UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

Centro Tecnológico Aragón

Metodología y procedimientos de auditoría para sistemas informáticos electorales

TESINA

que para obtener el título de:

INGENIERO EN COMPUTACIÓN

En modalidad de:

Memoria de desempeño de servicio social

P R E S E N T A:

ANGEL LEOPOLDO MORENO OLIVARES

ASESOR:

M. en C. Jesús Hernández Cabrera

Ciudad Nezahualcóyotl, Estado de México, 2018

VNIVERSIDAD NACIONAL AVFNºMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

SECRETARÍA ACADÉMICA

M. EN I. MARIO SOSA RODRÍGUEZ
Jefe de la División de las Ciencias Físico-Matemáticas
y de las Ingenierías,
Presente.

En atención a la solicitud de fecha 15 de enero del año en curso, por la que se comunica que el alumno ANGEL LEOPOLDO MORENO OLIVARES, de la carrera de Ingeniero en Computación, ha concluido el trabajo de **titulación "METODOLOGÍA Y PROCEDIMIENTOS DE AUDITORÍA PARA SISTEMAS INFORMÁTICOS ELECTORALES"**, bajo la opción de **"MEMORIA DE DESEMPEÑO DE SERVICIO SOCIAL"**, y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México a 15 de enero de 2018.
EL SECRETARIO

Lic. JOSÉ GUADALUPE PIÑA OROZCO

C p Asesor.
C p Interesado.

JGPO/vr

Agradecimientos y dedicatoria

A mis padres, que nunca dudaron en apoyarme, quienes siempre me han dado todo cuanto han podido e incluso más con el propósito de favorecer mi desarrollo profesional y personal. Ellos han estado en los momentos de mayor flaqueza para darme fuerza y han compartido también las grandes alegrías. Gracias a ellos que cimentaron las bases para convertirme en el hombre que ahora soy, vigilando el camino que tomaba para conducirme bajo los principios y valores.

A mi hermana, pues en ella, a pesar de ser más pequeña, veo un comportamiento ético ejemplar, digno de ser reconocido. Ella también ha estado ahí para mí, motivándome, exigiéndome, escuchándome.

A mis abuelos, tíos y tías, a mis primos, por ser una gran familia y estar ahí para mí.

Al amor de mi vida, mi mejor amiga y compañera, Raquel, quien no ha hecho más que brindarme su amor, apoyo y confianza, ella le ha dado impulso a mi vida entera.

Al maestro Jesús Hernández, quien ha guiado mi desarrollo a lo largo de este y otros proyectos, desde los primeros semestres ha sido un mentor al cual respeto, admiro y ahora también considero un gran amigo.

Al maestro Marcelo Pérez, con quien, a pesar de haber tomado escasas cuatro clases, me ha mostrado conocimientos invaluables, ha despertado mi curiosidad y motivado mi crecimiento. Él me dio el mejor de los regalos. Es un gran amigo y maestro de vida.

Al maestro Felipe de Jesús Gutiérrez, que considero un líder y también amigo, pues me apoyó en cuanto lo necesité y siempre tiene una sonrisa para todos.

Al ingeniero Jorge Arturo López, por su confianza para transmitirme las responsabilidades y la generosidad de brindarme una oportunidad, por su amistad.

Al ingeniero Miguel Ángel Sánchez, por brindar sus conocimientos como un gran profesor de programación, por aceptar mi revisión.

Al doctor Edgar Morales Palafox, por brindarme su apoyo, consejo y amistad.

A mi hermano por elección, Joaquín, por su amistad incondicional.

A mis amigos del laboratorio, de la carrera, de la infancia, de la vida, a los verdaderos amigos, todos los que me han dado algo de ellos, ustedes saben quiénes son.

A todos, sepan que estaré ahí para ustedes… ¡Gracias!

Tabla de ilustraciones

Índice

I Introducción

Este trabajo se basa en la experiencia y conocimientos adquiridos al realizar una auditoría a los sistemas PREP (Programa de Resultados Electorales Preliminares) y Conteos Rápidos del OPLE (Organismo Público Electoral Local) de Veracruz en el periodo que comprende de febrero a julio de 2016 y al sistema PREP del IEEM (Instituto Electoral del Estado de México) en el periodo de febrero a junio 4 del 2017, por lo que, a lo largo de éste, se usarán ejemplos referencias de estos eventos, mismas que no exponen datos sensibles ni infringen las cartas de confidencialidad firmadas por el ente auditor. Dichas referencias se harán respecto a las pruebas realizadas, más no se mencionan o revelan los resultados obtenidos en los procesos para proteger su confidencialidad.

Como objetivo principal de este trabajo propongo la simplificación del proceso de capacitación para estudiantes pertenecientes a nuevas generaciones que deseen integrarse al laboratorio de cómputo con intenciones de participar en los procesos de auditoría. Independientemente del área que sea de su interés (seguridad o funcionalidad), resulta imprescindible para cualquiera de ellos, el manejo (por lo menos básico) de los conceptos presentados en este documento si es que entre sus planes figura participar en procesos de esta índole. Un objetivo secundario, pero no menos importante, es la comprobación de la efectividad de la metodología para pruebas de seguridad propuesta y desarrollada en el laboratorio de cómputo con la colaboración de un servidor, analizando las herramientas utilizadas y su nivel de eficacia en cada una de las etapas de esta.

Una vez definido lo anterior y sin más preámbulos comenzaré a introducirlos en el tema.

En México, los procesos electorales han sido objeto de crítica y desconfianza, las cuales provienen tanto de la población como de los partidos, sin mencionar a los medios de comunicación, teniendo estos últimos la capacidad de infundir ideas y tendencias (sobre todo en el sector más limitado en cuestión de recursos). Todo esto se debe a la incertidumbre que reside en cada uno de estos grupos, provocada principalmente por la falta de conocimiento sobre el funcionamiento de los procesos que involucra el conteo de votos, no dejando a un lado la sensación de ajenidad respecto a lo que ocurre con los sufragios emitidos durante la jornada electoral, mismos que por ley, deben mantener la cualidad de secrecía.

No es un tema nuevo el que a lo largo de la historia de nuestro país se han suscitado eventos que han provocado pérdida de identidad nacional y ausencia de confianza en los gobiernos, que los mexicanos elegimos. Las elecciones en nuestro país, ya sean de gobernador, diputados, presidente o cualquier otro

funcionario, siempre han provocado y provocarán inquietudes acerca de la veracidad de los resultados y la posibilidad de que la corrupción se vea involucrada durante el proceso y campañas.

Lo anterior representó una razón suficiente para hacer obligatorio[1] el uso de los sistemas informáticos PREP y Conteos rápidos, herramientas informáticas, que aunque no erradican por completo el problema de desconfianza, si pueden mostrar de forma no comprometedora el funcionamiento de un conteo, además, tienen como propósito obtener tendencias oficiales, respecto a la jornada electoral, con lo cual se pretendía involucrar a la población en general en el proceso electoral y así brindar un nivel aceptable de confianza en los resultados finales emitidos en los cómputos distritales, sin embargo, nada garantizaba que los sistemas PREP y Conteos Rápidos cumplieran completamente sus funciones, no había forma confiable de verificar la seguridad, ni comprobar el desempeño adecuado, comprometiendo así la confiabilidad, disponibilidad y confidencialidad de la información manejada, o al menos así fue hasta que se hizo oficial y un requerimiento legal, la auditoría de estos. Este cambio permitió que la desconfianza disminuyera entre la población, al mismo tiempo que se fomentaba la participación ciudadana.

Una definición simple de auditar software es comprobar mediante pruebas específicas, que un sistema cumple de forma correcta las funciones para lo que fue creado, para después comunicarle al propietario o responsable del software en que partes su sistema tiene deficiencias y como podría mitigarlas. Esto claro, expone preguntas sobre las pruebas que se tienen que realizar, las metodologías que se deben seguir, los procedimientos y algunas otras cosas que involucran a la seguridad de la información con la auditoria de software, además de como el desconocimiento de esta podría afectar el desempeño y generar pérdidas a las organizaciones.

A lo largo de este documento se pretende sumergir al lector de forma básica en el área de seguridad y más específicamente en el pentest[2], puesto que es el área en la que colaboré con mi conocimiento y esfuerzo durante la ejecución de proyectos de auditoría informática. Este documento podrá ser usado como guía básica si se pretende conocer los procesos que implica el hacer una auditoria de seguridad a software electoral, esto claro, con el fin de recortar la curva de aprendizaje sobre el tema y así lograr eficientemente la puesta en práctica de algunos conceptos, herramientas y consejos que son bastante útiles cuando de auditoría de software electoral hablamos.

[1] El anexo 13 del nuevo reglamento de elecciones, publicado por el INE, establece que el uso de los sistemas PREP y Conteos Rápidos es obligatorio tratándose de elecciones federales.
[2] Pentest es el término recortado de Penetration Testing que es utilizado para referirse al hacking ético.

Es necesario aclarar que, aunque en este trabajo nos enfocaremos a las pruebas de penetración que se realizan en una auditoría de seguridad, también mencionaremos y tendremos en cuenta algunas otras áreas que están estrechamente relacionadas en el contexto de auditoría informática, sin embargo, no nos adentraremos demasiado en esos temas y por eso serán manejados como temas de consulta optativa recomendada.

En el primer capítulo (Marco teórico) se pretende familiarizar al lector con conceptos acerca de auditoría y sistemas electorales informáticos, así como seguridad de la información y pruebas de penetración. También describe la metodología que se utilizó para realizar las pruebas de penetración a los sistemas PREP y Conteos Rápidos, así como cada una de las fases que contempla la metodología.

El segundo capítulo detalla el proceso que implica una auditoría en sistemas electorales, desde el funcionamiento de los sistemas, el proceso que implican, pasando por las consideraciones en la creación de documentos como reportes o informes, importancia de las ventanas de pruebas, hasta como debe conducirse el auditor en las diversas situaciones que se presenten durante el proceso.

Por último, el tercer capítulo, nos acercará a las principales herramientas utilizadas para realizar las pruebas en la auditoría. Se hablará de algunas de estas más a detalle utilizando ejemplos prácticos y explicaremos en qué etapa de la metodología se puede utilizar cada una de estas.

Una vez comprendidos los temas anteriores podremos considerar que tenemos una idea más concreta de lo que implica la seguridad informática en los procesos electorales, entenderemos las etapas de una metodología básica para realizar pruebas de penetración, así como las herramientas que se utilizan. Con lo aquí expuesto el lector obtendrá un conocimiento base útil para el desempeño de actividades relacionadas a una auditoría informática. Es elección del mismo profundizar en su aprendizaje utilizando la bibliografía que se comparte al final de este documento.

II Marco teórico

Puesto que la cantidad de información disponible y la facilidad con la que se puede acceder a ella son factores que crecen constantemente, la seguridad se ha convertido en un aspecto esencial para los sistemas informáticos, usuarios y administradores, sobre todo porque hoy día es difícil imaginar un sistema que no requiera de una conexión a internet.

Dirigidos, que, en otras palabras, significa que están específicamente desarrollados para vulnerar cierta configuración de hardware y/o software en posesión de cierta organización, persona o entidad.

Y por otra parte están los no dirigidos, los cuales son más comunes, menos elaborados (aunque no por eso menos dañinos) y buscan explotar al grueso de los usuarios. Debido a esto y a la sensibilidad de la información que a veces manejan los sistemas actuales, es recomendable realizar pruebas periódicas al software para verificar que está preparado para resistir el ataque o mitigar los daños que este pudiera generar, sean aprobatorios, no es una garantía de seguridad total.

Para poder entender lo que es una auditoría de seguridad informática, será necesario conocer el concepto universal de auditoría y cómo puede esto relacionarse con la seguridad de la información y estos dos a su vez con el software. Una vez que se conozcan por separado los conceptos, será sencillo generar las relaciones entre estas partes para cimentar bien la idea de lo que es una auditoría informática.

En este capítulo analizaremos algunos conceptos importantes respecto a los sistemas electorales PREP y conteos rápidos. Con esto definiremos la terminología y también responderemos a ciertas preguntas como: ¿qué son?, ¿qué subprocesos los componen? y ¿cuáles son sus funciones? Con el objetivo de tener una idea clara de cómo una amenaza podría materializarse fácilmente si no se cuenta con las políticas, controles y procedimientos necesarios para contrarrestarla o mitigar los daños.

Abarcaremos una parte considerable de las pruebas de penetración y la metodología utilizada, mostraremos cuales son los límites que definen si estas pruebas son benéficas para la organización, o simplemente estamos siendo un atacante más.

Estos temas servirán de repaso y puesta al corriente sobre el tópico que se tratará a lo largo de este documento, que es, auditar a sistemas informáticos electorales con un enfoque dirigido a las pruebas de penetración.

Para las organizaciones que sean propietarias de software de un gran tamaño con funciones cruciales o importantes, la responsabilidad también crece, pues además de que su reputación está en juego si algo sale mal, podrían causar daños o malentendidos en procesos de alta prioridad, inclusive pérdidas de recursos de alto valor.

En cuanto al software electoral como el PREP o conteos rápidos el principal interesado son los Organismos Públicos Locales Electorales y en segundo plano, pero no menos importante el INE, quienes son responsables de este software y como el proceso en el que se ven implicados estos programas informáticos, son elecciones, a nivel distrital, estatal y nacional, no pueden darse el lujo de comprometer el proceso electoral o que su credibilidad como institución de gobierno se vaya en picada por un descuido que pudo ser evitado.

El hecho de que sea obligatorio el realizar una auditoría a los sistemas electorales PREP y conteos rápidos (que, aunque no presentan resultados finales, sí muestran las tendencias que apuntan a los resultados definitivos), brinda tranquilidad a la ciudadanía, que atenta a operación de la jornada electoral desde un punto de apreciación externo, solicita un nivel de certeza y confianza en las instituciones. Lo anterior es motivo suficiente para que la entidad responsable de estos sistemas cumpla con las necesidades y requerimientos que este tipo de proyecto representa, pues de existir algún contratiempo con el sistema durante el proceso electoral, no solo la reputación de esta se vería afectada.

Por otra parte, la entidad que desarrolle este software está obligada a cumplir con las necesidades y requerimientos que este tipo de proyecto representa, ya que, si por algún motivo ocurre algún problema con el sistema durante el proceso electoral, la reputación de esta se vería afectada.

Los activos[3] de las organizaciones se pueden ver afectados por muchos factores y resulta sencillo creer que el capital o los recursos tangibles son los únicos que podrían ser dañados, o bien, que son los únicos que aportan valor a la empresa, sin embargo, la información ha llegado a ser un recurso tan valioso, que incluso el comprometer datos sensibles podría llegar a generar grandes pérdidas de cualquier otro recurso.

La pregunta aquí es, ¿por qué la información puede ser tan valiosa? Bueno, quizá para nosotros en este momento no parezca valioso tener una base de datos, o un simple documento con muchos números y

[3] Los activos son aquellos recursos físicos y no físicos que tienen algún valor para las organizaciones.

esto se debe a que la información solo es útil cuando es comprensible, sin mencionar que la mayoría del tiempo y sobre todo en ambientes comerciales, esta información solo es conocida por unos cuantos, es por esto que las empresas tienen secretos valiosos respecto a los procesos que los hacen diferentes a sus rivales y les proporcionan cierto nivel de ventaja, permitiéndoles mantenerse dentro de la competencia.

Es debido a esto que a las empresas y organizaciones les preocupa e interesa el resguardo y protección de la información y con justa razón, pues a nadie le viene bien perder una lista de miles de clientes exclusivos o una base de datos donde se encuentre información de carácter privado, valores hash de contraseñas, números de cuenta y/o números telefónicos de miles o quizá millones de personas, etc. Pero, sobre todo, a ninguna empresa u organización ya sea de carácter público o privado le conviene perder su credibilidad por haber comprometido información delicada. Un claro ejemplo de esto fue la exposición de cerca de 90 millones de registros del padrón electoral mexicano en abril del 2016 (AN, 2016), información que fue almacenada de forma insegura por un partido político en un reconocido servicio de la nube, en el cual residen algunos de los servicios más importantes del mundo. El problema fue, que, al almacenar dicha base de datos sin contraseña, o algún tipo de mecanismo de seguridad, los nombres, domicilios y otros datos sensibles y personales de los mexicanos, quedaron susceptibles y a merced de casi cualquier persona que diera con estos.

Las consecuencias de esto podrían ser desastrosas para los afectados propietarios de dicha información, sin mencionar que la reputación del partido que comprometió los datos descendió junto con la confiabilidad del INE[4] e incluso la de la compañía que proporcionaba el servicio en la nube[5], y todo debido a la falta de políticas seguridad en el manejo de la información.

Pero… ¿Cómo saber si un sistema informático es seguro?, ¿cómo saber que el manejo de información es seguro?

Aun sabiendo que ningún programa o software podrá ser perfecto debido a su naturaleza cambiante y a que está hecho en gran parte por seres humanos (los cuales pueden cometer errores), es factibles dificultar la tarea de los atacantes mediante el uso de buenas prácticas, controles y políticas para aumentar la seguridad de dichos sistemas. Sin embargo, aunque lo anterior nos puede proporcionar cierto grado de confianza en el sistema, es recomendable realizar una auditoría informática y/o certificaciones,

[4] El Instituto Nacional Electoral es el organismo público encargado de los procesos electorales en México.
[5] El término *nube* se refiere a la infraestructura que soporta a los miles de servicios ofrecidos vía remota sobre internet.

sobre todo en software de gran tamaño, el cual puede llegar a manejar cantidades importantes de datos, así como información realmente sensible y de carácter crítico.

Auditoría

La auditoría surge en la antigüedad con la necesidad de asegurar que la mayoría de los aspectos de negocio cumplieran con lo que se esperaba de ellos y esto permitiera un mejor control de todas las operaciones que se realizaban. A pesar de que las primeras organizaciones realizaban auditorías solo para el ámbito financiero, con el tiempo el contexto empresarial cambió para dar paso a las evaluaciones en más de un área, sobre todo con el surgimiento de las tecnologías, las cuales han provocado una revolución al facilitar la automatización de muchos procesos, sin mencionar los cambios de paradigma que esto provocó. Las organizaciones han tenido que adaptarse y crecer para mantenerse dentro de la competencia, agregando nuevos aspectos al negocio, las variables de las que depende aumentan y con esto el riesgo de perder de vista la seguridad de toda la información involucrada. Esto dio pie al surgimiento de diferentes enfoques o tipos de auditoría, como son la contable (financiera), informática, fiscal, operacional, externa e interna, administrativa, entre otras, sin embargo, la que para nosotros será de interés en este documento es aquella que tiene como objeto de revisión los sistemas, procesos y tecnologías relacionados con la información manejada por los sistemas, es decir, nos concentraremos en una auditoría informática, enfocada en el aspecto operacional y de seguridad.

De forma general la Real Academia Española define auditoría como una "revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse" (RAE, 2015). Si bien aún no vemos muy claro como esto se puede relacionar con sistemas informáticos, no debemos preocuparnos, pues al avanzar en el capítulo formaremos conexiones entre estos y otros temas al grado de hacer comprensible la idea de una auditoría informática a sistemas electorales.

Después de toda evaluación, debe existir una etapa retroalimentación con la entidad evaluada en la que se haga de su conocimiento, los resultados obtenidos en las pruebas. Es por eso que otra buena definición de una auditoría es "la actividad que consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas" (Piattini, 2001).

Es un error común creer que no es necesaria la opinión profesional de una entidad ajena al proceso de desarrollo de cualquier proyecto, pues muchas veces al involucrarse en este, nos olvidamos de observar

de forma crítica y objetiva el esfuerzo impreso, las tareas desempeñadas y la calidad con la que se realizan, lo cual a su vez puede traer consecuencias graves proporcionales al grado de importancia del proyecto. Sin embargo, para que una opinión acerca de algún proceso pueda considerarse valiosa y de utilidad, es necesario que la entidad emisora este capacitada y cuente con profesionales que tengan conocimiento en el área a evaluar.

Es importante aclarar que haber sido auditado no garantiza la seguridad total del negocio, mucho menos que alguno de los procesos utilizados por la entidad evaluada sea seguro; El beneficio de una auditoría reside en identificar las áreas de oportunidad existentes en los procesos internos de la organización.

En cuanto a la clasificación de las auditorías podemos mencionar al menos dos de las más representativas, una de ellas, es la clasificación de acuerdo a la relación del ente auditor con la organización que va a ser auditada, mientras que la otra se basa en el objeto de evaluación.

Para la clasificación de acuerdo a la relación, los tipos de auditoría asociados son interna y externa. La primera es desarrollada por personal ligado laboralmente a la organización o empresa que se quiere someter a la evaluación, y se busca emitir informes y sugerencias que ayuden a mejorar los procesos que se lleven a cabo en esa organización. Por otra parte, la auditoría externa es realizada por un profesional que no está vinculado laboralmente a la organización, aunque los objetivos que se persiguen realmente son muy similares. Otra diferencia entre las dos categorías anteriores es que el informe para la auditoría interna es privado y solamente para conocimiento de la organización, mientras que, en la auditoría externa, personal externo a la misma puede contar con información importante.

Ahora, para aclarar el panorama sobre la clasificación de las auditorías, hablaremos de algunas subcategorías, las cuales son más específicas respecto al enfoque de evaluación, ya que se aplican en las diferentes áreas con las que una organización puede tener relación o interés durante el desempeño de sus actividades, de las cuales, mencionaremos algunas de las más relevantes:

- **Auditoría contable:** Se verifica que la información financiera de una organización esté apegada a las normas de cada país.
- **Auditoría de administración:** Se evalúa la forma de gestionar los procesos y recursos dentro de una organización o empresa.
- **Auditoría informática:** Se evalúa a los sistemas, además de los procesos, controles y tecnologías que lo rodean y sustentan, en el marco de la seguridad y funcionalidad.

- **Auditoría social:** Permite evaluar los resultados obtenidos por los programas y proyectos, el comportamiento ético en el proceso y el uso eficiente de los recursos económicos, técnicos y humanos.
- **Auditoría jurídica:** Es la que evalúa los procesos, procedimientos y controles relacionados con los aspectos legales dentro de una organización.

Ya que ahora conocemos el panorama de lo que es una auditoría, vamos a identificar en que clasificación entra el proyecto en el que se basa este trabajo.

La auditoría que se realizó en Veracruz, es de carácter externo, puesto que fue ejecutada por el Laboratorio de Cómputo de la Facultad de Estudios Superiores Aragón (entidad sin relación laboral con el OPLE de Veracruz) y el informe que mostró los resultados finales tuvo un carácter público, además también se considera una auditoría informática por el enfoque hacia las tecnologías y sistemas de información que manejamos, sin dejar de lado que puede ser considerada como operacional, puesto que verifico y constató la eficiencia y eficacia de los procedimientos.

Quisiera recalcar que en este trabajo está enfocado al aspecto de seguridad de la información dentro de la auditoría, principalmente en la metodología que se utilizó como base para la realización del pentest[6], así como las herramientas que fueron de utilidad para este procedimiento. También se abarcarán temas como detalles sobre los sistemas electorales, ética del auditor y consideraciones generales dentro de las que se mencionan las ventanas de tiempo, el alcance de los proyectos, redacción de informes, entre otros temas importantes para el auditor.

Auditoria informática

Un sistema informático es aquel que está conformado por hardware[7] y software[8] (mejor conocido como computadora), se utiliza para el procesamiento y envío electrónico de datos, por otra parte, un sistema de información es el "conjunto de varios elementos que recolectan (o recuperan), procesan, almacenan y distribuyen dicha información para apoyar la toma de decisiones y el control en una organización" (Gastélum C.), es decir, un sistema de información podría ser considerado como un todo que involucra

[6] Término abreviado para Penetration Testing con el que se conoce a las pruebas de penetración o hacking ético.
[7] El hardware es conocido como las partes físicas que componen una computadora o dispositivo electrónico.
[8] El software es considerado la parte lógica e intangible y que se ejecuta sobre el hardware.

muchos elementos para lograr un fin común, uno de esos elementos en la mayoría de las empresas son los sistemas informáticos.

Dicho lo anterior, podremos deducir que un sistema informático o computacional reside dentro de la generalidad de un sistema de información ya que funge como herramienta importante para obtener información útil y oportuna a través del uso de tecnologías, y como los datos que se manejan en estos sistemas pueden llegar a ser activos de alto valor o importancia para las organizaciones, entendemos que "la auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva acabo eficazmente los fines de la organización y utiliza eficientemente los recursos" (Piattini,2001).

Entonces, si al concepto general de auditoría le sumamos que esta revisión tiene que ser aplicada a un sistema automatizado que procesa información o parte de él, y tomamos en cuenta que ciertos requisitos deberían cumplirse sin dejar de lado la integridad, confidencialidad y disponibilidad del activo principal (la información) o los procesos tecnológicos que rodean al sistema, entonces, hablamos de una auditoría informática.

Dentro de casi toda organización que cuente con sistemas automatizados existen áreas en las que una auditoría informática podría ser aplicada y como ya aclaramos antes, esta podría ser enfocada a una o a todas las áreas que mencionaremos a continuación:

- **Base de datos:** Donde se evaluará los mecanismos de control de acceso, calidad e integridad de los datos y mecanismos de respaldo/recuperación ante contingencias.
- **Infraestructura:** Tecnologías utilizadas para la implementación de algún sistema, así como la calidad y rendimiento que estas ofrecen.
- **Gestión (administración):** El manejo de los recursos, los planes de recuperación en contra de desastres y continuidad del negocio.
- **Redes:** La estructura de la red interna, además de los controles y protocolos de recuperación, disponibilidad entre otros.
- **Seguridad:** Políticas y controles, además de análisis de riesgos.
- **Proceso de desarrollo de software:** Que la organización emplea buenas prácticas y metodologías de desarrollo en el ciclo de vida del mismo.

Ahora que ya conocemos lo que es una auditoría aplicada a los sistemas informáticos, nos queda responder a la siguiente pregunta:

¿A qué parte o en qué lugar de la empresa u organización se aplica la auditoría informática?

Si bien una auditoría puede aplicarse a toda la entidad a la que se desea evaluar, también podría enfocarse a un solo proceso o función de esta, pues todo depende de lo que la entidad auditada solicite y requiera, y es por esto que resulta necesaria la definición de los objetivos y responsabilidades que deberán cumplir tanto el ente auditor, como la organización que contrata o solicita sus servicios.

El objetivo de una auditoría informática por lo general es detectar la mayoría de flaquezas ocultas, ya sean administrativas o técnicas de un sistema informático y todos los procesos que se desarrollan alrededor de él, para después hacer entrega de información útil y confiable sobre los hallazgos realizados a la organización responsable, y así esta última, pueda tomar una decisión oportuna sobre como remediar los conflictos o disminuir los daños que las amenazas pudieran generar.

Puesto que objetivo del que hablamos puede resultar bastante general y quizá un poco difuso, es de suma importancia establecer un alcance que defina las actividades, pruebas y servicios que se brindaran como parte de la auditoría. Este punto debe definirse junto con el cliente desde el inicio del proyecto, con el fin de que ambos coincidan en los objetivos que se persiguen y de qué forma se planea lograrlos.

Muchas veces, durante el desarrollo de la auditoría, es común encontrarse con el desvío de esfuerzos y atención por parte del recurso humano, situación que podría generar errores y pérdida de recursos valiosos. Aquí es donde el alcance sumado a la experiencia de un profesional, ayudan a canalizar de manera adecuada el trabajo del personal para cumplir con los objetivos de forma eficiente y eficaz.

Cuando se tiene conocimiento del valor de los activos, es más sencillo vislumbrar cuales de estos requieren un nivel de seguridad más alto y cuáles no, del mismo modo, si conocemos a que partes del problema se debe enfocar una mayor cantidad de recursos para las pruebas, se generarán mejores resultados.

Un análisis de riesgos es un procedimiento que permite identificar, tanto al ente auditor como a la organización auditada, cuáles son los activos de mayor valor para priorizar la revisión a dichos activos.

En general, el proceso que sigue un análisis de riesgos se podría dividir en tres etapas:

> **Evaluación de activos. –** Se identifican los activos y su criticidad en base a la importancia para la organización.

Valoración de riesgos. - El cliente u organización tiene que involucrarse para definir junto con el profesional de seguridad en base a la posibilidad de ocurrencia y el impacto, la criticidad de estos riesgos.

Identificación de políticas. - En base al conocimiento obtenido sobre los riesgos latentes en las etapas anteriores, se determina si la empresa puede o no mitigar y en dado caso evitar los daños que podrían ser causados.

Como ya mencionamos, una auditoria informática puede tener diferentes enfoques. Nosotros hablamos de una auditoría de software concentrada en el aspecto de seguridad, sin embargo, el enfoque también puede incluir la revisión del desempeño del sistema, o del proceso de desarrollo del mismo.

Esto al final garantizaría que el resultado no solo muestre defectos y fortalezas particulares de un área, sino un panorama más amplio respecto al sistema, lo cual, a su vez proporcionaría al cliente un amplio rango de resultados que podrían ser valiosos para él.

