Artículo de Investigación. Revista Killkana Técnica. Vol. 6, No. 1, pp. 43-68, enero-abril, 2022.
ISSN 2528-8024. ISSN Elect. 2588-0888. Universidad Católica de Cuenca

Metodología breve para la ejecución de pruebas de intrusión. Caso de estudio

Quick methodology for intrusion testing. A case study

Martin Gonzalez Palomeque[1]

[1] Universidad de Cuenca

* martin.gonzalez@ucuenca.edu.ec
DOI: https://doi.org/ 10.26871/killkanatecnica.v6i1.949

Resumen

En la presente investigación se desarrolla una metodología para la ejecución de pruebas de intrusión que sea fácil y rápida de implementar para todo tipo de empresas, especialmente para empresas pequeñas que no cuentan con personal de TI o disponen de personal limitado en esta área. Para ello, la metodología desarrollada se basa en la ejecución de herramientas automatizadas, a la vez que suministra las técnicas y procesos necesarios para su correcta implementación. La aplicación del caso de estudio permitió comprobar que la metodología desarrolla-

da es efectiva, rápida y optimiza el uso de recursos. Los resultados demuestran la falta de conciencia por parte de las empresas en temas de ciberseguridad y dejan en evidencia el poco o nulo conocimiento de los profesionales de TI en esta área.

Palabras clave: *ciberseguridad, seguridad de la información, pruebas de intrusión, metodología.*

Abstract:

This research develops a methodology for executing intrusion tests of easy and fast implementation in all types of companies, especially in small companies that lack or have limited personnel in the IT area. In order to achieve this, the methodology uses of automated tools while providing the necessary techniques and processes for its appropriate implementation. The application of the case study proved that the methodology developed is effective, fast and optimizes resources. The results demonstrate the lack of awareness on the companies' part regarding cybersecurity issues and evidencing the lack of knowledge of IT professionals in this area.

Keywords: *cybersecurity; information security; intrusion testing; methodology.*

1. Introducción

La adopción de las tecnologías de la información en los procesos críticos de las empresas trae consigo beneficios que no se podrían obtener de otra forma [1]. Debido a esto, el uso de las TIC's se ha masificado en los últimos años y no solo en el campo empresarial e industrial, sino en el personal, educativo, de salud y demás ámbitos de la sociedad. Sin embargo, esta hiperconectividad no solo aporta beneficios, también supone riesgos latentes, que, de no gestionarse de manera adecuada, exponen a las empresas y sus activos digitales a cualquier cantidad de amenazas [2].

Las amenazas tecnológicas han evolucionado de tal manera, que resulta difícil etiquetarlas o clasificarlas [3], el virus informático se ha convertido en un abanico de herramientas sofisticadas que actualmente invalida la utilidad de los sistemas de detección y control tradicionales [2].

Así mismo, el incremento en el número de ciberataques en los últimos años es alarmante [4]. El mapa en vivo de ataques cibernéticos de Kaspersky [5] nos demuestra que el ciber crimen no discrimina país, región, persona, empresa grande o pequeña. El bajo costo y riesgo en la perpetración de este tipo de ataques, considerando que solo se precisa de un computador y una conexión a internet, son un factor relevante para este aumento acelerado. Un dato importante es que, las empresas son el objetivo principal y a las que están dirigidos la gran mayoría de estos ataques [6].

El problema principal se debe a la falta de implementación u omisión de controles de seguridad [2] muchas veces básicos dentro de las empresas, esto a su vez, según [4], es consecuencia del desconocimiento y falta de preparación de las empresas y profesionales de TI, y del presupuesto que asignan las empresas a asegurar sus activos digitales [7].

Continuando con [4], el problema va mucho más allá. En América Latina y el Caribe son pocos los países que han creado organismos dedicados a la gestión de temas de ciberseguridad. De los 32 países analizados, un tercio no cuenta con un marco legal sobre delitos informáticos, 12 han aprobado una estrategia nacional de ciberseguridad y tan solo 5 están adheridos a la convención de Budapest que facilita la cooperación internacional en la lucha contra el cibercrimen. Como si fuera poco, la brecha de 600 mil profesionales en el área de ciberseguridad, ha ocasionado que la lucha contra el cibercrimen en la región tenga un avance muy conservador.

En este punto, se vuelve evidente la necesidad de implementar políticas y controles a fin de proteger los activos digitales [8], dentro y fuera de las empresas. Las nuevas modalidades de trabajo remoto y teletrabajo, que vieron su popularidad gracias a la emergencia sanitaria global del virus COVID-19, representan nuevos retos para las empresas y profesionales de TI, ya que los equipos personales y las redes domésticas carecen de las seguridades que posee una infraestructura empresarial, por lo que es necesario personalizar las políticas con el fin de salvaguardar el bienestar de los dispositivos personales y la información contenida dentro de estos [9].

Como mencionamos anteriormente, las herramientas de detección y prevención actuales no son útiles frente a las nuevas amenazas cibernéticas, y la materialización de éstas, representan pérdidas de 50 mil millones por año, solo para América Latina [10]. Tal es así, que se ha visto una creciente popularidad del CaaS (Crimen como servicio), en el que un usuario novel y malicioso, puede adquirir en foros abiertos (anteriormente solo disponible en sitios clandestinos de la dark web), cualquier tipo de herramientas de hacking, para perpetrar ciberataques [11].

Sin duda alguna resulta abrumador considerar el escenario, es por esto que proteger los activos tecnológicos requiere de soluciones con un enfoque holístico, a decir de [12], la ciberseguridad involucra personas, procesos, tecnología e información. De la misma forma, [13] establece que la seguridad de la información se encarga de establecer las pautas, políticas o normas a seguir con el fin de proteger los activos digitales, y las cuales se expanden a toda una organización (infraestructura física, personas, procesos, etc), y la diferencia de la Seguridad Informática, la cual se limita a la parte operacional de una infraestructura tecnológica, dejando de lado lo que [14] considera como el eslabón más débil en la cadena de la ciberseguridad; el factor humano.

En este sentido, existen varios tipos de soluciones que una empresa puede tomar como contramedida a los ataques informáticos, como soluciones basadas en hardware, software, políticas, etc., sin embargo, resalta una que toma la óptica de un atacante y expone las vulnerabilidades de una infraestructura tecnológica con el fin de subsanarlas antes de que puedan ser aprovechadas por un atacante real, se trata de la prueba de intrusión o pentest.

Una prueba de intrusión o pentest es un ataque simulado y autorizado a una infraestructura en búsqueda de vulnerabilidades, con el fin de explotarlas de la misma forma en que lo haría un atacante real, y de esta manera proponer acciones correctivas [15]. No obstante, la ejecución de pruebas de intrusión no es una tarea sencilla. Esta actividad requiere conocimiento profundo de los tipos de ataques, las herramientas, métodos y técnicas [16], por lo que está de más decir, que la mayoría de empresas no cuentan con personal calificado, ni con los recursos económicos para contratar este tipo de servicios [17].

Para facilitar esta tarea, existen varias metodologías en el mercado, algunas de gran relevancia y reconocimiento como The Penetration Testing Execution Standard [18], el OSSTMM [19] y la NIST SP 800-115 [20], entre otras. La mayoría de las cuales siguen el mismo modus operandi; acercarse al objetivo, interactuar con el objetivo en busca de vulnerabilidades, explotar las vulnerabilidades encontradas y generar un reporte [21].

