

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



Framework para la entrega de Reportes de Test de Penetración a Aplicaciones Web

MIGUEL ANTONIO DÍAZ LIRA

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Luis Hevia
Profesor Co-referente: Raúl Monge

Noviembre - 2017

DEDICATORIA Y AGRADECIMIENTOS

Le dedico esta memoria a mis padres, quienes siempre me apoyaron durante toda mi formación, incluso en mis peores momentos académicos estuvieron allí empujando conmigo, sin lugar a duda fueron la luz que me guío por el camino del bien, la honestidad y la rectitud.

Adicionalmente quiero agradecer a mis amigos de la Universidad, Carla Mansilla, Camilo Domínguez, Javier Romero; Con quienes compartí certámenes imposibles y llantos por reprobado un global, muchas gracias a ellos y a todo el resto de la comunidad universitaria que conocí durante estos años de educación.

RESUMEN

Con el aumento de los ataques cibernéticos de hoy en día, es importante para las empresas e instituciones evaluar el nivel de protección que tienen sus sistemas informáticos. Para realizar esta evaluación se requiere realizar un test de penetración altamente técnico y especializado. Esta evaluación debe ser comprensible por el cliente para poder priorizar y diseñar una correcta estrategia de mitigación. Este marco de trabajo (desde ahora Framework) persigue apoyar al cliente a entender de mejor forma los entregables de estas evaluaciones y al profesional orientarlo a elaborar estos documentos.

Para realizar este framework se consideraron múltiples propuestas de otras entidades y se realizaron entrevistas con profesionales del área. Como resultado, el framework tuvo una excelente aceptación por parte de los profesionales e incluso fue validado con un cliente real.

Dentro de este documento, podrá encontrar el estado del arte de otras propuestas buscando el mismo objetivo, un marco teórico con el vocabulario técnico y una definición de las secciones que debe contener un informe técnico y ejecutivo. En la sección de anexos se encuentra un informe técnico y ejecutivo de demostración.

ABSTRACT

Today, cyber-attacks are more common than ever and for companies it's important to assess their level of protection against them. To do this task, it's mandatory to perform highly technical and specialized security assessments. This assessment must be understandable by the clients to be able to prioritize and design mitigation plans. This framework seeks to support the client to better understand the deliverables of these assessments and to guide the professional to prepare these documents.

To develop this framework, multiple proposal from different associations were analyzed and several interviews with security professionals were performed. As a result, the framework was very successful in its objectives by the professionals and it was even validated with a real client.

Inside this document, you can find the State of Art of different proposals seeking the same objective, a theoretical framework with technical vocabulary and a definition of the sections that a technical and executive reports must contain. On the annexed section you could find a demonstration of a technical report and executive report.

INDICE DE CONTENIDOS

RESUMEN.....	IV
ABSTRACT	IV
INDICE DE FIGURAS.....	X
INTRODUCCIÓN	2
CAPÍTULO 1	3
I. Definición del problema	3
II. Impacto de solucionar el problema.....	5
III. Participantes de la solución.....	6
IV. Entorno y Contexto.....	7
V. Restricciones.....	9
VI. Motivación.....	9
VII. Objetivos de la memoria	10
CAPÍTULO 2	11
ESTADO DEL ARTE.....	11
Reportes según: SANS Institute.....	11
Acerca de SANS Institute	11
Propuesta.....	11
Aporte principal.....	13
Reportes según: Offensive Security.....	14
Acerca de Offensive Security.....	14
Propuesta.....	14
Aporte principal.....	15
Reportes según: Pentesting-Standard.....	16

Acerca de Pentesting-Standard	16
Propuesta.....	16
Aporte principal	19
Reportes según: InfoSEC Institute	20
Acerca de InfoSEC Institute	20
Propuesta.....	20
Aportes Principales	22
CAPÍTULO 3	23
Metodología	23
Marco Teórico.....	24
Análisis de los entregables de Servicio	35
Análisis sobre el estilo de Reporte	36
Análisis sobre las secciones del Reporte	40
Detalle de las secciones:.....	44
Sección: Introducción	44
Sección: Alcance del Trabajo	45
Sección: Hallazgos Generales	46
Sección: Acuerdos.....	47
Sección: Conclusiones.....	48
Sección: Recomendaciones Generales.....	49
Sección: Objetivos del Servicio	50
Sección: Riesgo Consolidado	51
Sección: Metodología	53
Sección: Hallazgos Detallados	54

Sección: Anexos	54
Sección: Control Documental	55
Sección: Hoja de Ruta estratégica	56
Sección: Información de Contacto	57
Sección: Narración de la evaluación	58
Sección: Explicación de Explotación	59
Presentación de las vulnerabilidades	60
Identificadores Necesarios	60
Identificador Único	60
Nombre de la Vulnerabilidad	60
Severidad y Riesgo	61
Ubicación	61
Descripción	61
Recomendación	61
Identificadores Opcionales	61
Tipo de vulnerabilidad	61
Explotabilidad y Condiciones	62
Referencias	62
¿Cómo utilizar el Framework?	63
1.- Preparación con el cliente	63
2.- Ejecución de la actividad	63
3.- Preparación de los Informes	63
4.- Redacción de los Informes Técnicos	63
5.- Chequeo cruzado con el Cliente y cálculo del Impacto	64

6.- Redacción de los Informes Ejecutivos	64
7.- Presentación y cierre	64
CAPÍTULO 4	65
VALIDACIÓN DE LA SOLUCIÓN.....	65
Acuerdo de Evaluación con el Cliente Voluntario	65
Utilización del Estándar para los entregables	66
Contexto de la Evaluación	66
Metodología de Evaluación	66
Redacción de los entregables	67
Resumen de los resultados de la evaluación.....	69
Inyección de código	69
Vulnerabilidad en el código	69
Configuración.....	70
Mantenimiento.....	70
Evaluación de las partes involucradas.....	71
El cliente	71
Los profesionales	73
CONCLUSIONES.....	77
Sobre el alcances y limitaciones de la memoria.....	77
Sobre el impacto en los actores	78
Sobre la validez de los objetivos formulados	79
Sobre las contribuciones y aplicaciones del trabajo realizado.....	80
Contribución Educativa	80
Contribución Comercial y de Negocio	80

Aplicaciones del trabajo	80
Invitación a nuevas investigaciones relacionadas	81
REFERENCIAS BIBLIOGRÁFICAS.....	82
ANEXOS A - Reporte Ejecutivo Anonimizado	84
ANEXO B - Reporte Técnico Anonimizado.....	85

INDICE DE FIGURAS

Ilustración 1: Etapas para generar un reporte según SANS Institute.....	12
Ilustración 2: Tríada de la Seguridad de la Información.....	25
Ilustración 3: Pilares de la Seguridad según la consultora Deloitte	26
Ilustración 4: Servicios Hacking Ético	30
Ilustración 5: Pasos de un Test de penetración.....	31
Ilustración 6: NIST 800-30 Matriz de Riesgo.....	40

INDICE DE TABLAS

Tabla 1: Códigos de OWASP Testing Methodology Guide	33
Tabla 2: Documentos de ejemplos reportes de vulnerabilidades.....	35
Tabla 3: Secciones de un informe ejecutivo y técnico.	42
Tabla 4 - Identificadores de un Hallazgo.	60
Tabla 5 - Secciones solicitados por el cliente.	66

INTRODUCCIÓN

El avance de las tecnologías de la información y la transformación digital empuja a las empresas a montar más infraestructura, servicios en la nube y digitalizar sus procesos manuales. Esto invita no solo al avance tecnológico si no que también a realizarlo de manera segura frente a los ciberdelincuentes. Una los mecanismos que tienen las empresas para comprobar la seguridad de un nuevo servicio digital es realizar un test de penetración, esto significa contratar a un hacker de sombrero blanco para que simule un ataque y pruebe que tan vulnerable es el sistema. Si bien esta disciplina lleva un par de años funcionando en la industria ha tenido un foco extremadamente potente en la parte técnica de como ejecutarla, pero no así la parte más blanda, como es la de entregar los resultados de estas evaluaciones para que una contraparte sin altos conocimientos técnicos pueda entenderlo. Esta memoria busca plantear un framework que permita diseñar entregables de pentesting webs (dado que son las más comunes en la industria) para que los clientes puedan entender de manera más fácil estos entregables y al mismo tiempo apoyar a los profesionales del área a estructurar sus entregables siguiendo la misma línea.

Para realizar esto se estudiaron diversas propuestas de frameworks de distintas organizaciones de seguridad reconocidas a lo largo de todo el mundo y se trabajó directamente con profesionales que trabajan en el área. Utilizando esta información se planteó y declaró un framework de trabajo para que cualquier profesional de la seguridad y cliente pueda leer, entender y aplicar en sus evaluaciones.

El documento está dividido en 5 capítulos. El capítulo inicial describe el contexto en el que se desarrolla la memoria, presentando los objetivos y restricciones de la misma, a continuación, el capítulo 2 presenta el estado del arte actual respecto a las distintas propuestas de framework de organizaciones líderes en temas de seguridad. El capítulo 3 describe la metodología que se utilizó para analizar el estado del arte y trabajar con profesionales en el tema, en este capítulo se describe el framework creado y se entrega una guía de cómo utilizarlo. El capítulo 4 describe la validación de la propuesta utilizando el framework diseñado en el capítulo 3. Para esta validación se utilizó un cliente voluntario quien facilitó una plataforma web y los entregables fueron presentados al finalizar la ejecución. Adicionalmente se validaron los entregables con la ayuda de tres profesionales que se dedican a realizar Pentesting web. Finalmente, en el capítulo 5 se compilan todas las conclusiones que fueron apareciendo durante la elaboración de esta memoria y se entrega un cierre formal al escrito.

CAPÍTULO 1

I. DEFINICIÓN DEL PROBLEMA

Una excelente estrategia para identificar un problema es utilizar el diagrama de espina de pez, desarrollado por licenciado en química japonés Kaoru Ishikawa. Este modelo fue dividido en 5 espinas principales: Herramientas Automáticas, Disciplina y Pentesting¹, Clientes del Servicio, Proveedores de Servicio y Especialistas en seguridad. Todos estos son los diversos ámbitos desde donde se pueden observar las posibles causas del problema. A continuación, está presente el desarrollo lógico de estas situaciones.

La práctica de realizar *pentests* a un sistema informático es algo ampliamente solicitado por diversas industrias. El profesional Bruce Schneider (Schneider, 2016) lo deja claro en la siguiente cita:

"Quien no entiende la utilidad de realizar pentests, debe declararse vulnerable automáticamente"

Si bien esta actividad es importante, hay que destacar que las empresas no entienden que es lo que deben esperar al momento de recibir los resultados de un pentest, principalmente por que no son expertos en la materia, y contratar una contra parte técnica es un costo demasiado elevado. Es por esto por lo que es un gran desafío para las empresas exigir cuales debiesen ser los entregables de esta actividad, o determinar si lo recibido está completo o no.

Por otra parte, los hackers éticos que realizan estas actividades tienen sus propias formas de diseñar estos entregables, y si bien existen intentos de estandarización por organizaciones como SANS Institute (Alharbi, 2016), Pentest-Standard (Smith, 2016) o el desarrollado por Offensive-Security (Offensive, 2016) todos estos son distintos en redacción, enfoque, componentes, secciones, etcétera. Esta des homologación de reportes se debe a que cada uno de estos intenta generar un framework para la totalidad de los Pentests en todas sus variaciones: Web, Servidores, Aplicaciones de Escritorio, Sistemas Embebidos, entre otros. Otra situación presente en los proveedores de servicio es que el personal responsable del profesional, en algunos casos, no tiene la misma formación que el profesional, por lo que, si bien apoya desde una visión de alto nivel, la estructura de bajo nivel del entregable puede pasar inadvertido.

¹ Test de penetración (Penetration Test en inglés)

InfoSEC Institute reconoce esta situación como problema (Sheward, 2017). La organización indica que si bien existen cursos y talleres en los que enseñan a realizar estas actividades, no más del 10% del curso está orientado a la confección de los entregables a cliente. Esto es inconcebible considerando que entre el 40% y 50% del tiempo invertido durante los pentests es efectivamente desarrollando estos entregables. Esto denota una carencia de entrenamiento formal respecto a entregables, y que quede a disposición del especialista de seguridad sea autodidacta para generar estos reportes.