Una auditoría informática siempre tendrá una relación estrecha con la seguridad de la información debido a que una complementa a la otra con el propósito de beneficiar a la organización; claro está que no son lo mismo, es importante conocer que "la diferencia entre la auditoría en informática y seguridad en informática, se basa en que la auditoria evalúa y sugiere los lineamientos de control que permitan corregir desviaciones o lograr que el procesamiento de la información sea segura y confiable, en cambio, la seguridad se enfoca a la implantación y el cumplimiento de los lineamientos de control sugeridos por la auditoría" (Gómez Miranda P, 1998).

Seguridad Informática

El concepto universal de la palabra *seguro,* es la descripción de un estado en el que una entidad se encuentra libre de daño o riesgo alguno. Si asumimos que esa entidad, es la información, o bien, los dispositivos electrónicos, instalaciones y demás activos de una organización, será necesario que se establezcan políticas y controles que ayuden a prevalecer el estado de seguridad de los activos ante situaciones adversas o de riesgo.

Para que la protección de los activos dentro de una organización se considere exitosa, es de suma importancia que el personal tenga conocimiento de las tareas que deben desempeñar y como deben realizarlas para conseguir el objetivo. Esto debe estar dictaminado por las políticas y controles de

seguridad que los profesionales junto con los directivos deben diseñar basándose en un análisis detallado de las necesidades y deficiencias de los procesos en la organización, para posteriormente, plasmarlos en documentos oficiales y hacerlos de conocimiento interno. Las políticas son las que indican *que* debe protegerse de acuerdo con la situación, mientras que los controles explican la forma de ejecución o el mecanismo de apoyo para cumplir la política exitosamente.

Hoy en día, el uso de sistemas informáticos representa no solo la disminución de costos y el aumento de productividad, sino también el crecimiento de negocio que toda organización con interés en competir necesita. El uso de tecnologías trae consigo las ventajas de negocio que toda organización busca, sin embargo, con todo beneficio que los sistemas automatizados aportan, vienen riesgos de seguridad para la información que estos manejan.

La seguridad informática es el conjunto de acciones y procesos que se enfocan en la protección de dispositivos, comunicaciones y procesos que pertenecen a los sistemas informáticos dentro de una organización, además de la prevención de daños y recuperación de funcionalidad para mantener la continuidad de negocio.

Debido a la cantidad de variables inmersas en los sistemas informáticos y las organizaciones, es necesario concebir a la seguridad informática como un proceso en constante mejoramiento y no como producto final, pues los sistemas se encuentran constantemente expuestos a múltiples ataques, físicos y/o virtuales, cada día surgen nuevas amenazas y se descubren más vulnerabilidades, razón por lo cual no podemos asumir que el hecho de considerar que un sistema es seguro hoy, mañana también lo será. Es a causa de la ausencia de conciencia sobre seguridad informática, que muchas entidades encuentren que sus recursos están absolutamente comprometidos de un día a otro, aun cuando se creían inalcanzables por los delitos cibernéticos. Ni siquiera las marcas de renombre que invierten y dedican bastantes recursos en la seguridad de la información han logrado salir ilesos de la lluvia de ataques que día con día tienen lugar.

Dado lo anterior, quiero recalcar que la seguridad debe ser considerada como un proceso en el que deben participar por igual las áreas directivas, administrativas y operativas de las organizaciones; además, este debe ser actualizado y verificado constantemente para poder garantizar la integridad, confidencialidad y disponibilidad de la información, requisitos indispensables para mantener el estado de seguridad de la información. En la Figura 1, se observa un gráfico representativo de estas tres propiedades.

Figura 1.- Triada de la seguridad

"En general, se definen tres propiedades de la información fundamentales que deben garantizar los sistemas informáticos: confidencialidad, integridad y disponibilidad" (Lucena M., 2011). Estas propiedades conforman un concepto llamado triada de la seguridad o triada CIA (Confidentiality, Integrity, Availability), formado por tres principios, que a su vez se pueden considerar propiedades de la información necesarias para garantizar la procedencia, fiabilidad y veracidad de la misma. Estas propiedades se definen de la siguiente forma:

Confidencialidad. – Es la propiedad que impide que la información sea conocida por entidades no autorizadas.

Integridad. - Es la propiedad que busca mantener la información libre de modificaciones no autorizadas.

Disponibilidad. - Es la propiedad que permite el acceso autorizado a la información siempre que sea necesario.

Los sistemas informáticos trabajan sobre sistemas operativos, los cuales están estructurados por distintas capas de traducción que van desde los lenguajes orientados al problema en la parte superior, los cuales tienen un alto nivel de abstracción (cercano a nosotros), hasta el lenguaje ensamblador de bajo nivel de abstracción, que es la lógica digital que se ejecuta directamente en los circuitos que forman el hardware donde el sistema opera. A esta estructura de capas, que se muestra en la Figura 2 se le conoce como máquina multinivel. Dicha jerarquía facilita la comunicación entre el usuario final y el sistema operativo, sin embargo, el que sea sencilla para el usuario final, implica que en cada capa la complejidad aumenta para comunicarse con la inmediata inferior. En este sentido, quiero explicar que incluso debajo de las aplicaciones como el editor de textos, navegador de internet, reproductor e incluso IDE's, y otras herramientas especializadas que son utilizadas a diario por el usuario final, existen más programas que podrían ser vulnerados por los atacantes con conocimientos especializados en dichas capas. En consecuencia, si el sistema sobre el que los aplicativos se ve comprometido, también lo estará, la operatividad de la aplicación de interés, afectando así indirectamente a la organización propietaria o responsable.

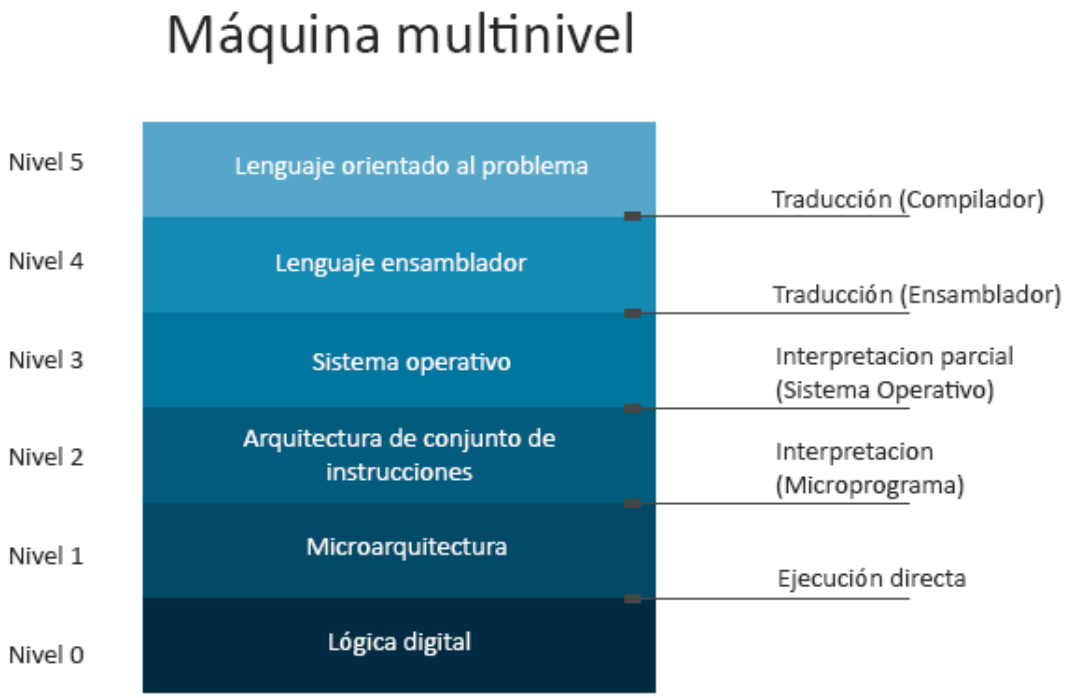

Figura 2.- Diagrama de máquina multinivel, estructura de capas

Ya que los sistemas informáticos pueden ser atacados incluso desde la plataforma que los soporta, estos "incorporan medidas para garantizar su seguridad prácticamente a todos los niveles, desde el hardware

hasta las interfaces de usuario, pasando por todas las capas del sistema operativo, los elementos dedicados a comunicaciones, etc." (Lucena M., 2011); o al menos, así debería ser.

La escala en que se basa este modelo de representación es el nivel de abstracción del lenguaje que se utiliza para comunicarse entre capas, es decir, mientras que con el hardware nos comunicamos a través de pulsos eléctricos, con las interfaces más avanzadas podemos hacerlo, inclusive, con nuestra propia voz, como es el caso de Siri[9] y otros modernos asistentes. Esto nos demuestra que entre más alto (más fácil de utilizar) sea el nivel de la capa que estamos utilizando, la comunicación entre nosotros y el dispositivo o software será más parecida a la comunicación que tenemos entre humanos utilizando el lenguaje natural. Caso contrario si intentamos comunicarnos con una capa de bajo nivel, pues el lenguaje será más complicado de entender para el usuario, por lo tanto, la comunicación entre él y la máquina requerirá de un proceso más complejo. Sin embargo, para que al usuario final le sea posible comunicarse de forma simple e intuitiva con los sistemas modernos, fue necesario que se desarrollaran múltiples sistemas intermedios entre la capa de usuario y el hardware.

Esto quiere decir que entre más sencillo sea utilizar algún dispositivo, cuanto más intuitivo sea el manejo de estos, el nivel de complejidad y cantidad de funcionalidades (casos de uso) aumentan en el ciclo de vida de desarrollo del software. Por su puesto, al aumentar el número de variables que interceden en el desarrollo de aplicativos es mucho más probable que ocurran omisiones, manejo indebido de información y errores durante el proceso.

Cuando hablamos de desarrollo de aplicativos, la ingeniería de software nos indica que el uso de buenas prácticas permite la implementación de controles de seguridad como lo son: la gestión de configuración, gestión de versiones y control de cambios, mismos que en la medida de lo posible, aumentan de forma considerable la fiabilidad y seguridad del producto final en comparación con un ciclo de desarrollo pobre.

La seguridad como hemos visto es un concepto que interactúa con las distintas áreas y procesos de una organización a través de los enfoques físico, tecnológico y administrativo.

Ya se habló de las capas inferiores a los sistemas en cuestión, sin embargo, también se debe tener en consideración la comunicación de nuestra aplicación con el exterior, pues es de ahí de donde provienen

[9] Siri es el asistente personal electrónico de Apple, el cual utiliza procesamiento del lenguaje natural, de la misma forma que su competencia, Cortana de Microsoft, Google Assistant por parte de Google, Bixby de Samsung y Alexa de Amazon.

los ataques o radican la mayoría de amenazas. Es en este punto donde el modelo TCP/IP de comunicación se convierte en el foco de atención para este documento.

Ahora que conocemos los aspectos de una organización que requieren de atención y volviendo a nuestro principal actor, los sistemas informáticos, diremos que la seguridad informática puede ser considerada como el conjunto de procesos que busca la prevención, aseguramiento, protección y recuperación de los activos involucrados con sistemas informáticos de una organización ante las amenazas latentes.

Con base en lo anterior, podemos deducir que las consecuencias que podría acarrear la ausencia de seguridad en la organización, en combinación con la criticidad y cantidad de activos, multiplicaría el número de daños de forma considerable.

Según Luis Castellanos[10] "podríamos clasificar las posibles consecuencias en dos categorías, pérdida de activos y violaciones a la ley" (Castellanos L., 2012). La pérdida de activos puede subdividirse en físicos, no físicos e intangibles:

Activos físicos

- Dinero
- Inventarios impresos
- Maquinaria o equipos

Activos no físicos

- Secretos comerciales
- Datos personales
- Procedimientos de negocio
- Datos sensibles

Activos intangibles

- Reputación
- Posicionamiento en el mercado

Y por otra parte están las posibles violaciones a la ley en consecuencia de la falta de un manejo adecuado y prudente de los recursos.

[10] El doctor Luis Castellanos es un experto en e-Learning, con maestría en Ingeniería en sistemas, docente universitario y editor de la revista académica digital "De Tecnología y Otras Cosas".

- Fraude
- Corrupción
- Extorsión
- Falsificación
- Robo
- Violación de contratos

Es por eso que la concientización de seguridad en el personal ejecutivo, administrativo y operativo es altamente recomendable para un ecosistema que se encuentra expuesto la mayor parte del tiempo a múltiples amenazas.

Cibercrimen: costos y repercusiones

A la fecha los delitos informáticos han crecido y hoy representan una parte importante de las pérdidas económicas a nivel mundial y nacional. Por ejemplo, en México, según Víctor Lagunes Soto, titular de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República, (2016) "el cibercrimen le cuesta a México más que el crimen organizado, y la tendencia va a la alta… Haciendo números junto con la industria los delitos cibernéticos cuestan a México 3 mil millones de dólares anuales" (CANIETI, 2016).

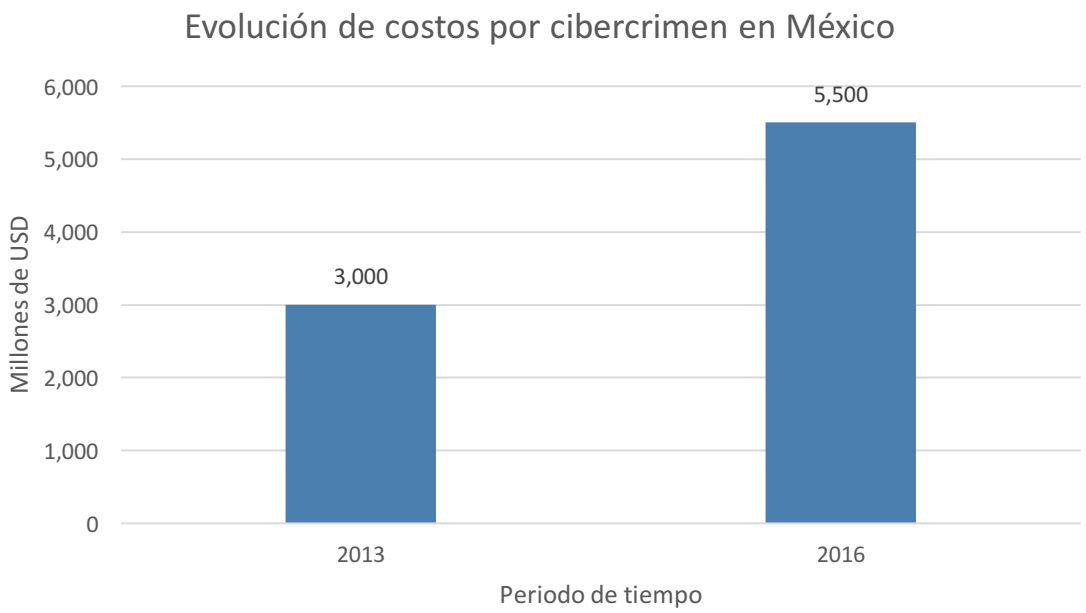

Figura 3.- Gráfica costos del cibercrimen

Según la gráfica de la Figura 3 el cibercrimen presenta un crecimiento abrupto y exponencial en cuanto a costes y daños generados a nivel nacional. En su último informe de ciberseguridad, Symantec afirma que tan solo en México los costos provocados por el cibercrimen en 2016 ascienden a los 5,500 millones de dólares, mientras que mundialmente y en el mismo año, el cibercrimen provoco pérdidas por 125,900 millones de dólares. Además de las pérdidas, Symantec nos comparte datos como que el 30% de usuarios en México no son capaces de identificar un correo apócrifo (phishing).

México ha escalado entre los demás países de América Latina para colocarse entre los primeros más afectados por el cibercrimen. En general estos números han crecido proporcionalmente con respecto a la cantidad de usuarios que ganan los dispositivos móviles, la facilidad para adquirir uno y la posibilidad de conectarse a internet. Hoy en día existen bastantes métodos de ataque, algunos de los más utilizados son:

- **Phishing**. - El atacante se hace pasar por otra entidad con la finalidad de obtener información sensible de la víctima.
- **Robo físico de dispositivos**. - El atacante obtiene de forma no autorizada el dispositivo y la información del propietario dentro de este para hacer uso de esta a su conveniencia.
- **Ransomeware**. - El atacante secuestra la información contenida en algún dispositivo mediante el cifrado de esta; acto seguido, el ciberdelincuente solicita un pago por la devolución de la información.
- **Denegación de servicio**. - El atacante podría valerse de la modificación de paquetes mal intencionados, así como el volumen de los mismos, para enviarlos al servidor víctima con el fin de provocar su saturación o inhabilitación, impidiéndole responder a partir de este momento a cualquier petición realizada.
- **Inyección de código**. - El atacante intenta ingresar código ejecutable en peticiones o querys para obtener acceso los dispositivos o bases de datos de la víctima.

Estos métodos de ataque son utilizados por usuarios mal intencionados para obtener algún beneficio o recurso de la víctima en cuestión.

Los ataques pueden ser clasificados en dos grandes rubros, los dirigidos y los no dirigidos, donde los primeros tienen como objetivo alguna organización, persona o entidad específica, mientras que los no dirigidos buscan afectar indiscriminadamente a quien lo permita o sea vulnerable. Un ataque dirigido está diseñado para burlar la configuración tanto de infraestructura, como de software establecidas por la víctima para proteger sus activos. Para poder lograr el cometido, el o los atacantes deberán estudiar detenidamente tanto el sistema, como su entorno, conociendo poco a poco sus debilidades hasta tener

suficiente información como para aumentar las probabilidades de éxito en el ataque, este proceso puede representar (en sistemas robustos) meses o incluso años de análisis de las variantes involucradas. Lo anterior depende de la complejidad de la configuración que la víctima en cuestión haya implementado. Este ataque funciona bajo la premisa de generar un daño a un objetivo específico, a sabiendas claro de que, en la mayoría de los casos, existe una jugosa recompensa.

Los ataques que no son dirigidos a un objetivo en específico por lo general son utilizados sobre la población promedio, se esparce la semilla de infección por algún medio masivo como puede ser correo electrónico, un enlace en redes sociales dirigiendo a una página externa, publicidad falsa, entre otras opciones, con la finalidad de robar información, sesiones, datos bancarios o cualquier otro recurso valioso. Este tipo de ataque se basa en el volumen de daños causados, entre mayor sea la cantidad de usuarios infectados, existen mayores probabilidades de obtener una buena recompensa.

El punto más débil de toda organización y sistema informático son las personas, ya sean desarrolladores, trabajadores o usuarios, quienes, al fin y al cabo, son seres humanos, propensos a sucumbir ante diversas tentaciones: la avaricia, gula, deseo sexual, etcétera, características altamente explotables por los atacantes, quienes buscan obtener la mayor cantidad de información que estos usuarios puedan proporcionar por si mismos antes de recurrir a un ataque mucho más complejo y elaborado, que bien podría costar meses de planificación. Un atacante intentará conseguir a través de técnicas de engaño y suplantación (phishing), cuanta información le sea posible, pues simplemente basta con recurrir a la curiosidad y el morbo de las personas para poder obtener información sin la necesidad de un esfuerzo mayor. Sin duda, y mientras el ser humano esté relacionado a los sistemas de información, esta seguirá siendo una forma bastante efectiva como primer punto de ataque para la obtención ilícita de información sensible y privada.

Si consideramos que a la fecha la mayoría de los usuarios en México cuentan con al menos un dispositivo, con el cual pueden conectarse a internet, y además, tenemos en cuenta la escasa concientización, cultura y conocimiento de la seguridad, que como usuarios *responsables*, deberíamos tener o por lo menos, conocer, son limitadas; entonces notaremos que el escenario que se muestra frente a nosotros, no es más que uno donde la ignorancia permite que seamos víctimas de los ciberdelitos, que día a día aumentan su complejidad y nivel de afectación.

Pruebas de penetración

También conocidas como pentest, las pruebas de penetración son evaluaciones a las que se somete un sistema informático con el fin de identificar sus puntos débiles, intentar explotarlos y posteriormente informar de los resultados a la organización que es responsable del sistema. También podrían considerarse como una serie de ataques bien intencionados, es decir, una serie de pruebas a las que se somete un sistema con previa autorización del cliente y son ejecutadas con la intención de detectar problemas para que sean corregidos y no para ser utilizados con el fin de perjudicar.

En el mundo de la seguridad informática, como en casi todo, existen dos bandos que podrían compararse con el bien y el mal, luz y oscuridad o cualquier otra analogía dual sobre la moral. Un atacante, también conocido como "Cracker" o "Black Hat", hará uso de todos los medios que estén a su alcance para encontrar la mayor cantidad de vulnerabilidades en los sistemas objetivo con el propósito de obtener de forma no autorizada e ilícita beneficios y recursos, entre otros, para uso propio o del mejor postor. Además, este usuario malintencionado no mostrará interés en los daños, pérdidas o riesgos que esto implica para él receptor del ataque; por otra parte y del otro lado de la balanza, se encuentra un profesional a quien podemos llamar "Ethical Hacker", "White Hat" o "Pentester", quien intentará penetrar el sistema hasta el punto que les sea posible, con el objetivo de encontrar (tal y como el atacante) las vulnerabilidades en el sistema objetivo, sin embargo, la obtención de esta información tiene un fin distinto, ya que busca advertir al cliente sobre estos hallazgos y así, este pueda mitigar los riesgos que representan para dificultar los intentos de ataques posteriores.

Es muy importante conocer las diferencias entre estos dos actores, pues a pesar de que la ejecución de un pentest requiere una ética sólida, discreción y precaución también es altamente recomendable, si no es que obligatorio, pensar como atacante e intentar hacer el mayor daño posible para exponer la mayor cantidad de debilidades que podrían existir en un sistema y con esto, obtener mejores resultados en la mayoría de las pruebas. Como menciona Patrick "es importante recalcar que los hackers éticos realizan muchas de las actividades usando muchas de las mismas herramientas que un atacante malicioso. En muchas situaciones un hacker ético deberá esforzarse para pensar y actuar como un auténtico hacker de sombrero negro. Entre más se asemejen las pruebas de penetración a un ataque del mundo real, será mayor el valor de los resultados para el cliente que paga por el PT" (Patrick Engebertson, 2011).

Estas pruebas podrían hacerse arbitraria e indiscriminadamente hasta encontrar lo que se busca, pero claro, esto podría llevarse mucho más tiempo del que se dispone para los proyectos, sin mencionar las dificultades que esto representaría en la organización del equipo de trabajo. En un futuro, resultaría en

pérdida de recursos valiosos como lo son el tiempo, esfuerzo e incluso contratos y relaciones con nuestros clientes.

Las pruebas de penetración pueden ser ejecutadas con tres enfoques distintos, caja negra, caja gris y caja blanca. La elección de cualquiera de los enfoques depende de las necesidades establecidas por el cliente. Estos enfoques existen con la finalidad de probar los sistemas simulando los tres perfiles básicos de un atacante; un atacante totalmente ajeno a la organización (caja negra), una atacante con mediano conocimiento y acceso a la organización (caja gris) y por último un atacante con un vasto conocimiento y posiblemente acceso a la organización (caja blanca).

El enfoque de caja negra es utilizado cuando al auditor no se le proporciona ningún recurso o información más que las referencias públicas, es decir, nombre de la organización y quizá alguna URL. A partir de esto, de él depende encontrar lo que sea necesario para probar la resistencia del sistema. Este podría ser considerado como el enfoque con mayor similitud a un ataque externo.

Se consideran pruebas de caja gris, si los recursos proporcionados al auditor incluyen un listado limitado (pero más extenso que en caja negra) de los recursos a los que podría intentar vulnerar. Este enfoque podría simular un ataque externo o bien, una intrusión interna. Para realizar la segunda, el auditor tendrá acceso a las instalaciones físicas de la organización, tal como un empleado. Esto permitiría al auditor probar vulnerabilidades dentro de la organización.

Por otra parte, las pruebas de caja blanca son las que necesitan de menos tiempo y recursos para su ejecución, pues la cantidad y detalle de los recursos proporcionados es mayor en comparación con los otros dos enfoques. Debido a lo anterior, las pruebas de caja blanca son utilizadas para probar con más detalle y en múltiples escenarios. Algunos de los recursos que pueden ser proporcionados para pruebas de este tipo son: diagramas de red detallados, incluyendo direcciones IP, listado de subredes existentes, lista de equipos y servicios disponibles, etc.

Metodología

Metodología según la Real Academia Española, es el conjunto de métodos que se siguen en el curso de una investigación científica y puesto que una auditoría podría considerarse una investigación en la que se busca determinar si la premisa *El sistema es lo suficientemente robusto y seguro para operar sin contratiempos y poder minimizar el impacto de cualquier situación adversa* es válida o no, entonces

concluimos que es necesaria una metodología para que los resultados del proceso de investigación, sean lo más benéficos posible para la organización.

Como se menciona implícitamente en el párrafo anterior, utilizar una metodología no solo es útil para el cumplimiento de requisitos o la credibilidad, también añade una guía que agiliza el trabajo del equipo en general, optimiza los recursos humanos y eficiente las tareas y procesos necesarios.

Existen metodologías y proyectos internacionales como Open Source Testing Methodology Manual (OSSTMM) y The Open Web Aplicaction Security Project (OWASP) en los que nos basamos para generar una metodología sencilla, mas no por eso, menos efectiva o completa.

Según el OWASP en la guía de su herramienta Zed Attack Proxy (ZAP), "es común que al realizar pruebas de penetración se sigan tres etapas básicas:

- **Exploración:** En esta etapa el encargado de realizar las pruebas intentará aprender todo sobre el sistema que será probado. Esto implica desnudar al sistema para identificar el software instalado, los dispositivos conectados, etc. Además, buscará revelar vulnerabilidades conocidas a las que el sistema podría ser susceptible, acceder a contenido oculto o cualquier otro indicio de debilidad.
- **Ataque:** Se intentará explotar las vulnerabilidades descubiertas en la primera etapa con el fin de determinar si existen, o no.
- **Reporte**: Por último, el encargado de las pruebas realizará un reporte con los resultados de las pruebas, incluyendo vulnerabilidades, como se explotaron y que tan complejo fue hacerlo, y la gravedad en caso de haber sido explotadas" (OWASP-ZAP, 2016).

Antes de utilizar este esquema de etapas para las pruebas de penetración, decidimos realizar algunas modificaciones, combinando esta base con elementos útiles mencionados por autores y profesionales dedicados al área, y que en conjunto eficientarían la repartición del trabajo y el uso de los recursos. Estas modificaciones culminaron en la división de la primera etapa, para formar dos, aún más específicas (Descubrimiento y Enumeración); esto permitiría dedicar más tiempo a la búsqueda de información, generar vectores de ataque con mayor probabilidad de ser efectivos y con esto, obtener información de utilidad para la siguiente etapa. La metodología resultante se utilizó al realizar pruebas de penetración a los sistemas electorales en los procesos electorales de Veracruz en 2016 y IEEM 2017 y es bastante similar a las etapas sugeridas en la guía de ZAP, sin embargo, nuestras variantes nos permiten ajustarnos a los requisitos de los proyectos dependiendo la situación y necesidades del cliente para lograr los objetivos requeridos, en tiempo y forma.

La metodología utilizada para evaluar al PREP en Veracruz y en el Estado de México está compuesta por cuatro etapas principales: descubrimiento, enumeración, análisis de vulnerabilidades/explotación y reporte, las cuales tienen objetivos particulares que van desde hallar información relacionada con la institución o cliente, obtención de información privada, vulnerar el sistema o subsistemas para obtener acceso a la información sensible así como informar de lo encontrado y sugerir como solucionarlo, claro siempre teniendo en cuenta la privacidad de la información y resultados obtenidos a lo largo de estas etapas. En la Figura 4 se muestra un diagrama de la metodología empleada durante los proyectos.

Figura 4.- Diagrama de metodología para pruebas de penetración utilizada para realizar auditorías a sistemas electorales

Aunque la metodología que se utilizó podría considerarse como básica, no por eso es menos efectiva, ya que contiene de forma un poco más detallada las fases del procedimiento más utilizado para un hacking ético[11] según Karina Astudillo.

La primera etapa, el descubrimiento, consta de búsqueda y recopilación de información relacionada con la entidad a evaluar o *víctima* (puesto que, aunque bien intencionado el pentest, al fin y al cabo, es un ataque). Este objetivo puede ser alcanzado de dos formas, pasiva o activamente. La primera, consta de consultas a información que es pública de forma que no afecte el desempeño del sistema, por lo tanto, no se requiere más que utilizar los medios adecuados (internet, periódico, redes sociales, etc.) para hallar este conjunto de datos que posteriormente podrían convertirse, o no, en información valiosa; La otra forma de obtener información es intrusiva y podría requerir de autorización del cliente para ser realizada. Como dice Astudillo, para este tipo de obtención de información hay una interacción directa con el objetivo o víctima, además algunos ejemplos de los que la autora maneja como técnicas de reconocimiento activo son barrido de ping, conexión a un puerto específico, ingeniería social y mapeo de red.

En la segunda etapa, se enumeran los resultados de la primera y se organizan de tal forma que nos permitan idear (planear) una o varias opciones de ataque para vulnerar el sistema que se está evaluando, estas opciones se conocen como vectores de ataque. Esta etapa debe ser tomada en serio, ya que de ella depende que, durante la siguiente fase, análisis de vulnerabilidades/explotación, los hallazgos muestren realmente la mayor cantidad de problemas o vulnerabilidades, es por esto que necesita de todo el conocimiento y creatividad del Ethical Hacker para obtener, no solo volumen, sino, calidad en los vectores que genere a partir de los datos obtenidos en la primera etapa.