Por otro lado, [22] afirma que el uso de metodologías para la ejecución de pruebas de intrusión, no aporta mejoría alguna, ni en la ejecución, ni al resultado final de la misma. [21] expone que toda implementación es distinta, y que se debe considerar el uso de las metodologías, en base a los requerimientos de cada empresa. Finalmente, [22] concluye en su estudio, que las empresas que prestan servicios de seguridad, implementan parcialmente estas metodologías dependiendo el caso, o simplemente deciden no hacerlo, esto debido a la complejidad requerida para su implementación.

Dentro de este marco, se busca con el desarrollo del presente trabajo, contrarrestar algunas de las problemáticas expuestas en párrafos anteriores, al elaborar una metodología para la ejecución de pruebas de intrusión orientada a empresas pequeñas, tomando la clasificación de [23], y con un enfoque práctico, que sea relativamente fácil de ejecutar, que, utilizando un mínimo de recursos nos permita conocer el estado actual de una empresa en materia de seguridad, y que sea adaptable y repetible. De la misma forma, se espera con el uso de la herramienta, generar una cultura de seguridad en las empresas.

Es importante mencionar que la metodología propuesta no se limita a su uso en infraestructuras pequeñas, no obstante, en una escala macro, existen varias otras consideraciones que requieren de soluciones a la medida y que ofrecen altos niveles de fiabilidad en sus resultados.

2. Metodología

Empezaremos analizando a breves rasgos algunas metodologías existentes [18] [19] [24] consideradas de gran relevancia dentro de la industria a fin de obtener una visión genérica de una prueba o test de intrusión, a la vez que podemos encontrar técnicas o ciertos planteamientos que puedan servir de base para la metodología propuesta.

2.1 Análisis de metodologías existentes

2.1.1 PTES (Penetration Testing Excecution Standard)

Metodología desarrollada en el año 2009 por un grupo de profesionales de todas las áreas. Se enfoca en identificar el "valor de negocio" de los riesgos asociados a los activos tecnológicos. Considerada muy completa, ya que se estructura de 7 fases que cubren todos los aspectos relacionados a la ejecución de pruebas de intrusión, incluyendo los aspectos no técnicos [18]. La guía técnica de implementación provee los procedimientos y la estructura básica para implementar un test de intrusión [25].

Fases:

1. Interacciones Previas: Actividades previas a la ejecución del test necesarias para elaborar una adecuada planificación en la que se definen el alcance, tiempos, fechas, horarios, costos, y demás reglas de ejecución, con el fin de ser lo más claro y transparente en cuanto a requerimientos y evitar futuras controversias.

2. Recolección de información: Consiste en recolectar la mayor cantidad de información sobre el objetivo a través de técnicas OSINT, con el fin de aumentar los posibles vectores de ataque para fases posteriores. El PTES provee una extensa colección de fuentes y métodos en su sitio web para facilitar esta actividad.

3. Modelado de amenazas: Consiste en anticipar cualquier tipo de amenaza 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.

4. Análisis de vulnerabilidades: Consiste en la búsqueda de vulnerabilidades presentes en el objetivo utilizando varias técnicas automáticas y manuales. A través de correlación específica y categórica, se procede a realizar una validación de las vulnerabilidades encontradas. Finalmente se realiza una investigación a fondo de las vulnerabilidades encontradas, su forma y posibilidad de explotación, daño potencial, etc.

5. Explotación: Se enfoca en establecer un acceso no autorizado a un sistema o recurso de una infraestructura a través del uso de exploits y pasando por alto la seguridad implementada.

6. Post explotación: Consiste en la valoración del equipo comprometido, la relevancia de la información contenida dentro de este y la utilidad del mismo para comprometer otros activos de la red. En esta fase, las Reglas de Compromiso están diseñadas para proteger los intereses tanto de cliente como de auditor, al asegurarse que los activos no están sujetos a riesgos innecesarios.

7. Reporte: El PTES considera 2 reportes finales, el Resumen ejecutivo, que está enfocado en proveer un valor de negocio a la ejecución y a los resultados del test, por lo que está dirigido a quienes están a cargo de la direc-

ción y estrategia de la empresa. El reporte técnico contiene los detalles técnicos del test en cada una de sus fases, las recomendaciones para subsanar los errores técnicos, califica la exposición y riesgo de la organización y provee una conclusión.

2.1.2 CEH (Certified Ethical Hacker)

Es un programa de certificación que valida los conocimientos de los profesionales en temas de seguridad y ethical hacking. Se diferencia de otras metodologías al tomar un enfoque externo, ya que provee las técnicas y herramientas utilizadas por hackers maliciosos para la ejecución de pruebas de penetración [24], sin embargo busca distanciarse de la imagen de estos últimos, al proveer un código de ética a sus profesionales, que de no ser sostenido, significa el retiro y la invalidación de su certificación [26]. Esta metodología está orientada a la práctica y consta de 5 fases.

Fases:

1. Reconocimiento (footprinting): Consiste en recolectar la mayor cantidad de información del objetivo haciendo uso de técnicas de reconocimiento activo y pasivo, siguiendo el método provisto por el CEH. Es el punto de partida que permite planificar las fases posteriores.

2. Escaneo de redes: Utiliza técnicas de escaneo de red, puertos y vulnerabilidades, a fin de obtener una visión general de la infraestructura del objetivo.

3. Enumeración: A través de consultas directas se busca obtener más información acerca de los servicios que se están ejecutando, el estado de los puertos, etc., a fin de encontrar posibles métodos de entrada a la infraestructura del objetivo.

4. Análisis de vulnerabilidades: Consiste en la búsqueda de debilidades en un activo de red, ya sea errores de configuración, vulnerabilidades conocidas, ausencia de parches, etc., para luego proceder a clasificar estas vulnerabilidades según su severidad. Por último, a través de un informe recomendar las acciones a seguir para remedias las vulnerabilidades encontradas.

5. System Hacking (Hackeo del sistema): Con toda la información recolectada en las fases previas, el auditor intenta vulnerar el sistema comprometiendo su seguridad. La metodología en esta fase sigue de esta forma; obtener acceso, escalar privilegios, mantener acceso y eliminar rastros.

2.1.3 OSSTMM (The Open Source Security Testing Methodology Manual)

Creada por el ISECOM con la colaboración de más de 150 profesionales de todas las áreas, está orientada a la medición de la seguridad en un nivel operacional [19]. Para esto se enfoca en el análisis de las superficies de ataque de una organización, en los controles de seguridad implementados, en la eficacia de los mismos, y realiza un análisis de brecha entre la situación actual y la deseada. Establece varios tipos de test genéricos para poner a prueba los llamados canales operacionales, obtener las métricas derivadas y finalmente elaborar un informe. Es considerada todavía una metodología de mucha relevancia ya que considera la totalidad de los canales de operación empresarial (físico, humano, telecomunicaciones y redes de datos) [27]. Consta de 4 fases.

Fases:

1. Inducción: Se basa en el análisis de la organización y su entorno. Consiste en la revisión de la cultura, normativa, políticas, etc., para

obtener una idea del alcance, el tipo de test requerido y sus restricciones.