Otra de las situaciones interesantes con respecto a los test de penetración es que es una disciplina que no nació con el objetivo de defender sistemas, sino más bien con el de atacarlos. La actividad de pentesting permite, mediante una actitud ofensiva, encontrar las falencias en los sistemas, esto nace de hackers quienes aprendieron a destruir primero, por lo que no está dentro de las actividades reportar lo encontrado a la entidad que se desea destruir, esto también causa que la metodología y sus entregables varíen de cada profesional, ya que debe improvisar algo que jamás aprendió de manera formal. Finalmente, esta disciplina lleva poco tiempo en el mercado, por lo que se ha ido ajustando poco a poco lo que un entregable debe presentar.

En el artículo (Alharbi, 2016), InfoSEC destaca el problema como algo importante. Declara que desarrollar estos entregables es un arte, el cual una vez dominado permite a las empresas ahorrar dinero y tiempo en sus compromisos, al mismo tiempo genera una mejor relación comercial entre la empresa y sus clientes, los cuales definitivamente volverán a confiar en los servicios entregados.

Continuando con lo investigado por InfoSEC, la organización indica que uno de los mayores problemas al momento de escribir estos reportes es que el profesional a cargo de redactarlos debe explicar algo altamente técnico a alguien quien no está a su mismo nivel. Usualmente se realizan suposiciones en las que cualquiera que trabajara en TI² entendería, pero no siempre el lector final de estos reportes es alguien quien domina el tema.

Otro ámbito que influye en la entrega de servicios como el pentesting son las herramientas automáticas que se utilizan durante estas ejecuciones. Si bien estas herramientas entregan buenos resultados realizan informes genéricos, que no tienen una orientación a la empresa que se está auditando. Cada herramienta distinta trae sus propios reportes, con sus secciones e identificadores que creen necesarios a entregar. Resultado de esto, si la siguiente persona que realiza la evaluación no ha adquirido la misma herramienta (usualmente cuestan sobre los 1000 USD) el proceso ya no es compatible porque el reporte estará sujeto a dicha tecnología.

De esto nace la necesidad de crear un framework que permita al hacker ético saber qué entregar al momento de realizar un pentest a una aplicación web, así como al mismo

² Tecnologías de la Información

tiempo entregar una guía de lo que el cliente debiese recibir al momento de solicitar este servicio.

II. IMPACTO DE SOLUCIONAR EL PROBLEMA

El solucionar este problema permitiría a las empresas tener un referente o una guía de lo mínimo que tienen que tener estos servicios a nivel de entregables, permitiendo especificar las expectativas y las exigencias al momento de levantar una licitación. Por otra parte, la homologación de estos entregables permite manejar una base mínima de conocimiento para que las empresas entiendan la utilidad y resultados del servicio, permitiendo planificar y programar lo que realmente necesitan, de qué forma y con cuál alcance solicitar el servicio.

Adicional a esto, el framework invita a establecer (o proponer) un lenguaje base para hablar y tratar servicios relacionados. Es posible ver como en ciertas estandarizaciones, por ejemplo, la ISO9001:2015 (Estándar de Calidad) o la ISO27000:2016 (Estándar de Seguridad de la información) tienen secciones dedicadas a establecer vocabulario y definiciones de términos técnicos, los cuales son necesarios para conversar de estos temas. Para motivos de esta memoria se utilizará el vocabulario de la ISO/IEC27000:2016 (Standard, 2016), agregando términos si así lo amerita, dado que ya es un vocabulario ampliamente utilizado por el mundo profesional de la seguridad informática y grupos dedicados a esta disciplina. Por otra parte, este vocabulario considera otras estandarizaciones como la ISO2:1996, la ISO3282-8 y gran parte de la ISO9000:2015.

Otro de los beneficios que trae la homologación de los entregables es que los informes podrán ser comparables entre diversos ejecutores y también los mismos informes a lo largo del tiempo. Adicionalmente se podrá observar cómo ha evolucionado el sistema de seguridad independiente de quien realice la evaluación. Existen empresas hoy en día que tienen políticas de cambiar año a año la empresa que realiza estas evaluaciones, y si cada empresa trae su propio entregable, con su propia estructura, entregables y formas queda en responsabilidad del encargado de Seguridad entender si han mejorado o empeorado o si siguen igual.

Este framework también permite a empresas de servicios seguir una norma para la entrega de sus informes, sin la necesidad de "*reinventar la rueda*". A los *pentesters* nuevos también les permite tener una base conocida sobre la cual generar estos informes, dado que en muchas compañías acá en Chile (Por ejemplo, *Dreamlabs*³) una de las pruebas

³ <https://dreamlab.net/>

necesarias para postular al trabajo es realizar un pentest y entregar un informe sobre los resultados.

III. PARTICIPANTES DE LA SOLUCIÓN

El participante de la solución considera a Gerentes y oficiales de seguridad de las tecnologías de la información (CISOs⁴) de las empresas. Esto es debido a que la seguridad de los activos de información son responsabilidad de estos cargos en las empresas. Estos profesionales son responsables de que la información de la compañía, uno de sus activos más importantes, permanezca íntegra, confidencial y disponible durante todo su ciclo de vida.

En ocasiones, las empresas están reguladas por políticas internas. Por ejemplo, en las empresas financieras o Bancos suelen tener evaluaciones de seguridad periódicas. Por otra parte, existen regulaciones internacionales como la HIPAA⁵ para las instituciones de Salud, la cual les exige ciertas políticas de seguridad que deben cumplir. Existe por otro lado aquellas organizaciones que manejan información de tarjetas de crédito de MasterCard y Visa. Para poder utilizar estas tarjetas de crédito en sus transacciones, tanto en línea como en sus locales físicos, las empresas deben cumplir el estándar internacional llamado PCI-DSS⁶. La PCI-DSS exige, en términos generales, que las empresas cumplan con doce requisitos para poder trabajar con estas tarjetas (Rouse, 2016), uno de los cuales es *"Probar con regularidad los sistemas y procesos de seguridad"*. Los test de penetración son necesarios para cumplir con este requisito. Estos pentest debe estar bajo la norma NIST SP800-115 (Wright, 2016), la cual especifica ocho puntos a seguir, pero nuevamente y tal como se ha comentado en la sección anterior la parte en que habla de cómo realizar el reporte de seguridad (entregable a cliente) son meramente 7 secciones referenciales las cuales están descritas de manera superficial. Es importante recordar que más allá de las técnicas utilizadas para realizar el servicio, el entregable final es el que entrega real valor al servicio.

Los clientes (empresas) no son los únicos participantes de esta solución, también lo son quienes brindan este servicio, quienes como parte de su proceso de pentesting es fundamental considerar las actividades previamente realizadas. Si todas las empresas participan utilizando el mismo modelo, este proceso se realiza de manera trivial, dado que no tiene que haber una inversión de tiempo por parte de los consultores en entender la anterior evaluación, por lo que pueden revisar de manera mucho más expedita.

⁴ Chief Information Security Officer, Oficial de Seguridad de la Información

⁵ Health Information Privacy - <https://www.hhs.gov/hipaa/index.html>

⁶ Payment Card Industry - Data Security Standard

Finalmente, el Gobierno de Chile es el tercer participante, a quien le podría ayudar esta solución dado que en su programa de gobierno Comité Interministerial de Ciberseguridad describen sus ejes principales de operación, presentando 6 puntos para resguardar la seguridad informática en Chile (Chile, 2016). Estos puntos son:

- Infraestructura de la información
- Prevención, persecución y sanción del cibercrimen
- Sensibilización, formación y difusión en ciberseguridad
- Cooperación y relaciones internacionales
- Desarrollo Industrial y productivo en ciberseguridad
- Institucionalidad de la ciberseguridad

La solución de este problema aportaría al eje número uno (1), en la cual uno de sus sub-puntos indica "La definición de requisitos y estándares de seguridad".

IV. ENTORNO Y CONTEXTO

El crecimiento e implementación de las tecnologías de la información en las empresas chilenas crece cada año, cada vez más y más empresas abandonan el papel y digitalizan sus documentos, reemplazan sistemas de contabilidad manuales por ERPs⁷, ofrecen servicios en línea y aumentan los puntos de contacto con sus clientes. A todo este crecimiento se suma el constante y exponencial avance de las tecnologías de la información.

Esta continua expansión obliga a las empresas a aumentar sus infraestructuras tecnológicas, a externalizar sus servicios digitales, adquirir nuevas tecnologías e implementar nuevo software de gestión. Junto con este crecimiento los ciberdelicuentes han aprovechado estos desarrollos tecnológicos para encontrar vulnerabilidades de seguridad en las empresas con el fin de adquirir, destruir o modificar la información en ellas con fines lucrativos, fama o simplemente dañar la imagen de una compañía. Estos delitos afectan directamente la tríada de la seguridad (Confidencialidad, Integridad y Disponibilidad) de la información.

Como medida mitigatoria a esta amenaza, las empresas contratan hackers éticos para realizar evaluaciones periódicas de seguridad a sus infraestructuras. Los Hackers son

⁷ Enterprise Resource Planning, Planificación de Recursos Empresariales

personas con un gran conocimiento en tecnología, altamente especializadas con habilidades que permiten detectar y explotar vulnerabilidades en sistemas informáticos, estos conocimientos pueden ser utilizados para cometer crímenes los cuales por definición serían *ciberdelicuentes*, cuando este conocimiento se utiliza para detectar brechas de seguridad y mejorar la seguridad de la empresa son llamados *hackers éticos*.

El proceso mediante el cual un hacker ético realiza una evaluación de seguridad es llamado Test de penetración o Pentest (del inglés, *Penetration Test*). Durante este proceso, el profesional simula un ataque informático a un sistema en particular, identificando y reportando cualquier vulnerabilidad que pueda ser explotada con la finalidad de afectar la tríada de seguridad. Estos reportes son de vital importancia para que las empresas puedan preparar sus sistemas por si llegase ocurrir un ataque por parte de un ciberdelincuente.

Uno de los aspectos importante de los cuales esta des homogenización existe es porque la evaluación de seguridad es una materia relativamente nueva y muy inmadura. Hay que considerar que esta disciplina existe dada la naturaleza de la informática, algo que, si bien ha evolucionado mucho en los últimos 40 años, sigue siendo algo relativamente amplio, evolutivo y aún en vías de estandarización, por lo tanto, no es posible esperar algo distinto de la disciplina de la seguridad informática. Por otra parte, y tal como se ha mencionado en otras secciones de esta memoria, los hackers éticos que trabajan en este tipo de evaluaciones suelen ser autodidactas (Armerding, 2016), si bien existen certificaciones y cursos de seguridad estos cursos suelen ser orientados a técnicas, más que metodologías para reportar.

En los intentos de realizar frameworks para los reportes de seguridad buscan una generalización de todos los servicios de seguridad en un mismo estándar, lo cual no es necesariamente algo bueno. Este dilema ya lo vivió el campo de la Inteligencia Artificial. Los investigadores comenzaron abarcando todo el aspecto de la vida humana en una sola inteligencia artificial, abarcando todo. Este acercamiento jamás tuvo frutos dado que no era posible, en un solo esfuerzo, simular la inteligencia completa del humano, algo que realmente ni si quiera un humano es capaz de hacer, es por ello por lo que existen las especializaciones y el mismo enfoque tuvo la Inteligencia Artificial. Continuando esta lógica es que se busca en esta memoria limitarlo a un campo en específico.

Volviendo al tema central, otro de los aspectos y variables que le han dado forma a estos entregables (reportes) son las herramientas automáticas de seguridad. Hoy en día existen herramientas que automatizan evaluaciones simples que de manera manual tomaría meses en realizar, pero que solo toman algunos minutos. Estas herramientas generan un entregable final en forma de reporte (usualmente un PDF), que tiene su propia estructura.

Existen empresas que se han adaptado a esta estructura, pero al mismo tiempo es posible ver que diversas herramientas generan reportes distintos, lo que le da más variedad a la generación de entregables.

V. RESTRICCIONES

Es importante considerar que este trabajo de memoria debe tener ciertas limitaciones, dado que está programado en un marco de desarrollo de 6 meses, por lo que se definen las siguientes restricciones para el trabajo.

- **Enfocado a la realidad del País:** La memoria estará orientados a la realidad chilena en términos de seguridad, esto significa considerar las industrias que operan en este país y las regulaciones nacionales que existen.
- **Pentesting web:** El mayor porcentaje de evaluaciones de seguridad son a aplicativos webs, esto se debe a que cada software basado en esta tecnología ha sido principalmente desarrollado a medida, es decir, orientados a las necesidades de las compañías. Usualmente las empresas que desarrollan estas aplicaciones colocan su preocupación en que el sistema funcione, no que sea seguro, por lo que suelen ser los mayores puntos de vulnerabilidad en las empresas.
- **A la Información recopilada en estos meses:** Debido al límite de tiempo destinado a la memoria (6 meses), estará limitada a las entrevistas, investigaciones y desarrollo de esta en ese periodo de tiempo.