El análisis de vulnerabilidades es nuestra tercera etapa y es en la cual se ponen a prueba la mayoría de elementos que componen al sistema. Estas pruebas pueden ser tanto automatizadas como manuales; las primeras, se realizan con ayuda de herramientas especializadas para explotación de vulnerabilidades como son Loic, SlowLoris (para ataques de denegación de servicio), Nessus (para análisis de vulnerabilidades), entre otros, mientras que las segundas, tienden a ser un poco más detalladas y específicas, debido a que requieren mayor participación del auditor, en la fabricación paso a paso los ataques, y la interpretación de los resultados obtenidos. Para determinar si un sistema es o no tiene

[11] Karina Astudillo dice que las fases correspondientes al hacking ético son el reconocimiento, escaneo, obtención de acceso, redacción de informe, entrega de informe.

vulnerabilidades conocidas, es necesario someterlo a ataques controlados, donde se prueben los límites del mismo, de ahí que la explotación vaya de la mano con el análisis de vulnerabilidades.

Por último, está el informe. Al redactar un informe o dictamen, se debe tener en cuenta que este, no necesariamente será leído por un profesional de TI (Tecnologías de la información), ya que la mayoría de los malentendidos entre el cliente y el profesional, se deben a dos factores principales, la poca capacidad del profesional para comunicar aspectos técnicos de forma comprensible para otros y el temor o desinterés que muestran las personas tecnológicamente alfabetizadas. De ahí la frustración de muchos profesionales al intentar comunicar los hallazgos y conceptos importantes a personal ajeno a las tecnologías. El caso anterior es algo bastante común entre las áreas técnicas y administrativas dentro de las organizaciones y por eso, quiero hacer hincapié sobre la importancia de la redacción, así como la criticidad de las palabras utilizadas en los reportes. En la práctica es de suma importancia que al redactar un informe de carácter público se consideren elementos como:

- Que tantos aportes puede generar un comentario u opinión
- Repercusiones que el informe podría tener para la organización
- El vocabulario utilizado
- Responsabilidad del ente auditor al realizar afirmaciones

Ya que la función del auditor es apoyar la tarea de robustecer el sistema en cuestión y no exhibirlo ante los posibles agresores. Por eso la ética debe ir de la mano con todas las actividades que el auditor ejecute y que estén relacionadas con el sistema u organización.

Existen dos tipos de reportes, técnico y ejecutivo. El primero va dirigido por lo regular al área y personal de la organización evaluada, que se dedican a instalar, configurar y mantener los dispositivos, redes, y entornos necesarios para el funcionamiento de sus aplicativos; en él se detalla cada hallazgo obtenido con evidencias gráficas o no gráficas además de una explicación técnica especificando puertos, servicios, datos sensibles, la forma en que se llegó a ellos y una recomendación de solución por cada una de las vulnerabilidades descubiertas. Los reportes ejecutivos por otro lado se dirigen al personal administrativo de altos rangos como gerentes, jefes de departamento y directivos de empresas o áreas. Este tipo de informe contiene en mayor parte, el impacto que las vulnerabilidades descubiertas podrían generar en el proceso o negocio que hace uso de la aplicación auditada, además, se agrega una opinión acerca del sistema y sus características de seguridad.

Cuando la auditoría se realiza a una entidad del sector privado, ambos tipos de informes se manejan con el nivel de secrecía que solicite el cliente, por lo general, de las puertas hacia adentro y en algunas ocasiones con secrecía máxima, al grado de que solo ciertas personas puedan conocer el contenido de estos.

Por otra parte, y como sucedió en los últimos proyectos que participé, cuando las instituciones pertenecen al sector público, además de participar en eventos de un nivel estatal con los que se define el rumbo de algún estado, los informes se manejan de ciertas formas. Estas instituciones por lo general solicitan de 2 a 3 informes parciales y un informe final, donde cada uno de los parciales representa una parte de las actividades realizadas y los hallazgos obtenidos a partir de estas, mientras que el informe final (de carácter público) contiene la opinión que realiza el ente auditor. Los informes parciales tienen un nivel de privacidad elevado, puesto que solo serán conocidos por la institución, en específico, por el área responsable del sistema y los recursos allegados a él. Los informes parciales se dividen en dos secciones, reporte técnico y ejecutivo, los cuales anteriormente mencionamos a quien van dirigidos. El informe final solamente contiene opiniones del auditor que no comprometen al sistema ya que son redactadas con cuidado, siendo precisos en las palabras que se utilizan, para no exponer alguna vulnerabilidad al público en general.

Ahora que conocemos con mayor detalle las actividades y objetivos pertenecientes a cada una de las etapas de la metodología utilizada, podremos profundizar un poco más sobre la auditoría, la ética del auditor, las herramientas utilizadas y como aplicar todo esto cuando de auditar sistemas electrónicos electorales se trata.

OWASP

El Proyecto Abierto de Seguridad en Aplicaciones Web por sus siglas en ingles OWASP, es una organización internacional sin fines de lucro enfocada al mejoramiento de la seguridad en el software, especialmente, aplicaciones web. “Estuvo en línea por primera vez el 1 diciembre de 2001 y se estableció como organización sin fines de lucro en Estados Unidos en abril del 2004 para garantizar la disponibilidad y el apoyo para la organización” (OWASP, 2016).

A través de la publicación de documentos y herramientas (de uso libre) desarrollados por su comunidad de profesionales voluntarios, busca que tanto las organizaciones como profesionistas dedicados a la

creación de software tengan presente que la seguridad es un aspecto que debe considerarse siempre que se desarrolle un nuevo sistema.

Esta organización siempre mantiene las puertas abiertas para cualquier aporte o persona que quiera unirse a la comunidad. Es por eso que mantiene disponibles las opciones de iniciar un nuevo proyecto, para lo cual sugieren una serie de pasos a seguir para obtener mejores resultados, o bien, actualizar uno existente, para lo cual, basta con seleccionar alguno que sea de nuestro interés para después unirse al grupo de personas que trabajen en él.

Hacer uso tanto de herramientas como de documentación generada por OWASP permitió al equipo de trabajo obtener mejores resultados de las revisiones efectuadas a los diferentes sistemas. La ejecución del proyecto en general se benefició con la implementación de la metodología aunada a el uso de buenas prácticas, así como herramientas proporcionadas por OWASP.

OWASP es una organización conocida y respetada mundialmente, debido a esto, el uso de documentación y herramientas desarrolladas por esta comunidad brindan un nivel de confianza mayor al cliente, además de favorecer la concientización sobre seguridad en las organizaciones sin la necesidad de realizar costosas inversiones.

Ahora que ya sabemos cuál es el objetivo de OWASP y que es lo que hace para acercarse a este, debemos explicar cómo benefició al proyecto el haber utilizado las herramientas y documentación que esta organización pone a disposición de cualquier persona que quiera acercarse a la seguridad en el software.

Durante la ejecución de las pruebas que se realizaron en los proyectos en conjunto con el OPLE de Veracruz y el IEEM se hizo uso de algunas de las herramientas desarrolladas por la organización y su comunidad, mismas que se detallaran en un capítulo posterior y que fueron utilizadas en diferentes etapas de los proyectos.

OSSTMM

El Open Source Security Testing Methodology Manual (OSSTMM por sus siglas en inglés), es un proyecto que surge a finales del año 2000 con el objetivo de proporcionar una metodología completa para realizar una evaluación de seguridad efectiva y libre de suposiciones. Para el año 2005 dejó de ser considerado como solo un marco de trabajo basado en buenas prácticas, dando pie a su transformación como metodología de evaluación a nivel operativo. Un año después, el conocimiento y experiencia de los colaboradores permitió que OSSTMM se convirtiera en un referente respecto a pruebas confiables de

seguridad convirtiéndolo en un estándar que iba más allá de solo realizar pruebas para cumplir con alguna legislación o regulación.

En su tercera versión, el manual contiene descripciones específicas para la ejecución de pruebas operativas de seguridad y abarca todos los canales posibles a los cuales pueden ser aplicadas tanto pruebas como evaluaciones de seguridad. Su objetivo es identificar que tan bueno es el funcionamiento de la seguridad en una organización. Lo anterior se logra a partir de no suponer que las soluciones, herramientas y procesos se comportarán tal y como la teoría lo dice, además, la metodología sugiere la verificación del funcionamiento adecuado de los mecanismos utilizados para garantizar la seguridad.

OSSTMM hace hincapié en que una amenaza solamente resultará efectiva en el momento que interactúe directa o indirectamente con el recurso objetivo, de otra forma esta no representa riesgo alguno. En ese sentido, el manual explica que la *seguridad total* solo es alcanzable siempre y cuando, el activo que se quiere proteger y la amenaza se encuentren completamente aislados uno del otro (situación poco probable en ambientes actuales); de otra forma, el nivel de aseguramiento del activo será proporcional a la calidad de controles y mecanismos de seguridad utilizados.

“La seguridad no tiene que durar por siempre; basta con que dure más que cualquier entidad que pueda notar su ausencia” (OSSTMM,2010).

Sistemas informáticos electorales

Son sistemas informáticos y de comunicación diseñados exclusivamente para automatizar procesos de recolección de datos y contabilización de actas durante las elecciones locales o federales en México. Debido a la criticidad de las tareas que desempeñan, es necesario garantizar la integridad, confidencialidad y disponibilidad tanto de la información que estos manejan como de la infraestructura sobre la que se ejecutan.

Los objetivos que tienen estos sistemas varían dependiendo el propósito para el cual fueron concebidos, por ejemplo, la función del PREP radica en la digitalización y contabilización de las actas que contienen los resultados de cada casilla para obtener un resultado no final al concluir las primeras veinticuatro horas después de concluida la jornada electoral. A pesar de que la naturaleza del resultado obtenido por el PREP no es definitiva, el sistema realiza el conteo del total de actas utilizadas durante la elección, lo cual, permite la obtención de un resultado bastante aproximado al que se obtendrá en el cómputo distrital, entregando así al público en general una aproximación al resultado final. Por otra parte, el sistema de Conteos Rápidos tiene como objetivo la recolección de la información contenida en las actas pertenecientes a una muestra aleatoria previamente seleccionada, para después realizar una proyección estadística de los resultados de la elección.

La sensibilidad de la información manejada por ambos sistemas, además del reglamento que los rige, obliga a los responsables de estos, a garantizar la seguridad de los activos inmersos en este proceso, ya que uno de los activos preponderantes y que los institutos deben mantener de forma cabal, es la credibilidad.

Terminología

Antes de comenzar a explicar cómo operan los sistemas PREP y Conteos Rápidos, será necesario aclarar algunos conceptos específicos relacionados con los mismos, los cuales ayudarán a comprender cada una de las etapas que se llevan a cabo durante su ejecución el día de la elección. Debido a que estos sistemas representan el principal objeto de evaluación en el proceso de la auditoría, es necesario analizar y comprobar el cumplimiento de los lineamientos que delimitan sus características y que a su vez son parte fundamental de los requerimientos que se deben cumplir para considerar tanto al PREP como Conteos Rápidos, aceptables y funcionales para llevar a cabo su tarea.

Los lineamientos son publicados por la autoridad electoral nacional, el INE y como ya mencionamos anteriormente, en ellos se publican las obligaciones del organismo a cargo de los sistemas electorales, entre ellas, el someter a evaluación por parte de terceros al sistema en cuestión.

Sin más preámbulos, comenzaremos con las actas de escrutinio y cómputo (AEC), las cuales son documentos en los que se asienta el resultado obtenido por casilla, por cargo de elección. Tienen que ser firmadas por el funcionario de casilla (previamente capacitado por las autoridades distritales) correspondiente para tener validez y que sean trasladadas al Centro de Acopio y Transmisión de Datos(CATD).

El CATD es el lugar al cual llegan las actas para su digitalización y posterior envío hacia el centro de cómputo distrital. Existe un CATD por cada junta distrital.

OPLE son las siglas de Organismo Público Local Electoral asignadas a los institutos electorales locales pertenecientes a cada entidad de nuestro país. Los OPLE se encargan de la organización para las elecciones locales correspondientes a la entidad en que se ubican.

Los Capacitadores Asistentes Electorales (CAE) pertenecientes al proceso de Conteos Rápidos, registran la información asentada en las Actas de Escrutinio y Cómputo al término de la elección para informar a la junta distrital correspondiente.

COTAPREP y COTECORA son los Comités Técnicos Asesores para el PREP y Conteos Rápidos respectivamente, están constituidos por una selección de expertos (provenientes de instituciones de educación superior) en temas como tecnologías de la información y estadística entre otros. Su principal función es proporcionar información oportuna para mejorar el desempeño de estos sistemas.

Programa de Resultados Electorales Preliminares (PREP)

Habiendo explicado antes un poco de la terminología que se utiliza dentro del contexto de los sistemas electorales, pasaremos al primer sistema electoral del que hablaremos, el PREP, sistema que según la norma del Instituto Nacional Electoral, "recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las AEC de las casillas que se reciben en los CATD autorizados por el Instituto o por los OPLE en el ámbito de su competencia" (INE, 2015).

El PREP inicia operaciones justo después de haber concluido la jornada electoral, es decir, a las dieciocho horas para elecciones locales y veinte horas para elecciones federales, una vez que todas las casillas se encuentren cerradas. El conteo de votos en cada una de las casillas es el primer paso y lo que da pie para que los funcionarios de casilla plasmen los resultados en el Acta de Escrutinio y Cómputo, misma que es firmada por el presidente de casilla. A partir de este punto, el AEC deberá ser trasladada y entregada por el mismo presidente de casilla a la junta distrital correspondiente mediante un protocolo seguro y funcional. Una vez entregada, una copia del AEC pasa a manos del CATD para ser digitalizada y enviada al centro de cómputo central para su posterior procesamiento. Una vez en el centro, cada una de las actas deben ser capturadas, recapturadas y validadas para que los datos contenidos en ellas puedan ser publicados por el sistema principal. Durante las siguientes veinticuatro horas a partir del inicio de funciones, el sistema actualizará los datos cada cierta cantidad de minutos (depende del acuerdo del OPLE correspondiente) con el fin de mantener actualizada la información que se publica en el portal oficial, donde no solo se aprecian la cantidad de votos por partido, sino también, la cantidad de votos nulos, el porcentaje de actas capturadas, contabilizadas y no contabilizadas.

Para explicar lo que este sistema tiene como tarea, diremos que el PREP es un sistema que involucra recursos de diferentes tipos, ya sean humanos, tecnológicos y de comunicaciones, los cuales colaboran entre sí para entregar los resultados preliminares no oficiales de las elecciones a través del procesamiento de los resultados asentados en cada una de las Actas de Escrutinio y Cómputo. En la Figura 5 se muestra el esquema de proceso que sigue el sistema PREP.

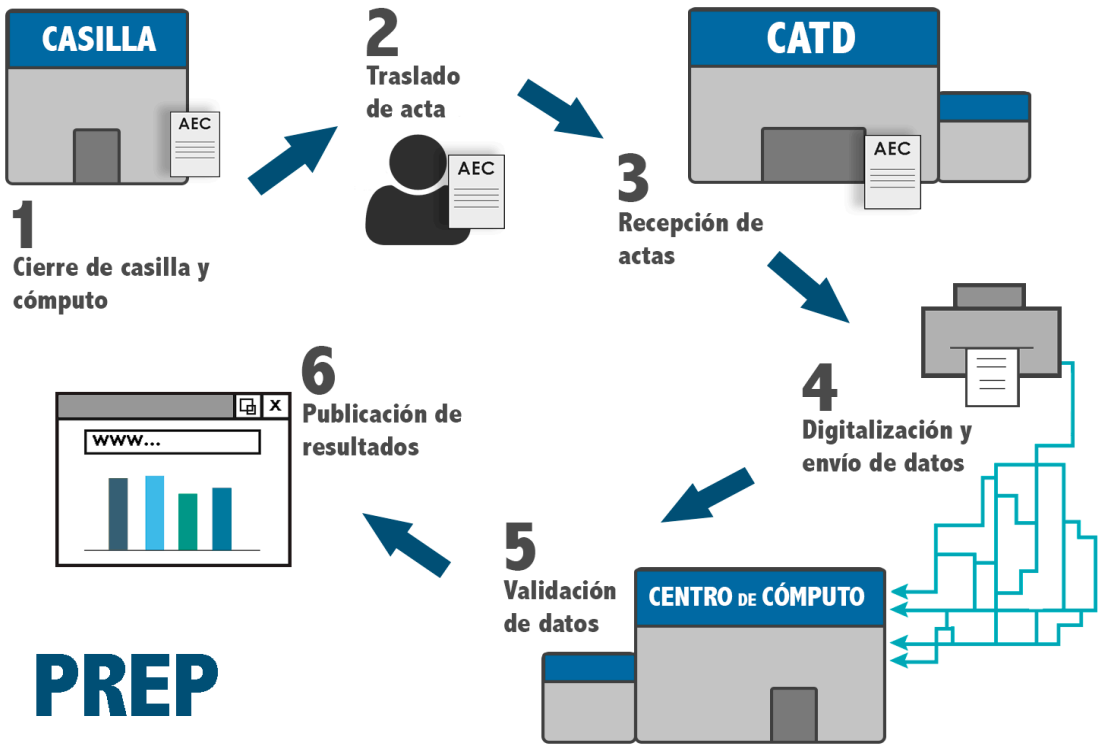

Figura 5.- Esquema de proceso para el sistema PREP

Conteos Rápidos

El proceso que Conteos Rápidos debe llevar a cabo inicia con la generación de una muestra aleatoria representativa del total de casillas por parte del Comité Técnico Asesor de Conteos Rápidos (COTECORA), posteriormente, al término de la jornada electoral, los funcionarios de cada una de las casillas seleccionadas en la muestra deberán comunicar vía telefónica al centro de cómputo, la información asentada en las AEC pertenecientes a la muestra. Una vez que la información es recibida en el centro de cómputo, se captura y recaptura con fines de verificación; COTECORA, determinará cuando el porcentaje de captura comience a mostrar resultados poco variables e irreversibles. Por último, resta la entrega del informe de resultados al consejo general y consejero presidente, para que después estos sean publicados. En la Figura 6 se muestra en un diagrama el proceso simplificado con imágenes.

La principal diferencia entre ambos sistemas radica en que el PREP debe contabilizar y procesar el total de actas, mientras Conteos Rápidos solamente utiliza una muestra de este total.

En la siguiente figura se puede apreciar el proceso que sigue conteos rápidos a partir de la selección de las casillas pertenecientes a la muestra, hasta la publicación de los resultados.

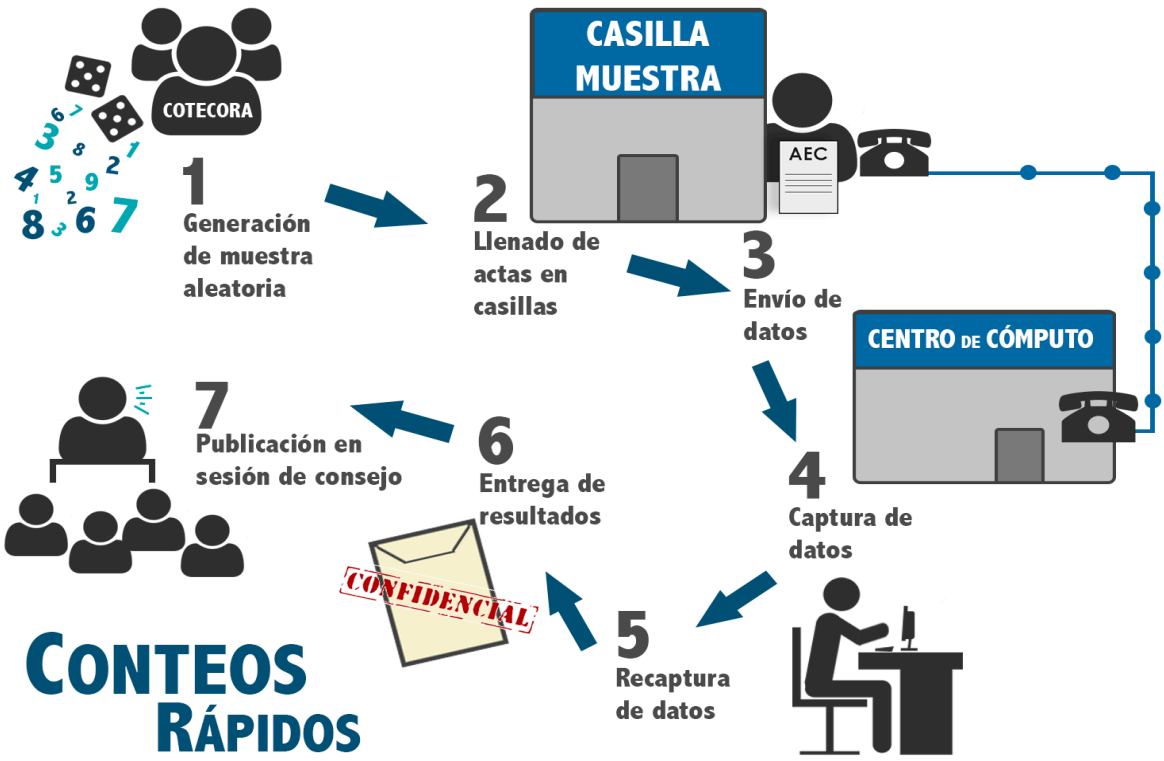

Figura 6.- Esquema de proceso para sistema Conteos Rápidos

III Auditoria de seguridad informática a sistemas electorales

Ahora que conocemos las bases necesarias para determinar lo que una auditoría de sistemas informáticos tiene por objetivo, trasladaremos esos conocimientos a un enfoque aún más específico: Los sistemas informáticos electorales. Entenderemos los procedimientos que implica una auditoría a sistemas electorales considerando que para un evento de estas dimensiones es necesario tener en consideración un mayor número de variables asociadas a sistemas de este tipo.

El INE es la máxima autoridad electoral y es el encargado de la organización de procesos de la misma índole en nuestro país. Como toda organización tiene activos tangibles e intangibles que debe proteger para garantizar la integridad de sus funciones y los servicios que ofrece a los partidos, ciudadanos, e instituciones. Entre los activos intangibles más valiosos que el instituto debería proteger se encuentran:

La credibilidad, transparencia, confianza, etc.

Mientras que entre los activos que pueden percibirse como tangibles se encuentran:

Bases de datos, Urnas (durante procesos electorales), Actas de escrutinio y cómputo, sistemas informáticos, infraestructura tecnológica, etc.

La necesidad de renovar y reafirmar la confianza depositada en las autoridades electorales de México fue el detonante principal para la creación de sistemas como el PREP y Conteos Rápidos, los cuales tienen por objetivo informar de forma oportuna un resultado preliminar (informativo, no oficial) además de una proyección estadística sobre el desenlace del proceso.

Los sistemas PREP y Conteos Rápidos están regulados por los lineamientos oficiales establecidos para cada uno de ellos. Dentro de estos documentos se indica la obligatoriedad de una evaluación en términos de seguridad y funcionalidad a dichos sistemas, la cual, debe ser ejecutada por una entidad imparcial y ajena al responsable del aplicativo, con el fin de anular cualquier opinión tendenciosa o subjetiva y asegurar que el dictamen sea en beneficio del proceso electoral.

Ética y comportamiento del Auditor

Un auditor que tenga experiencia en ejecución de pruebas de penetración tiene la capacidad y los recursos para vulnerar y obtener una gran cantidad de recursos del sistema que está auditando en cuestión de horas o incluso minutos, sin embargo, como profesional, y, sobre todo, siendo universitarios no debemos obtener beneficio alguno de nuestra de su posición y conocimiento, mucho menos lucrar con la información obtenida en las pruebas.

Es por eso que un auditor deberá conducirse con una intención benéfica para la organización en cuestión (cliente), además de ser oportuno con la información generada a partir de los descubrimientos y como representantes de la Facultad de Estudios Superiores Aragón, estamos obligados durante el proceso de auditoría a ser imparciales en la evaluación, responsables con las acciones que tomamos y consientes durante la redacción de informes.

El auditor que tiene por objetivo criticar los sistemas sin fundamento, no está aportando mucho al robustecimiento de la seguridad en estos sistemas, simplemente es un espectador más, que aplica un juicio con un fin poco constructivo.

Proceso general

Como regulador y encargado de la totalidad de los eventos electorales en el país, el Instituto Nacional Electoral es responsable ante los ciudadanos, partidos políticos y otras organizaciones que depositan su confianza cada periodo electoral en él.

Para que una entidad externa a las organizaciones electorales pueda realizar una auditoría a los sistemas que esta solicita, existe un proceso de selección en el que participan instituciones del sector público y privado. La institución seleccionada como auditor debe cumplir con los requisitos impuestos por los lineamientos oficiales, donde algunas de las características que se solicitan es la experiencia previa en auditorías, profesionales capacitados o con algún grado superior a licenciatura, entre otros.

Una vez que se ha seleccionado a la entidad auditora, se prosigue a generar los contratos (convenios) que amerite el tipo de proyecto. En nuestro caso, la universidad necesita establecer un convenio con la institución (OPLEV o instituto local) que solicita la auditoría. En el convenio se establece el alcance del proyecto y las responsabilidades tanto del cliente como del auditor. Las actividades que se van a realizar durante el tiempo designado en el cronograma se definen en el alcance del proyecto, dichas actividades

se establecen de acuerdo con las necesidades del cliente y las posibilidades del auditor considerando los recursos disponibles para realizar esta evaluación, es decir, se debe realizar un análisis de riesgos y planeación de actividades de acuerdo con las necesidades del cliente. Ambas partes tienen obligaciones que deben cumplir en tiempo y forma si se quiere que los resultados sean acorde a lo esperado.

Cuando las firmas necesarias para el convenio se han terminado de recolectar y este es aprobado por ambas partes, se procede a la solicitud de autorización del cliente para ejecución de pruebas sobre infraestructura, acceso a código fuente, así como ventanas de tiempo para las evaluaciones, revisiones pertinentes a los servidores y redes de la organización, además de las remediaciones que el cliente tenga que realizar para cubrir las vulnerabilidades encontradas.

Idealmente, los tiempos acordados previamente para revisiones y evaluaciones deben ser respetados por ambas partes, sin embargo, en la práctica, debido a la naturaleza del software, la burocracia dentro de las instituciones y otros factores de peso mayor, estas ventanas de tiempo se modifican con mucha facilidad, especialmente por parte del cliente. Este aspecto es bastante delicado, sobre todo cuando los tiempos se ven reducidos de forma repentina, pues esto provoca que las pruebas que se habían planificado para un periodo de una cantidad de tiempo, ahora se tendrán que ejecutar en menos. Esto sin duda se puede lograr, siempre y cuando se cuente con una gran cantidad de recursos humanos y tecnológicos, por ende, la ausencia o poca cantidad de los mismos podría mermar la productividad del equipo destinado a estas tareas, provocando que los objetivos no se alcancen al cien por ciento.

Para disminuir los cambios radicales en las ventanas de tiempo, es necesaria la concientización con el cliente en este aspecto e incluso realizar las peticiones de autorización para ejecución de pruebas por escrito, solicitando sean firmadas por el responsable del sistema auditado. Lo último bien podría ser útil en casos donde participan más de una entidad auditora, ya que, en caso de existir algún malentendido debido a una vulneración de seguridad, la autorización firmada por el responsable del sistema permitirá aclarar la situación permitiendo reconocer quien es el verdadero responsable del ataque.

Una práctica obligatoria para todo auditor es la obtención de evidencia (logs, capturas, entre otros) de las pruebas realizadas, pues es esta la forma de comprobar su trabajo y que este haya sido realizado en los tiempos acordados. Sin evidencia, cualquier opinión emitida, así como cualquier declaración, podrían ser fácilmente desacreditadas; situación a todas luces desprestigiadora para nosotros como entidad auditora.

La institución que solicita la evaluación debería contar con políticas y controles que le permitan, por lo menos, identificar (y de preferencia controlar) cualquier actividad que pueda considerarse sospechosa en

sus redes, servidores públicos e instalaciones. De esta forma la organización tendría mejor manejo de todo lo que ocurra con sus activos y podría asignar espacios de tiempo para la realización de pruebas manteniendo un entorno controlado.

En general este tipo de organizaciones tienen un sistema de control de acceso con mecanismos como detección de metales, registros a la entrada del edificio y de cada área dentro del mismo, sensor de proximidad, CCTV, etc. Sin embargo, para que estos sean realmente efectivos, requieren de la correcta capacitación del personal, lo cual es un área de oportunidad en la cual toda organización debería invertir para robustecer la seguridad y con esto proteger de una forma efectiva los activos.

Concluido el análisis de las necesidades presentadas por el cliente y obtenidas las autorizaciones necesarias para la realización de las pruebas, se prosigue a ejecutar la primera fase de la metodología de pruebas de penetración. Durante el descubrimiento, se identifica la mayor cantidad de recursos pertenecientes a la organización, que son accesibles de una forma no intrusiva, utilizando la observación y en ocasiones herramientas de uso común, como el navegador web.

Una vez que se recolectó una buena cantidad de información en la primera etapa, se procede a organizar y analizar el cúmulo de información para generar vectores de ataque. Durante este segundo análisis se sopesa la criticidad de cada uno de los hallazgos y se apartan los datos que no generan ningún aporte para los vectores de ataque propuestos.