2. Interacción: Consiste en interactuar con el objetivo y sus activos digitales a través de actividades de verificación y auditoria, con el fin de obtener respuestas y analizarlas.
3. Investigación: Consiste en identificar las respuestas o emanaciones que produce el objetivo en la fase de interacción, esto nos revela los procesos y activos de valor, y sus seguridades.
4. Intervención: Consiste en intervenir en los recursos que consume el objetivo con el fin de provocar cambios en su comportamiento.

2.2 Estudio comparativo entre metodologías existentes

Para este pase, se ha hecho uso del Método de Estudio de Similitud entre Modelos y Estándares MSSS [28] el cual parte considerando 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.

Aplicándolo a nuestro estudio, obtenemos una vista general de las metodologías analizadas, como se ve en la tabla 1.

Tabla 1. Datos comparativos de las Metodologías seleccionadas.

Metodología	Alcance	Filosofía	Estructura
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
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

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 auditoría.	1. Inducción 2. Interacción 3. Investigación 4. Intervención

Seguidamente, consideramos relevante comparar las metodologías, en base a algunas características relevantes en orden con nuestra orientación, para lo que elaboramos una lista de verificación, la cual se demuestra en la tabla 2.

Tabla 2. Lista de verificación de características relevantes

Metodología	PTES	CEH	OSSTMM
Provee una guía técnica de aplicación		X	
Provee las herramientas para su aplicación	X	X	
Enfoque específico en la práctica		X	
Contempla los pasos del proceso genérico de pentest	X	X	
Cubre aspectos no técnicos relacionados al test	X		X

Por último, considerando el enfoque requerido para nuestra metodología, analizamos los objetivos y carencias de cada metodología estudiada, en relación a la orientación práctica. Los resultados se observan en la tabla 3.

Tabla 3. Objetivos de las metodologías en relación con el enfoque práctico.

Metodología	Enfoque	Objetivos	Relación con la ejecución practica
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 traducirlos a un lenguaje de negocio	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 hacking. No provee lineamientos técnicos de como ejecutar pruebas de penetración

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
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 nos permitió observar que la metodología CEH es la que más se alinea a lo requerido por nuestra metodología por lo que la consideraremos como base principal para el desarrollo de nuestra herramienta.

2.3 Desarrollo de la metodología propuesta

Gracias a la revisión y análisis comparativo de las diferentes metodologías estudiadas, tenemos una visión genérica del proceso de ejecución de pruebas de intrusión, por lo que estamos en la condición de sintetizar lo aprendido y adaptarlo en base a los requerimientos de nuestra metodología.

De esta manera, hemos estructurado nuestro modelo con la siguiente disposición:

Fase 1: Definición del alcance

Fase 2: Escaneo

Fase 3: Análisis de vulnerabilidades

Fase 4: Explotación

Fase 5: Reporte

De manera general, la tabla 4 presenta las características más relevantes de la metodología propuesta, a la vez que justifica las decisiones de diseño con el fin de proveerle sentido.

Tabla 4. Características generales de la metodología propuesta.

Fases	Objetivo	Actividades	Metodología Base	Justificación
1. Definición del alcance	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 por nivel de severidad y posibilidad de explotación. Buscar y analizar los métodos de explotación.	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 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.

A continuación, desarrollaremos el planteamiento de cada fase y facilitaremos el conocimiento para su correcta aplicación.

2.3.1 Fase 1: Definición del alcance

A pesar de tener enfoque práctico, se ha considerado importante incluir una fase previa a la ejecución en la que se establezcan acuerdos y compromisos necesarios para garantizar una adecuada logística que resulte beneficiosa tanto para el cliente como para el auditor. En esta fase se realiza la planificación del test y se definen aspectos como:

- Rangos de IP
- Dominios
- Puertos
- Horarios para la ejecución del test
- Fechas de inicio y fin
- Entregables
- Honorarios
- Restricciones y exclusiones
- Acuerdos de confidencialidad, entre otros.

Luego de definir estos y otros aspectos no contemplados anteriormente, se generan los documentos que autorizan legalmente al auditor a iniciar la ejecución del test.

En esta fase pueden ser útiles los siguientes documentos:

- Contratos de trabajo
- Formularios de autorización
- Acuerdos de confidencialidad, etc.

2.3.2 Fase 2: Escaneo

Se ha omitido la fase de reconocimiento ya que la misma se encuentra implícita en la fase anterior, por lo que podríamos decir, que nuestra metodología está basada en un test de caja blanca.

Esta fase es la combinación de las fases de escaneo y enumeración del CEH, ya que la naturaleza del método se basa en la ejecución de herramientas automatizadas, las que en la práctica, permiten realizar estas acciones al mismo tiempo. La fase consta de 2 actividades:

Escaneo de red y puertos: Con el uso de herramientas automatizadas, se procede a escanear la red con el objetivo de encontrar los hosts que se encuentran activos, los puertos que se encuentran abiertos y los servicios que ejecutan. También es importante elaborar un diagrama de red con el fin de obtener una visión general de la infraestructura del objetivo, a la vez que podemos anotar hallazgos importantes y consultarlos de forma visual.

Escaneo de vulnerabilidades: Consiste en obtener un listado de las vulnerabilidades presentes en la infraestructura del objetivo a través de escáneres automatizados, para proceder a analizarlas en la fase posterior.

Se recomienda a partir de esta fase, documentar todo lo relacionado a la ejecución del test con el fin de respaldar el trabajo realizado, los hallazgos encontrados y facilitar la elaboración del reporte final. Herramientas útiles para esta fase son, nmap, nessus, draw.io para la elaboración de diagramas y keepnote o cherry tree para realizar anotaciones.

2.3.3 Fase 3: Análisis de vulnerabilidades

Consiste en el análisis de las vulnerabilidades encontradas a través del método de correlación específica, del proceso de validación de la fase de análisis de vulnerabilidades del PTES. El cual consiste en cotejar las vulnerabilidades encontradas, en bases de datos de vulnerabilidades utilizando su id de CVE (Common Vulnerabilities and Exposures).

Para ello es necesario, antes que nada, clasificar u ordenar las vulnerabilidades encontradas, de

acuerdo a su daño potencial o criticidad. Aquellas de criticidad alta tendrán más probabilidades de una explotación exitosa, por lo que se recomienda empezar por ellas.

Seguidamente, se procede a la búsqueda de un exploit adecuado haciendo uso de bases de datos de vulnerabilidades como cve.mitre, exploit-db, rapid7 o vuldb. Estas bases de datos generalmente contienen los métodos de explotación, exploit, payloads, el código fuente y las indicaciones necesarias para la explotación.

La correlación especifica no siempre es exitosa, por lo que también será necesario realizar una búsqueda manual en base a los puertos, servicios y versiones encontrados en la fase anterior. En este paso son útiles herramientas como searchsploit o metasploit framework. Es sumamente importante recalcar que los exploits encontrados están desarrollados para el sistema, servicio y versión que se ejecuta en el host objetivo, ya que, de no hacerlo, podríamos perjudicar de forma permanente el sistema.

Debe señalarse, que lo que busca la metodología es poner a prueba la seguridad de una infraestructura, y bajo ningún motivo perjudicar los sistemas y activos digitales dentro de ésta, por lo que la búsqueda de exploits y payloads estará orientada a la obtención de un shell remoto únicamente, y no a alterar la operación normal de los equipos, como por ejemplo, el uso de ataques DOS.