VI. MOTIVACIÓN

Desde el punto de vista de un cliente, justificar la realización de estas actividades a la alta gerencia es una tarea compleja pero fundamental. La empresa rapid7 indica que usualmente los departamentos TI reciben una gran negativa cuando solicitan realizar estas actividades (Rapid7, 2016). Los comentarios recibidos suelen ser los siguientes:

- ¿No hemos invertido suficiente en Firewalls y Seguridad? ¿Por qué ahora me dices que necesitamos probarlos?
- ¿Me estás diciendo que no conoces lo suficientemente bien tus sistemas como para conocer sus vulnerabilidades?
- ¿Me estás solicitando contratar profesionales para intentar romper nuestros sistemas?

Y la verdad es que, si bien desde el punto de vista de la seguridad informática tiene un enfoque de rechazo, no es así cuando se habla por ejemplo de vehículos o edificios. Existen legislaciones que prohíben la entrega de un automóvil o un edificio sin sus respectivas pruebas de seguridad, sin embargo, para el sector informático existen pocas regulaciones o las que existen son antiguas. Por otra parte, ser arquitecto o administrador de sistemas no significa conocer todos los riesgos asociados a su operación, ya que el área de especialización de estos profesionales es desde el lado operacional, no de seguridad, la cual es una especialización diferente. En pocas palabras *"el administrador de sistemas TI"* coloca su esfuerzo en que el sistema funcione, y lo haga de manera correcta. En muchas ocasiones esto deriva en reducir la seguridad de los sistemas.

Sin embargo, una vez convencida la alta gerencia, es importante indicar cuáles serán los entregables del servicio contratado, y que objetivos del departamento TI ayudará a cumplir. Es por esto por lo que es fundamental para los clientes entender qué es lo que deben recibir, y qué es lo que podrán hacer con estos entregables.

Desde el punto de vista de un *pentester* o de una empresa de seguridad es importante lograr presentar de manera correcta, clara y concisa los resultados de su evaluación. De esto depende la satisfacción del cliente, la calidad del trabajo y la posible recontractación de servicios.

VII. OBJETIVOS DE LA MEMORIA

El objetivo general de esta memoria es proponer un estándar para la redacción y presentación de informes de pentesting de seguridad a aplicaciones webs para empresas. Para lograr esto se definen los siguientes objetivos específicos:

- Definir una guía de contenido mínimo y estructura para la generación de reportes de pentesting web
- Definir una pauta de lectura de estos informes orientados a clientes finales
- Establecer un vocabulario para servicios de pentesting web (Basado en ISO27000)

CAPÍTULO 2

ESTADO DEL ARTE

Para lograr proponer un estándar es necesario realizar un análisis sobre el estado de arte con respecto a los reportes de Pentesting web propuestos por distintas instituciones. Este primer acercamiento permitirá identificar las secciones y estructuras de reportes en sus propuestas y por otro lado permitirá clarificar ideas respecto al tema de interés.

Reportes según: SANS Institute

Acerca de SANS Institute

SANS⁸ Institute es una organización establecida en 1989 con el fin de investigar de manera colaborativa los temas relacionados con la Seguridad Informática. Con más de 165.000 profesionales de seguridad a lo largo del mundo es reconocida como una de las instituciones más grandes dedicadas al tema del mundo. La enorme cantidad de cursos y documentos relacionados a la Seguridad Informática la posiciona como uno de los entes referentes respecto a esta materia. (SANSInstitute, 2016).

Propuesta

La institución publicó el año 2010 el documento "*Writing a Penetration Testing Report*" (Alharbi, 2016), que en español significa "Escribir un reporte de un Test de penetración".

Este reporte indica declara que un test de penetración es inútil si el resultado final no es tangible, es por eso por lo que le otorga un énfasis especial al desarrollo de estos reportes. El documento de SANS Institute indica que el entregable de un test de penetración debe representar el resultado de una serie de evaluaciones de seguridad, recomendaciones y documentación sobre los activos evaluados.

Un fenómeno detectado por la institución indica que estos reportes suelen ser ásperos y difíciles de comprender por los clientes (tanto gerencia como técnicos), y que al mismo tiempo generar estos reportes significa un esfuerzo monumental para los consultores de seguridad.

Para abordar estos problemas, la SANS define 4 etapas para realizar un reporte de seguridad.

⁸ SysAdmin Audit, Networking and Security

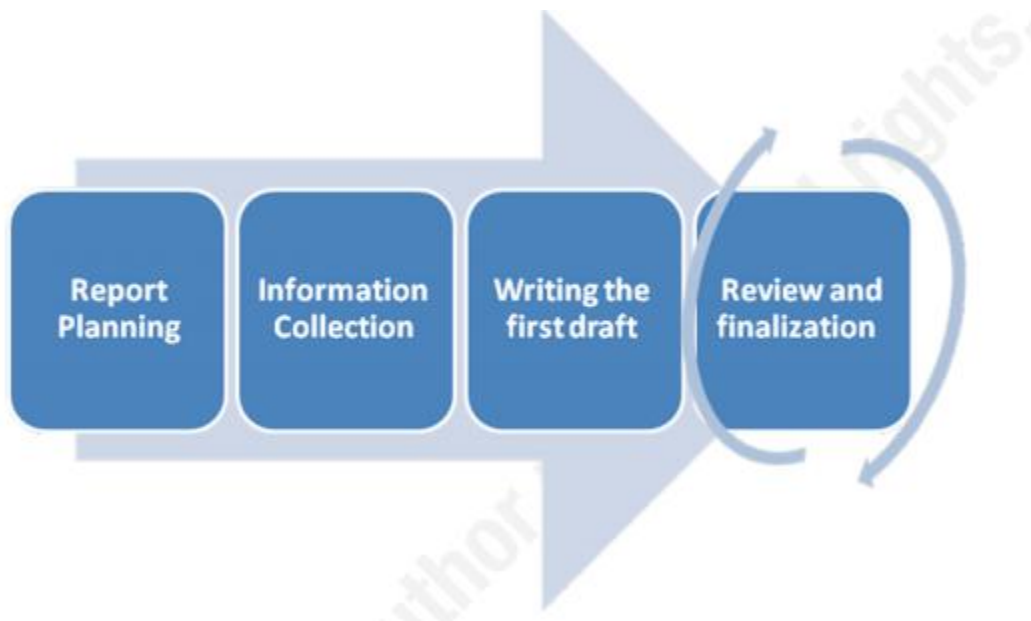


Ilustración 1: Etapas para generar un reporte según SANS Institute

Fuente: SANS Institute

Sans especifica en su documento que estas etapas representan el ciclo de vida de la escritura de un reporte, considerando dentro de este ciclo la realización del mismo.

En una primera etapa, indica que parte de la creación del reporte de vulnerabilidades (*Report Planning*) es identificar de manera clara cuáles son los objetivos y el alcance de la evaluación realizada e indicarlos en el reporte. Esto tiene como finalidad de que el lector entienda de que se trata el texto que tiene en sus manos y cuáles son los objetivos que persigue. Adicionalmente, es necesario indicar y establecer en la que espacio temporal se ubican los resultados de la evaluación. Datos como fechas de inicio, finalización o ventanas de tiempo son necesarios para que el lector logre contextualizar de manera correcta los resultados que está leyendo. Siguiendo a estas dos secciones, es necesario tener claridad de las audiencias que recibirán el informe para discernir el nivel técnico con que el texto debe ser redactado. Finalmente indica que es importante indicar el tipo de clasificación de documento: Confidencial, Publico, FYEI⁹; e identificar de manera clara y objetiva quienes tienen acceso al documento.

Luego de ser coordinada esta información con el cliente y anotada de manera inmediata en el reporte comienza la segunda etapa de escribir el reporte: La recolección de información (*Information Collection*), durante esta etapa es fundamental escribir notas de

⁹ FYEI: For Your Eyes Only, solo para los ojos del lector

seguimiento y avance de la evaluación, así como también anotar de manera metódica las herramientas utilizadas para que de esta forma no se omita ningún procedimiento y resultado al momento de escribir el reporte. Una vez finalizado el trabajo (la evaluación de seguridad) comienza la tercera fase, en donde se recomienda realizar un primer borrador con los resultados anotando de manera ordenada todos los hallazgos encontrados.

La última etapa del proceso es la revisión continua de los resultados escritos con el cliente y otros profesionales para tener segundas opiniones en los resultados expresados en el documento o ciertas partes que pudieron no haber quedado claras. Luego de explicar las fases de escritura del documento (como proceso completo), realiza un recorrido completo sobre las secciones que deben estar presentes en el informe y las características de cada una.

Finalmente, el documento creado por Sans presenta un reporte de ejemplo para orientar al lector considerando la parte ejecutiva y técnica parte de un mismo documento. Este escrito define las vulnerabilidades encontradas punto por punto indicando, por cada una de estas, la severidad, el nivel de amenaza, un análisis y su respectiva recomendación.

Desde un punto de vista de esta memoria, el documento presenta puntos interesantes sobre la confección del reporte de vulnerabilidades, indicando la importancia de definir secciones y sus respectivos contenidos, así como implementar un proceso a seguir para el pentester.

Aporte principal

Puntualmente se pueden extraer los siguientes aportes:

- Definir un ciclo de confección de informe que considere las opiniones del cliente.
- Confeccionar el informe durante la ejecución de la actividad para no dejar puntos afuera.
- Destacar información relacionada a la ejecución y a los resultados por separado.
- Revisar el informe con el cliente antes de emitir un resultado final.

Reportes según: Offensive Security

Acerca de Offensive Security

Offensive Security es una empresa de consultoría cuyo foco es la seguridad informática. Esta consultora plantea un enfoque ofensivo para proteger los sistemas informáticos, a diferencia de un enfoque defensivo. Un enfoque defensivo se centra en medidas pro activas, tales como instalar actualizaciones de seguridad, buscando y solucionar vulnerabilidades a medida que las auditorías de seguridad las detectan. Un enfoque ofensivo se centra en tener medidas reactivas ante un potencial ataque, buscando el origen de este mitigando el ataque en vivo. Esto les ha permitido tener una visión distinta sobre los métodos de protección y, por ende, los métodos para evaluar vulnerabilidades (Ivy Wigmore, 2016).

Propuesta

Es importante destacar que el enfoque ofensivo no implica actuar solamente cuando una empresa está bajo ataque, sino más bien simular varios ataques y proteger de manera proactiva a los activos de información, es por esto por lo que el reporte propuesto por Offensive Security está orientado a una narración de los hechos más que a separar por puntos las vulnerabilidades encontradas.

Estos reportes cumplen con una narración estilo bitácora para del proceso de penetración del Hacker Ético, indicando en cada instancia los pasos realizados para comprometer el sistema, mostrando evidencia gráfica y emitiendo una declaración del riesgo de seguridad que esto implica para la empresa. En el apéndice de reporte indican de manera escueta el listado de vulnerabilidades detectadas, indicando severidad, descripción, impacto y remediación para la mitigación.

La estructura principal de estos reportes es la siguiente:

- Resumen Ejecutivo.
- Narración del Ataque (Indicando los pasos de la penetración).
- Conclusiones
- Apéndices

Al momento de analizar los reportes, se logra ver que están orientados principalmente para el área técnica de la empresa, destinando solo un par de párrafos al área ejecutiva o de alto nivel quien no maneja estos temas con facilidad. Sin embargo, presenta algo interesante a considerar para esta memoria y es el estilo narrativo y enlazado de vulnerabilidades. Este estilo presenta la importancia de no sólo explicar la vulnerabilidad

en sí, si no que el proceso de descubrimiento detrás de ella, explicando desde el punto de vista del pentester como la encontró y explotó de manera satisfactoria. Por otro lado, este estilo demuestra que las vulnerabilidades se encadenan entre sí de algún modo, que existen prerequisites y que no todos los hallazgos son independientes entre sí.

Aporte principal

Puntualmente se pueden extraer los siguientes aportes:

- Estilo narrativo para explicar una vulnerabilidad.
- Relación entre hallazgos detectados.
- Descripción del proceso de descubrimiento.
- Evidencia del proceso de descubrimiento, no solo de la vulnerabilidad.

Reportes según: Pentesting-Standard

Acerca de Pentesting-Standard

Pentesting-Standard es un grupo conformado por profesionales cuyo foco es la seguridad de la información. El grupo comenzó debido a una conversación que sostuvieron algunos fundadores de este grupo acerca de la poca importancia que se estaba dando a los test de penetración en la industria. La fundación de este grupo comenzó con 6 personas con el objetivo de estandarizar los test de penetración con la finalidad de dar valor agregado a dicha actividad.