Enumerados los recursos e información encontrados en la etapa anterior, proseguimos a ejecutar el análisis de vulnerabilidades a la infraestructura y sistemas informáticos, usando como yesca para el fuego, los vectores generados previamente. Estos vectores son los iniciadores para cada uno de los intentos de vulneración que se pretende realizar. Siempre existe la posibilidad de que un ataque no llegue más allá de las posibilidades del mismo vector, permitiendo clasificar a este como un falso positivo. Por otra parte, los vectores que resulten en ataques exitosos deberán ser documentados con evidencia y redacción de lo ocurrido durante el proceso. La etapa en la que se prueban los vectores en búsqueda de la obtención o vulneración de algún recurso se le conoce como análisis de vulnerabilidades.

Terminada la fase de análisis de vulnerabilidades, toda la evidencia debe ser organizada y presentada en un documento (informes parciales) donde se asiente un registro de las pruebas realizadas, así como los hallazgos y la criticidad de los mismos. La generación de reportes es de suma importancia, ya que a través de ellos es como se le da conocimiento a la organización que fue auditada sobre las vulnerabilidades

existentes, el nivel de riesgo que corre con cada una de ellas, así como sugerencias de solución para las mismas.

Cuando la organización conoce las debilidades de sus sistemas, se otorga un periodo de remediación, del cual, el objetivo principal es corregir, mitigar o prevenir que los hallazgos obtenidos durante las pruebas se conviertan en situaciones reales durante el proceso de las elecciones. Estas correcciones se realizan en base al criterio del cliente, sin embargo, como ente auditor, se le hacen recomendaciones al respecto, esperando sean de utilidad y vayan acorde a las necesidades de la organización.

A lo largo del proceso de organización y desarrollo del proyecto, se realiza por lo menos un simulacro de actividades, en el cual se simula la totalidad de actividades planeadas para el día de la elección. Se realizan pruebas de backup de energía en plena actividad, también se utiliza personal que provea de seguridad física (por lo general una organización privada), además de controles de seguridad como es el uso de gafetes para mantener el control de accesos en las entradas principales y áreas críticas. Estos simulacros se realizan con el fin de identificar las áreas con posibilidad de ser robustecidas antes de la ejecución final, sin mencionar que se busca conocer el funcionamiento más aproximado a una situación real. Como auditores debemos estar presentes durante el desarrollo de los mismos, observando y evaluando el comportamiento de los sistemas, así como, el desempeño, conocimiento y aplicación tanto de políticas como controles por parte del personal en todos los niveles jerárquicos. Solo presenciando el curso del proceso en una situación más *realista* podremos identificar los defectos que no son visibles cuando las pruebas son estáticas.

Un atacante cuenta con todo el tiempo que necesita para la preparación y puesta en marcha de un ataque. En contraste, el pentester en ocasiones cuenta con tiempos y recursos limitados, esto debido a diferentes factores, tales como: el temor y resistencia que el cliente ofrece, la disponibilidad de la infraestructura, y en buena medida la burocracia que en los trámites reside; esto sin duda provoca que las posibilidades del auditor para obtener mejores resultados, se reduzcan considerablemente, sin embargo contar con un equipo de personas bien capacitado y experimentado permite sortear los contratiempos emergentes y alcanzar los objetivos planteados inicialmente.

Pentest a sistemas electorales

Debido a las modificaciones de requerimientos, los sistemas electorales (como la mayoría del software), son propensos a sufrir cambios de último momento, lo cual, complica el panorama para el auditor, en especial cuando de cronogramas y espacios de tiempo para ejecución de pruebas se trata. Durante cada uno de los proyectos en los que participamos existieron modificaciones de este tipo, situación que retrasó la ejecución de las pruebas previstas en el calendario. Este punto es común dado el tipo de institución responsable del sistema, pues muchas veces el papeleo o burocracia dentro de una organización pública provoca el lento funcionamiento de los procesos, desde la instalación de la infraestructura, hasta las aprobaciones de ventanas de tiempo para ejecución de pruebas.

Concluidas las pruebas y hechas las recomendaciones, se debe dar paso a remediaciones pertinentes que logren mantener la funcionalidad y seguridad, una vez concluido el periodo de correcciones, como auditores verificamos cuales correcciones fueron hechas y cuáles no, ya sea por falta de tiempo o el poco impacto que tengan en el sistema.

Otro factor que reduce los tiempos disponibles para que el auditor pueda ejecutar sus tareas, es la intervención de varios proveedores de servicios como plantas de respaldo eléctrico, la instalación de equipos y red necesarios (si es el caso). Si la organización responsable del evento electoral no realiza una buena planeación cronológica de las actividades entre proveedores, accesos a instalaciones etc. El resultado podría concluir en una fila de espera para la instalación de diferentes servicios necesarios en un mismo espacio de tiempo.

Recordemos que, en eventos electorales hay una fecha límite no postergable para que los sistemas sean funcionales y seguros. Esta fecha es el día de la elección. A partir de esto, concluimos que, si un proveedor depende de la previa instalación de otro servicio, las actividades programadas para ciertas fechas deberán ser postergadas, esto se traducirá en la reducción del tiempo disponible para el cumplimiento de objetivos. En el caso de nosotros como auditores, dependemos de que la totalidad de los servicios estén funcionales y completamente instalados, pues nuestra tarea radica en evaluar el sistema y las condiciones sobre las que todo el proceso funcionará. Entre menos tiempo disponible tenga un auditor para realizar las pruebas necesarias, mayor será la probabilidad de que el alcance previamente acordado no se cumpla al cien por ciento, provocando que la evaluación sea parcial. Por esto, se sugiere realizar una planeación previa de actividades, considerando un tiempo máximo y mínimo para cubrir la totalidad de las mismas. Mantener una buena y constante comunicación con el cliente, es una práctica que favorece el cumplimiento en tiempo y forma de los objetivos planteados en la auditoría.

Otras consideraciones

Una vez que se han revisado los sistemas y se ha informado al responsable sobre las vulnerabilidades que este presento durante las pruebas, es necesario otorgar un tiempo de remediación en el cual la organización debería centrarse en la mitigación de las mismas. Por su puesto, la entidad auditora realiza sugerencias para la remediación de los hallazgos obtenidos. Una vez terminado el plazo otorgado, como auditor, debemos proceder a verificar, estén o no solventados los problemas de seguridad, pues de esto dependerá la redacción de los reportes e informes posteriores.

Muchos factores pueden perjudicar la integridad del proceso electoral, uno de ellos es la falta de información o manipulación indebida de la misma. Es por eso que creo necesario el énfasis en la correcta construcción de reportes e informes, pues sin duda, es uno de los aspectos más delicados asociados a la auditoría de sistemas electorales.

Sabemos que, a lo largo de una auditoría de este tipo, pueden entregarse entre tres y cuatro informes a la organización auditada, y como habíamos mencionado anteriormente, los lineamientos indican que deben entregarse al menos dos informes parciales de naturaleza privada, es decir, únicamente para conocimiento del cliente y un informe final, cuyo contenido se publica con el fin de dar a conocer ante la audiencia el resultado de la evaluación realizada. Los informes parciales están formados por dos partes, la parte directiva y la técnica, mientras que un informe final contiene únicamente la redacción general del comportamiento del sistema.

Es debido a que la credibilidad representa sin duda uno de los activos de mayor valor para los organismos responsables de la logística de las elecciones, el que un auditor deba imprimir especial atención en la redacción y generación de informes, de lo contrario, la posibilidad de que exista una interpretación no deseada por parte de los medios de comunicación o el público en general crece con cada frase o inclusive palabra que en otro contexto perjudique a la evaluación realizada.

IV Herramientas de "pentest"

Existe la idea errónea de creer que un hacker es aquella persona que se siente frente a una computadora a teclear mientras ríos de información fluyen en su pantalla, imágenes detalladas aparecen y la información que desea, se muestra mágicamente, depurada y formateada de forma impecable. Si bien, esta idea no resulta tan descabellada en estos días, ya que existen herramientas tan poderosas que son capaces de analizar información por si solas, realizar búsquedas en cantidades increíblemente grandes de información e incluso capaces de realizar ataques específicos automatizados; siempre será invaluable la participación de un profesional con conocimientos sólidos para desempeñar tareas como una oportuna planeación del uso de las herramientas, además de una correcta interpretación de los resultados obtenidos por las mismas.

Las herramientas actuales están hechas con un enfoque tan amigable con el usurario, que casi cualquier persona con un poco de conocimiento en cómputo y redes, es capaz de perpetuar un ataque pasando desapercibido. Sin embargo, esperamos que la ideología del lector vaya más allá de buscar un manual donde aprender a utilizar algunas herramientas y se oriente hacia la comprensión del funcionamiento y la interpretación de todos los conocimientos que implica la utilización de las mismas durante un proyecto como este.

En este capítulo, se pretende realizar un acercamiento con la práctica durante las pruebas de penetración, por lo tanto, mostraremos el funcionamiento de las herramientas que se utilizaron durante los proyectos en conjunto con el IEEM y OPLE de Veracruz, aplicadas en aplicativos web controlados.

FOCA

Fingerprinting Organizations with Collected Archives por sus siglas en ingles FOCA, es un software que permite hacer búsquedas de metadatos e información oculta en archivos. Permite analizar una gran variedad de formatos como los que están asociados a Microsoft Office, Open Office, PDF e incluso analiza archivos con formato svg (Scalable Vector Graphics). FOCA utiliza tres motores de búsqueda para la obtención de los archivos disponibles en los sitios web, Google, Bing y DuckDuckGo (poco utilizado), los cuales en conjunto aumentan la cantidad de archivos que están disponibles para análisis.

En el caso de los proyectos del OPLE de Veracruz y IEEM se utilizó para la obtención de metadatos como usuarios, sistemas operativos, clientes, servidores y posibles contraseñas asociados a los archivos disponibles en los sitios web del cliente.

Compañía/desarrollador: Eleven Paths

Licencia: Open Source

Etapa de metodología: Descubrimiento

Sitio Web: https://www.elevenpaths.com/es/labstools/foca-2/index.html

Uso de herramienta:

Al ejecutar por primera vez la herramienta, podremos apreciar la pantalla inicial que nos muestra el logo de la herramienta, junto con la leyenda “FOCA final version” como muestra la Figura 7.

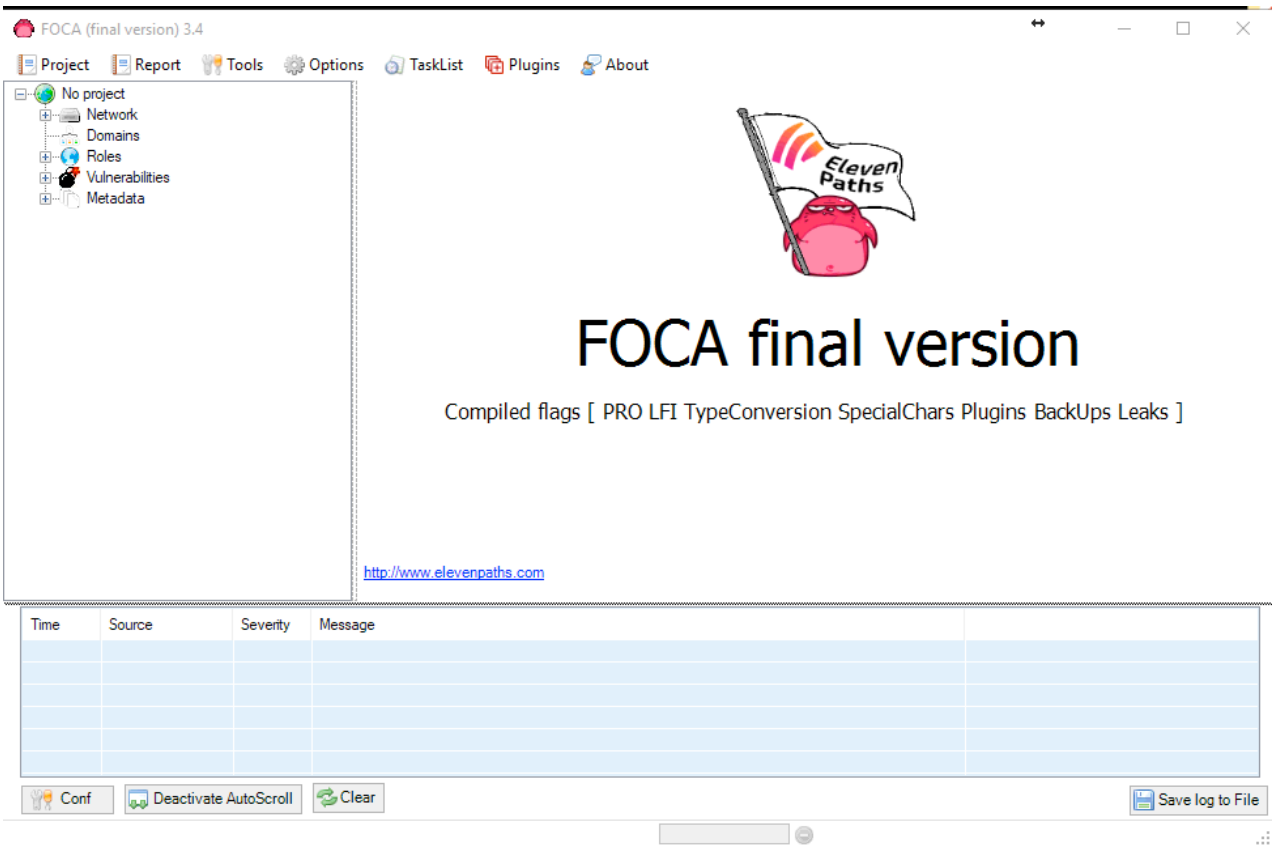

Figura 7.- Pantalla principal de FOCA

Para crear un nuevo proyecto, haremos clic sobre la pestaña *Project* ubicada en la esquina superior izquierda, y posteriormente en la opción *new project*, lo que desplegará una pantalla donde se establecerán: nombre de proyecto, el sitio objetivo y la carpeta de guardado como se puede apreciar en la Figura 8.

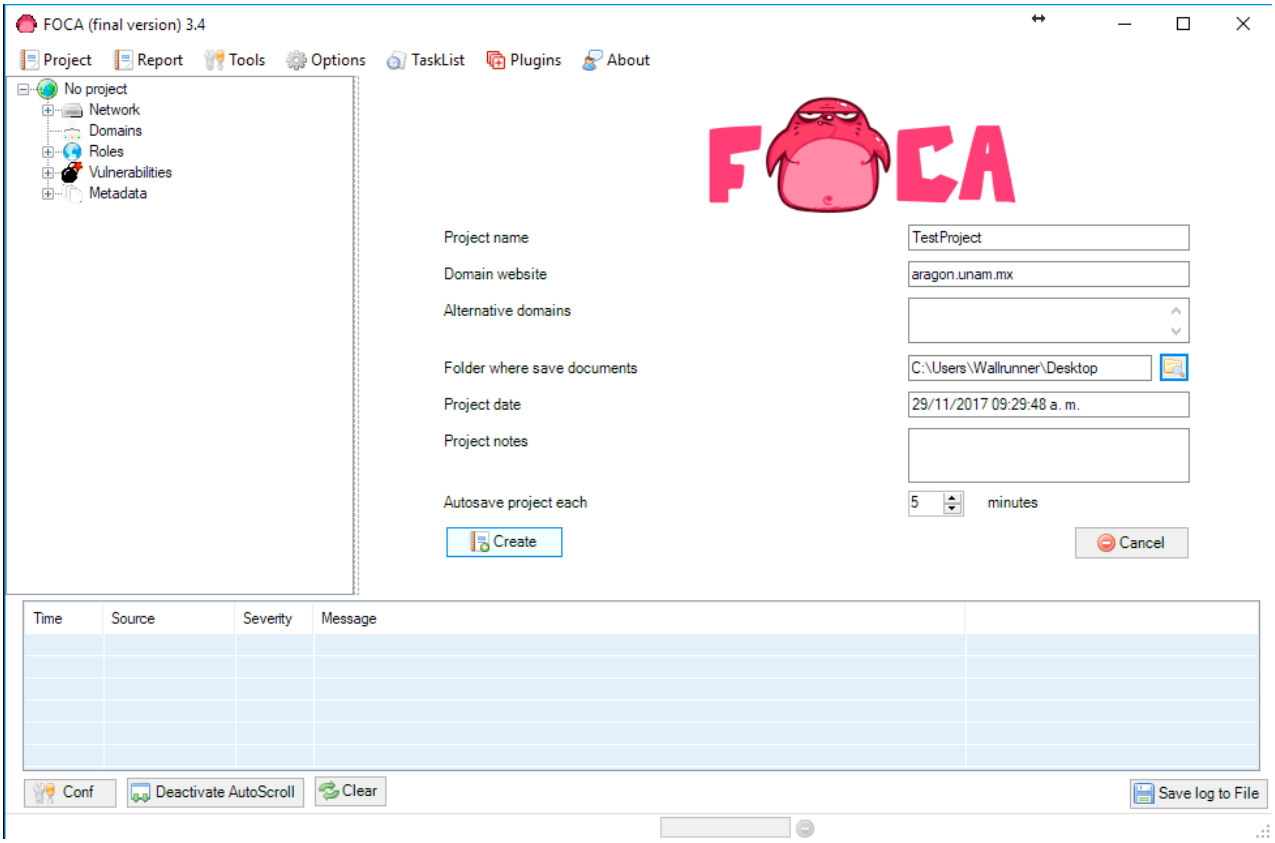

Figura 8.- Creación de nuevo proyecto en FOCA

Una vez hecho lo anterior, haremos clic en el botón *Create*. Se nos solicitará la asignación de un nombre para guardar el proyecto. Estableceremos uno y haremos clic en *Guardar*, Figura 9.

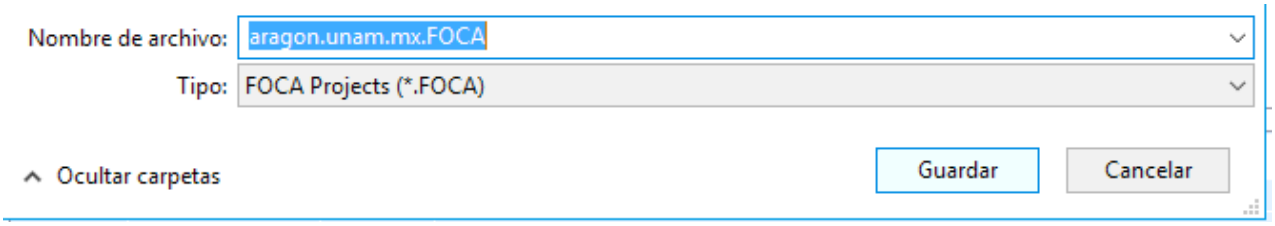

Figura 9.- Asignación de nombre para archivo de guardado

Guardado el proyecto, se despliega la pantalla donde empezaremos a trabajar, en ella se puede distinguir un botón con la leyenda *Search All* como se muestra en la Figura 10, haremos clic sobre él, lo que iniciará la búsqueda de documentos en el dominio objetivo.

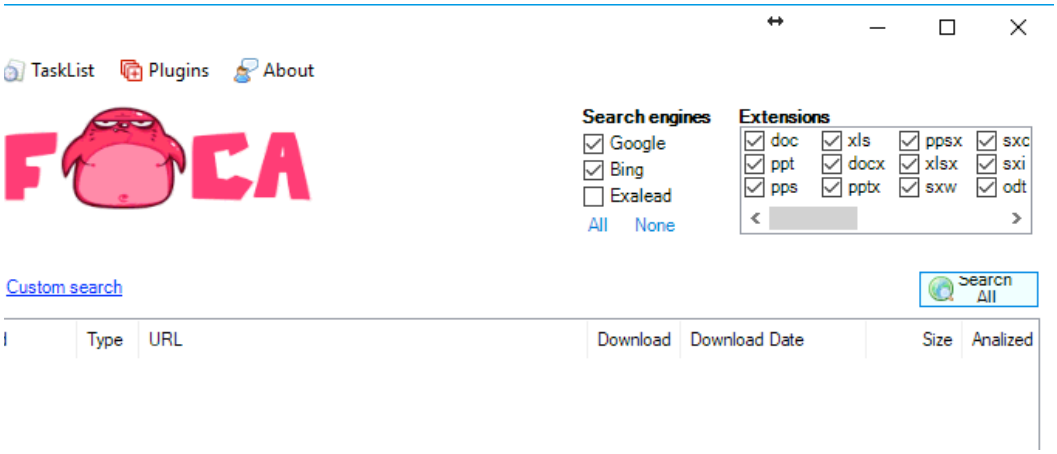

Figura 10.- Inicio de búsqueda de archivos

Una vez que FOCA haya encontrado todos los archivos disponibles en los sitios, será necesario descargarlos, por lo que haremos clic derecho sobre cualquiera de los archivos y posteriormente haremos clic sobre la opción *Download all* como se muestra en la Figura 11.

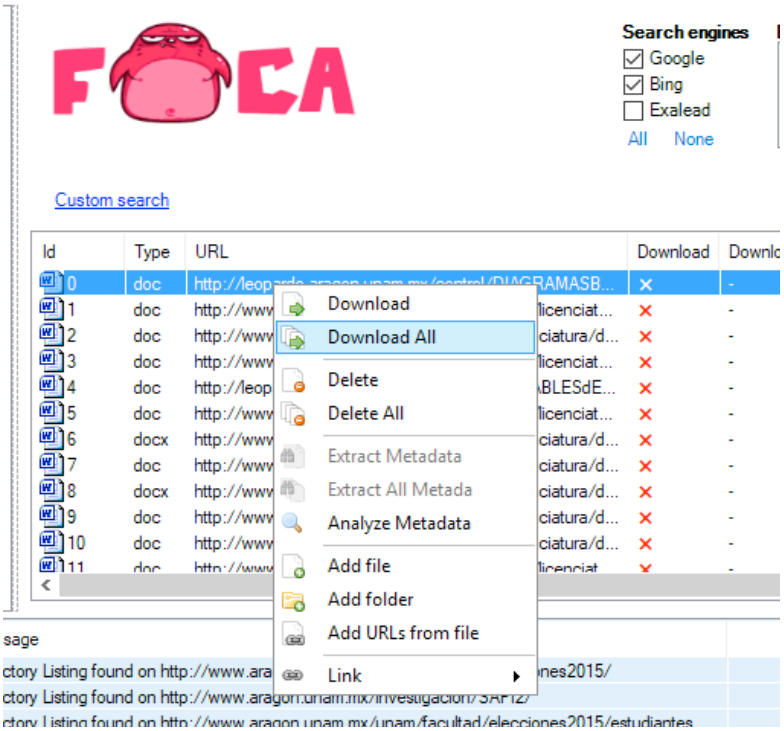

Figura 11.- Inicio de descarga de archivos

La descarga de todos los archivos demorará algo de tiempo y estará completa cuando todos los archivos tengan el indicador de descarga exitosa, lo cual es señalado con un punto verde en la columna *download*, tal cual se muestra en la Figura 12.

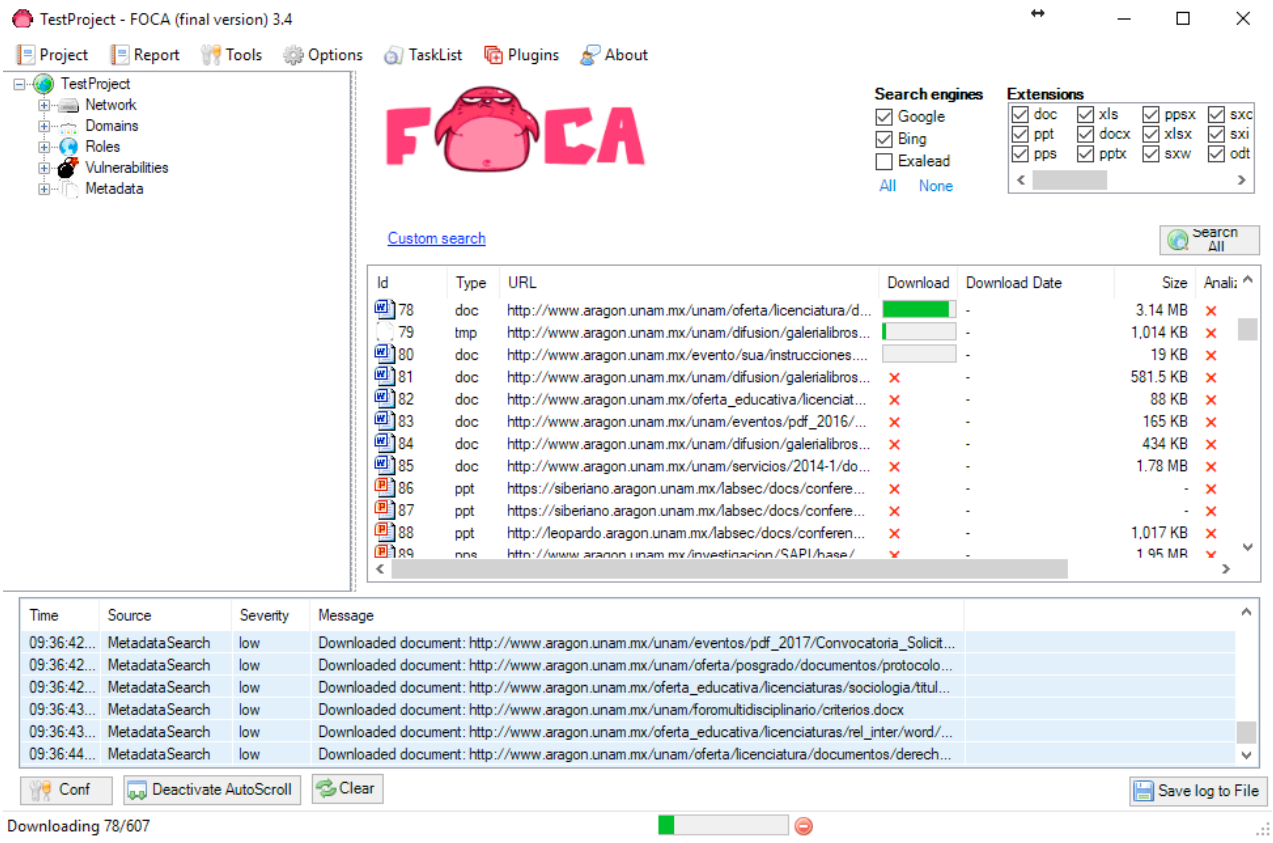

Figura 12.- Descarga en progreso de la totalidad de archivos encontrados

Algunos de los documentos mostrarán una equis roja en lugar de un punto verde como se muestra en la Figura 13, esto se debe a que la descarga no se puedo completar y debe ser reiniciada solo para estos archivos.

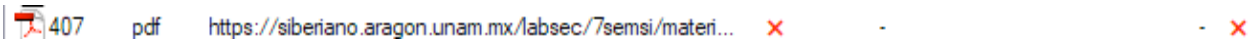

Figura 13.- Archivo con interrupción o falla de descarga

Una vez que todos los archivos se hayan descargado, haremos clic derecho sobre cualquiera de ellos y posteriormente haremos clic sobre la opción *Analyze Metadata*, esto dará inicio al análisis de todos los documentos obtenidos del sitio. En la Figura 14 se muestra el procedimiento anterior.

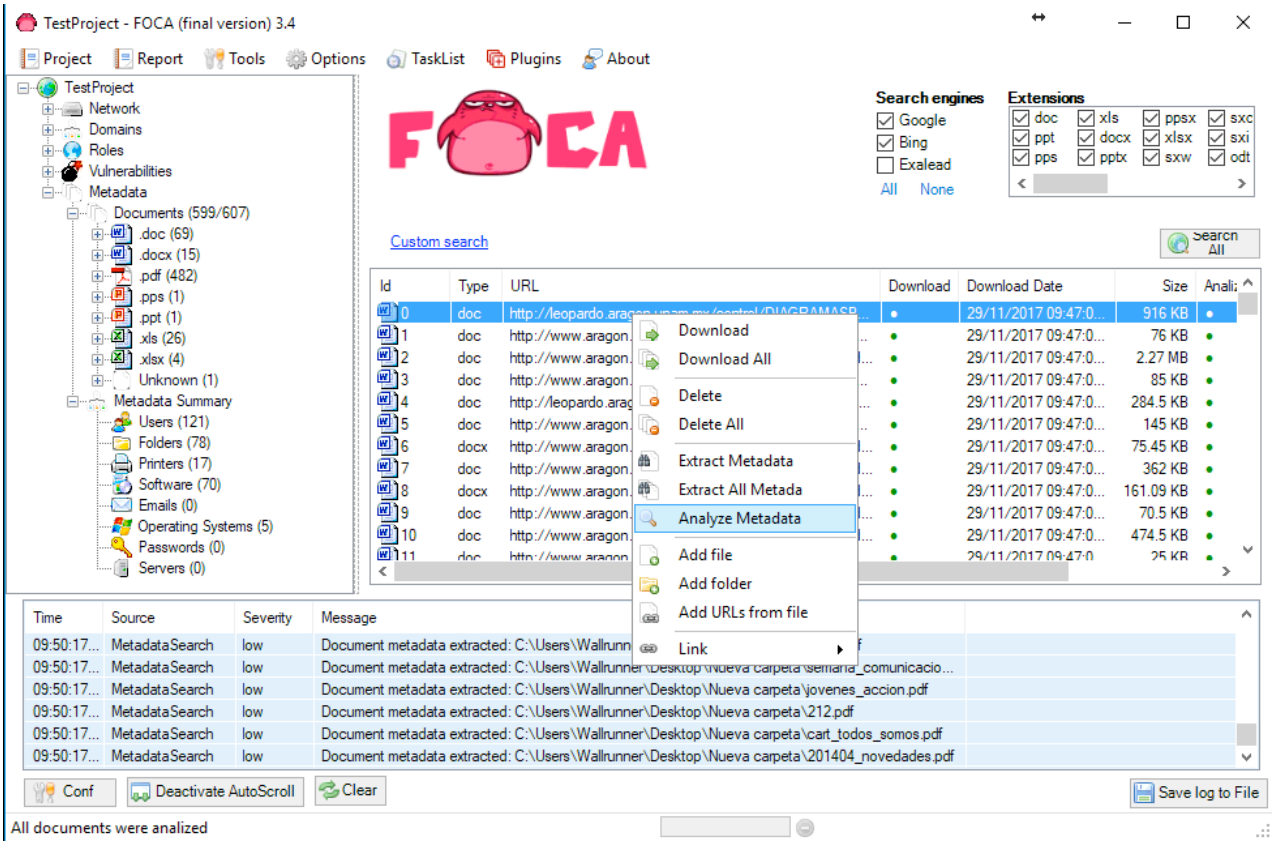

Figura 14.- Extracción y análisis de metadatos

Completado el análisis, es recomendable exportar los resultados a un documento donde puedan detectarse los datos que sean sensibles y se hayan encontrado durante el análisis.