Una vez encontrado el exploit adecuado, procedemos a la fase de explotación.

2.3.4 Fase 4: Explotación

Esta fase consiste en poner a prueba el exploit encontrado. Nuevamente se recomienda hacerlo desde un inicio con las vulnerabilidades de criticidad alta y en los hosts que tienen mayor relevancia para el beneficiario del test, a fin de proveer evidencia de los riesgos existentes y concientizar al cliente sobre el impacto de negocio que ocasionaría un host comprometido.

Para la ejecución de esta fase, es posible utilizar los exploits descargados de las bases de datos de vulnerabilidades utilizando las guías disponibles o los menús de ayuda que generalmente vienen contenidos dentro del mismo exploit. Otra herramienta muy útil para la explotación es Metasploit Framework, la cual contiene gran cantidad de auxiliares, exploits, payloads y otras utilidades que facilitan en gran manera la tarea de explotación.

[29] recomiendan de manera insistente, realizar pruebas de los exploits descargados de internet en ambientes controlados antes de utilizarlos en un ambiente real, esto con el fin de evitar daños a los sistemas y a la operación normal de la empresa. Los exploits podrían hacer más de lo que dicen hacer y podríamos estar perjudicando en lugar de proporcionando un servicio a la empresa.

Al obtener un Shell remoto en un host objetivo finaliza la fase de explotación, ya que es evidencia suficiente de haber vulnerado la infraestructura del cliente. Puesto que en la práctica no resulta tan sencillo, en el caso de haber fallado el exploit, es necesario repetir el proceso con la siguiente vulnerabilidad de criticidad alta encontrada en la fase anterior.

Si el exploit ha tenido éxito, no se recomienda dar seguimiento al resto de vulnerabilidades encontradas, sobre todo por cuestiones de tiempo y seguridad. En este punto se ha cumplido el objetivo del test al exponer los riesgos presentes en la infraestructura objetivo.

Como en las fases anteriores, se recomienda documentar todo el proceso, tomar capturas y guardar la ejecución de comandos en archivos de texto, ya que servirán de anexos para el reporte final, además de que sirven de evidencia del trabajo realizado.

2.3.5 Fase 5: Reporte

Consiste en la elaboración de un reporte final en base a lo realizado y los resultados obtenidos en cada una de las fases del test. El auditor debe ser capaz de sintetizar la información relevante y generar un resumen ejecutivo de fácil comprensión, considerar que no todas las personas a quienes va dirigido el reporte final poseen entendimiento en temas de tecnología ni manejan terminología técnica.

Seguido, se recomienda incorporar todo lo realizado a modo de narrativa, a fin de proveer una línea de tiempo que ayude a comprender de principio a fin el proceso ejecutado. Por último, se requiere el criterio del auditor sobre el estado general de la infraestructura y una breve recomendación. Los archivos de texto con la ejecución de los comandos, las capturas de pantalla y los reportes generados de la ejecución de las herramientas, serán parte del apéndice y servirán de soporte para el tratamiento de las vulnerabilidades encontradas a través de hojas de ruta y planes de acción y prevención de riesgos.

A manera de plantilla, se recomienda incluir por lo menos los siguientes puntos:

- Resumen ejecutivo
- Metodología Utilizada (por ejemplo, caja gris orientada al network assesment)
- Narrativa o cronología del test
- Conclusiones y recomendaciones
- Apéndice

2.3.6 Flujograma

Para ilustrar lo desarrollado en párrafos anteriores, se ha elaborado un flujograma (figura 1) de la metodología propuesta, con el objeto de ofrecer una herramienta visual y de fácil comprensión, al mismo tiempo que servirá de soporte para una correcta ejecución.

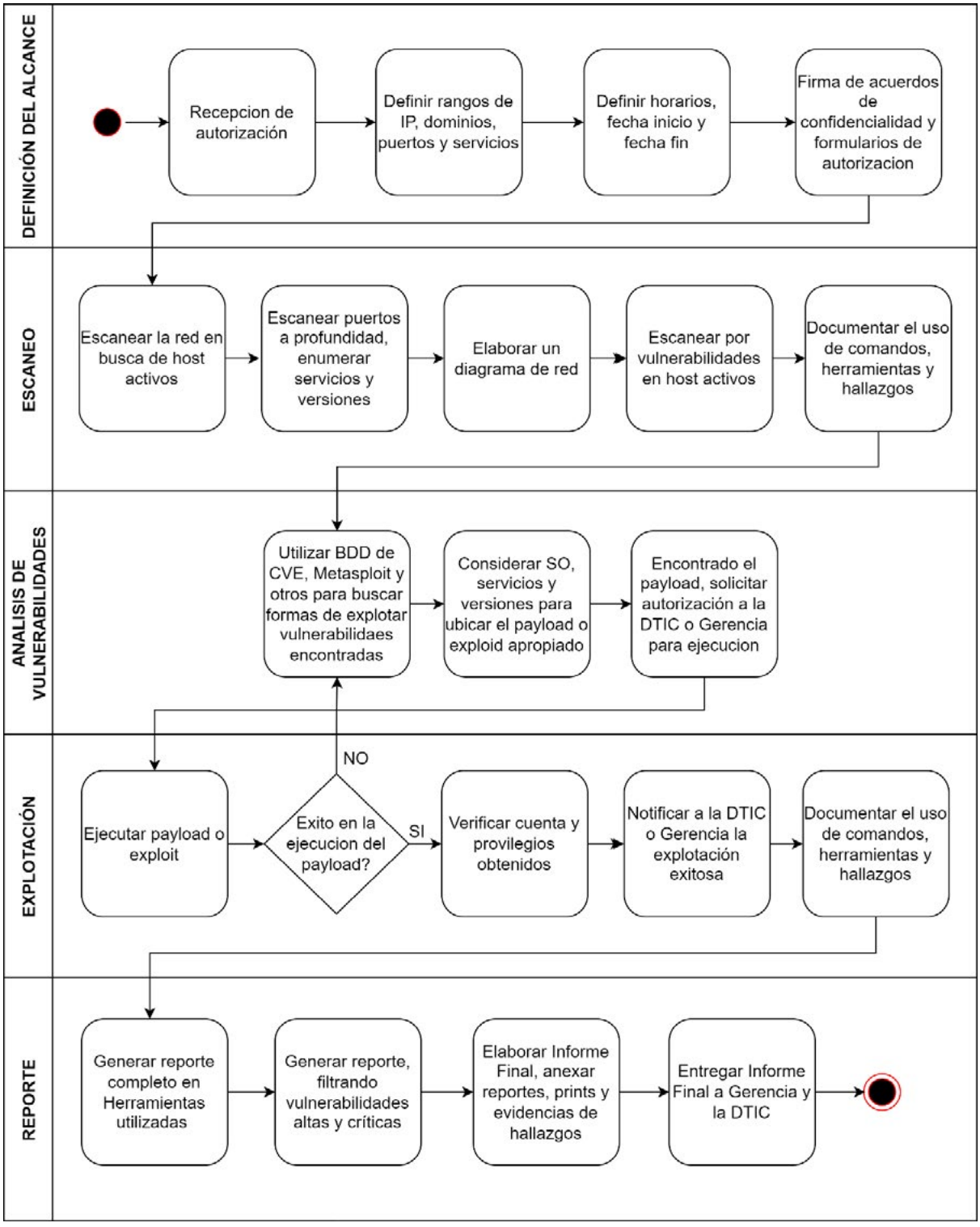

Figura 1. Diagrama de flujo metodología propuesta

2.4 Aplicación del caso de estudio

Luego de haber desarrollado la metodología, lo siguiente es evaluar la utilidad de la misma a través de un caso de estudio. En las siguientes líneas vamos a ir desglosando la metodología y aplicando los conocimientos aprendidos en cada una de sus fases.