Hoy en día, el grupo ya cuenta con 20 profesionales de seguridad representantes de múltiples industrias tales como la financiera, vendedores de seguridad, consultores, investigadores, el mismo SANS Institute, proveedores de servicios, entre otros. Esto permite tener variadas visiones sobre las distintas necesidades de seguridad que cada una de estas industrias exige, considerando estándares internacionales y regulaciones legales que las mismas deben cumplir para operar.

El compromiso realizado por este grupo de profesionales es lograr presentar un estándar formal para realizar test de penetración, considerando desde la metodología para realizarlos, así como también la redacción de reportes ejecutivos y técnicos. Si bien el grupo no busca considerar todos los escenarios posibles (dado que existe una infinidad de ellos), tiene la intención de definir una línea base para lo mínimo requerido en un test de penetración.

Propuesta

El primer punto de la propuesta según Pentesting-Standard (Smith, 2016) indica la importancia de separar el reporte en dos documentos distintos, uno ejecutivo y otro técnico. Esto tiene la finalidad de comunicar los objetivos, metodología y resultados a distintas audiencias, cada uno con un estilo de presentación y detalle diferentes. Esto marca la primera diferencia con los reportes propuestos por SANS y Offensive Security.

En primera instancia se declara como debe ser el reporte ejecutivo. Este reporte debe comunicar de manera clara al lector cuales son los objetivos que el pentesting realizado intentó cubrir, así como explicar de manera sencilla los hallazgos y los riesgos asociados a las vulnerabilidades. Desde un punto de vista ejecutivo este reporte debe permitir identificar de manera ágil quienes son los afectados por estas vulnerabilidades y cuáles son los impactos que puede tener estas vulnerabilidades para la empresa.

Pentesting-Standard recomienda incluir en el reporte ejecutivo seis (6) secciones:

1. Trasfondo
2. Postura General
3. Perfil de Riesgo
4. Hallazgos Generales
5. Resumen de Recomendaciones
6. Hoja de ruta estratégica

La primera sección es llamada **Trasfondo**, la cual busca explicar al lector el propósito de la evaluación, detalles y alcances de la evaluación, un resumen con los hallazgos y las contramedidas recomendadas a un muy alto nivel.

La siguiente sección es llamada **Postura General**, la cual tiene por objetivo indicar cuál es la postura general de seguridad de la compañía con respecto a los hallazgos encontrados durante la evaluación. Declaraciones como *Carencia de políticas de parchado o Validaciones insuficientes de entradas del usuario* son el tipo de frases las que se esperan en esta sección.

La tercera sección se llama **Perfil de Riesgo**, esta sección cumple con dos objetivos principales, el primero es definir el sistema de puntaje que se utilizará para declarar los riesgos de las vulnerabilidades y el segundo objetivo es declarar utilizando este mismo sistema de puntaje el riesgo general de la empresa. En esta sección indica que puede ser utilizado cualquier sistema de puntaje, sin embargo, recomienda usar algo llamado DREAD¹⁰.

La cuarta sección se llama **Hallazgos Generales** la cual busca describir los hallazgos generales de la evaluación realizada. Esta sección debe entregar una sinopsis de las vulnerabilidades sin entrar en detalles de cada una de ellas, si no que al contrario intentar generalizarlas lo más posible y en lo posible representarlas en gráficos fáciles de entender (Gráficos de tortas, barras, lineales, de puntos, etcétera).

La quinta sección es llamada **Resumen de recomendaciones** en donde el lector debe entender en gran nivel como las recomendaciones ejecutivas a realizar para mitigar de mayor forma el riesgo detectado, esto va de la mano con la sexta y última sección llamada

¹⁰ DREAD: Damage + Reproducibility + Exploitability + Affected users + Discoverability

Hoja de ruta estratégica en donde el profesional presenta y recomienda un plan a seguir para trabajar y mitigar estas vulnerabilidades de alto nivel.

Por otra parte, Pentesting-Standard presenta una propuesta para el reporte técnico. Este reporte está orientado a aquella audiencia que debe solucionar estas vulnerabilidades, por lo que debe ser capaz de comunicar de manera técnica el alcance de la evaluación, cuáles fueron sus objetivos, cual fue la metodología y listar las vulnerabilidades detectadas. Este reporte debe identificar también quienes fueron los involucrados en el proceso de evaluación, entregando métodos de comunicación en caso de dudas puntuales.

Y en el reporte técnico siete secciones:

1. Introducción
2. Recolección de información
3. Evaluación de Vulnerabilidades
4. Confirmación de Explotación
5. Post Explotación
6. Riesgo y Exposición
7. Conclusiones

La primera sección es la **Introducción**. Esta debe permitir al lector técnico entender detalles como la identificación de las personas que realizaron el pentest, información de contacto, activos involucrados en la evaluación, objetivos de la evaluación, alcance de la evaluación, acercamiento de la evaluación, definición del sistema de puntaje utilizado.

Una vez definidas las bases sobre las cuales el informe se redacta entra en juego la siguiente sección, llamada **Recolección de información**. Esto va de la mano con el ciclo de pentesting declarado por EC-Council, en la cual la primera parte de todo pentesting es la recolección de información. En esta sección es importante declarar todo lo encontrado por el equipo, desde información pública, privada, del personal que trabaja en la empresa, etcétera. Esto permite descubrir al lector el nivel de exposición y la información que utilizaron los profesionales para buscar vulnerabilidades.

La tercera sección se llama **Evaluación de Vulnerabilidades**. Esta sección la hemos visto en las otras propuestas de estándar de este estado del arte, en la cual se expresa de manera detallada las vulnerabilidades detectadas durante la evaluación. Esta declaración va de la

mano con la cuarta sección llamada **Confirmación Explotación**. En esta sección del documento Pentesting-Standard declara que no toda vulnerabilidad puede ser explotada, sin embargo las cuales es posible llegar una explotación deben ser revisadas con sumo detalle para dar información relevante respecto a un posible escenario de ataque que aproveche esta vulnerabilidades, en esta sección se encuentran detalles tales como: Tiempos de explotación, objetivos afectados, actividades relacionadas, como es posible explotar, cuáles son los vectores de ataque y cualquier otro tipo de información que pudiese ser relevante.

La quinta sección es llamada **Post Explotación** y busca declarar de manera clara y concisa lo que pudiese ocurrir si un atacante explota estas vulnerabilidades de manera satisfactoria. Esto permite al lector entender la extensión de un posible ciberataque a su organización utilizando estas vulnerabilidades detectadas. Adicionalmente esto ayuda considerablemente a colocar un correcto nivel de riesgo a la empresa.

La penúltima sección se llama **Riesgo y Exposición**, la cual cumple el mismo propósito que la sección número 3 del reporte ejecutivo y es la de entregar un valor promedio de riesgo y exposición a la que la compañía se encuentra.

Finalmente está la última sección llamada **Conclusiones**, en las cuales mediante opiniones y declaraciones profesionales apoya al mejoramiento continuo de la postura de seguridad de la empresa y da cierre al reporte en sí.

Aporte principal

Puntualmente se pueden extraer los siguientes aportes:

- Importancia de separar el reporte ejecutivo del técnico según audiencias.
- Separación entre riesgo y vulnerabilidad
- Las preocupaciones de los ejecutivos son los riesgos.
- Las preocupaciones de los técnicos son las vulnerabilidades.
- Declaración de las secciones de cada reporte.
- Definición por parte del escritor del sistema de puntaje.

Reportes según: InfoSEC Institute

Acerca de InfoSEC Institute

El InfoSEC Institute es una empresa que fue fundada en 1998 por un equipo de expertos en temas de seguridad. Su objetivo es claro: Crear una empresa que ofrezca el mejor entrenamiento posible para sus estudiantes en temas de seguridad. Cuenta con más de 47.000 estudiantes, 90+ cursos y más de 17 años de experiencia. A la fecha (2017) ha ganado más de 28 premios de reconocimiento mundial en el ámbito de la industria.

Propuesta

Tal como los grupos anteriormente mencionados, InfoSEC también plantea la importancia de escribir un reporte de seguridad (Sheward, 2017). Lo propuesto por el instituto hace especial referencia al estilo con que los reportes se escriben, ya que en la mayoría de los casos tienden a ser completamente técnicos, dejando a toda la parte gerencial fuera. El documento invita a realizar ciertas preguntas con respecto a la redacción del informe, incluso hace alusión a lo que propone SANS Institute con respecto al ciclo de creación del informe. Invita a cuestionar situaciones como *¿Para quién es el reporte?* ya que dependiendo de esa pregunta es necesario colocar un especial énfasis en una estrategia de solución o netamente caer en situaciones técnicas inmediatamente. Esto es realmente importante a destacar dado que una mala comprensión del informe puede significar en empeorar la situación o riesgo de seguridad que la empresa en cuestión puede tener. Si el cliente se lleva una mala idea de lo que debe priorizar o cuáles son sus riesgos puede causar desastres importantes en la empresa.

Otro factor relevante destacado en el documento escrito por el instituto es que el resultado de un proceso científico y las reglas dictan que, como todo proceso científico este debe poder ser repetible por algún agente externo. Si el reporte no explica de manera clara y concisa los resultados y como se llegaron a ellos es poco probable que otra persona, con el reporte en mano pueda repetir el proceso. Lo que va muy de la mano con lo presentado por la propuesta de Offensive Security.

Al igual que los reportes anteriores, InfoSEC presenta una propuesta sobre lo que debe contener un informe de resultados de un pentest. La institución presenta siete (7) secciones diferentes, las cuales cumplen distintos propósitos.

- Portada
- Resumen Ejecutivo
- Resumen de las Vulnerabilidades
- Detalles de los Evaluadores
- Herramientas Utilizadas
- Alcance del Servicio
- Cuerpo del Reporte

La primera que hace hincapié es **La portada**. Esto es algo que en las anteriores propuestas no había sido detallado. InfoSEC incluso hace alusión a que es una sección “*obvia*” sin embargo lo que incluye esta sección no es obvio. Sin embargo, indica que esta portada debe tener un nombre clarificador sobre lo que presentará el informe, con la intención de no confundir con otras evaluaciones realizadas a la misma compañía. Lo interesante declarado en esta sección es que el formato del informe: portadas, estilos, contenido; debe ser acordado con el cliente, con la finalidad de que pueda presentarlo a auditores u otras empresas de la forma.

La siguiente parte que presenta es el **Resumen ejecutivo**. InfoSEC indica que esta sección no puede ser superior a una página, dado que tiene una orientación netamente ejecutiva y al final del día, es un resumen. Recomiendan evitar declarar metodologías, herramientas o técnicas utilizadas, sino más bien aferrarse a los resultados de la evaluación de la manera más escueta y precisa posible. Proponen como ejemplo la siguiente frase:

“Hemos realiza un test de penetración perteneciente a [...] y hemos encontrado los siguientes hallazgos de seguridad [...] los que podrían representar a la empresa un riesgo en los siguientes aspectos [...]”.

Finalmente indican que las últimas líneas de este resumen deben ser una conclusión definitiva sobre lo evaluado.

La tercera sección es el **Resumen de las vulnerabilidades**, el cual cumple el mismo objetivo que en las anteriores propuestas. De manera precisa y concisa agrupar las vulnerabilidades encontradas según sus características, incluyendo gráficos y números totales para que el lector pueda ver de manera rápida cuanto trabajo hay que realizar para remediar los hallazgos encontrados. Esto también debe permitir tener una visión rápida del riesgo promedio en que la empresa se encuentra. Este resumen debe ser simple para el lector.

La cuarta sección son los **Detalles de los evaluadores**. Es importante el aporte que InfoSEC agrega acá dado que indica que es necesario indicar los nombres de los evaluadores que realizaron las pruebas con la finalidad de que el área TI se pueda comunicar con ellos directamente en caso de tener dudas o dificultades entiendo alguno de los hallazgos. Incluso indica que según las normas del CHECK de Inglaterra esto es obligatorio (Centre, 2017).

La quinta sección es **Herramientas utilizadas**. Esta sección permite al lector entender que herramientas y procedimientos utilizados durante la evaluación y en caso de que sea necesario reproducir las pruebas realizadas por los pentesters. Es importante destacar que no se realiza una explicación exhaustiva de su uso, tan solo se indica el nombre de la misma y la versión utilizada. La sección que va de la mano con esta es el **Alcance del servicio**, que al igual que en las otras propuestas indica lo que se evaluó y lo que no se evaluó.