Para dar paso a la generación del reporte, tendremos que hacer clic en el menú *Report*, lo que desplegará la pantalla de selección de tipo de reporte, donde elegiremos para este ejemplo, la opción *Metadata Report*. La Figura 15 muestra el desarrollo del procedimiento anterior.

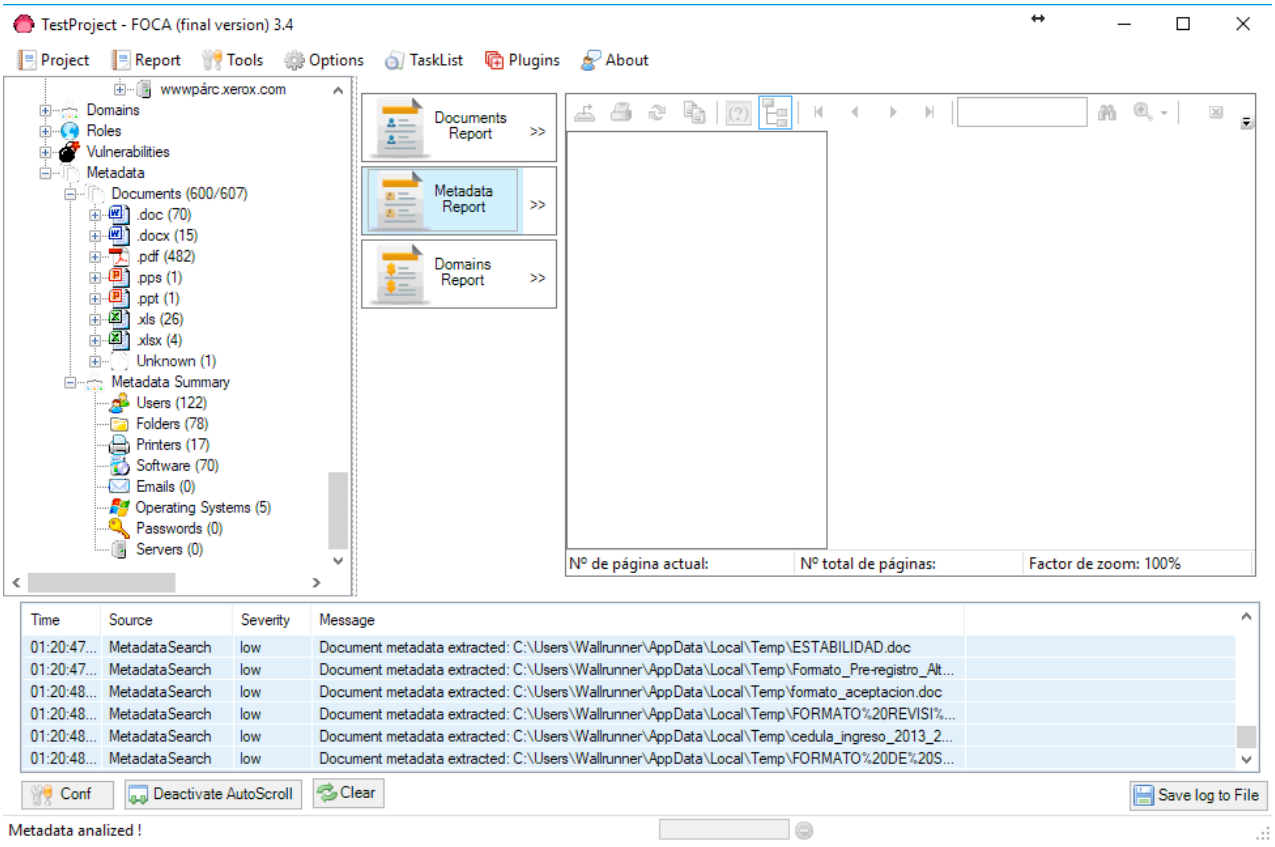

Figura 15.- Selección de tipo de reporte

Seleccionando la opción de reporte, aparecerá una ventana en la que marcaremos las casillas de las categorías que nos gustaría incluir en el reporte, así como sus atributos. En este caso, seleccionaremos todos ellos tal como muestra la Figura 16.

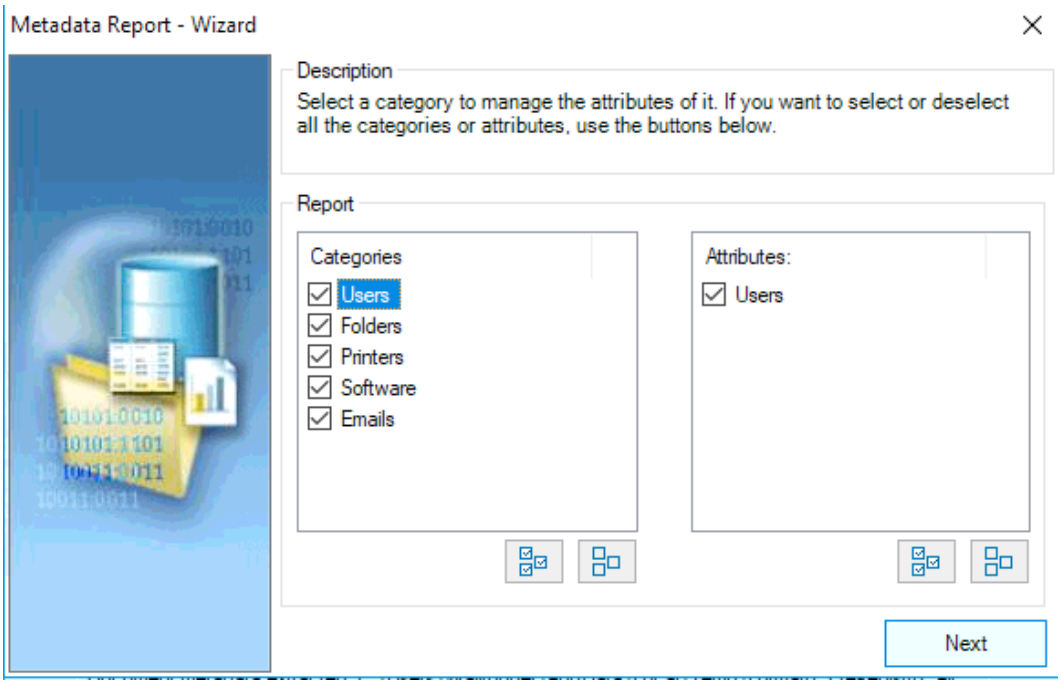

Figura 16.- Selección de categorías para el informe

Habiendo seleccionado las categorías y atributos de cada una de ellas que deseamos en el reporte, haremos clic sobre el botón *Next*. La siguiente pantalla de configuración de reporte aparecerá solicitando marcar las casillas de las gráficas que deseamos aparezcan en el mismo. En este ejemplo seleccionaremos las dos primeras y la penúltima. En la Figura 17 podemos observar que las opciones seleccionadas corresponden a las gráficas de metadatos para grupos, usuarios y software.

Cuando se haya terminado de marcar las opciones, procederemos a hacer clic sobre el botón *Build*, lo que iniciará el proceso de generación del reporte.

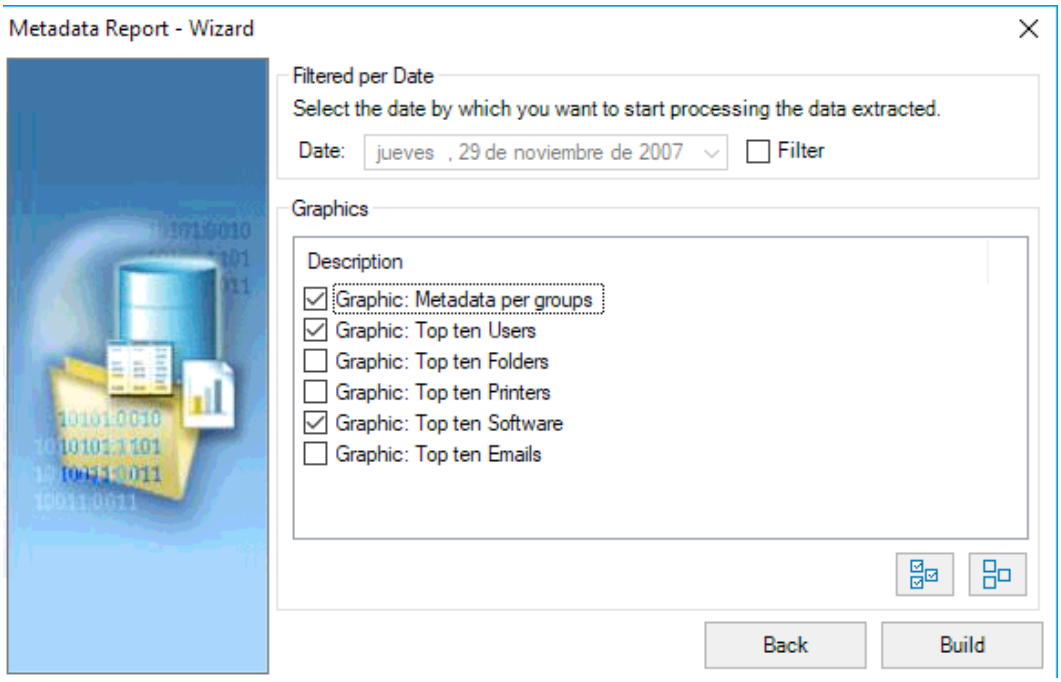

Figura 17.- Selección de gráficas ilustrativas para el informe

Cuando el reporte se haya generado, se mostrará una previsualización del mismo, donde podremos verificar que los datos y las gráficas sean los que deseamos que aparezcan en él. Las ilustraciones Figura 18 y Figura 19 muestran la vista previa del reporte y gráficas obtenidas del análisis.

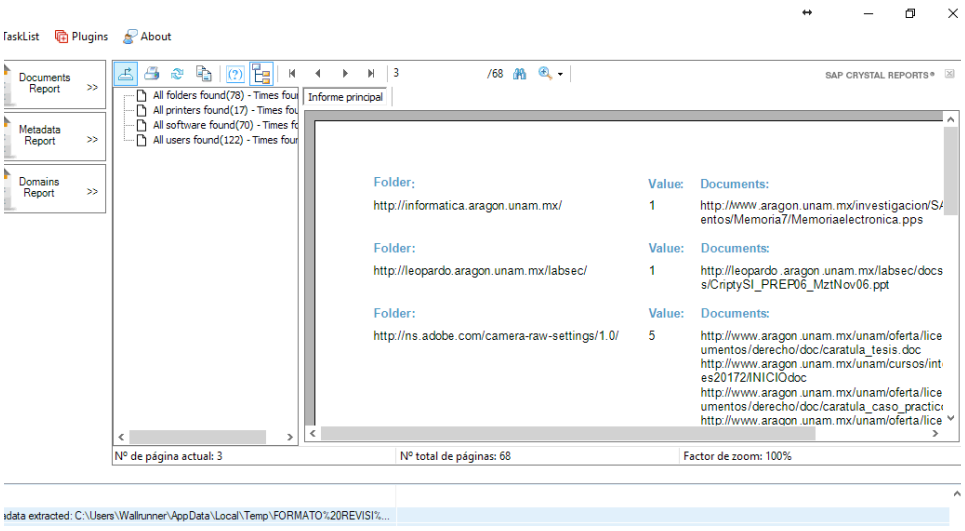

Figura 18.- Vista previa del informe generado

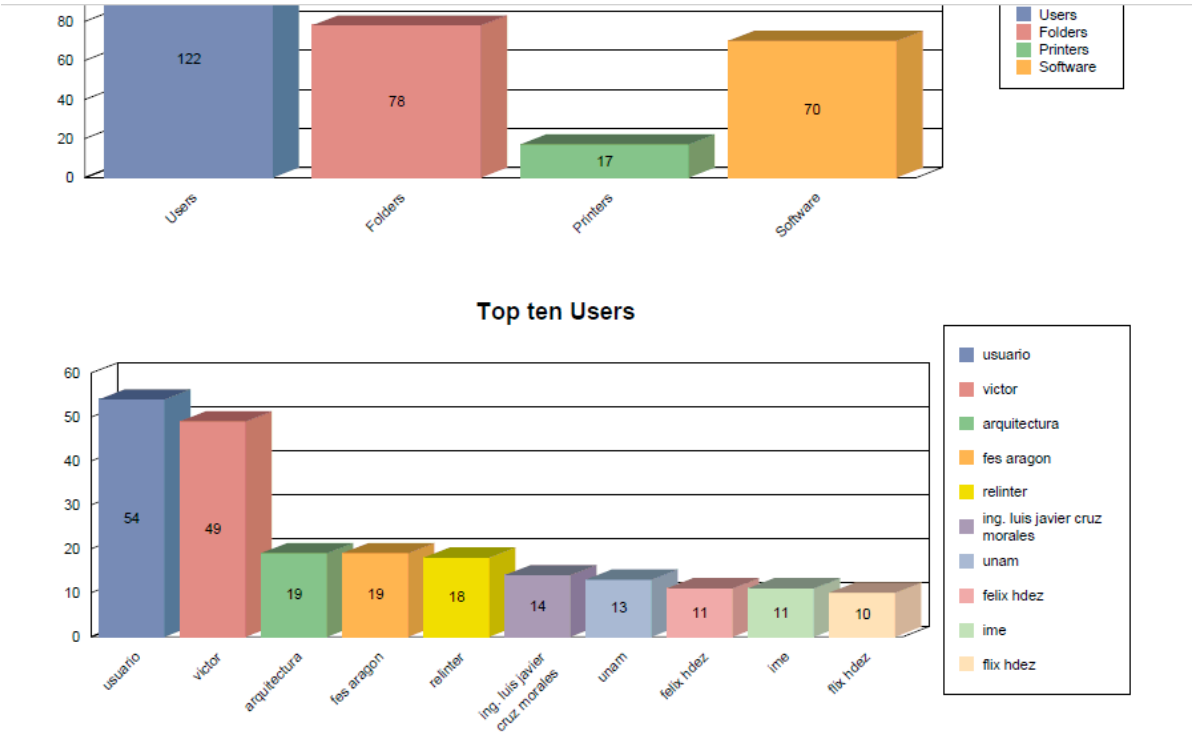

Figura 19.- Vista final de informe generado (gráficas ilustrativas)

Nmap

Network Mapper es el nombre completo de una herramienta utilizada comúnmente en pruebas de penetración para realizar escaneos de red, que proporcionan información acerca de que dispositivos están conectados en la red, que servicios ofrecen, cuales están cerrados y cuales abiertos, así como los sistemas operativos que se ejecutan en ellos.

Durante el descubrimiento realizado en las pruebas de penetración se utilizó nmap como herramienta principal para escaneos de red e identificación de objetivos. Durante el enumeramiento, los resultados arrojados por la herramienta permitieron la generación de vectores con mejores probabilidades de éxito.

Compañía/Desarrollador: Gordon Lyon (nmap.org)

Licencia: Open source

Etapa de metodología: Descubrimiento

Sitio Web: https://nmap.org/

Uso de herramienta:

Como ejemplo del funcionamiento de Nmap, mostraremos como se realiza un escaneo en una red privada, además de explicar el comando necesario y las opciones que se utilizaron.

Siempre que se realicen pruebas relacionadas con alguna red, es necesario comprobar que estamos conectados a la red que deseamos analizar, por eso ejecutamos el comando *ifconfig*, el cual arroja la configuración de red actual para nuestro dispositivo. La Figura 20 muestra el resultado de ejecutar el comando anterior.

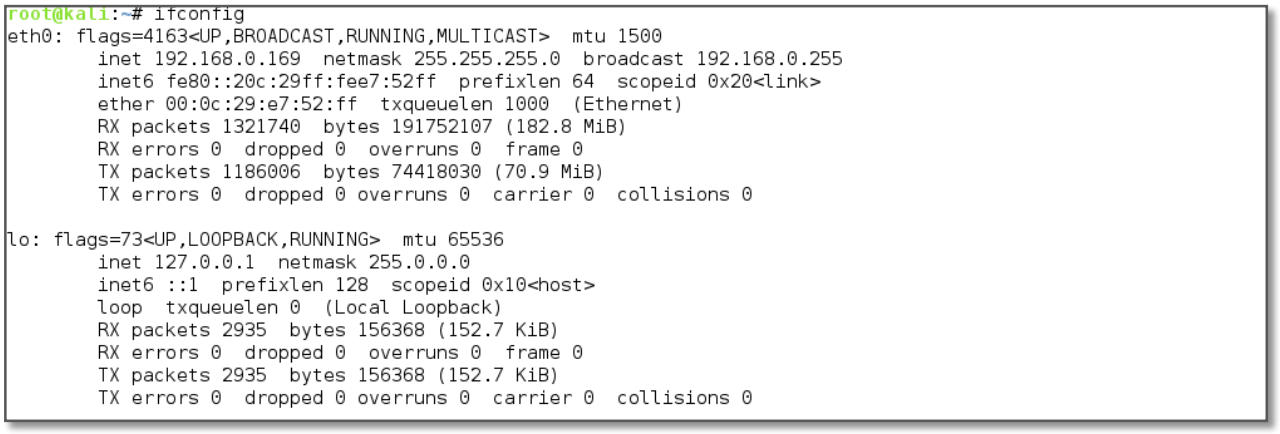

Figura 20.- Configuración de red para el equipo que realizará la prueba

Posteriormente ejecutamos el comando siguiente para iniciar el escaneo de los dispositivos:

```
# nmap -T4 --top-ports 10 -sN -sV -O -oA <Testscan> 192.168.0.0/24
```

Donde -T4 significa el tiempo de sondeo (0-5 donde 5 es menor tiempo), --top-ports 10 especifica que deberán analizarse los diez puertos más comunes, sN se utiliza para que el escaneo sea enfocado a TCP, mientras que -Sv permite un escaneo de versiones de los servicios disponibles. La opción O solicita el análisis de sistema operativo, y, por último, oA solicita la exportación de los resultados a los tres formatos disponibles con el nombre *TestScan*. Por último, colocamos el id de red que queremos analizar seguido de la máscara de red correspondiente. En la Figura 21 podremos observar la salida del comando.

```
root@kali:~# nmap -T4 -sN -sV -O --top-ports 10 -oA TestScan 192.168.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-18 00:42 EST
Nmap scan report for 192.168.0.85
Host is up (0.00077s latency).
PORT     STATE         SERVICE    VERSION
21/tcp   open|filtered tcpwrapped
22/tcp   open          ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
23/tcp   open|filtered tcpwrapped
25/tcp   open|filtered tcpwrapped
80/tcp   open|filtered tcpwrapped
110/tcp  open|filtered tcpwrapped
139/tcp  open|filtered tcpwrapped
443/tcp  open|filtered tcpwrapped
445/tcp  open|filtered tcpwrapped
3389/tcp open|filtered tcpwrapped
MAC Address: 00:50:BF:51:B3:3D (Metalligence Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 3.19, Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.102
Host is up (0.00020s latency).
PORT     STATE  SERVICE       VERSION
21/tcp   closed ftp
22/tcp   open   ssh           OpenSSH 7.5 (protocol 2.0)
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http          Apache httpd 2.4.27 ((Unix) PHP/7.1.7)
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 0C:4D:E9:A8:55:6B (Apple)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=11/18%OT=22%CT=21%CU=33990%PV=Y%DS=1%DC=D%G=Y%M=0C4DE9
OS:%TM=5A0FC85C%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=RD%I
OS:I=RI%TS=A)OPS(O1=M5B4NW5NNT11SLL%O2=M5B4NW5NNT11SLL%O3=M5B4NW5NNT11%O4=M
OS:5B4NW5NNT11SLL%O5=M5B4NW5NNT11SLL%O6=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W3
OS:=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW5SLL%CC=Y
OS:%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=4
OS:0%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%
OS:A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RU
OS:CK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 1 hop
```

Figura 21.- Comando Nmap en ejecución, mostrando salida en la terminal

ZAP

Zed Attack Proxy es el nombre de la herramienta que nos permite realizar un rastreo de los hiperenlaces dentro de un sitio web, de esto, se obtiene una lista de todos los enlaces disponibles en los recursos públicos del aplicativo. Además de permitirnos realizar *web crawling* [12]de los sitios, ZAP es capaz de realizar un análisis de vulnerabilidades, el cual, resulta bastante útil, siempre y cuando no se dé por hecho

[12] El término web crawling se refiere al consumo e inspecciones de recursos web de forma automatizada, a partir de una lista de URL, identificando enlaces dentro de los sitios, para posteriormente inspeccionarlos uno a uno, realizado por un programa informático conocido como web spider o araña web.

que los resultados son absolutamente correctos o, en otras palabras, no podemos permitirnos reportar una vulnerabilidad como tal (resultado positivo) sin comprobar que realmente exista.

En la etapa de descubrimiento y enumeración, ZAP fue utilizado para identificar la mayor cantidad de recursos dentro de la aplicación web de forma automatizada. El análisis de vulnerabilidades que se obtuvo a través de esta herramienta facilitó la discriminación de los falsos positivos, así como la identificación anticipada de algunos defectos en la aplicación.

Compañía/Desarrollador: OWASP

Licencia: Open source

Etapa de metodología: Descubrimiento, Análisis de Vulnerabilidades

Sitio Web: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Main

Uso de herramienta:

Al abrir la herramienta, lo primero que observaremos es un cuadro de selección de tres opciones como se muestra en la Figura 22, de las cuales seleccionaremos la primera (que guardará la sesión con un nombre basado en el tiempo y hora actuales) y solamente marcaremos el checkbox al final de las opciones si queremos que la herramienta recuerde y establezca esta elección como predeterminada. Por último, daremos clic sobre el botón *Iniciar* para establecer la configuración deseada.

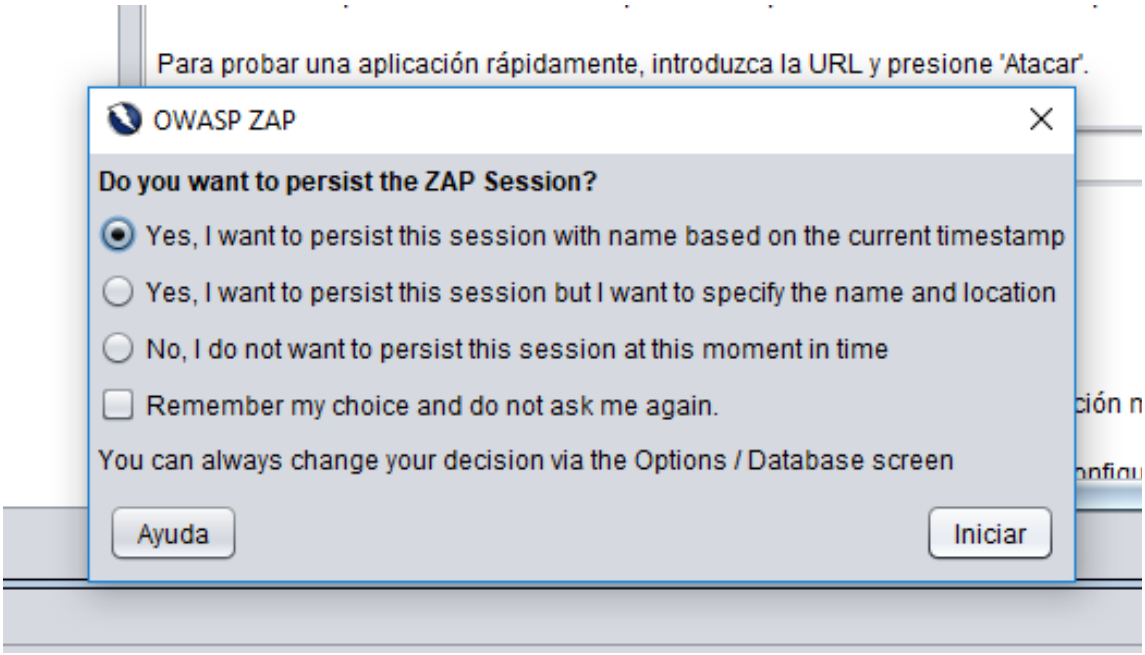

Figura 22.- Ventana de persistencia de sesión

Una vez iniciada la herramienta, escribiremos la URL de la aplicación o sitio que deseamos analizar en el editor de texto ubicado en la pestaña de inicio rápido, en este caso utilizamos como objetivo (con fines ilustrativos) el sitio del Centro Tecnológico Aragón, como se muestra en la Figura 23.

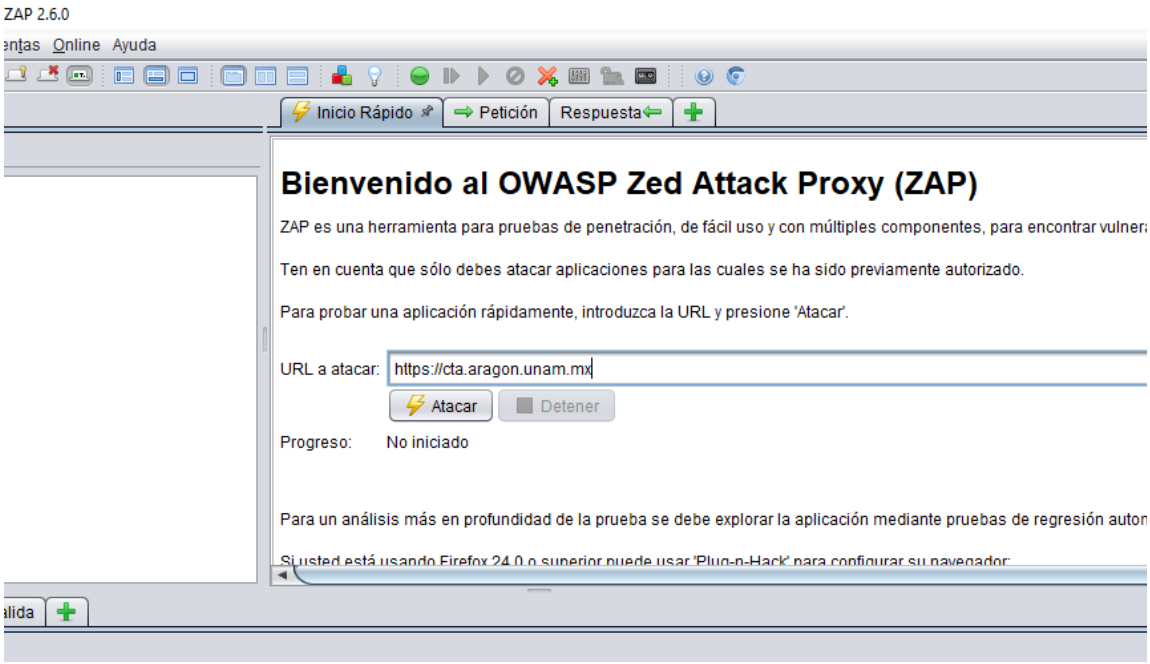

Figura 23.- Pantalla principal de la herramienta

Establecido el objetivo, hacemos clic sobre el botón con la leyenda *Atacar* que además tiene el ícono de un rayo. Esta acción dará inicio al *web spider* y análisis de vulnerabilidades. En la Figura 24, se puede apreciar el inicio de los escaneos.