La infraestructura seleccionada para el caso de estudio corresponde a una pequeña empresa ecuatoriana en la ciudad de Azogues que cuenta con 17 empleados, cada uno con un equipo de cómputo con conexión a internet. Luego de que se ha recibido la autorización para la aplicación de la metodología por parte del dueño de la empresa, procedemos con la primera fase.

Antes que nada, es importante mencionar que la información de carácter sensible y confidencial, obtenida por el resultado de la ejecución de comandos y herramientas ha sido enmascarada con el fin de preservar la anonimidad de la empresa, evitar poner en riesgo sus activos digitales y dar cumplimiento al acuerdo de confidencialidad.

2.4.1 Definición del alcance

En esta fase, hemos mantenido una reunión con la Gerencia de la empresa y con el área de TIC's con el objeto de definir lo establecido en el apartado anterior. Para ello y como resultado de la reunión, se han elaborado 2 documentos:

- Formulario de autorización de prueba de intrusión: en el que se definen los aspectos técnicos (rangos de ip, puertos, dominios, horarios de ejecución, etc) y se recibe la autorización expresa para ejecutar esta labor.
- Acuerdo de confidencialidad: Establece las condiciones para el uso de la información proporcionada por la información y resultado de la ejecución del test.

Existen en internet disponibles varias plantillas de los documentos enumerados anteriormente los cuales podemos modificar en beneficio del cliente y el auditor, y según los requerimientos del test.

En la gran mayoría de los casos, será necesario notarizar estos documentos a fin de contar con un respaldo legal en al caso de presentarse controversias futuras.

2.4.2 Escaneo

Empezamos conectando el equipo auditor (hack box) a la red de la empresa y verificando el segmento de red en el que nos encontramos (figura 2).

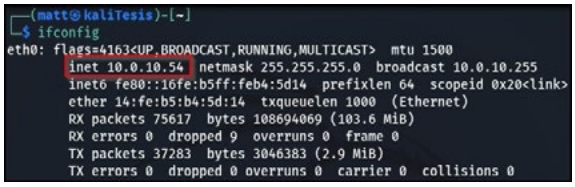

Figura 2. Verificación segmento de red

Pasamos al escaneo de red, en la misma terminal utilizando la herramienta nmap con el siguiente comando (figura 3):

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

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

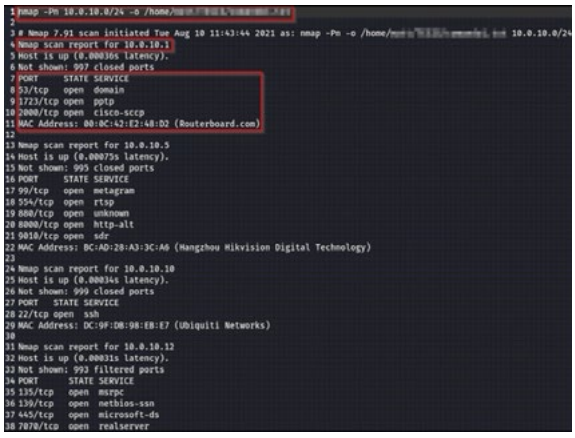

Figura 3. Escaneo de red con nmap

De esta forma obtenemos los hosts que se encuentran activos. También se obtiene información adicional como puertos, información de tarjetas de red, y algunos servicios que están en ejecución, sin embargo, en este caso solo nos interesan los hosts activos, con los que podemos ir elaborando un diagrama de red y con los que realizaremos el escaneo de puertos más profundo, para ello utilizamos el siguiente comando:

nmap -T4 -p- 10.0.10.1

- -T4: utiliza una plantilla predeterminada (0: sigiloso y lento, 5: ruidoso y rápido)
- -p-: selecciona todos los puertos (65535) para el análisis

La salida del comando la podemos ver en la figura 4.

```
└─$ nmap -T4 -p- 10.0.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 11:58 -05
Nmap scan report for 10.0.10.1
Host is up (0.0049s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
1723/tcp open  pptp
2000/tcp open  cisco-sccp
4365/tcp open  unknown
4532/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds
```

Figura 4. Escaneo de puertos con nmap

El comando devolvió información adicional en comparación con el anterior, ahora procedemos a enumerar cada puerto disponible. Ya que el ejemplo anterior corresponde al escaneo de puertos en un router, procederemos de ahora en adelante, por fines académicos, a demostrar la ejecución de comandos en un host de la red. El comando para enumerar los puertos es el siguiente:

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, versiones, ejecución de scripts y otros más.
- -p: especifica el puerto, puertos o rango de puertos dentro del análisis

La salida del comando la podemos ver en la figura 5.

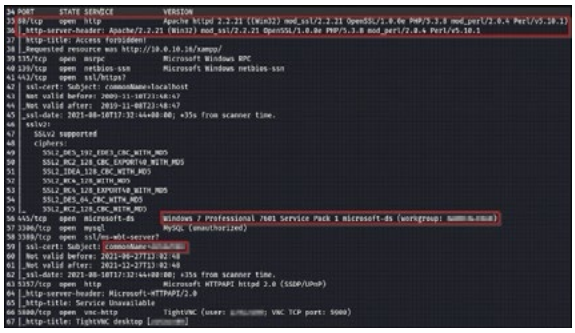

Figura 5. Enumeración de puertos con nmap

La ejecución del comando nos devuelve información valiosa como el sistema operativo, su versión, el nombre de host y grupo de trabajo, también nos presenta información importante en cuanto a puertos y servicios en ejecución y sus versiones respectivas. Esta información será de gran utilidad para la fase de análisis de vulnerabilidades.

En este punto podemos ir actualizando nuestro diagrama de red, por considerarse una herramienta de consulta rápida y útil como nos demuestra la figura 6. Para ello se ha utilizado la herramienta draw.io y se recomienda incluir sistemas (Windows 7 para todos los hosts en este caso), números de puertos y servicios activos.

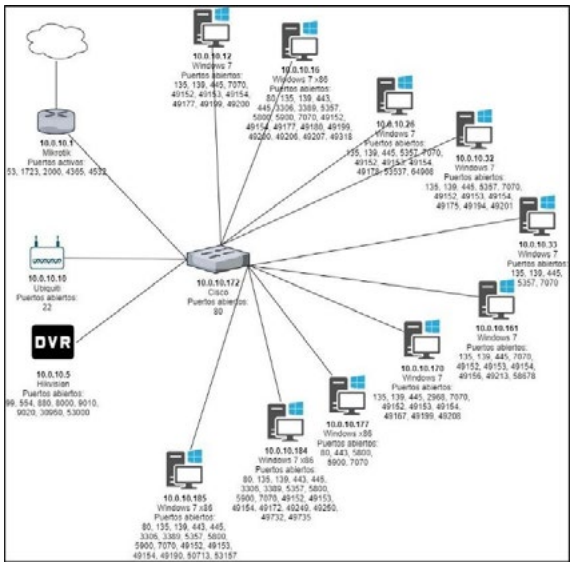

Figura 6. Diagrama de red

Posteriormente, pasamos al escaneo de vulnerabilidades. Ya que hemos encontrado únicamente 10 hosts disponibles en la red, utilizaremos la herramienta Nessus que en su versión gratuita nos permite escanear hasta 16 hosts al mismo tiempo. Para redes que contengan más de 16 hosts disponibles se recomienda considerar el uso de la herramienta OPENVAS que es igual de potente que Nessus, pero de libre uso.