Finalmente, la parte más importante: **Cuerpo del reporte**. Es en esta sección donde se busca detallar todos los hallazgos encontrados para que el equipo técnico del cliente pueda resolverlos y entenderlos. Es necesario indicar cada vulnerabilidad por separado, con su respectivo impacto, riesgo, que tan posible es que esta vulnerabilidad sea explotada, y que tan complejo es resolver la vulnerabilidad. Adicional a estos detalles es importante indicar un resumen de la vulnerabilidad y todos los activos que se ven afectados por la misma. Finalmente es importante adjuntar la evidencia necesaria y sus recomendaciones de remediación.

Aportes Principales

Puntualmente se pueden extraer los siguientes aportes:

- El formato (gráfico) del informe debe estar acordado con el cliente.
- Un fuerte enfoque ejecutivo versus uno técnico.
- Indicar los contactos que realizaron las evaluaciones para apoyar en caso de ser necesario.

CAPÍTULO 3

Metodología

Para realizar una propuesta de estándar para los entregables de un servicio de test de penetración web se realizará el siguiente plan de trabajo.

Una correcta elaboración de una propuesta de estándar nacional debe considerar contextualizar toda esta información en el escenario país, por lo mismo se realizó considerando tres entrevistas a distintos profesionales que realizan estas actividades, los tres pertenecientes a importantes empresas nacionales, en particular E-Sign¹¹, Entel CyberSecure¹² y Aiuken Solutions Chile¹³. Como estos profesionales no son los únicos actores involucrados en la solución se conversó con una empresa cliente de estos servicios: Entel S.A.¹⁴. En estas entrevistas se destacaron sus expectativas y sus experiencias al momento de recibir estos entregables.

Para comenzar a desarrollar este framework, se declara un marco teórico, el cual tiene por objetivo de que el lector esté alineado con los conceptos, terminología, definiciones, procesos y servicios que se desarrollan durante el transcurso de un test de penetración web. Luego de definir el marco teórico se presentará un cuadro comparativo acompañado de los resultados del análisis realizado entre las distintas propuestas existentes de entregables para estos servicios, indicando sus respectivos componentes, metodologías y propuestas de cada uno. Se realizó esta comparación destacando sus ventajas y desventajas en cada componente con la finalidad de extraer lo mejor de cada una de ellas.

Con la información recopilada de diversas soluciones a este problema a lo largo del mundo y sumado a la experiencia en actores nacionales se normalizó la información para proponer los componentes y estructura de los entregables desde un punto de vista Cliente y Proveedor orientado a un contexto nacional.

Una vez finalizada la propuesta, se realizó una validación ejecutando un test de penetración de seguridad y entregando los resultados a un cliente voluntario y anónimo, recopilando su apreciación y resultados. La anonimidad del cliente es necesaria dada la sensibilidad de los datos presentados. Este reporte se presentó a los actores y se recopilaron sus recomendaciones y opiniones, solicitando una validación profesional sobre la propuesta.

¹¹ <https://www.e-sign.cl/>

¹² <http://www.entel.cl/ciberseguridad/>

¹³ <http://www.aiuken.com/>

¹⁴ <http://www.entel.cl/>

Marco Teórico

A continuación, se presentan conceptos y terminologías que surgieron durante la entrevista a los profesionales, clientes y en base a la experiencia de quien escribe esta memoria.

Estándar: Por definición un estándar es "algo que sirve como tipo, modelo, norma, patrón o referencia". La importancia de un estándar es establecer líneas bases entre los participantes de una solución o un sistema, en esencia es la acción de ponerse de acuerdo en cómo hacer algo. Estándares existen para muchas situaciones, tales como desarrollar un producto, entregar un servicio, desarrollar material, programar software, protocolos de comunicación entre muchos otros. Existe un organismo llamado la Organización Internacional de Normalización (ISO por sus siglas en inglés) que busca crear estándares internacionales para su libre uso.

Uno de los ejemplos de estándar más conocidos es la ISO27001, la cual tiene como objetivo especificar los requisitos para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Este estándar representa una serie de acuerdos generales de cómo debiese una empresa u organización establecer procedimientos para proteger y gestionar la información que se utiliza a diario. Otro estándar conocido es el ISO9001, el cual tiene como objetivo especificar los mismos requisitos que la ISO27001, pero para el Sistema de Gestión de la Calidad (SGC). En Chile existen más de 537 empresas certificadas (Tecnológico, 2017) en este estándar. Sin embargo, la organización ISO no es la única que establece estándares, existe el Instituto de Ingeniería Eléctrica y Electrónica (conocido como IEEE) quien ha introducido varios estándares para que la industria de la tecnología utilice los mismos mecanismos, protocolos y acuerdos para que independiente de quién desarrolle una tecnología, estas sean compatibles entre sí. Uno de los estándares más conocidos es el IEEE 802.11, el cual especifica las normas de funcionamiento y comunicación de las interfaces inalámbricas WLAN. Existen más organizaciones para diversos estándares, como Web, construcción de edificios, aviones, etcétera.

Finalmente, el estándar permite al grupo humano y tecnológico lo siguiente:

- Compartir expectativas de construcción, recepción y operación.
- Entregar un marco de trabajo en común que permite que los trabajos sean compatibles entre sí independiente de quién los construye.
- Ahorrar tiempo y esfuerzo en acordar terminologías, procedimientos, entregables, etcétera.

Seguridad de la Información: La seguridad de la información es un concepto bastante amplio y no simple. Abarco múltiples aspectos sobre el cuidado, protección y manejo de la información. Sin embargo, existen tres conceptos que engloban las actividades para mantener la seguridad de la información: Integridad, Confidencialidad y Disponibilidad. A estos tres conceptos en conjunto se les dice “La tríada de la seguridad de la información”.

Tríada de la seguridad de la información: La tríada de la seguridad es un modelo basado en las tres propiedades que tiene la información. Este modelo permite dimensionar los tres aspectos en que la información, como activo de empresa, puede verse comprometida (INFORMATICA, 2017).



Ilustración 2: Tríada de la Seguridad de la Información

Fuente: InfoSegur

La **confidencialidad** de la información es la propiedad que determina quién tiene acceso a los datos, tiene por objetivo determinar los permisos para su respectivo acceso. Un caso común al hablar de confidencialidad de la información es por ejemplo los proyectos de propiedad intelectual de una empresa. Es claro que para una entidad esto es información confidencial y sólo debe ser manejada por un grupo reducido de la empresa y sus

respectivas partes interesadas. Si por algún motivo esta información fuese filtrada por algún funcionario o interceptada por un externo se estaría violando la propiedad confidencial de la misma.

La **integridad** de la información es la propiedad que busca mantener los datos íntegros a lo largo de todo su ciclo de vida, esto quiere decir que solo puede ser modificada por aquellas personas y entidades que tengan autorización para hacerlo. En caso de que un actor no autorizado realice modificaciones a algún dato se estaría violando la propiedad de integridad de la misma. Un ejemplo simple de esto sería cuando un alumno modifica su plantilla de notas antes de entregársela a sus padres. El alumno estaría violando la integridad de la información quien solo tiene autorización el profesor para modificar estos datos.

Finalmente existe la **disponibilidad**. La disponibilidad es la propiedad de la información que indica que los datos deben estar disponibles para ser accedidos, modificados o transmitidos en cualquier instante en que las personas con autorización lo requieran. Cualquier actividad (deseada o indeseada) que evite que la información sea accedida por las partes autorizadas es una violación directa a la disponibilidad de información.

Protección de la tríada: La consultora Deloitte divide las actividades para proteger la tríada de seguridad de la información en 3 pilares: Estar seguro, ser vigilante y ser resiliente (Deloitte, 2014).

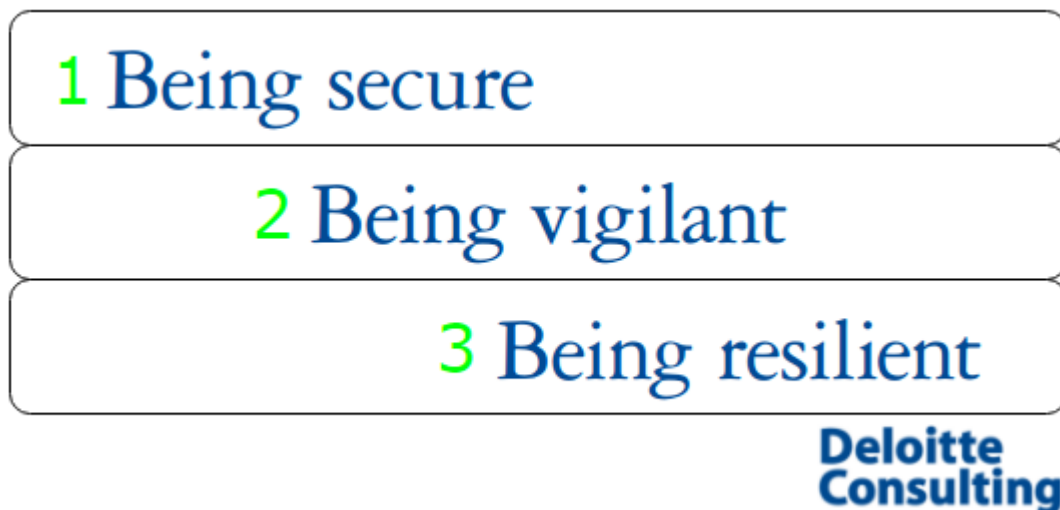


Ilustración 3: Pilares de la Seguridad según la consultora Deloitte
Fuente: Elaboración Propia

El primer pilar (Being Secure – Estar Seguro) se categoriza como toda aquella actividad que tiene por objetivo preparar a una organización para estar lo más seguro posible. Actividades más usuales para preparar a una empresa son las siguientes:

- Consultorías de seguridad de la información (Análisis GAP, Preparación del SGSI, Revisión de procesos, etcétera).
- Test de penetración / Servicios de Ethical Hacking.
- Análisis de vulnerabilidades.
- Adopción de normativas de cumplimiento (PCI DSS para manejo de tarjetas de crédito, HIPAA para hospitales, DISA STIG, etcétera).
- Campañas de sensibilización y concientización de la seguridad.
- Desarrollo de políticas y procedimientos de seguridad.
- Preparación de sistemas de monitoreo y mantención (Alertas y casos de uso).
- Actividades de mantenimiento diario (Actualización de la CMDB, revisión de cumplimiento normativo, planes de actualización, planes de mitigación, etcétera).

Estas actividades se realizan de manera preventiva para preparar de la mejor forma a la empresa ante un potencial ataque hacker. Es fundamental destacar que estas actividades deben ser realizadas de manera periódica y recurrente, no son actividades con las cuales basta realizarlas solo una vez, la tecnología cambia, evoluciona, las necesidades de la industria cada día son más exigentes al igual que sus usuarios y los hackers están día a día descubriendo nuevas formas de comprometer empresas.

En base a la analizado en la sección anterior, se hace evidente que no basta con estar seguro, hay que ser vigilante (Beign Viligant). Ser vigilante tiene por objetivo estar monitorizando de manera constante posibles ataques que puedan haber cruzado todas las barreras que se levantaron en el pilar anterior. Nuevos ataques, técnicas y vulnerabilidades nacen día a día.

En el reporte realizado por RiskBased Security publicado a principios del año 2017, llamado *Vulnerability Quickview 2016* (RiskBased Security, 2016) indican que durante el año 2016 se descubrieron más de 15.000 vulnerabilidades, incrementando un 85.3% desde el año 2011. La mayor parte de las soluciones y políticas de seguridad que se implementan durante el primer pilar son en base a ataques conocidos y diseño de escenarios posibles, pero no basta con esto, es necesario estar atento a cualquier

anomalía o comportamiento extraño a nivel de red en caso de que se esté aplicando un nuevo ataque desconocido.

Uno de los conceptos relevantes en este aspecto son los *ZeroDay*, los ZeroDay por definición son todas aquellas vulnerabilidades descubiertas por investigadores de seguridad a las cuales aún no existe un parche oficial por parte del fabricante (desarrollador) del producto en cuestión. Los ZeroDay son una de las mayores amenazas hoy en día en el aspecto de seguridad, ya que en caso de no estar vigilantes a su explotación pueden tener resultados catastróficos.

En marzo del año 2017 se liberó un ZeroDay de severidad crítica que afectaba un software llamado Struts2 (un módulo para presentar páginas web basado en Java). Desde el día de su liberación se detectaron cientos de miles de ataques a lo largo de todo internet, intentando comprometer la mayor cantidad de servidores posibles. Cuando se liberó esta vulnerabilidad el equipo de Struts2 demoró 8 días en parchar la vulnerabilidad, sin embargo, la vulnerabilidad estuvo presente en el software durante 5 años, lo que indica que pudo haber sido explotada con anterioridad sin que ninguna empresa hubiese estado preparada para ello, sin embargo, empresas que poseen un servicio de inteligencia y están vigilantes a estas amenazas pudieron bloquear el ataque sin mayor riesgo. Las actividades más usuales para ser vigilante en una empresa son las siguientes:

- Monitorización de la actividad de red de la organización.
- Monitorización de los registros de auditoría
- Inteligencia sobre el comportamiento de usuarios y activos de la organización.
- Validación de controles de cambios según políticas de seguridad
- Monitorización de cumplimiento normativo

Usualmente estas actividades se llevan a cabo en un lugar llamado Secure Operation Center (SOC), el cual cuenta con servicios 24x7x365 de monitoreo y mantención de los sistemas.