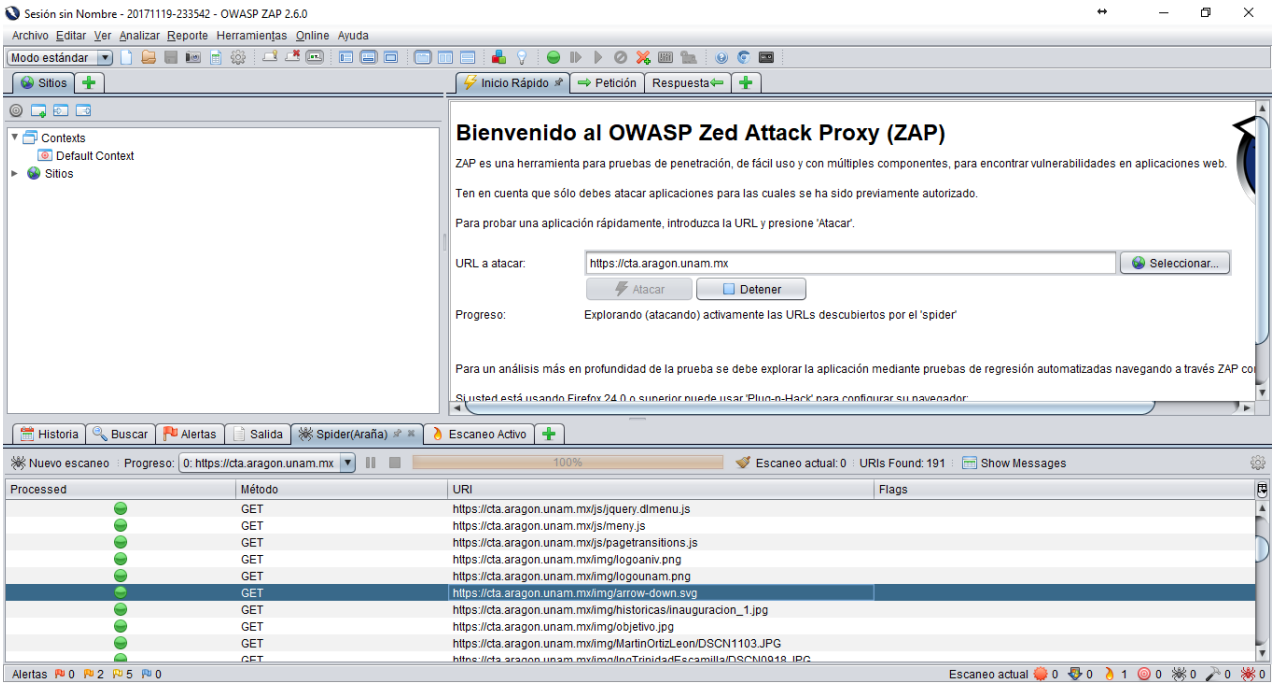

Figura 24.- Inicio de los escaneos, (crawling y vulnerabilidades)

Los escaneos que ZAP realiza por defecto son Crawling (por medio de un spider) y el análisis de vulnerabilidades. Durante el proceso se mostrará una barra de color naranja que mostrará el progreso de cada uno de los escaneos que se realicen. La Figura 25 muestra el análisis de vulnerabilidades en proceso.

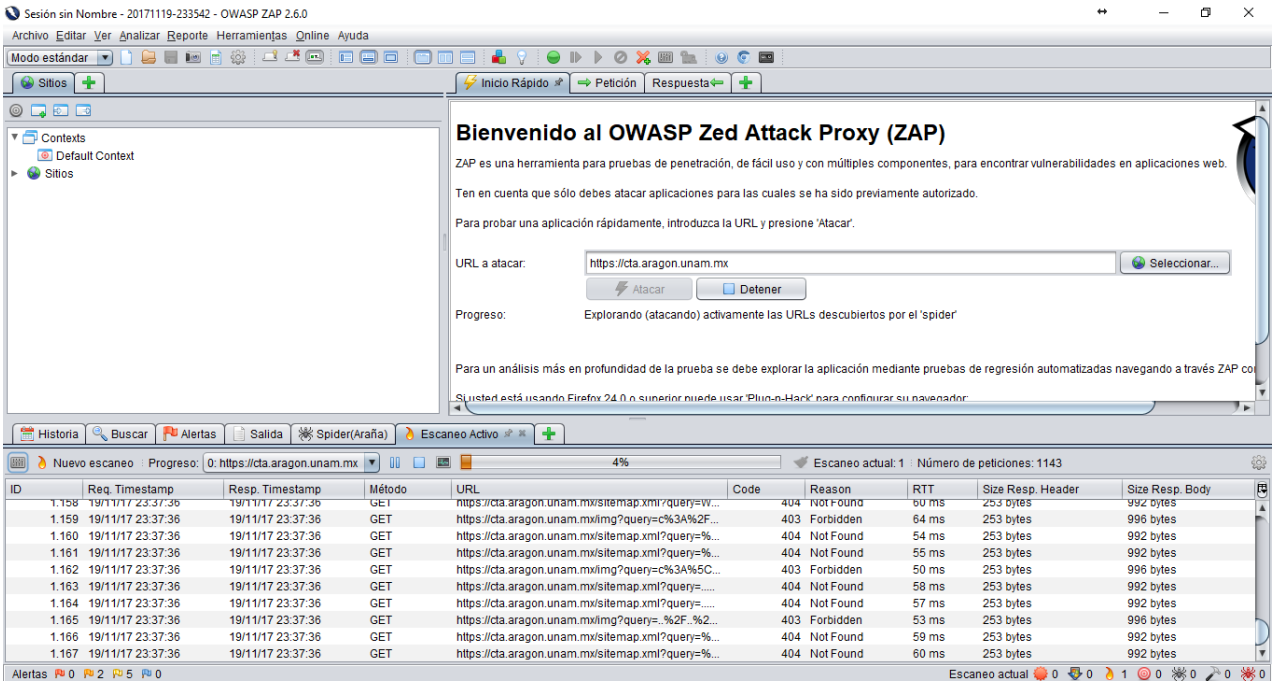

Figura 25.- Análisis de vulnerabilidades en proceso

Una vez que todos los procesos terminen, la barra de color naranja habrá desaparecido y se mostrará un recuadro con las alertas resultantes del análisis de vulnerabilidades tal cual se muestra en la Figura 26.

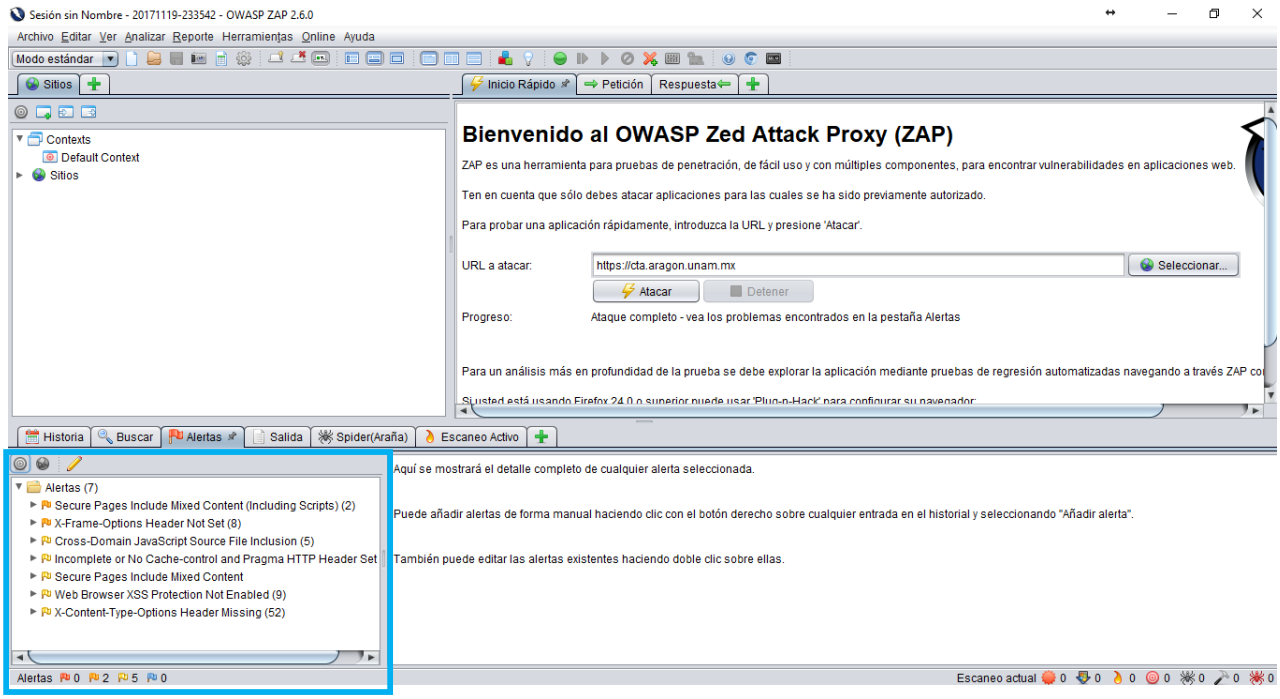

Figura 26.- Escaneos terminados, y alertas de vulnerabilidades encontradas

Para obtener un informe de resultados obtenidos durante el análisis de vulnerabilidades, basta con hacer clic sobre el menú *reporte* y después sobre las opciones generar informe, ya sea HTML o XML, en el caso del ejemplo seleccionamos el formato HTML como muestra la Figura 27.

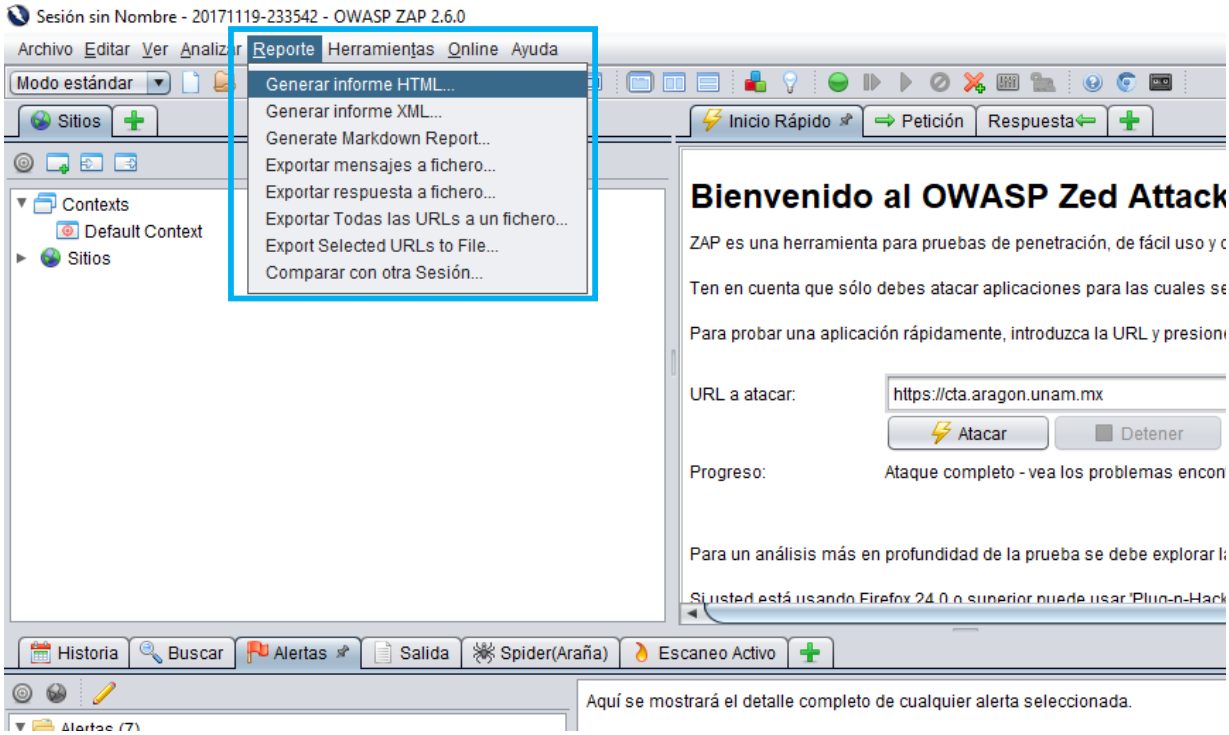

Figura 27.- Generación de informe de resultados del análisis de vulnerabilidades

La acción anterior desplegará una pequeña ventana, en la cual estableceremos el nombre del archivo y la carpeta donde queramos guardar el archivo del informe, Figura 28.

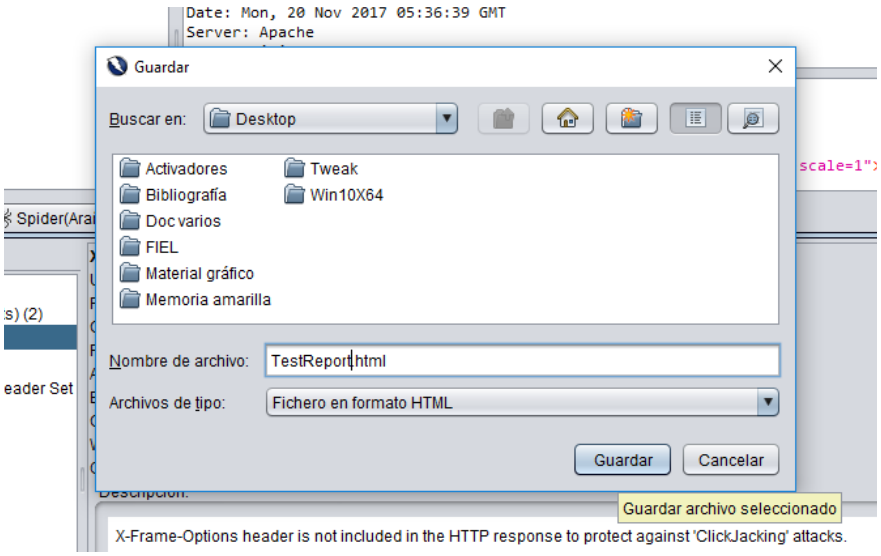

Figura 28.- Guardado de archivo de exportación de análisis de vulnerabilidades

La presentación del informe en formato HTML se muestra en ambas, Figura 29 y Figura 30. En él se desglosa una descripción de la vulnerabilidad, así como la URL de los recursos que la herramienta identificó como sensibles a ese tipo de ataque.

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	5
Informational	0

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://cta.aragon.unam.mx/index.html
Method	GET
Parameter	X-Frame-Options
URL	https://cta.aragon.unam.mx/directorio/
Method	GET
Parameter	X-Frame-Options
URL	https://cta.aragon.unam.mx/historia.html
Method	GET
Parameter	X-Frame-Options
URL	https://cta.aragon.unam.mx/

Figura 29. - Sección de informe del análisis de vulnerabilidades en formato HTML

Medium (Medium)	Secure Pages Include Mixed Content (Including Scripts)
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://cta.aragon.unam.mx/historia.html
Method	GET
Evidence	http://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js
URL	https://cta.aragon.unam.mx/coordinacion.html
Method	GET
Evidence	http://cdn.onnoschwanen.com/images/ui/arrow-down.svg
Instances	2
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Other information	tag=script src=http://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js
Reference	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
CWE Id	311
WASC Id	4
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://cta.aragon.unam.mx/
Method	GET
Parameter	X-XSS-Protection

Figura 30. - Sección de informe de análisis de vulnerabilidades en formato HTML

Por último, si se desea contar con el listado de las URL que se consultaron, debemos hacer clic sobre el menú *reporte* y después en la opción *Exportar todas las URL a un fichero* para obtenerlo, Figura 31.

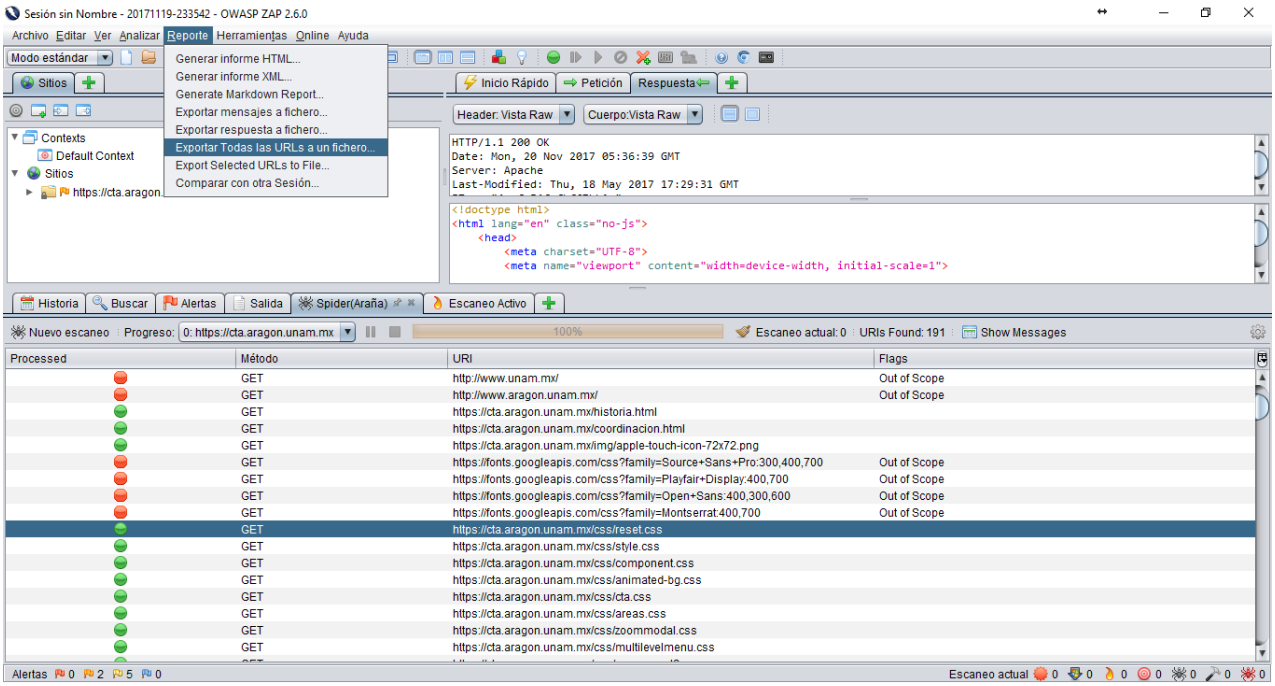

Figura 31.- Exportación de las URL encontradas durante el proceso de crawling

Nessus

Nessus es un analizador de vulnerabilidades automatizado, el cual permite detectar los puntos deficientes de un sistema o red. La constante actualización (semanal) de los plugins que utiliza para los análisis, es sin duda, lo que mantiene esta herramienta entre las mejores para este tipo de tareas. Sumado a lo anterior, la generación de reportes de forma automatizada es una de las características que hace de Nessus una herramienta completa y eficiente.

Compañía/Desarrollador: Tenable

Licencia: Software propietario

Etapa de metodología: Análisis de vulnerabilidades y Generación de Reportes

Sitio Web: https://es-la.tenable.com/products/nessus-vulnerability-scanner

Uso de herramienta:

Una vez que instalamos Nessus en el sistema operativo deseado (MacOs en este caso), es necesario abrir un navegador e intentar acceder a localhost a través del puerto 8834; será necesario utilizar el protocolo HTTP sobre TLS, Figura 32.

Figura 32.- Acceso al servidor local por el puerto 8834 mediante protocolo HTTPS

Una vez hecho lo anterior, aparecerá un aviso de conexión no segura debido a la ausencia del certificado, por lo que será necesario dar clic sobre el enlace con la leyenda *AVANZADA* (Figura 33) que desplegará la opción de *continuar a localhost (no seguro)*, Figura 34, sobre la que daremos clic.

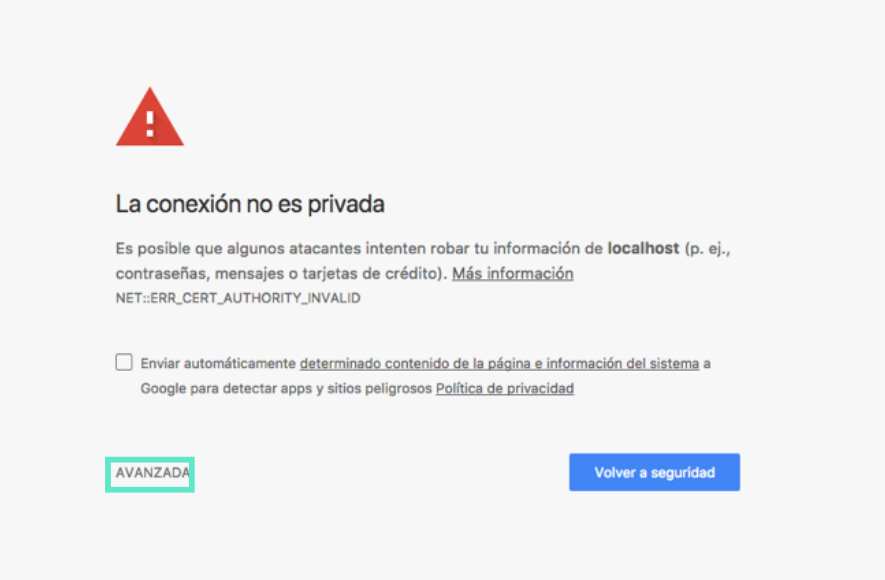

Figura 33.- Aviso de conexión no privada, debido a la ausencia de certificado confiable

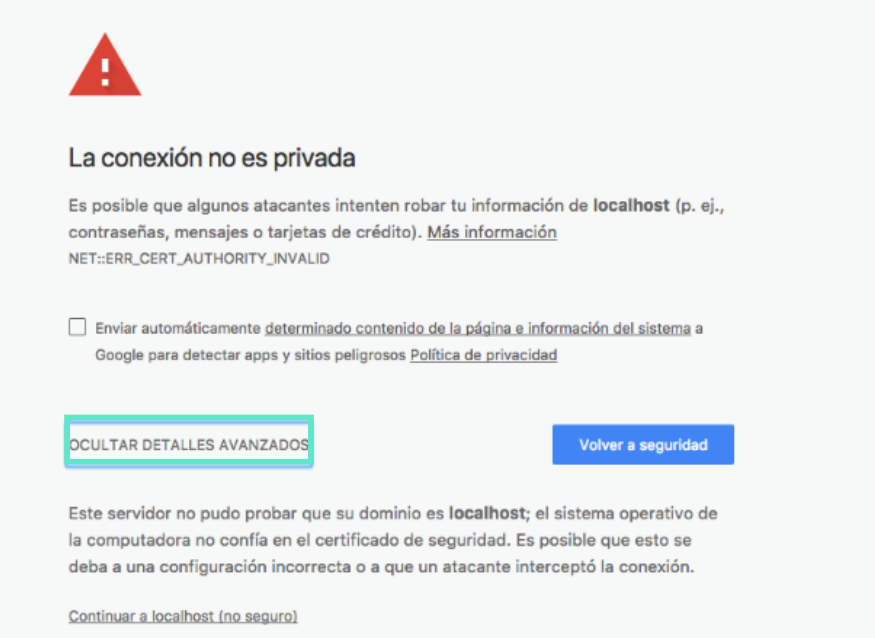

Figura 34.- Opciones avanzadas para continuar la conexión al servidor local

Una vez que hayamos hecho clic en el enlace para continuar al sitio, se mostrará la pantalla de creación de configuración inicial para la herramienta, donde haremos clic sobre el botón *Continue* como lo muestra la Figura 35.

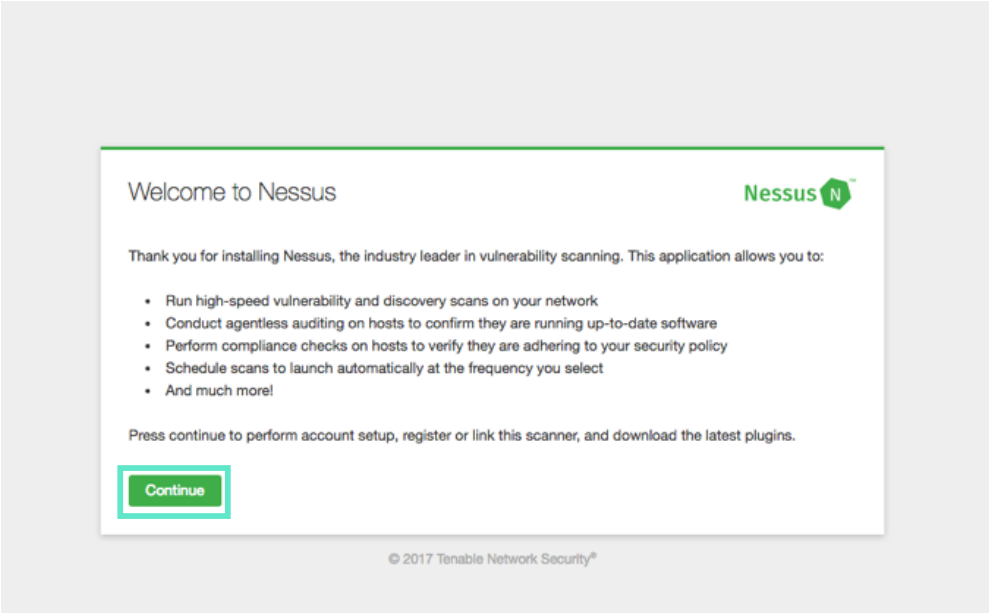

Figura 35.- Página de configuración inicial para Nessus

La herramienta mostrará una pantalla de creación de credenciales para un usuario como la Figura 36 muestra. Una vez introducidos el usuario y contraseña haremos clic sobre el botón *Continue*.

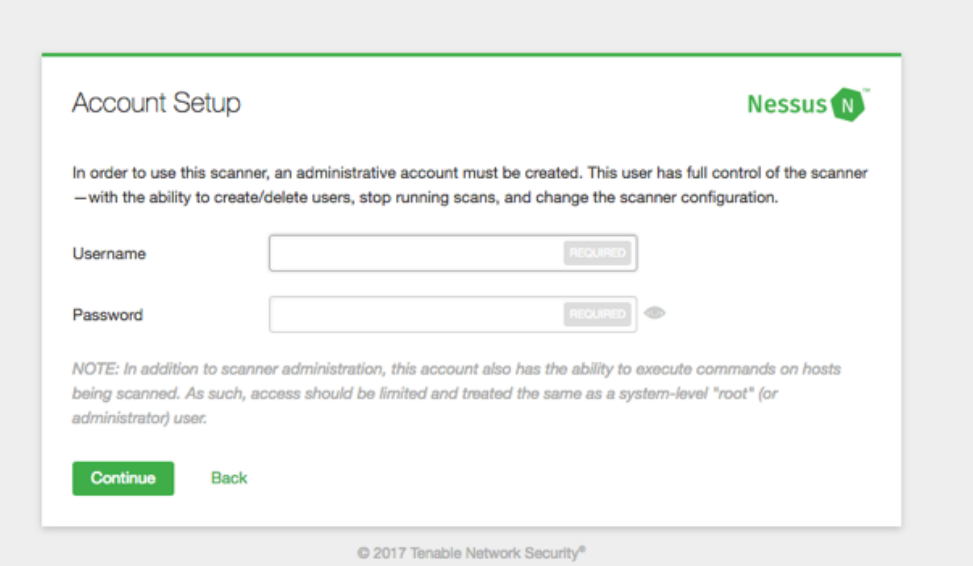

Figura 36.- Creación de credenciales para acceder al servidor local

En este punto será necesario tener cerca el código de activación que recibimos por parte de Tenable, pues lo introduciremos en la pantalla de activación del producto, Figura 37. Hacemos clic en el botón *Continue* para terminar la configuración de Nessus.

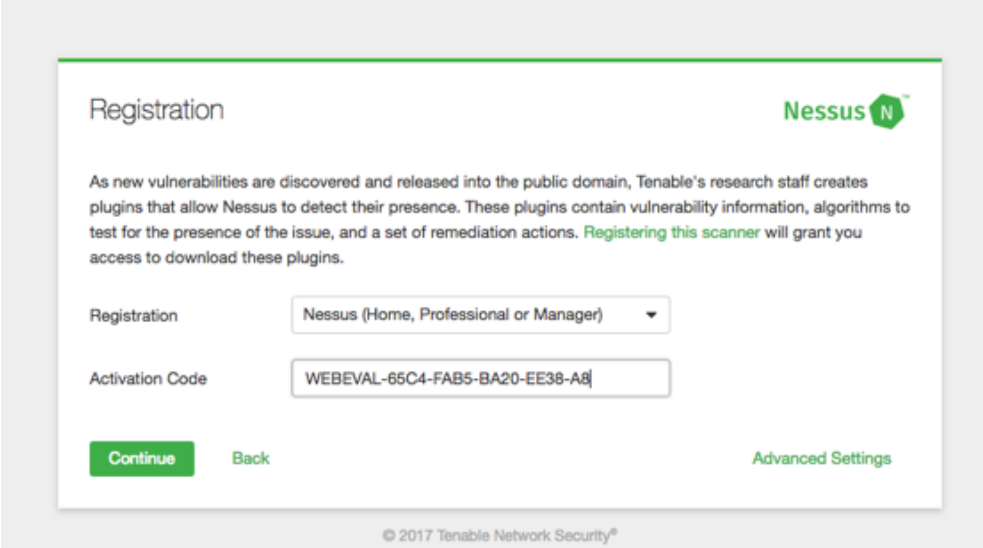

Figura 37.- Activación del producto por medio de llave

Una vez activado el producto, aparecerá un recuadro de inicio de sesión como se muestra en la Figura 38 donde ingresaremos el usuario y contraseña que establecimos durante la configuración de la herramienta.