Iniciamos la herramienta y seleccionamos la opción Basic Network Scan, dentro de la sección New Scan. Le damos un nombre y una descripción a nuestro escáner e ingresamos las direcciones IP de los hosts activos descubiertos en los pasos anteriores, como se ve en la figura 7.

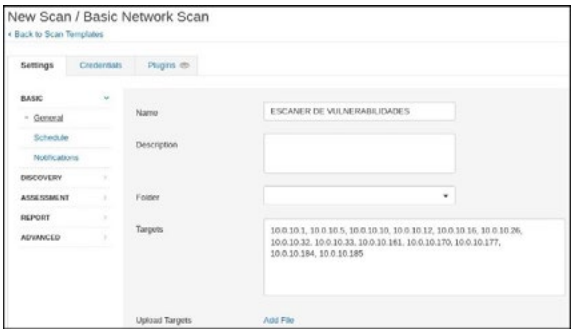

Figura 7. Configuración básica Nessus 1

De las configuraciones por defecto, partimos a modificar únicamente la opción Scan Type a todos los puertos como se ve en la figura 8.

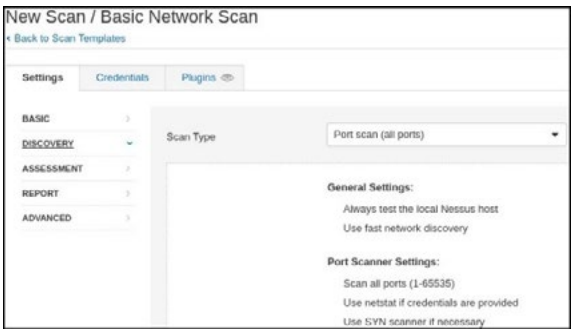

Figura 8. Configuración básica Nessus 2

Acto seguido, guardamos el test y procedemos a ejecutarlo desde la sección My Scans. Una vez concluido el escaneo, ingresamos a los resultados para continuar con la siguiente fase.

2.4.3 Análisis de vulnerabilidades

Como nos muestra la figura 9, la interfaz de la herramienta Nessus nos permite verificar el número total de vulnerabilidades encontradas, a la vez que las clasifica por host y sub clasifica de forma visual, por severidad.

Figura 9. Resultado Nessus - Escaneo

Si seleccionamos un host, Nessus nos muestra las vulnerabilidades presentes dentro de ese host clasificándolas por grupo de amenaza. Para continuar con el flujo propuesto, deshabilitamos la clasificación de amenazas y ordenamos los resultados por severidad, empezando por las de carácter crítico y accedemos a la primera vulnerabilidad listada, tal como se muestra en la figura 10.

La herramienta despliega múltiples vulnerabili-

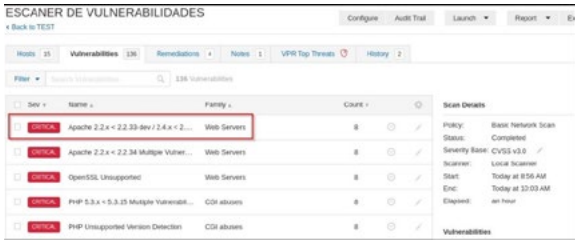

Figura 10. Resultados Nessus – ordenados por severidad

dades encontradas y la información relacionada a cada una. Al final, como demuestra la figura 11, se encuentra la id de la CVE que podemos consultar en las bases de datos de vulnerabilidades por sus respectivos exploits, o podemos usar herramientas como searchsploit o metasploit framework para validad su aplicabilidad en este caso, tomando en cuenta siempre, los sistemas, servicios y versiones en ejecución en el sistema objetivo.

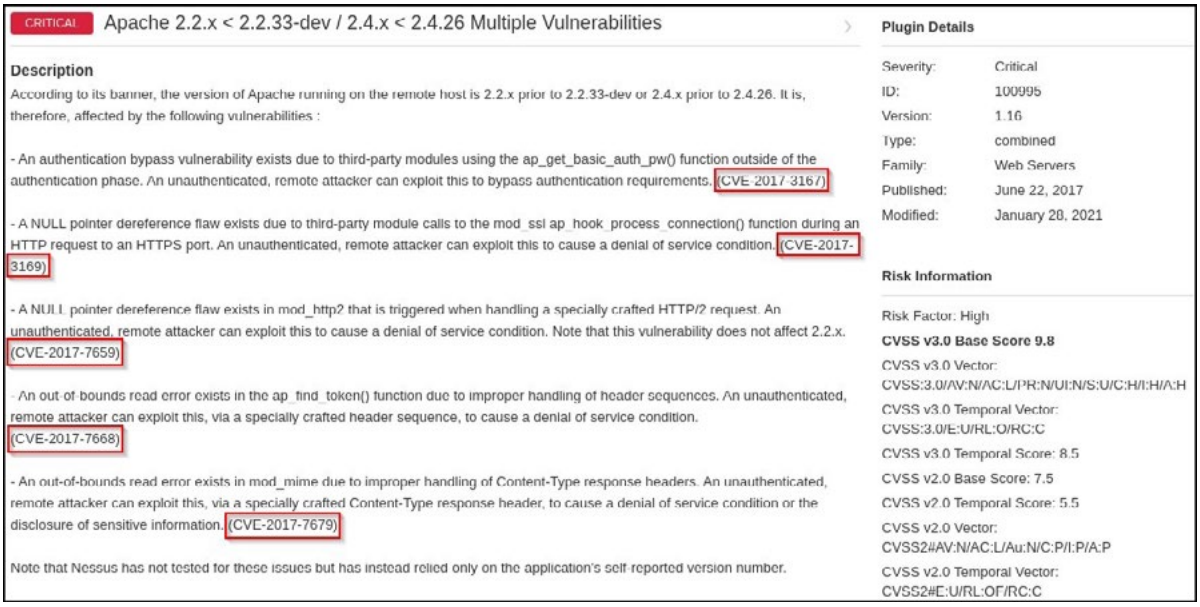

Figura 11. Información Nessus - vulnerabilidad Apache

Luego de realizar una búsqueda exhaustiva en searchsploit y metasploit sin encontrar un exploit adecuado para nuestro caso, procedemos a utilizar una base de datos de vulnerabilidades. Al igual que con las otras herramientas, no tenemos éxito en la búsqueda de un exploit apropiado. Como podemos ver en la figura 12, existen varios exploits disponibles, pero ninguno para sistemas Windows 7.

