y su indebida divulgación o utilización causa un perjuicio.

CLÁUSULA QUINTA. - MATERIALES:

Todos los materiales como, documentos, actas de reunión, fichas de consumo, entre otras que son entregadas al **RECEPTOR DE LA INFORMACIÓN** por parte de [redacted] se considera como información confidencial y se debe guardar absoluta reserva de la misma.

CLÁUSULA SEXTA. - SANCIONES:

Para la aplicación de sanciones se tomará en cuenta lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley Orgánica del Sistema Nacional de Registro de Datos Púbicos y demás normativa aplicable; sin perjuicio de las acciones civiles y penales que procedan en cada caso.

CLÁUSULA SÉPTIMA. -:

En los casos en que la información sea calificada como "Reservada" o "Confidencial" por mandato legal, las entidades que suscriben el presente acuerdo evaluarán la pertinencia de entregar o no dicha información.

CLÁUSULA OCTAVA. - DOCUMENTOS HABILITANTES:

Para la suscripción del presente instrumento, las partes presentarán las respectivas delegaciones o nombramientos que les permita actuar en representación de las entidades intervinientes.

CLÁUSULA NOVENA. - VIGENCIA:

[redacted]

El presente instrumento tendrá una vigencia de cinco años a partir de la fecha de suscripción.

CLÁUSULA DÉCIMA - ACUERDO TOTAL:

Este acuerdo incluye el total entendimiento entre las partes con relación a la materia de la cual se trata este documento. Cualquier añadidura o modificación a este acuerdo deberá ser hecha por escrito y firmada por ambas partes.

CLÁUSULA DÉCIMA PRIMERA: NOTIFICACIONES. –

En el evento de que se produzca el incumplimiento de alguna de las cláusulas estipuladas en el presente acuerdo, la parte afectada, notificará del incumplimiento a la máxima autoridad de la institución involucrada, sin perjuicio de las acciones y sanciones previstas en la normativa vigente.

Una vez comprendido por los comparecientes el contenido y efectos del presente instrumento expresamente se ratifican en él, para fe y constancia se firma el presente documento por quienes en él intervinieron, en la ciudad de [redacted] el día 06 del mes de agosto del año 2021, en dos ejemplares del mismo tenor y validez.

[redacted]

Ing. Martin Gonzalez Palomeque
C.I. 0301588091
Auditor

5