Figura 38.- Pantalla de inicio de sesión de la herramienta

Una vez iniciada nuestra sesión, se nos mostrará la pantalla principal del sistema, en ella podremos reconocer un menú lateral donde se incluyen categorías como *My Scans* y *Policies*. Estas categorías nos permitirán crear, modificar o eliminar escaneos y políticas para utilizarlas después, Figura 39.

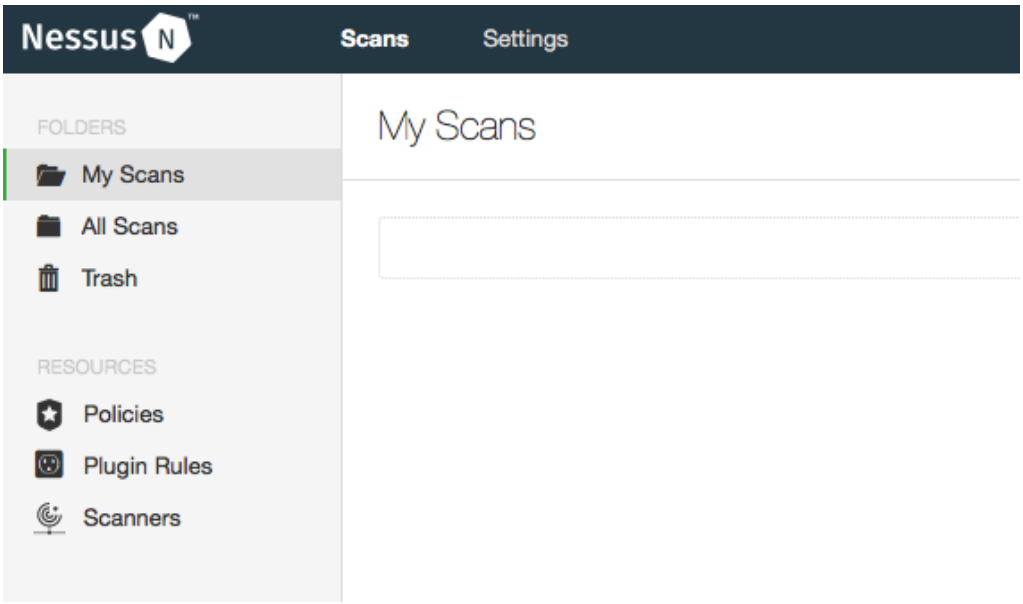

Figura 39.- Apartado para creación, selección y edición de escaneos

Procederemos a hacer clic sobre la categoría de políticas para desplegar la pantalla de creación y edición de políticas como se aprecia en la Figura 40.

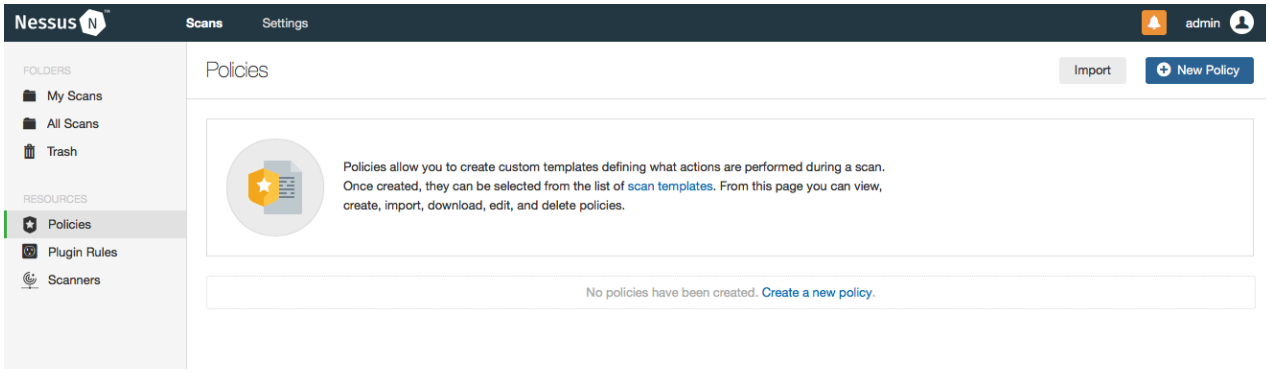

Figura 40.- Apartado para creación, selección y edición de políticas de escaneo

Una vez en la pantalla de creación de políticas, haremos clic sobre el botón ubicado en la esquina superior derecha para desplegar las opciones disponibles.

Para este ejemplo, utilizaremos una plantilla de escaneo avanzado, señalada en la Figura 41. Una vez ubicada la plantilla, procederemos a hacer clic sobre ella, lo que desplegará un formulario que deberemos llenar de acuerdo con las necesidades.

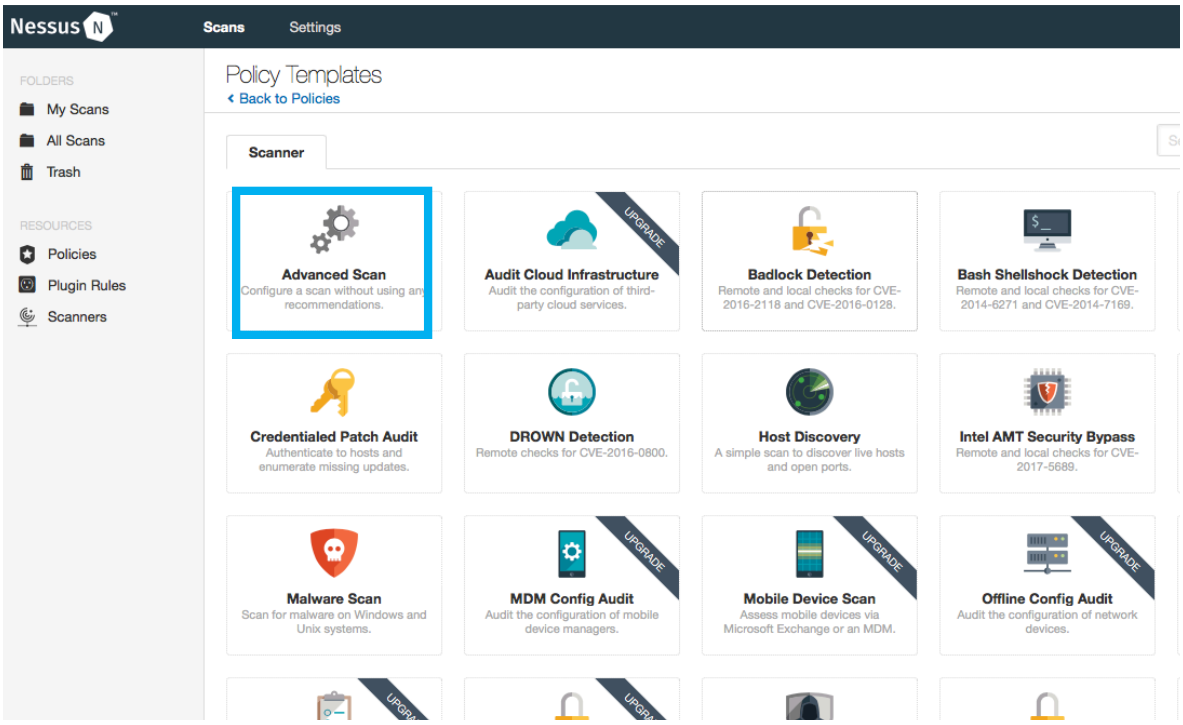

Figura 41.- Plantillas de políticas de escaneo

En el formulario podremos apreciar cuatro pestañas de configuración para la política, Settings, Credentials, Compilance y Plugins.

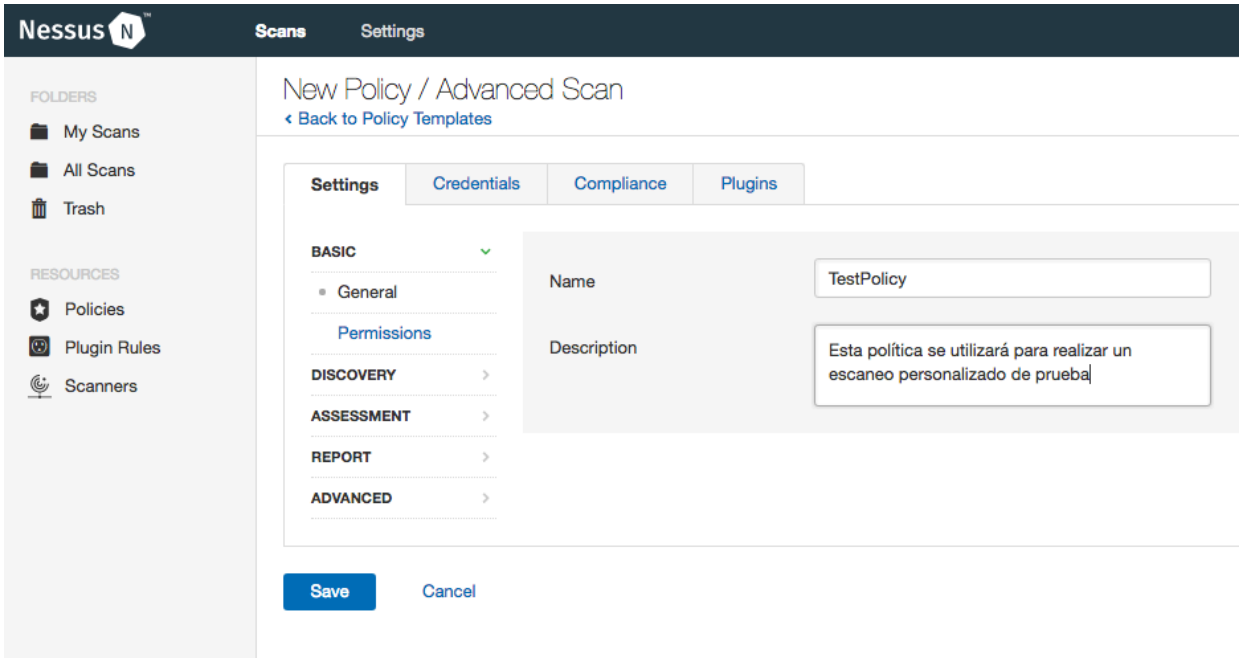

Figura 42.- Creación de una nueva política totalmente personalizada

Posicionados en la pestaña settings en el apartado basic -> general, asignaremos un nombre para la política y una descripción que nos permita identificarla y diferenciarla rápidamente de otras. Figura 42.

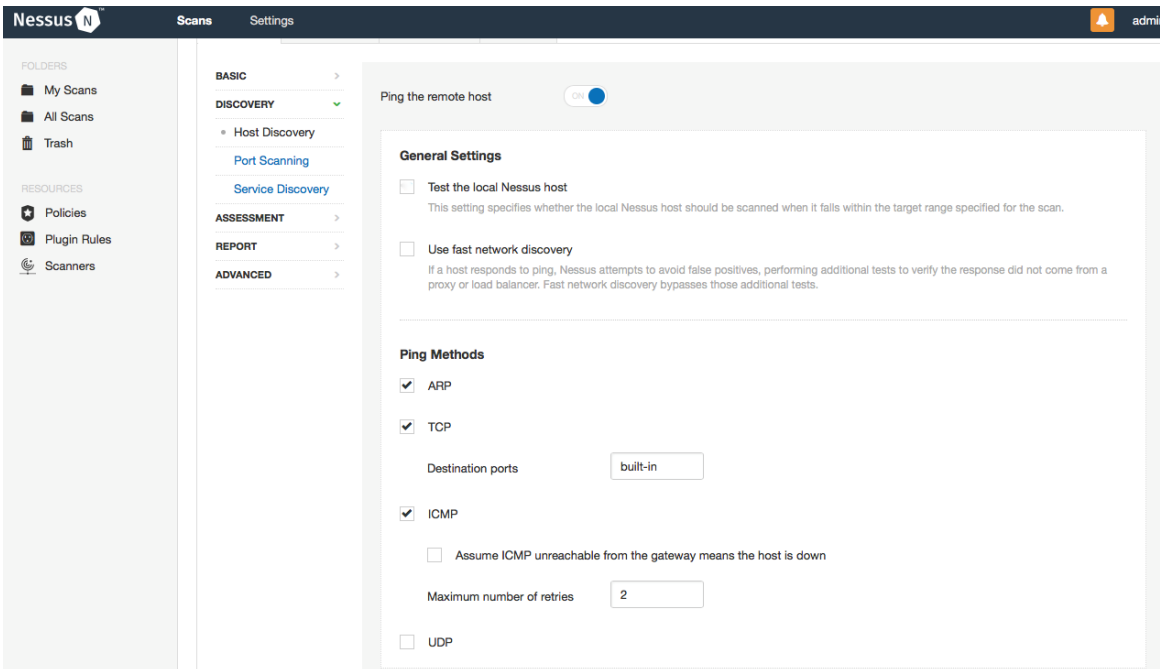

Figura 43. - Apartado de descubrimiento de equipos

Una vez asignados nombre y descripción, entraremos a la sección *discovery->host discovery* como se muestra en la Figura 43, donde verificaremos que la opción *Test the local Nessus host* se encuentre desmarcada y además todos los métodos de ping estén marcados, excepto UDP, esto con el fin de acelerar el proceso de análisis de vulnerabilidades.

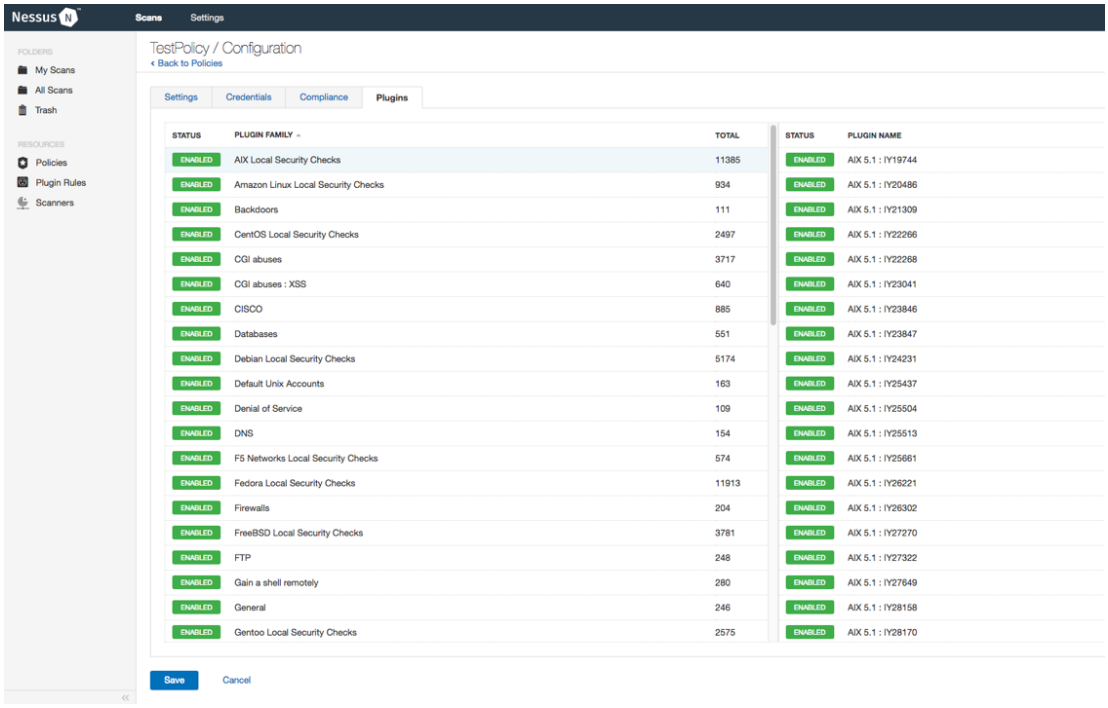

Figura 44.- Plugins seleccionados

Posteriormente pasaremos a la pestaña *Plugins*, para verificar que todos los plugins se encuentren activos. Bien podríamos seleccionar solo los más útiles de acuerdo con el perfil de los dispositivos objetivo, sin embargo, para este ejemplo seleccionaremos todos ellos para lograr percibir la mayor cantidad de problemas posibles, Figura 44. Una vez hecho lo anterior, haremos clic en el botón *Save* para guardar la política.

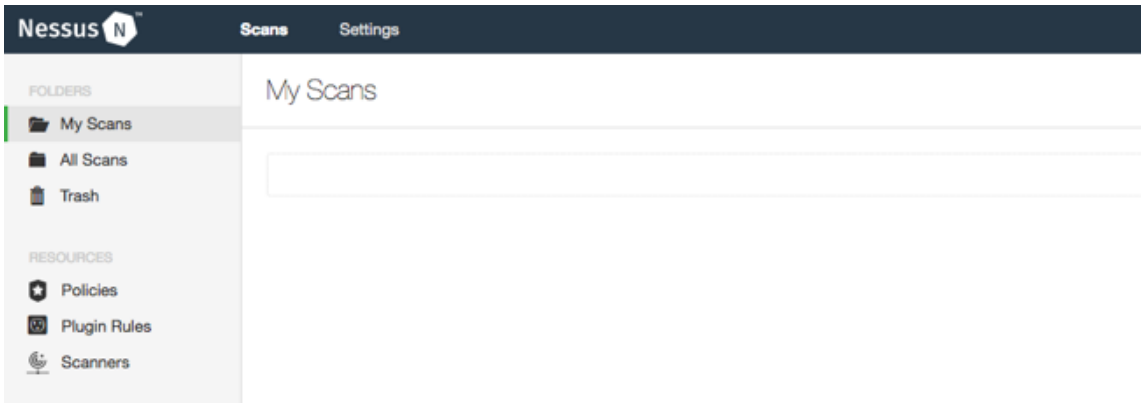

Figura 45.- Sección de escaneos

Para continuar, haremos clic sobre la sección *My Scans*, ubicada en el menú lateral principal. Esto desplegará una pantalla con los escaneos disponibles para ser ejecutados, Figura 45. Ahí podremos observar la política que antes guardamos con el nombre *TestPolicy*, Figura 46, misma que seleccionaremos para configurar el escaneo.

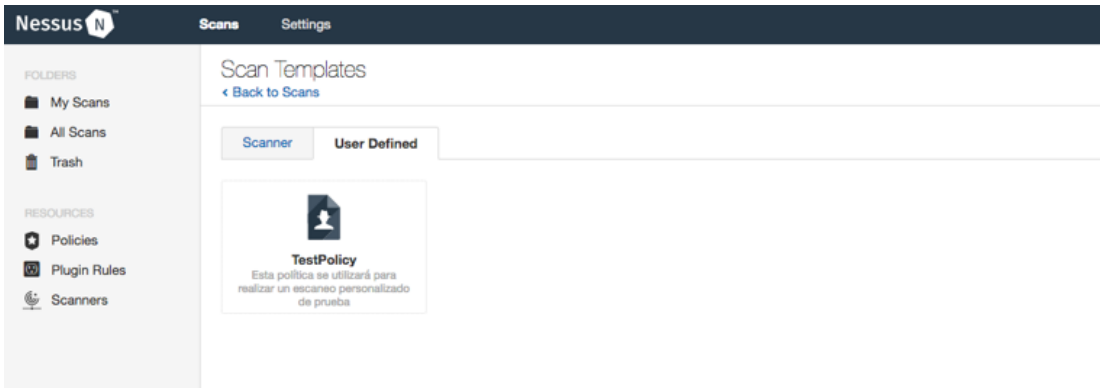

Figura 46.- Selección de política personalizada creada previamente

Una vez que hayamos seleccionado la política, una pantalla de configuración del escaneo se desplegará tal cual se muestra en la Figura 47. Ahí asignaremos un nombre, descripción, ubicación de almacenamiento, la política (seleccionaremos la política previamente creada *TestPolicy*) y las IP objetivo.

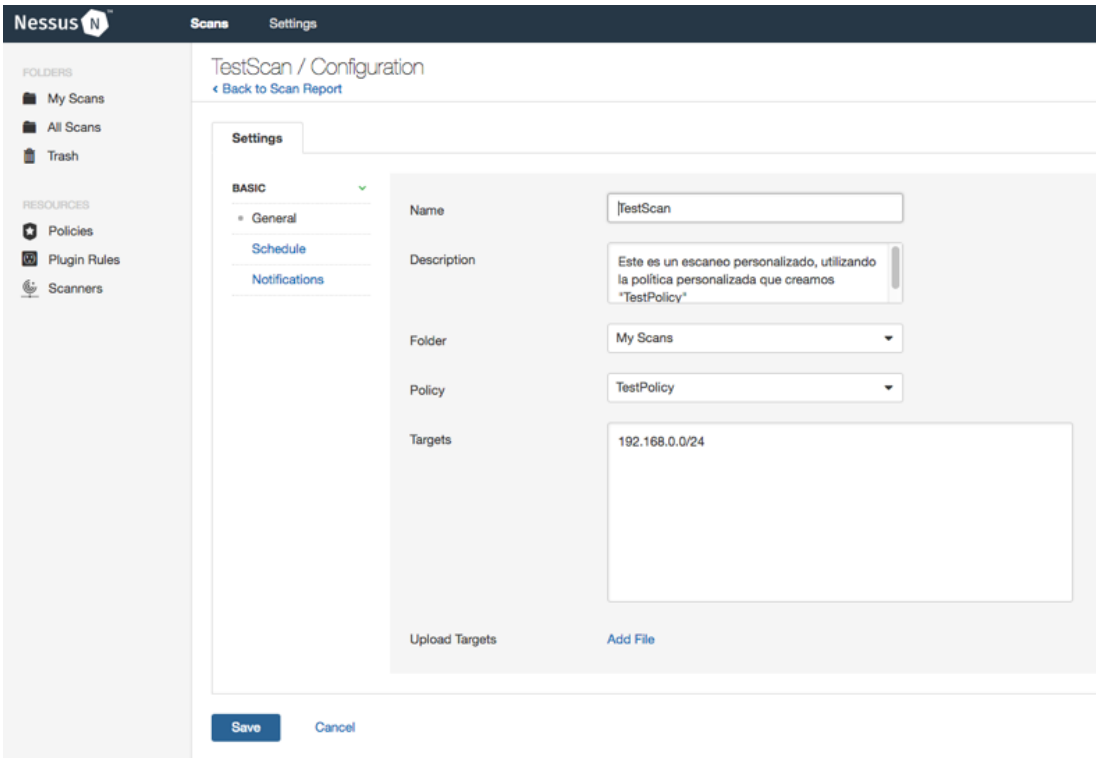

Figura 47.- Pantalla de configuración del escaneo (Nombre, Política, Objetivos, etc.)

Una vez configurado el escaneo, haremos clic sobre el botón *Save* de color azul para guardar los cambios hechos en la configuración del mismo. Ya guardado el escaneo, se nos mostrará una lista con los escaneos disponibles. En este ejemplo solo se puede ver un elemento en dicha lista, pues es el único configurado.

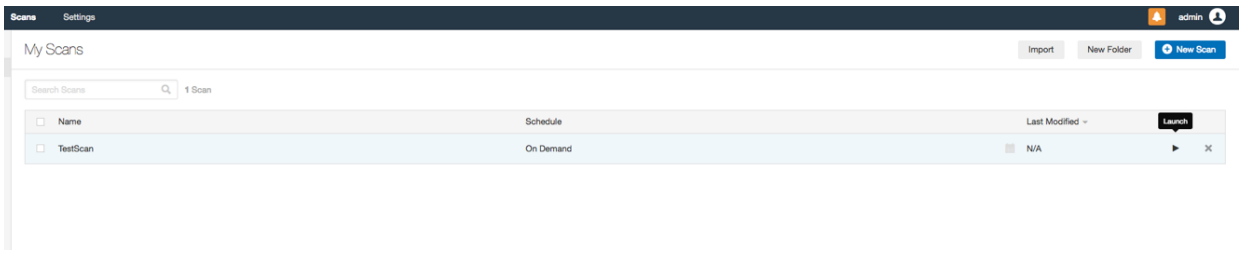

Figura 48.- Ejecución de escaneo previamente configurado

El siguiente paso será hacer clic sobre el botón con el símbolo *Play* ubicado en el extremo derecho del escaneo como se muestra en la Figura 48; esto dará inicio al análisis de vulnerabilidades.

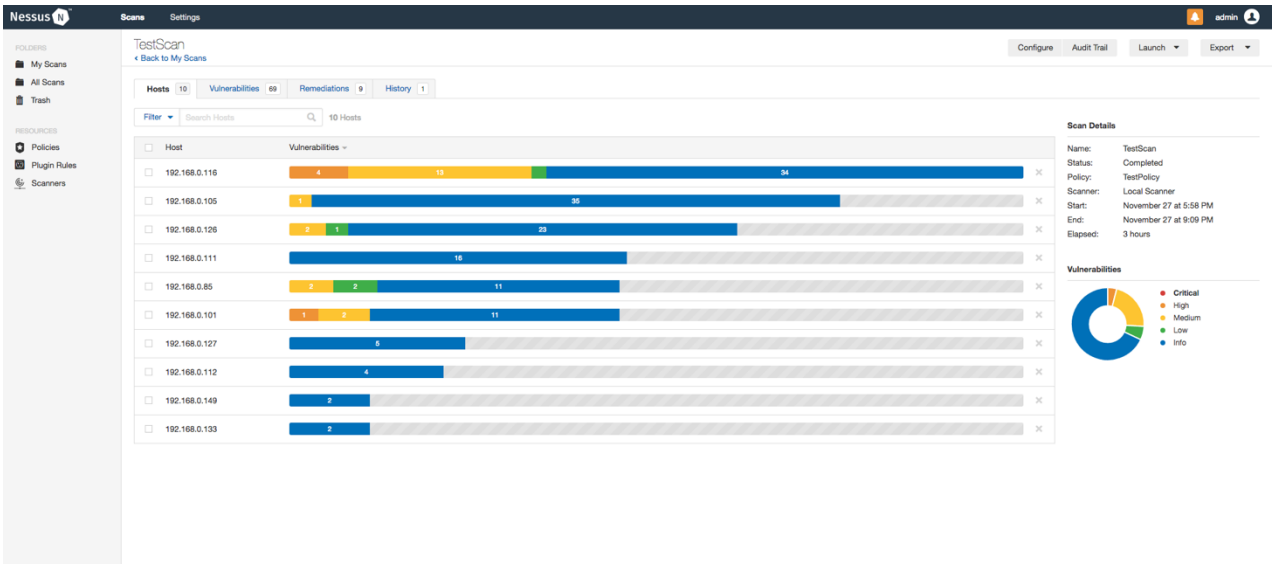

Figura 49.- Resultados mostrados por cada dispositivo encontrado

Cuando hayan transcurrido algunos minutos, podremos observar un listado de las IP analizadas, además de una gráfica por cada dispositivo en proceso de análisis, que muestra las vulnerabilidades encontradas y su criticidad, Figura 49.

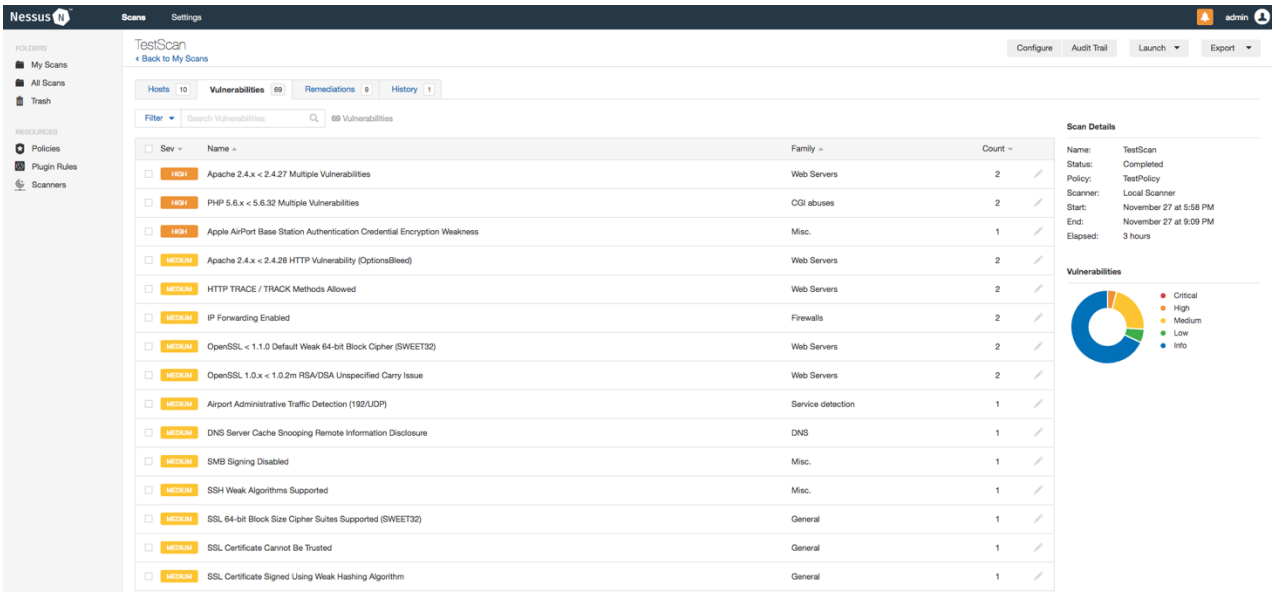

Figura 50.- Vulnerabilidades encontradas en todos los dispositivos, ordenadas por criticidad

Los hallazgos pueden consultarse incluso en tiempo de ejecución del análisis, sin embargo, solo hasta haber concluido el proceso del mismo se obtendrá la totalidad de resultados. En la Figura 50 se puede apreciar las vulnerabilidades encontradas para uno de los dispositivos, ordenadas por grado de criticidad, y junto a ellas una breve descripción.