Una empresa u organización que cuenta con estos dos pilares está en buena posición para mantener la tríada de seguridad.

Por otro lado, es virtualmente inevitable que un hacker en algún minuto penetre todas las defensas y sistemas de monitoreo, incluso empresas con impecables sistemas de seguridad y control han sido comprometidas. Sin embargo, el tercer pilar puede ser la diferencia entre un desastre y un incidente de seguridad controlado. El ser resiliente

indica la capacidad para anteponerse a la adversidad, es la habilidad que permite a una empresa recuperarse de un desastre o evitar algún desastre en curso. La resistencia real de la seguridad en una empresa es su capacidad de aguantar golpes, o en este caso, hackeos. En esta área las empresas pueden preparar las siguientes actividades:

- Preparar planes de recuperación de desastres (DRP)
- Entrenar un equipo de respuesta a incidentes de seguridad (CSIRT)
- Preparar un plan de comunicación público efectivo (en caso de filtraciones de información)
- Preparar sistemas de respaldo comunicacional y de infraestructura crítica

Finalmente, una empresa capaz de estar preparada, ser vigilante y ser resiliente está realizando su mayor esfuerzo por proteger la tríada de seguridad de la información. Algo importante destacar de estos tres pilares es que para ser implementados es necesario poseer un nivel de maduración empresarial/tecnológico importante, ya que de ser implementados de golpe puede tener un gigantesco costo monetario y cultural a los procesos propios de la empresa. Se recomienda avanzar paso a paso, primero ser Seguro mediante los servicios propuestos, luego ser Resiliente y finalmente Vigilante. Esto es un consejo que nació de la entrevista con los especialistas de seguridad al momento de presentar los tres pilares de seguridad.

Servicios de Test de penetración y Hacking Ético: Esta memoria se concentrará en el primer pilar (Estar Seguro) y en particular en el servicio de Test de penetración y Servicios de Ethical Hacking. Es importante en este punto dar respuesta a una de las mayores consultas por parte de los clientes con respecto a estos servicios.

¿Cuál es la diferencia entre Hacking Ético (Ethical Hacking) y los de test de penetración (pentesting)?

En la industria se ofrecen de dos formas: Como si fuesen lo mismo y como servicios separados. Luego de múltiples conversaciones con los prestadores de servicios y los clientes se propone la siguiente distinción:

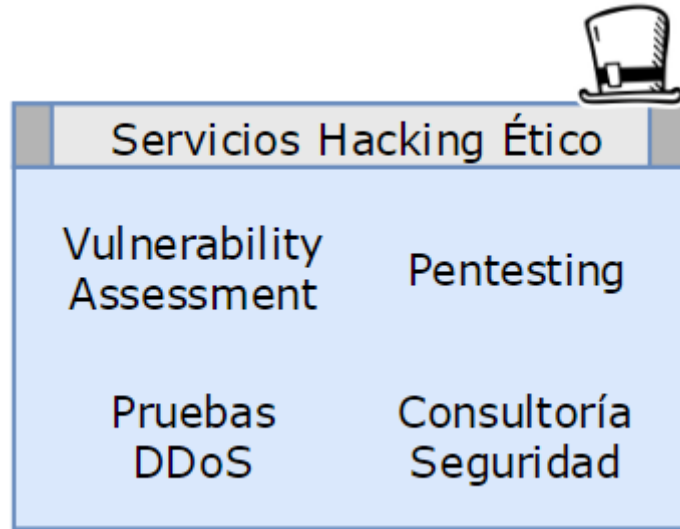


Ilustración 4: Servicios Hacking Ético

Fuente: Elaboración Propia

Los servicios de Hacking Ético son todos aquellos que son ejecutados por Hackers de sombrero blanco (Personas con nivel de "hacker" pero que utilizan su conocimiento y habilidades para proteger en vez de destruir sistemas). Estos servicios pueden ser consultorías de seguridad, revisiones manuales de código fuente de software, detección y evaluación de vulnerabilidades, test de penetración, pruebas de sistemas de manera exhaustiva, pruebas de denegación de servicios, entre otras actividades.

En particular los test de penetración son uno de los tantos servicios que los Hackers Éticos pueden entregar, tienen por objetivo comprometer un sistema computacional interrumpiendo así la tríada de seguridad de la información.

Servicio de Test de penetración: Durante un test de penetración se realizan una serie de actividades con la finalidad de detectar potenciales vulnerabilidades que permitan a un atacante violar la tríada de seguridad de la información. El profesional debe realizar la actividad de manera ética y con sumo cuidado, reportando así todos los hallazgos y con el mayor detalle.

De manera resumida, un test de penetración se compone de los siguientes pasos:



Ilustración 5: Pasos de un Test de penetración

Fuente: Nouaman Hini

- **Reconocimiento:** Es la actividad de conocer al objetivo de manera pasiva y no invasiva.
- **Escaneo:** Generar un listado de posibles puntos vulnerables para ganar acceso, colocando énfasis en aquellas que permiten comprometer al sistema.
- **Ganar Acceso:** Es explotar las vulnerabilidades enumeradas con el fin de obtener acceso interno.
- **Mantener acceso:** Una vez dentro del sistema, es necesario crear una puerta trasera o algún mecanismo para volver a entrar a diestra y siniestra.
- **Borrar huellas:** Eliminar cualquier rastro que pueda alertar a la víctima que ha sido comprometida.

Un test de penetración se puede ejecutar desde múltiples puntos de vista, como por ejemplo simular un ataque al perímetro expuesto a internet de una empresa (test de penetración externo). Esta actividad permitirá a la empresa entender cuál es su exposición a hackers de todas partes del mundo que deseen comprometer a la empresa. Otra actividad bastante común es un simular un ataque desde el interior de la empresa (test de penetración interno), actuando como si un *insider* fuese el atacante. Un *insider* es usualmente algún empleado descontento con la empresa o que está a punto de ser reclutado por la empresa rival. El test de penetración interno permite a una empresa

saber cuál es su exposición al riesgo desde dentro de sus propias redes, con accesos limitados.

Durante el test de penetración, interno o externo, el experto pondrá ojo en cualquier activo de la empresa que le permita obtener información o ganar un mayor control sobre la red objetivo. Sin embargo, durante la etapa de Identificación (paso 1 de **Ilustración 5: Pasos de un Test de penetración**) existe un especial énfasis a servidores con puertos de comunicación no encriptados, routers de comunicación y aplicaciones web.

Proyecto OWASP TOP10: Evaluación seguridad Web: El proyecto OWASP TOP10 (Open Web Application Security Project - TOP10 Vulnerabilities) es una de las consideraciones a tomar en cuenta cuando se habla de tests de penetración web. El proyecto realiza un estudio cada tres años indicando cuales son las 10 vulnerabilidades más comunes detectadas en los sitios web. La última versión fue desarrollada el año 2013, sin embargo, sigue siendo vigente hasta el día de hoy. Según el estudio las 10 vulnerabilidades más comunes son:

1. Inyecciones de código
2. Manejo incorrecto de sistemas de autenticación y sesiones
3. Cross-Site Scripting
4. Referencia insegura a objetos
5. Configuraciones inseguras de seguridad
6. Exposición de datos sensibles
7. Control incorrecto de niveles de usuario
8. CSRF
9. Utilización de componentes con vulnerabilidades conocidas
10. Redirecciones no validadas

Una correcta evaluación de seguridad debiese revisar como mínimo la presencia de estas 10 vulnerabilidades.

Test de penetración Web (OWASP Testing Methodology): Un test de penetración web es una sub actividad de un test de penetración normal, cuyo objetivo es el comprometer y corroborar que los controles de seguridad y validación puestos en una determinada aplicación web mantengan la tríada de seguridad intacta. Este proceso considera realizar

un análisis exhaustivo de cualquier vulnerabilidad, amenaza, falla técnica o debilidad que presente una determinada aplicación web.

Existe una metodología llamada *OWASP testing methodology*, la cual tiene por objetivo presentar un estándar para realizar tests de penetración web. La guía busca que las evaluaciones sean consistentes, reproducibles, rigurosas y que estén bajo un control de calidad constante, especificando cuáles son las etapas y fases para realizar un pentesting web (OWASP, 2016)¹⁵.

A grandes rasgos, la metodología incluye 11 categorías a ser evaluadas, cada una con su respectivo identificador.

Tabla 1: Códigos de OWASP Testing Methodology Guide, Fuente: OWASPPProject

Categoría	Código
Recolección de información	OTG-INFO
Test de configuración y despliegue del servidor	OTG-CONFIG
Controles de identidades	OTG-IDENT
Controles de autenticación	OTG-AUTHN
Controles de autorización	OTG-AUTHZ
Manejo de sesiones	OTG-SESS
Validación de entradas de usuario	OTG-INPVAL
Manejo de errores	OTG-ERR
Criptografía en comunicaciones y almacenamiento de información	OTG-CRYPT
Controles de la Lógica de la aplicación	OTG-BUSLOGIC
Controles por el lado de cliente	OTG-CLIENT

¹⁵ https://www.owasp.org/index.php/Web_Application_Penetration_Testing

Al momento de descubrir alguna vulnerabilidad durante esta ejecución es importante indicar en cuál etapa fue descubierto. Para ello recomienda utilizar las siglas de Tabla 1: Códigos de OWASP Testing Methodology Guide.

Test de penetración web caja negra, gris y blanca: Este tipo de test es sin ninguna información adicional más que un punto de partida, el cual puede ser la URL del sitio web o su dirección IP/Dominio. La labor del *pentester* es intentar penetrar el sistema sólo con la información disponible en internet o en los mismos sistemas. Este tipo de evaluación permite entender cuál es su exposición de la aplicación web a agentes completamente ajenos a la empresa.

Test de caja gris: Los test de caja gris son aquellos con credenciales limitadas de sistema, es una extensión del test de caja negra. En esta evaluación no sólo se tiene la URL del sitio web o su dirección IP/Dominio, sino que además el *pentester* tiene ciertas credenciales de usuario válidas que fueron entregadas por el cliente. Este tipo de evaluación permite entender cuál es la exposición de la aplicación web desde empleados con sus credenciales comprometidas o riesgos de un *insider*.

Usualmente este tipo de evaluación se solicita cuando la aplicación web a ser evaluada existe detrás de un "Inicio de sesión" y es necesario evaluar el contenido interno. Cabe destacar que esta evaluación debiese comenzar con un test de caja negra y utilizar las credenciales una vez que el test de caja negra ha acabado.

Test de caja blanca: Este tipo de test son aquellos en que cuentan con completo acceso al sistema a ser evaluado, con credenciales de usuario hasta administrador, acceso al código fuente y a *logs* del sistema. Sin duda este es la evaluación más completa de las tres y la que permite detectar la mayor cantidad de vulnerables posibles en la aplicación web, pero también es la más larga y costosa de realizar.

Herramientas de Evaluación de Seguridad web: Para realizar estos test de penetración web existen herramientas en el mercado que facilitan la detección de vulnerabilidades. Estas herramientas son capaces de realizar miles de pruebas por segundo, y descubrir vulnerabilidades que a un humano puede tardar días en realizarlo. Es por eso por lo que muchas empresas basan sus análisis de seguridad en los resultados que estas herramientas entregan, sin embargo, no es suficiente.

Estas herramientas cuentan con una gran base de datos con cientos de pruebas predefinidas para evaluar una aplicación web, pero estas pruebas son genéricas. Cada aplicación web es única en su diseño, propósito y el negocio que sustenta, por lo que la realización de pruebas manuales y específicas es altamente recomendable para tener una visión holística del real riesgo de seguridad que la aplicación tiene.

Es importante destacar que un porcentaje de las vulnerabilidades que estas herramientas encuentran son falsos positivos. Por definición, los falsos positivos son hallazgos o pruebas que se consideran verdaderas, pero luego se demuestran falsas, por lo que es importante corroborar manualmente cada una de las vulnerabilidades detectadas por la herramienta con el fin de que el reporte sea lo más realista posible.