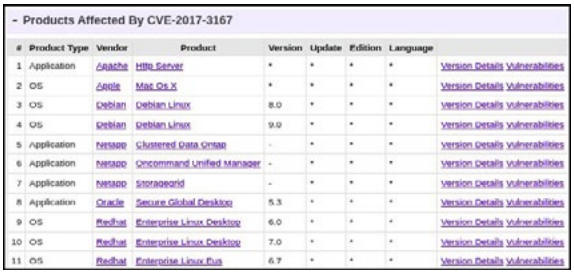

Figura 12. Resultados CVE – productos afectados

Ya que no hemos tenido éxito en la búsqueda de exploits para esta vulnerabilidad, continuamos con el flujo y seleccionamos la siguiente vulnerabilidad en la lista. Como podemos ver en la figura 13, hemos encontrado la vulnerabilidad MS17-010 del protocolo smb.

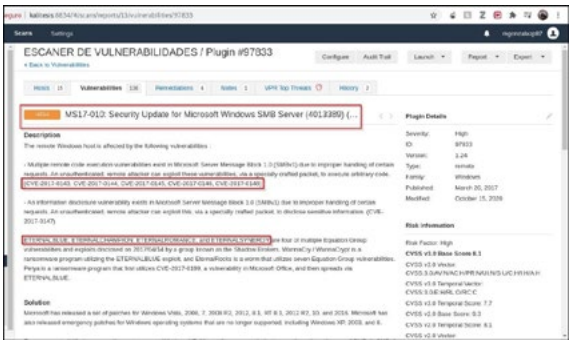

Figura 13. Información Nessus - vulnerabilidad MS17-010

Haciendo una búsqueda rápida en Google, encontramos que la vulnerabilidad MS17-010 o más conocida como Eternal Blue [30], es una vulnerabilidad muy destacada, es explotable en sistemas Windows y permite la ejecución de código remoto que es lo que buscamos. Dando seguimiento al hallazgo, realizamos una búsqueda en Metasploit Framework y encontramos el exploit ms17_010_eternalblue (figura 14), por lo que procedemos a la siguiente fase.

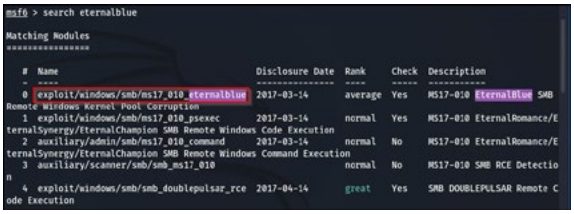

Figura 14. Resultados Metasploit Framework – Búsqueda eternalblue

2.4.4 Explotación

La explotación es la fase más sencilla, si hemos realizado bien las fases anteriores. En este caso hemos encontrado el exploit eternalblue en la herramienta Metasploit Framework, por lo que procedemos a seleccionarlo para su uso con el comando use, tal como se observa en la figura 15. En la misma podemos observar también, el payload cargado por defecto. Si no tenemos problema con el payload seleccionado, procedemos a configurar el parámetro rhosts con la dirección IP del objetivo, y finalmente utilizamos el comando run para ejecutar el payload. Si todo se ejecuta de manera adecuada, veremos la palabra WIN (o FAIL en el caso de que el exploit ha fallado) y en la última línea de la terminal de comandos, el prompt de nuestro Shell remoto.

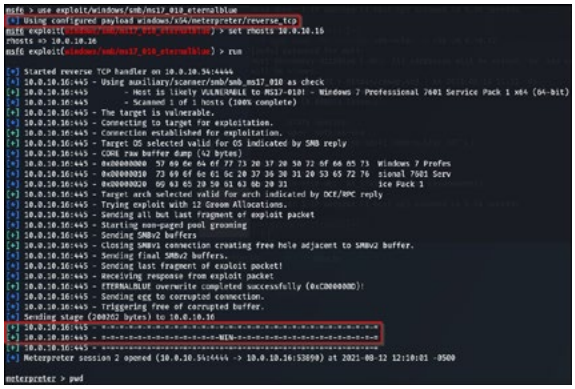

Figura 15. Resultados Metasploit Framework – Selección y ejecución de exploit

En este caso, el payload seleccionado ha funcionado en el primer intento. Dependiendo de varios factores, puede ser necesario ejecutar el exploit un par de veces para que funcione, o en otros casos será necesario cambiar el tipo de payload (modular o no modular, reverse o bind) hasta encontrar uno q funcione.

En este punto, el auditor puede ejecutar comandos para comprobar el nivel de privilegios (ver figura 16), revisar configuraciones, o realizar acciones de post explotación como escalar privilegios. Para nuestra metodología, hemos cumplido en demostrar una explotación exitosa por lo que documentamos todo el proceso, notificamos a la Gerencia o Dirección de Tecnología, y pasamos a la siguiente fase.

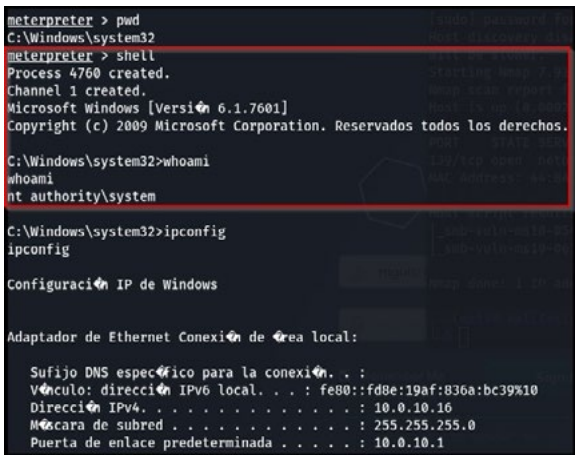

Figura 16. Metasploit Framework – Sesión de Meterpreter

2.4.5 Reporte

El reporte final elaborado para este caso es extenso y contiene información sensible que de ser publicada podría llegar a comprometer la seguridad de la empresa, por lo que el mismo fue entregado directamente a la gerencia para su gestión interna. Las indicaciones para la elaboración del reporte se encuentran en el apartado 2.3.5.

3. Resultados y Discusión

La figura 17 nos muestra un numero alarmante de vulnerabilidades encontradas, sobre todo si consideramos el tamaño de la infraestructura. Las amenazas de severidad critica señalan una infraestructura altamente vulnerable que fácilmente podría ser comprometida y pondría en riesgo los activos digitales de la empresa.

Figura 17. Nessus – Resultados generales

Las herramientas utilizadas para hacerlo además de un computador y un navegador de internet fueron, Kali Linux, Nmap, y Nessus, las cuales son herramientas gratuitas (Nessus permite escanear hasta 16 hosts en su versión gratuita) coincidiendo con el Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (2020) en el bajo costo que requiere un ataque informático. Así mismo, la implementación de la metodología en el caso de estudio ha tomado alrededor de 20 horas de trabajo, dando un promedio de 4 horas por fase, el cual podrá variar en cada caso, dependiendo del alcance del test y la experiencia del auditor.

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

Resulta evidente pensar que en la empresa, la seguridad de la información no es un tema prioritario, probablemente por desconocimiento del riesgo al que están expuestos, ya sea por parte de la gerencia o por el área de TI. Dado que no podemos generalizar los resultados, esperamos que el caso sea aislado.

Cabe destacar la importancia de una fase previa a la ejecución de una prueba de intrusión, como lo es en este caso la Definición del Alcance. Si bien en la metodología propuesta, es una fase muy pequeña, nos permite obtener información relevante y los documentos necesarios para elaborar una adecuada planificación que garantice la ejecución del test en un ambiente seguro tanto para el cliente como para el auditor.