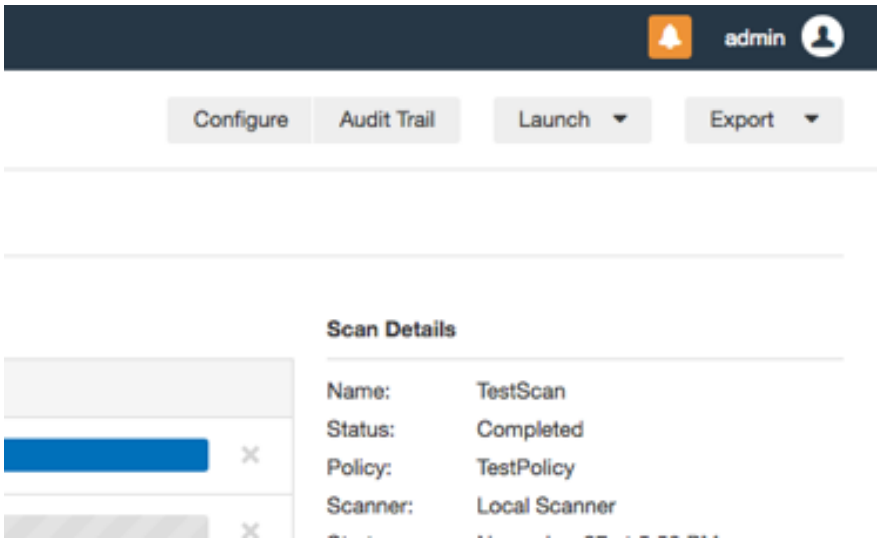

Figura 51.- Generación del reporte

De ser necesario, Nessus ofrece la opción de generar un reporte detallado, incluyendo gráficas e incluso recomendaciones para remediación de las vulnerabilidades. Basta con hacer clic sobre el combo box con la leyenda *Export*, para seleccionar después el formato deseado para exportar el reporte. Figura 51.

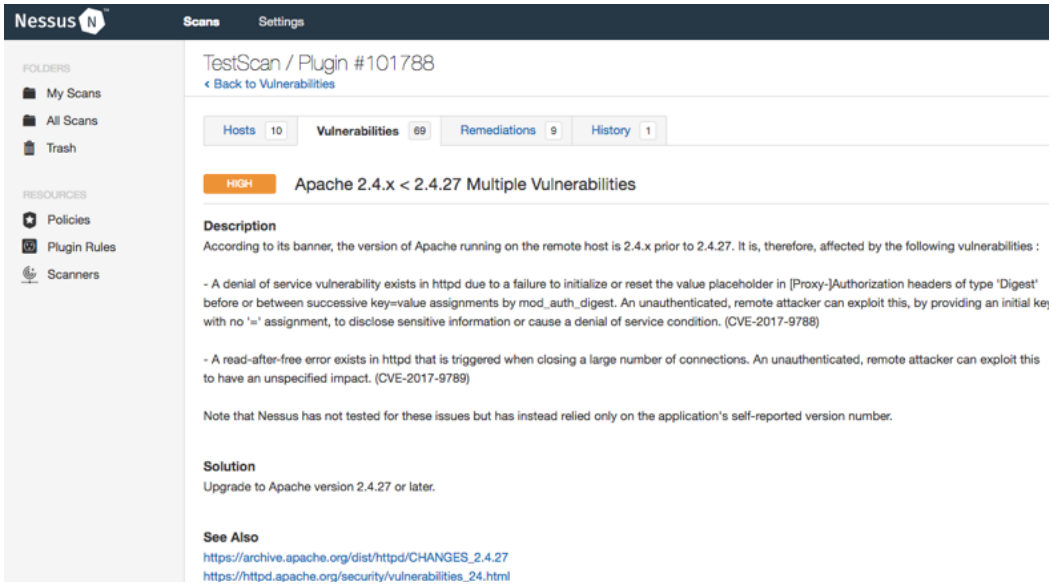

Figura 52.- Detalle de una de las vulnerabilidades encontradas

Al hacer clic sobre alguna de las vulnerabilidades encontradas será posible acceder a información detallada de la misma. La Figura 52 muestra el detalle de una de las vulnerabilidades encontradas en uno de los dispositivos analizados.

Wireshark

Esta herramienta es uno de los analizadores de protocolos de red más utilizados, comúnmente empleado para monitoreo y análisis del tránsito de paquetes en una red. Creado por Gerald Combs en 1998, Wireshark permite una buena administración de cualquier red a través de las múltiples opciones que ofrece para el monitoreo y análisis. Esta herramienta hace uso de las interfaces disponibles en el equipo anfitrión para capturar el tráfico de la red a la cual el dispositivo se encuentra conectado. Mediante la captura de los paquetes que viajan a través de esta red, permite al usuario realizar un monitoreo y análisis de tráfico de red.

Compañía/Desarrollador: Gerald Combs

Licencia: Open source

Etapa de metodología: Análisis de vulnerabilidades

Sitio Web: https://www.wireshark.org/

Uso de herramienta:

Antes de iniciar la herramienta, se ejecuta el comando *ifconfig* para conocer la configuración de red que tiene establecida el dispositivo desde el cual realizaremos el monitoreo. Esto tiene como finalidad conocer el segmento de red al cual estamos conectados, así como la IP asignada a nuestro dispositivo, que a su vez, nos permitirá identificar los paquetes que sean enviados por o destinados a nuestro dispositivo.

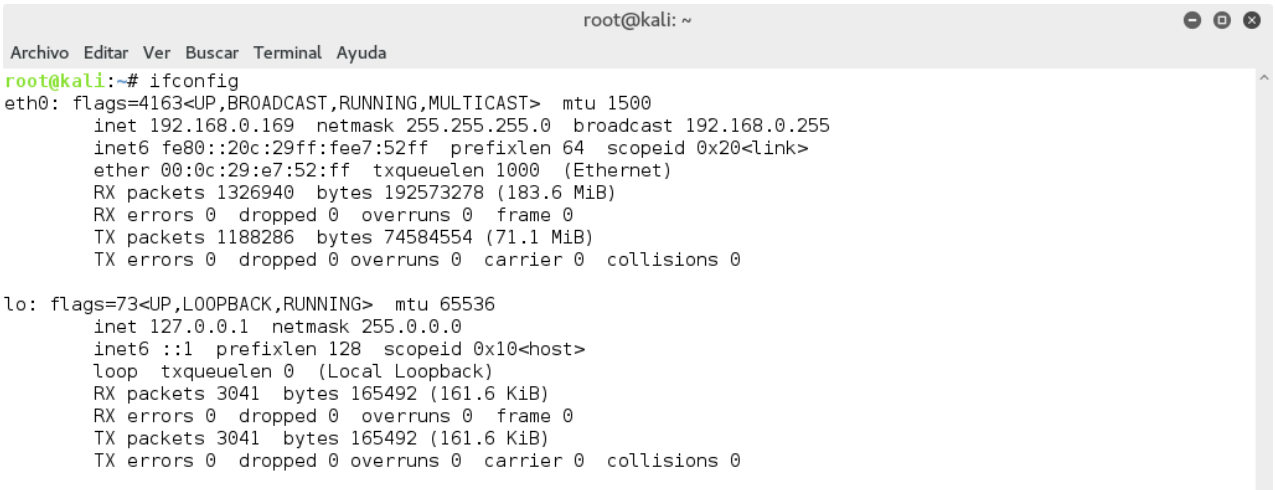

Figura 53.- Configuración de red del equipo atacante

La Figura 53 muestra la salida del comando ifconfig, donde se puede apreciar la configuración de red del dispositivo atacante.

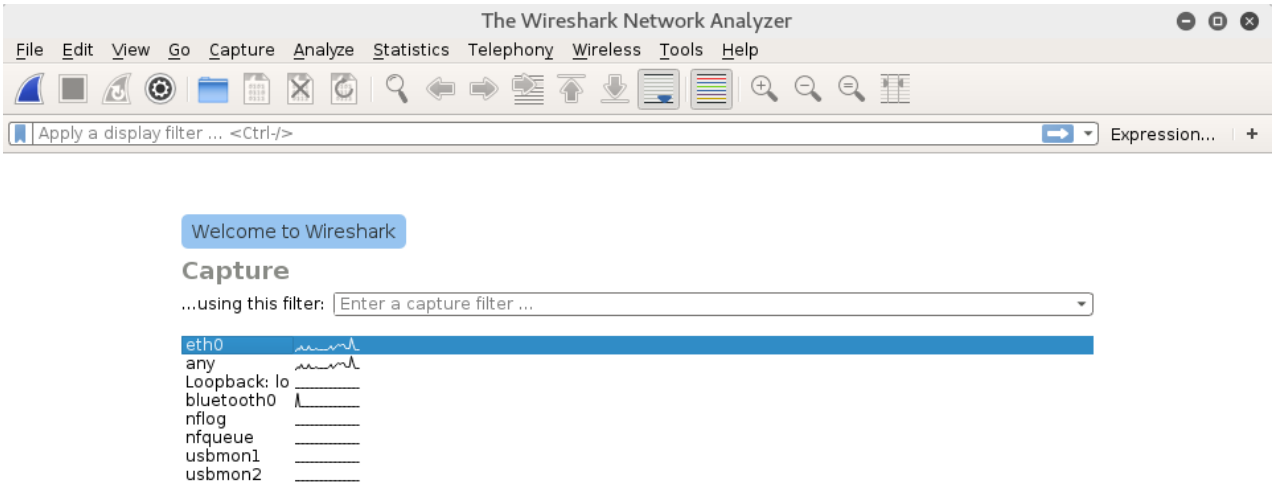

Figura 54.- Selección de interfaz a monitorear

Una vez que conozcamos la configuración de red, procedemos a abrir Wireshark. La pantalla de inicio muestra un listado de las interfaces disponibles y con una pequeña gráfica, la actividad en tiempo real de cada una de ellas tal cual lo muestra la Figura 54.

Hacemos clic sobre la interfaz *eth0* para iniciar el monitoreo de la red a través de esta interfaz. El tráfico de la red comenzará a ser capturado por la herramienta, por lo que el espacio de almacenamiento en el dispositivo que la ejecute se verá reducido proporcionalmente al tiempo que se capturen los diferentes paquetes que viajan sobre la red.

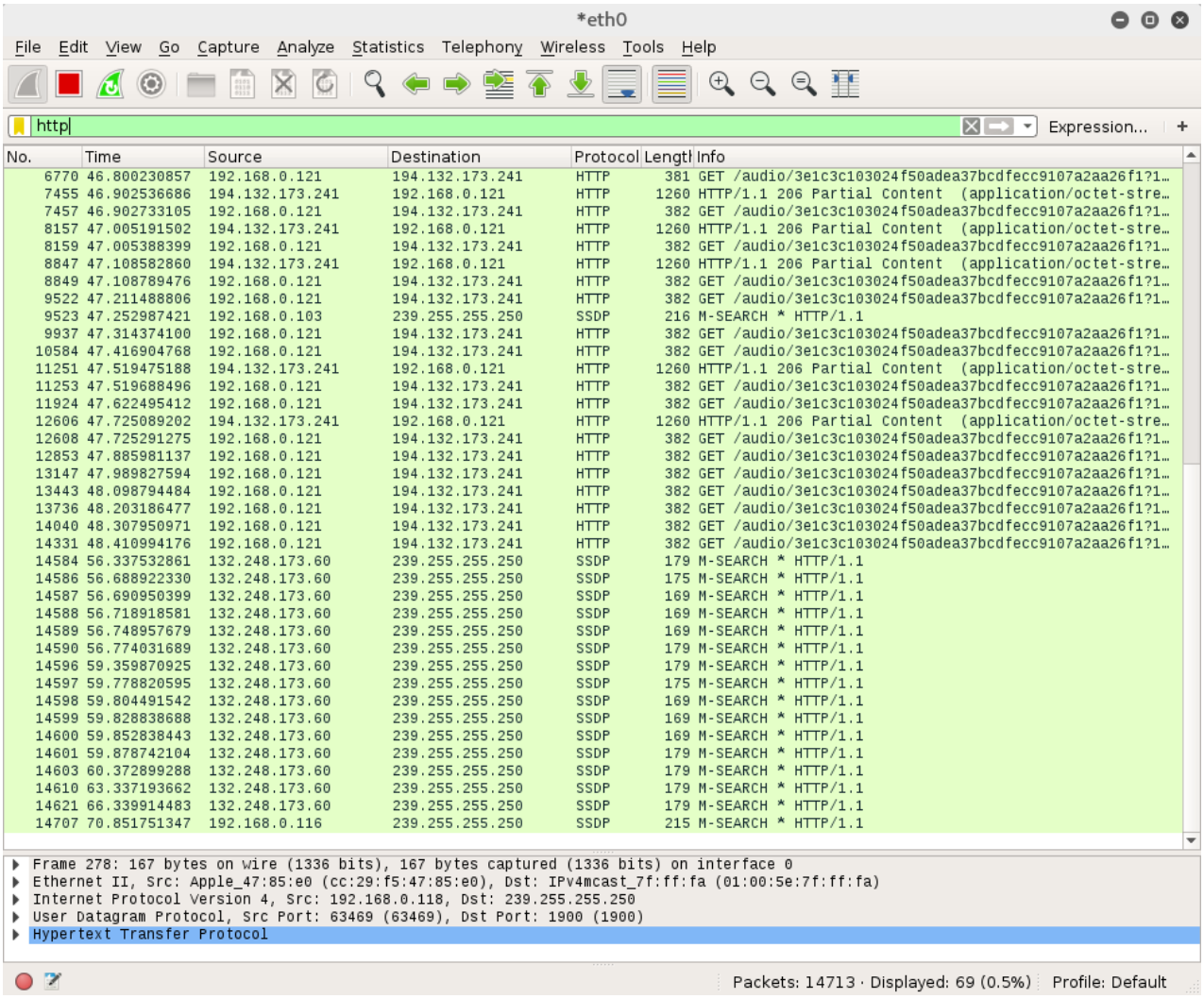

Figura 55.- Filtrado de peticiones por protocolo HTTP

Para facilitar la búsqueda de algún paquete en específico es posible realizar un filtrado de los paquetes que son capturados, ya sea por IP origen o destino, dns, o bien protocolo, como es el caso de la Figura 55, que permite ver el filtrado de todo el tráfico que viaja sobre HTTP.

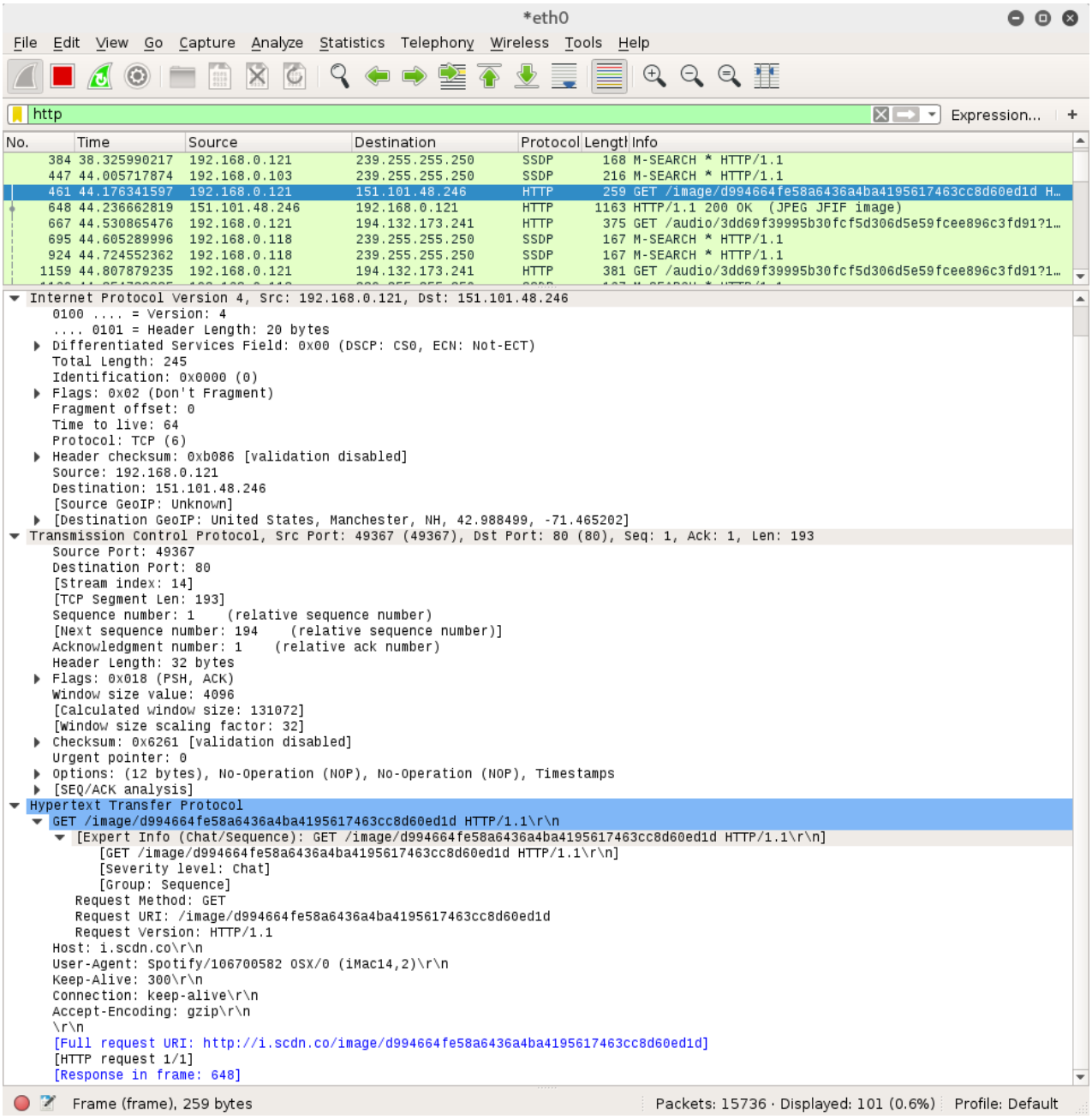

Figura 56.- Detalle de una de las peticiones HTTP

Al abrir el detalle de uno de los paquetes capturados, podemos identificar su estructura y contenido. Por ejemplo, el paquete seleccionado en la Figura 56, es una petición GET en la que se solicita un recurso gráfico.

V Conclusiones

Las instituciones en general, publicas y privadas, tienen huecos importantes de seguridad, no todas lo saben y aún peor, así operan. En el mundo moderno, ya no es aceptable la idea de una organización que no considere a la seguridad informática como un aspecto imprescindible, es más, si lo que buscan es crecer dentro del mercado y convertirse en un prestador de servicios competente, sin duda alguna deberían adoptar como prácticas básicas, el correcto manejo de información y aseguramiento de la misma en cada uno de las estructuras y procedimientos que se relacionen directa e indirectamente con la organización misma.

Es cierto que las organizaciones pueden llegar funcionar sin concebir a la seguridad como un proceso indispensable, existen múltiples empresas que hasta la fecha no tienen una conciencia de seguridad, pese a ello, radican sin ningún problema, pero ¿por cuánto tiempo? Basta con que ocurra un incidente que provoque una pérdida considerable de recursos para darle un giro total a toda idea que se tenía sobre seguridad dentro de esas organizaciones y con esto llevarlas hasta una precaria situación.

El problema se agrava cuando aumenta la cantidad y criticidad de la información que maneja, así como el valor de sus activos. Ya que los procedimientos y actividades nunca fueron planificados con una metodología de seguridad, (quizá por ahorrar costos) será necesario un replanteamiento, primero, de los procesos críticos de la organización, continuando con aquellos que sean secundarios, pero no por eso menos importantes; toda esta renovación acarreará gastos igual o más fuertes que los que anteriormente se pretendían evitar, lo cual, en lo personal me hace concluir que valen más un buen análisis y planteamiento oportunos y consientes de la seguridad de los activos.

La seguridad implica costos, en ocasiones bastante altos, pues entre mayor nivel de seguridad se pretenda alcanzar, mayor tendrá que ser la inversión que se realice. Esta es una de las razones por las cuales pequeñas y medianas organizaciones prefieren continuar ejerciendo evitando el gasto que genera el correcto aseguramiento de los activos, ya sean propios o de terceros. Si nos situamos en el plano de las instituciones electorales, podremos notar que, a pesar de las deficiencias en materia de seguridad de la información, estas continúan en constante actualización y capacitación para cubrir de la forma más adecuada posible las áreas de oportunidad.

Sin hacer a un lado a las instituciones, pero adentrándonos más en cuestiones computacionales, podemos afirmar que como parte de la naturaleza cambiante del software, los errores son intrínsecos al mismo, algo que difícilmente podremos cambiar y deja disponible un abanico de posibilidades a los atacantes

para encontrar alguna vulnerabilidad y explotarla, sin embargo, lo anterior no significa que debamos abandonar la contienda porque aparentemente el problema no tiene solución, todo lo contrario, debe representar un incentivo a trabajar constantemente para evitar que los ataques de usuarios mal intencionados puedan tener éxito.

Ahora bien, si la diferencia entre un sistema informático cualquiera y los sistemas electorales radica tanto en los activos que maneja, como el ámbito en el que se utiliza, en este caso, las elecciones, comprenderemos que no es lo mismo comprobar el funcionamiento de un sistema que automatiza una operación que puede ser de carácter privado, a evaluar un sistema que podría ser consultado por un país completo, donde no puede existir duda alguna sobre la veracidad de los resultados que entrega, pues estos se publicarán, primero, a nivel local, pudiendo alcanzar consultas como ya habíamos dicho, a nivel nacional.

Para identificar las posibles áreas de oportunidad dentro del software que es auditado, como es el caso del software electoral, las herramientas que automatizan pruebas son bastante útiles y aunque no deberían representar la única opción dentro del repertorio de un auditor, los resultados que entregan pueden hacer mucho más eficaz el trabajo de identificar vulnerabilidades. La constante actualización en cuanto a al manejo y funcionamiento de dichas herramientas es esencial para mantener siempre un alto nivel de productividad en las pruebas realizadas con las mismas.

A lo largo de los periodos en los que se hacía uso de las herramientas para realizar pruebas de seguridad, se detectó un mayor porcentaje de productividad en comparación con aquellos donde las pruebas eran ejecutadas manualmente, sin embargo, se detectaban falsos positivos en los resultados arrojados por algunas de las herramientas utilizadas, es decir, al intentar comprobar manualmente que los hallazgos permitían explotar vulnerabilidades, descubríamos que en realidad estos no lo hacían. Debían clasificarse como hallazgos informativos.

Con lo anterior nos situamos frente a una realidad sobre las herramientas utilizadas en automatización de pruebas. Estas pueden resultar de mucha ayuda y utilidad, siempre y cuando, se tengan las pertinentes consideraciones respecto a los hallazgos que estas puedan arrojar.

Ahora bien, como conclusión al objetivo principal de este trabajo, me concierne que es posible vincular a los alumnos con proyectos que tienen un alcance mayor del que un aula permite, siempre y cuando, se les proporcionen las herramientas adecuadas capacitándolos en áreas específicas, guiándolos y haciendo uso

de los conocimientos que obtienen a lo largo del curso de sus estudios en la facultad, pero, sobre todo, cuando el alumno muestre interés en involucrarse con las áreas relacionadas a los proyectos de auditoría.

Para lograr esto, es necesario concientizar a los alumnos acerca de cómo debería desenvolverse un profesional en el mundo laboral, las capacidades que necesita, así como que conocimientos son indispensables para desempeñar sus funciones aprovechando al máximo su potencial. Hacerlos participes de las actividades que se realicen en conjunto de las organizaciones que requieran de los servicios del Laboratorio de Cómputo, les mostrará el panorama de responsabilidades y obligaciones que un profesional adquiere al involucrarse con el mundo laboral formal.

A través de este trabajo se pretendió disminuir la curva de aprendizaje de los alumnos que deseen formar parte del equipo dedicado a la seguridad informática en los proyectos de auditoría dentro del Laboratorio de Cómputo. De esta forma, los alumnos, actualizarán sus conocimientos al mismo tiempo que refuerzan y aplican los adquiridos previamente. Como parte del proyecto de vinculación entre la Facultad de Estudios Superiores Aragón y las organizaciones del sector público (como es el caso del instituto y organismos electorales) y privado, el Laboratorio de Cómputo permite el acercamiento con el entorno laboral exterior a los alumnos destacados, a través de la participación en proyectos profesionales. En un futuro, los alumnos que hayan a travesado este proceso, contarán con un nivel de experiencia considerable y sobre todo demostrable, siendo esto, un gran beneficio como profesionales de la computación, sin mencionar el impulso que representa para la carrera de un recién egresado.

Al producir estudiantes mejor preparados y con experiencia en el ámbito laboral, el Laboratorio de Cómputo no solo ampliará la red de profesionistas que se forma entre las diferentes generaciones provenientes de la Facultad de Estudios Superiores Aragón, si no también, abrirá camino para nuevas posibilidades de vinculación con más organizaciones, logrando que cada vez más alumnos y egresados puedan sumarse a este proyecto de crecimiento institucional.

Sin perder de vista lo anterior y como ya lo hemos comprobado, el proceso de auditar un sistema informático es una tarea compleja, requiere por parte del profesional, conocimientos sólidos en redes, ingeniería de software y seguridad informática. Por eso, los alumnos deberían recibir una preparación previa y completa, que con el tiempo y práctica, pueda convertirse en habilidades sólidas, bien cotizadas en el ambiente laboral.

Atendiendo al punto previo y debido a la cantidad de tareas que involucra el proceso de auditoría y el volátil periodo de tiempo que los alumnos forman parte del Laboratorio de Cómputo, existe como área de

oportunidad, la capacitación a un nivel básico dentro de un corto lapso de tiempo a los alumnos más sobresalientes en áreas como ingeniería de software y seguridad informática, con el fin de poder delegarles tareas sencillas que les permita aportar sus conocimientos en algunas etapas del proceso. Esto genera una situación de ganar – ganar entre alumno e institución, pues el primero obtiene preparación y experiencia al participar en proyectos vinculados con organizaciones públicas, mientras que la institución y en particular el Laboratorio de Cómputo obtienen el beneficio de continuar con el desarrollo de proyectos, sin perder de vista el aspecto académico.

Referencias

1. Gómez P., Vázquez F. y Álvarez F. (1998). *Auditoría y Seguridad Informática*. México: Editorial Spanta.
2. Sandoval H. (2012). *Introducción a la auditoría*. México: Red Tercer Milenio.
3. Piattini M. G. y Del Peso E. (2001). *Auditoría Informática un Enfoque práctico*. (2 ed.). México: Alfaomega.
4. Engebretson P. (2011). *The Basics of Hacking and Penetration Testing*. USA: Elsevier.
5. Castellanos L. (2012). *Seguridad en Informática*. España: Editorial Academia Española.
6. Diccionario de la lengua española. (2015). RAE. 22/10/2016, Recuperado de: http://dle.rae.es/?id=4NVvRTc
7. CANIETI. CANIETI Nacional. (2016). Hacia una estrategia nacional de ciberseguridad y protección de datos [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=6P0q4qFqMlc
8. DOF. (2015). ACUERDO del Consejo General del Instituto Nacional Electoral, por el que se aprueban los Lineamientos del Programa de Resultados Electorales Preliminares. 16/11/2016, Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=5388923&fecha=15/04/2015
9. INE. (2015). Lineamientos del programa de resultados electorales preliminares. 30/10/2016, Recuperado de: http://www.ine.mx/archivos2/Alterna/2015/PREP/CentroDeAyuda/rsc/pdf/Lineamientos_PREP.pdf
10. OWASP-ZAP. (2016). OWASP ZAP 2.5 Getting Started Guideh.16/02/2017, Recuperado de: https://github.com/zaproxy/zaproxy/releases/download/2.4.0/ZAPGettingStartedGuide-2.4.pdf
11. Gastélum C. y Covarrubias A. (Sin fecha). Introducción a los sistemas de información. Instituto Tecnológico de Sonora. 13/03/2017, Recuperado de: http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p3.htm.
12. Gutiérrez C. (2012). We live security. Buenos Aires, Argentina.: ESET. Recuperado el día 22 de marzo de 2017 de http://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/
13. AN. (2016). Aristegui Noticias. Ciudad de México, México.: Aristegui Noticias. Recuperado el 13 de febrero de 2018 de https://aristeguinoticias.com/2704/mexico/subimos-lista-nominal-de-electores-a-amazon-y-hubo-asalto-cibernetico-movimiento-ciudadano/