Vulnerabilidad de Seguridad: A lo largo del marco teórico se ha mencionado la palabra vulnerabilidad unas cuantas, de veces, por lo que es importante definirla. Una vulnerabilidad, desde el punto de vista de seguridad de la información, es toda aquella situación que ofrece la posibilidad de realizar ataques contra un sistema. Esto incluye desde fallas de programación en software, virus, contraseñas por defecto, sistemas configurados de manera incorrecta, errores humanos al compartir información, hasta incluso las notas adhesivas pegadas en las pantallas de los usuarios.

Las vulnerabilidades tienen múltiples características, tales como el Riesgo, Severidad, un identificador, rango de activos que son vulnerables, explotabilidad de la vulnerabilidad, categoría, etcétera. Todas estas propiedades serán discutidas durante la definición de los entregables más adelante en la memoria.

Análisis de los entregables de Servicio

Todos los servicios presentados en la sección anterior deben tener algún entregable tangible, ya sea un informe, una serie de vídeos, evidencias fotográficas, etcétera. Para esta memoria se estudiaron las siguientes propuestas de entregables y fueron compartidas con los especialistas de seguridad, quienes aportaron con su conocimiento.

La Tabla 2: Documentos de ejemplos reportes de vulnerabilidades. contiene los diversos documentos analizados para generar el estándar propuesto en la memoria. Adicionalmente se complementó con la experiencia del memorista desarrollando esta actividad.

Tabla 2: Documentos de ejemplos reportes de vulnerabilidades. Fuente: Elaboración propia

Documento	Autor
Writing a penetration testing report	SANS Institute
Penetration Test Report	Offensive Security
Reporting	Pentest-Standard.org
The art of writing Penetration test reports	INFOSEC Institute

Documento	Autor
Qualys ENTERPRISE Scan Report	Qualys
Acunetix Web Application Security - Developer Report	Acunetix

Los documentos analizados están disponibles en internet y son de uso público. Los primero cuatro documentos de la tabla son ejemplos que las mismas instituciones elaboraron a modo de ejemplo, y los últimos dos, son reportes de ejecuciones directas de las herramientas Qualys¹⁶ y Acunetix¹⁷, conocidas herramientas profesionales de evaluaciones de vulnerabilidades web. Es importante destacar que las herramientas sólo emiten reportes técnicos dado que no tienen inteligencia ni contextualización del negocio, pero para fines de esta memoria sirvieron para la sección técnica de los reportes.

A continuación, se presentan los resultados del análisis y el armado de una propuesta formal para el desarrollo de entregables para los test de penetración web. Se tratarán en el siguiente orden:

- Estilo de reporte
- Secciones del reporte
- Detalle de las secciones
- Presentación de las Vulnerabilidades

Análisis sobre el estilo de Reporte

Aterrizar algo altamente técnico como un test de penetración al público objetivo no es una tarea fácil. En los distintos reportes analizados existen visiones distintas del “*Cómo reportar lo encontrado*”. En la propuesta de Offensive Security realizan una narración lineal de la actividad realizada por los hackers, mostrando en cada punto que fue lo que pudieron penetrar desde un punto de vista altamente técnico, mostrando evidencia por cada hallazgo que realizaban. Dedicar un par de párrafos a dar una visión general de lo ocurrido indicando el riesgo para que la audiencia no-técnica tenga una noción de riesgo.

Esto se contrasta a los reportes presentados por SANS y Pentest-Standard, en donde existe una gran dedicación a explicar a de manera detallada las condiciones, suposiciones

¹⁶ <https://www.qualys.com/>

¹⁷ <https://www.acunetix.com/>

y alcance de la evaluación, dejando para la sección técnica el detalle individual de cada vulnerabilidad detectada. Obviamente un reporte va orientado a la audiencia técnica y otra a la gerencial. En resumen, Offensive Security se presenta una bitácora de eventos de un hacker, en cambio sus contrapartes SANS y Pentest-Standard están más orientados al riesgo por activo vulnerable, pero...

¿Cuál utilizar?

Para responder esta pregunta es necesario entender cuál será el público objetivo de esta evaluación y cuál es la finalidad de realizar esta actividad. Existen casos en que el cliente quiere saber qué tan lejos podría llegar un atacante penetrando sus redes y otros en los que el cliente necesita presentar un informe de seguridad a algún tipo de empresa auditora o algún cliente que le esté exigiendo la evaluación.

Esta situación hace evidente que ambas son necesarias, pero por separado y no juntas. Los tres informes analizados mezclan la sección gerencial y la técnica en el mismo entregable, jesto significa que el mismo documento tiene dos audiencias distintas! Se propone separar el informe en dos documentos distintos, que puedan ser completamente separables dependiente de la audiencia: Un **informe ejecutivo** e **informe técnico** por separado.

En general, la audiencia técnica tiene un mayor interés en remediar las vulnerabilidades, tener claridad dónde debe actuar y cuáles son los pasos que seguir para mitigar el problema, versus una audiencia gerencial cuyo interés está enfocado en entender el riesgo en general al cual están expuestos y el plan estratégico propuesto a seguir desde un punto de vista de seguridad y negocio.

Con esta separación se presenta una de las primeras definiciones para este estándar de entregables:

DEF-1

Los informes de seguridad deben ser dos ejemplares: Un informe ejecutivo y un informe técnico.

El informe ejecutivo debe proveer una visión estratégica y de riesgo general sobre el entorno evaluado sin entrar en detalles técnicos, versus un informe técnico que está enfocado a entender las vulnerabilidades y ubicar dónde se deben realizar las mejoras.

El informe técnico debe ser escrito con una visión explicativa de la situación de seguridad de los activos de la empresa, describiendo de manera específica cuáles son las vulnerabilidades encontradas y la respectiva severidad de cada una de ellas.

Este informe como mínimo debe explicar los tecnicismos de las vulnerabilidades detectadas y sus respectivas recomendaciones de mitigación, identificando de manera precisa el activo o activos vulnerables colocando énfasis en el impacto de lo que pudiese ocurrir en caso de que se pueda explotar la vulnerabilidad. En la siguiente sección de la memoria se especifica la manera de presentarlos y en cual sección debiesen estar presentes.

Una de las consideraciones al momento de realizar el informe técnico es de qué manera la empresa que lo recibirá tiene distribuidas las responsabilidades. Para ejemplificar esto imaginar que un cliente tiene 10 páginas web que necesitan ser auditadas, existe la posibilidad de que el cliente tenga 10 responsables distintos, entonces hace sentido agrupar las vulnerabilidades encontradas por página web para que puedan distribuir el informe técnico por cada uno de los responsables. ¿Qué ocurre si las 10 páginas web tienen responsables por módulos? Es decir, existe un responsable del *back-end*¹⁸, otro es responsable del servidor (hosting) y otro del *front-end*¹⁹. En este caso hace sentido desarrollar el informe agrupando vulnerabilidades por cada módulo. Es por esta razón que al momento de desarrollar el informe es importante acordar con el cliente cuál es la audiencia del informe técnico.

DEF-2

Pentester: Acordar con el cliente como necesita que se agrupen las vulnerabilidades en el informe técnico según su audiencia.

Cliente: Tener claridad de cómo repartirá el informe técnico según lo encontrado.

Tan importante como tener un informe técnico detallado es importante entender las necesidades de un informe ejecutivo. El informe ejecutivo debe tener una especial consideración en su audiencia, la cual no es técnica. Este informe no debe utilizar en ningún tecnicismo a menos que sea estrictamente necesario, la audiencia de este informe necesita responder de manera simple y eficiente las siguientes preguntas:

- ¿Qué fue lo que se evaluó?
- ¿Cuál fue el alcance de las pruebas?

¹⁸ Bases de datos y procesamiento de la información de una página

¹⁹ Sección visual de la página.

- ¿Cuándo se evaluó?
- ¿Cuál es el riesgo al cual está expuesta la empresa?
- ¿Dónde debo priorizar?

Desde el punto de vista de la gerencia es importante entender cuál fue la extensión de lo evaluado para que exista una contextualización de lo que se discutirá en el informe. Para una empresa puede ser distinto un informe crítico de seguridad en alguna sucursal a el mismo informe crítico sea de su casa central. Por otra parte, es importante entender el alcance de las pruebas acordadas y lo que está fuera del alcance para no causar confusión sobre lo que fue evaluado y lo que no.

La respuesta a la tercera pregunta permite a los lectores del informe entender el periodo sobre el cual se realizaron las pruebas y estas vulnerabilidades tienen sentido. Esta información también entrega una temporalidad que permitirá ubicarse al momento de leer este informe en el futuro y poder compararlo con otras ejecuciones en fechas posteriores.

La cuarta respuesta indica el riesgo cibernético al cual la empresa está expuesta. Es importante en este punto realizar una distinción entre riesgo y severidad. El riesgo tiene una relación inescrutable con el negocio y su funcionamiento, este indica el impacto que existe caso de que una o varias vulnerabilidades sean explotadas con repercusiones sobre la continuidad de su negocio y en el peor de los casos, pérdidas monetarias. Para calcular el riesgo es necesario contar con la severidad de las vulnerabilidades y la importancia que ese activo representa para el negocio. La severidad tiene relación con el impacto técnico y la posibilidad de explotación que tenga una vulnerabilidad en el activo. Es posible que una vulnerabilidad sea categorizada como crítica pero que su riesgo sea substancialmente bajo para el negocio. Un ejemplo de esto puede ser una vulnerabilidad en un Acceso *WiFi* de una cafetería, la cual tiene una vulnerabilidad trivial que permite al atacante realizar una denegar el servicio (*DDoS*) y cortar todo acceso *WiFi* del lugar. Si este acceso *WiFi* está pensando para los clientes, es probable que no sea un activo crítico en el correcto funcionamiento de la cafetería. En esta situación se declara una vulnerabilidad de severidad Alta (fácil de explotar y genera disrupción completa del servicio) sin embargo su riesgo es bajo para la cafetería. Esto no significa que no deba ser solucionada, pero debiese tener una menor prioridad sobre vulnerabilidades que afecten al negocio.

La definición de la severidad queda a disposición del *pentester* y el riesgo debe ser calculado en conjunto con el cliente. Para calcular el riesgo se presenta la siguiente matriz basada en lo especificado en el NIST 800-30²⁰:

Matriz de Riesgo		Impacto Organizacional		
		Alto	Medio	Bajo
Severidad Técnica	Alto	Alto	Medio	Bajo
	Medio	Medio	Medio	Bajo
	Baja	Bajo	Bajo	Bajo

Ilustración 6: NIST 800-30 Matriz de Riesgo, Fuente: Elaboración Propia

DEF-3

Pentester: Presentar la severidad de la vulnerabilidad considerando su factibilidad de explotación y el impacto técnico que tiene esta explotación.

Cliente: Calcular el riesgo de la vulnerabilidad en base a su impacto de explotación a nivel empresa.

Análisis sobre las secciones del Reporte

Luego de realizar una lista de los componentes que se encuentran presentes en los reportes fue evidente que hay algunos que se repiten y otras que son únicas de cada uno de ellos. Las secciones en común son:

- Introducción
- Alcance del Trabajo
- Objetivos del Servicio
- Metodología
- Riesgo Consolidado
- Hallazgos Generales

²⁰ <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

- Hallazgos Detallados
- Recomendaciones Generales
- Conclusiones
- Anexos

Las secciones únicas de cada informe fueron:

- Control Documental
- Acuerdos
- Narración de la evaluación
- Hoja de ruta estratégica
- Información de Contacto
- Explotación

Un informe que contenga toda esta información no necesariamente es un buen informe. El documento debe entregar la información suficiente para cumplir el requerimiento que el cliente tiene. Es probable que no exista interés en contar con una hoja de ruta estratégica, ya que el cliente planificará la estrategia para afrontar lo detectado con el oficial de seguridad de la empresa. Existirán casos en que al cliente no necesitará el informe ejecutivo ya que los resultados irán directamente a la sección técnica para remediar. Por otra parte, realizar el informe completo significa bastante trabajo para el *pentester*, por lo que para lograr un común acuerdo sobre las secciones a entregar es un ahorro de tiempo para quien escribe y quien lee.

Para resolver esta situación de manera estratégica, se propone acordar con el cliente las secciones que hacen sentido a ser entregadas basado en sus necesidades. Algunas secciones se declararán como mínimas para mantener el objetivo de que los informes sean comparables en el tiempo e independiente de su ejecutor, sin embargo, otras secciones serán opcionales y quedarán disponibles para ser utilizadas posterior a común acuerdo entre cliente y *pentester*.

DEF-4

Pentester: Entender cada una de las secciones y orientar al cliente cuales mejorarán el objetivo que desea cumplir.