4. Conclusiones y recomendaciones

Los resultados del caso de estudio nos proveen una clara idea de cómo se gestiona la seguridad en las empresas pequeñas. A experiencia del autor, el escenario es genérico y se repite en la mayoría de los casos. La implementación de soluciones basadas en hardware y software como firewalls y antivirus proporcionan un falso sentido de seguridad, en la que los profesionales de TI entran en una zona de confort básicamente a la espera de

ataques informáticos y poniendo en riesgo los activos tecnológicos de las empresas. En ese sentido, es necesario considerar a la seguridad de la información desde un enfoque holístico, como una solución integral que considere 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.

Al igual que las otras metodologías analizadas, la metodología propuesta contempla todos los pasos de un proceso genérico de pentest, sin embargo, al tener una orientación al análisis de red, permite ser mas especifica en sus requerimientos. Esto minimiza la ambigüedad en la comprensión de criterios, que, en comparación con las otras metodologías, complican su implementación

En este aspecto, la metodología presentada ha cumplido con los objetivos propuestos al ofrecer una herramienta útil, 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 obtener 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.

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.

Bibliografía

[1] M. L. S. Limón y M. H. D. la G. Cárdenas, “Tecnologías de información y desempeño organizacional de las pymes del noreste de México”, *Rev. Venez. Gerenc.*, vol. 23, núm. 82, pp. 298–313, 2018.

[2] E. J. Santiago y J. Sánchez Allende, “Riesgos de ciberseguridad en las Empresas”, *Tecnol. Desarro.*, vol. 15, núm. 0, Art. núm. 0, dic. 2017, Consultado: el 9 de enero de 2022. [En línea]. Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174

[3] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions”, *Comput. Secur.*, vol. 30, núm. 8, pp. 719–731, nov. 2011, doi: 10.1016/j.cose.2011.08.004.

[4] “Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe”, Banco Interamericano de Desarrollo, 2020,

2020. Consultado: el 14 de agosto de 2020. [En línea]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[5] "MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky", *MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky*. https://cybermap.kaspersky.com/es (consultado el 13 de enero de 2022).

[6] "The Top 6 Industries At Risk For Cyber Attacks - RedTeam Security". https://www.redteamsecure.com/blog/the-top-6-industries-at-risk-for-cyber-attacks (consultado el 29 de marzo de 2022).

[7] R. Vargas Borbúa, L. Recalde Herrera, y R. P. Reyes Ch., "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa", *Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance*, jun. 2017, Consultado: el 14 de agosto de 2020. [En línea]. Disponible en: http://repositorio.flacsoandes.edu.ec/handle/10469/12199

[8] D. Santo Orcero, *Pentesting con Kali: aprende a dominar la herramienta Kali para hacer tests de penetración y auditorías activas de seguridad*. 2018.

[9] M. Ortiz Osorio, "Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia.", nov. 2021, Consultado: el 13 de enero de 2022. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/44501

[10] R. Gonzalez, "Estiman en $87 mil 940 millones pérdidas anuales por ataques cibernéticos | La Prensa Panamá", *La Prensa*, el 20 de junio de 2019. Consultado: el 7 de agosto de 2020. [En línea]. Disponible en: https://www.prensa.com/economia/Estiman-millones-perdidas-anuales-ciberneticos_0_5331966763.html

[11] U. Akyazi, "Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum", p. 15, 2021.

[12] Á. M. Rea Guamán, "Madurez en la identificación y evaluación de riesgos en ciberseguridad", phd, E.T.S. de Ingenieros Informáticos (UPM), 2020. Consultado: el 9 de enero de 2022. [En línea]. Disponible en: https://doi.org/10.20868/UPM.thesis.65871

[13] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, "La seguridad informática y la seguridad de la información", *Polo Conoc.*, vol. 2, núm. 12, Art. núm. 12, mar. 2018, doi: 10.23857/pc.v2i12.420.

[14] V. Greavu Serban y O. Serban, "Social Engineering A General Approach", *Inform. Econ.*, vol. 18, núm. 2/2014, pp. 5–14, jun. 2014, doi: 10.12948/issn14531305/18.2.2014.01.

[15] J. L. Guillen Zafra, "Introducción al pentesting", Universitat de Barcelona, 2017. [En línea]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

[16] V. Casola, A. De Benedictis, M. Rak, y

U. Villano, “Towards Automated Penetration Testing for Cloud Applications”, en *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, jun. 2018, pp. 24–29. doi: 10.1109/WETICE.2018.00012.

[17] J. S. Ferrer Bustos, “Pruebas de penetración en las redes de datos en cualquier entidad pública o privada.”, mar. 2021, Consultado: el 10 de enero de 2022. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/40111

[18] “The Penetration Testing Execution Standard”. http://www.pentest-standard.org/index.php/Main_Page (consultado el 6 de junio de 2020).

[19] ISECOM, “OSSTMM 3”. 2010. [En línea]. Disponible en: www.isecom.org/OSSTMM.3.pdf

[20] kaitlin.boeckl@nist.gov, “NIST SP 800-115”, NIST, el 12 de enero de 2020. https://www.nist.gov/privacy-framework/nist-sp-800-115 (consultado el 13 de enero de 2022).

[21] C. A. Castro Vasquez, “Pruebas de penetración e intrusión”, jul. 2019, Consultado: el 10 de enero de 2022. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6273

[22] N. J. van den Hout, “Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies”, Royal Holloway, University of London, 2019. [En línea]. Disponible en: https://www.researchgate.net/publication/335652869_Standardised_Penetration_Testing_Examining_the_Usefulness_of_Current_Penetration_Testing_Methodologies

[23] G. Chávez Cruz, J. Campuzano Vásquez, y V. Betancourt Gonzaga, “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, vol. 14, pp. 247–255, dic. 2018.

[24] Ec Council, *CEH Ethical Hacking and Countermeasures* v11. 2020.

[25] D. Dalalana Bertoglio y A. F. Zorzo, “Overview and open issues on penetration test”, *J. Braz. Comput. Soc.*, vol. 23, núm. 1, p. 2, feb. 2017, doi: 10.1186/s13173-017-0051-1.

[26] R. Slayton, “Certifying ‘ethical hackers’”, *ACM SIGCAS Comput. Soc.*, vol. 47, núm. 4, pp. 145–150, jul. 2018, doi: 10.1145/3243141.3243156.

[27] O. Sierra, “ANALISIS Y PRUEBAS DE NIVELES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LAS GUIAS DEL OSSTMM v3”, p. 11, nov. 2018.

[28] G. P. Gasca Hurtado, “Estudio de similitud del proceso de gestión de riesgos en proyectos de outsourcing de software: utilización de un método”, *Rev. Ing. Univ. Medellín*, vol. 9, núm. 17, pp. 119–130, jul. 2010.

[29] R. Martí y J. Lloret, “Desarrollo e implementación práctica de un PENTEST”, sep. 2016, Consultado: el 25 de agosto de 2020. [En línea]. Disponible

en: https://riunet.upv.es/handle/10251/70164

[30] Z. Liu, "Working mechanism of Eternalblue and its application in ransomworm", *ArXiv211214773 Cs*, dic. 2021, Consultado: el 17 de enero de 2022. [En línea]. Disponible en: http://arxiv.org/abs/2112.14773