Cliente: Considerar el objetivo de esta evaluación e indicar las secciones que permitirán obtener la información necesaria.

La tabla 3 cuenta con un listado de secciones y su importancia en cada uno de los documentos. Se marcó como "Necesario" a aquella sección que debe estar presente en el informe, como "Opcional" a aquel elemento opcional y como "No" a aquellas secciones que no debiesen ser incluidas en el informe. Es importante destacar que, si bien la lista presenta 16 secciones, esto no quiere decir que exista alguna limitación a sólo lo presente en la lista, tanto el *pentester* como el cliente pueden agregar nuevas si así lo amerita, sin embargo, para ser compatibles con el framework, deben cumplir con las secciones obligatorias.

Cada sección de la Tabla 3 se discutirá a continuación de la misma en el siguiente punto y contendrá un ejemplo aportado por uno de los *pentesters* entrevistados. Hay que considerar que el informe técnico y el ejecutivo son documentos por separado, por lo que se marcará a cuál informe pertenece cada uno. De manera adicional es importante mencionar que esta tabla no establece el orden lógico en que las secciones deben presentarse ya que eso queda a criterio del *pentester* y el orden en que desee presentar los resultados. Finalmente, tampoco se consideran secciones básicas pertenecientes a un escrito, así como índice, portada, contraportada, etcétera.

Tabla 3: Secciones de un informe ejecutivo y técnico. Fuente: Elaboración Propia

Sección	Informe Ejecutivo	Informe Técnico
Introducción	Necesario	Necesario
Alcance del Trabajo	Necesario	Necesario
Hallazgos Generales	Necesario	Necesario
Acuerdos	Necesario	Necesario
Conclusiones	Necesario	Necesario

Sección	Informe Ejecutivo	Informe Técnico
Recomendaciones Generales	Necesario	Opcional
Objetivos del Servicio	Necesario	Opcional
Riesgo Consolidado	Necesario	Opcional
Metodología	Opcional	Necesario
Hallazgos Detallados	No	Necesario
Anexos	No	Opcional
Control Documental	Opcional	Opcional
Hoja de ruta estratégica	Opcional	Opcional
Información de Contacto	Opcional	Opcional
Narración de la evaluación	No	Opcional
Explicación de Explotación	No	Opcional

DETALLE DE LAS SECCIONES:

Sección: Introducción

Ficha	Introducción
Informe Ejecutivo	Necesario
Informe Técnico	Necesario
Descripción	Independiente si se está realizando un informe de seguridad o un documento, cualquier escrito dirigido a un grupo de personas debe tener una introducción adecuada, en donde quede de manera clara y explícita el propósito del documento y la audiencia a la cual está focalizado. La introducción además cumple con el objetivo ser una puerta de entrada al lector, invitándolo a leer el texto y preparándolo para lo que va a leer. En ciertas ocasiones a esta sección también se le llama Contexto, lo que es válido dado que cumple el mismo objetivo.
Ejemplo	Introducción “En el marco del proceso interno de revisión realizado por [cliente], la empresa [proveedor] ha desarrollado distintas actividades con el objetivo de presentar información valiosa en lo que respecta al estado actual de la seguridad de la información de la aplicación web [url]. Este documento tiene por objetivo orientar a la alta gerencia de [cliente] a mejorar sus controles de seguridad.” [...]

Sección: Alcance del Trabajo

Ficha	Alcance del Trabajo
Informe Ejecutivo	Necesario
Informe Técnico	Necesario
Descripción	La sección “alcance del trabajo” debe especificar de manera clara cuál fue la extensión de la actividad indicando cuales aplicaciones web fueron parte del test de penetración web, las actividades que se realizaron, el periodo de tiempo en la cual se realizaron y lo que está fuera del alcance. Esta última parte permite al entender que cosas no fueron evaluadas durante la ejecución del test de penetración y así no generar falsas expectativas de la actividad realizada.
Ejemplo	Alcance del Trabajo “El alcance de este trabajo y los entregables fueron: • Ethical Hacking de una (1) aplicación web ([URL]) desarrollada por el cliente, analizada entre los días [periodo de tiempo] del año [año]. • Verificar la mitigación de las vulnerabilidades detectadas en el informe técnico [informe de comparación], realizado por la empresa [otro_proveedor] el año [año]. • Entrega de un Informe ejecutivo y otro técnico, el cual permita a la empresa [cliente] mejorar la seguridad de su plataforma web. Lo que está fuera del alcance es lo siguiente: Pruebas de denegación de servicio sobre la plataforma web.” [...]

Sección: Hallazgos Generales

Ficha

Informe Ejecutivo

Informe Técnico

Descripción

Hallazgos Generales

Necesario

Necesario

Los hallazgos son aquellas desviaciones de seguridad detectadas durante la ejecución del test de penetración, cada vulnerabilidad detectada representa un hallazgo.

La sección de hallazgos generales se representa mediante gráficos de torta, de barras o históricos. Esta sección debe permitir al lector entender la situación actual de manera global a nivel de hallazgos y los respectivos puntos vulnerables. Si la evaluación está considerando una ejecución anterior es necesario denotar la evolución desde la última evaluación a la actual.

Esta sección es necesaria en ambos informes para entender la globalidad de la situación a nivel de hallazgos y cuantas vulnerabilidades están presentes.

Ejemplo

Resumen de Vulnerabilidades

A continuación se presenta un cuadro resumen con todas las vulnerabilidades encontradas; separadas y catalogadas por su origen y severidad.

		Vulnerabilidades			
		Severidad			Total
		Alta	Media	Baja	
Origen	Aplicación	0	0	0	0
	Configuración	0	0	5	5
	Versión	0	0	2	2

Severidad

Alta 0%
Media 0%
Baja 100%

Origen

Versión 29%
Aplicación 0%
Configuración 71%

■ Alta ■ Media ■ Baja ■

■ Aplicación ■ Configuración ■ Versión

Sección: Acuerdos

Ficha	Acuerdos
Informe Ejecutivo	Necesario
Informe Técnico	Necesario
Descripción	En caso de que exista algún acuerdo para realizar el test de penetración esta es la sección que debe ser presentados. Los acuerdos son situaciones conversadas entre el cliente y el pentester para realizar la evaluación dentro del tiempo acordado y en las condiciones necesarias. Los atacantes no tienen límite de tiempo al momento de realizar sus fechorías, pero los pentesters sí. Cualquier situación especial que se tuvo que acordar entre ambas partes debe estar presente en esta sección. Para el informe ejecutivo basta con indicar las condiciones bajo las cuales se realizaron las pruebas, para el informe técnico es necesario detallar de manera explícita todos los acuerdos y salvedades que se necesitaron para realizar la actividad.
Ejemplo	Acuerdos “Para la correcta evaluación de la aplicación web se desactivó el Web Application Firewall, se detectaron vulnerabilidades y se volvieron a probar para revisar si el appliances estaba funcionando de manera correcta. Adicionalmente se necesitaron dos credenciales de usuario para realizar pruebas de movimientos laterales. [...]”

Sección: Conclusiones

Ficha	Conclusiones
Informe Ejecutivo	Necesario
Informe Técnico	Necesario
Descripción	Las conclusiones, como en todo trabajo escrito, entregan valor al documento. Representan la síntesis de lo realizado, indicando los puntos más importantes encontrados y lo que se pudo extraer, en esencia, de la actividad. Esta sección invita al lector a entender las razones de fondo por las cuales las vulnerabilidades y riesgos encontrados están ahí en primer lugar. Si bien un informe puede presentar cientos de vulnerabilidades relacionadas a parches de actualización no instalados y suena obvio que es necesario parchar, la real conclusión que el profesional debe indicar es que no existe una política de parchado de equipos.
Ejemplo	Conclusiones: • infraestructura que soporta al sitio es potencialmente vulnerable y quedará obsoleta a partir del [fecha]. • Dada las vulnerabilidades detectadas es probable que no exista un proceso de Hardening y Mantención de activos en la empresa. • Las vulnerabilidades detectadas el año [fecha] fueron mitigadas con éxito. Cabe señalar que la implementación de certificados digitales presenta oportunidades de mejora que permitirían mitigar vulnerabilidades propias de esta tecnología. [...]

Sección: Recomendaciones Generales

Ficha	Recomendaciones Generales
Informe Ejecutivo	Necesario
Informe Técnico	Opcional
Descripción	La sección de recomendaciones generales tiene por objetivo entregar una visión global de las acciones de alto nivel para mitigar las vulnerabilidades, colocando énfasis en lo más crítico a ser solucionado. No trata de plantear un plan de acción, pero si una estrategia desde el punto de vista de la seguridad de la información. Esta sección debe estar presente en el informe ejecutivo ya que le permite al lector planificar una estrategia, sin embargo, es opcional en el informe técnico.
Ejemplo	Recomendaciones Generales: • Mitigar vulnerabilidades altas referentes a la filtración de código en el sitio. • Mitigar los problemas de configuración existentes tanto en los sitios web, como en el servidor web. • Implementar una política de buenas prácticas (Ej. Eliminar metadatos) para la publicación de archivos de ofimática en internet. • Revisión y análisis de la conectividad en las redes internas, particularmente sobre el acceso compartido con otras empresas. • Revisar las políticas de usuarios en los servidores productivos. • Actualización de software utilizado y compra de licencias originales. [...]

Sección: Objetivos del Servicio

Ficha	Objetivos del Servicio
Informe Ejecutivo	Necesario
Informe Técnico	Opcional
Descripción	La sección de Objetivos del servicio debe indicar, tal como su nombre lo indica, cuáles son los objetivos que se persiguen en el informe a entregar. Estos objetivos pueden variar según la lógica con la cual se requirió el pentest.
Ejemplo	Objetivos del Servicio “La empresa [EMPRESA] ha efectuado un conjunto de actividades para evaluar la seguridad de los sistemas internos y externos de [cliente] (en adelante la [siglas]). Esta actividad tuvo como objetivo identificar y analizar las posibles vulnerabilidades web a las que se encuentra expuesta la empresa para poder ayudarla en su certificación PCI DSS. [...]”

Sección: Riesgo Consolidado

Ficha	Riesgo Consolidado
Informe Ejecutivo	Necesario
Informe Técnico	Opcional
Descripción	El riesgo consolidado es el indicado real de riesgo al cual la empresa está expuesta ante una amenaza cibernética. La forma de denotarlo puede ser desde un puntaje o una nota, sin embargo, la medida debe quedar lo suficientemente clara para que el lector entienda la situación actual de la empresa. Esta sección no solo debe considerar la nota de riesgo, sino que también debe exponer de manera simple y agrupada las diversas vulnerabilidades detectadas durante la evaluación. Un especialista puede encontrar 30 vulnerabilidades distintas, pero si todas representan el mismo riesgo debe indicarse como uno solo y no 30 vulnerabilidades por separado, ya que eso se deja para la sección de hallazgos detallados. Esta sección es necesaria en el informe ejecutivo para que la parte gerencial entienda los diversos riesgos a los que la empresa está expuesta. Es importante no caer en tecnicismos e ir directo a los riesgos. Esta sección es opcional para el informe técnico, entregará un contexto general al especialista, pero no es necesario.
Ejemplo	Riesgo consolidado “Las vulnerabilidades detectadas pueden ser caracterizadas en 4 tipos distintos, presentando riesgos de distinta naturaleza para la [empresa]. Algunos de ellos son más severos que otros, sin embargo, ciertas vulnerabilidades en conjunto pueden ser peligrosas. A continuación, se presentan los impactos potenciales que estas vulnerabilidades representan, agrupadas por tipo de riesgo.”

Ejemplo (Continuación)

- Inyecciones SQL (CRITICO): Las inyecciones SQL permiten a un atacante extraer, modificar o eliminar información almacenada en los servidores. Estas vulnerabilidades fueron notificadas inmediatamente al momento de ser encontradas.
- Identificación de un manejo incorrecto en los errores del servidor Web: El servidor permite a un atacante obtener información interna de la compañía a través de errores, así como rutas internas del servidor o versiones de software. Esta información puede ser útil para planificar ataques potenciales sin afectar al sitio directamente.
- Identificación de Errores en la configuración SSL y certificados inválidos: La utilización de SSL permite al usuario proteger la información que se transmite entre el usuario y el servidor. Se identificó una configuración errónea del SSL y la utilización de certificados inválidos o autogenerados. Esto permitiría a un atacante descryptar la información que se transmite y modificarla. Esto pone en riesgo la confidencialidad e integridad del sitio.
- Identificación de envío de credenciales en texto plano: En determinados servicios, un atacante que esté espiando la red podría extraer credenciales de inicio de sesión de los usuarios.

[...]

Sección: Metodología

Ficha	Metodología
Informe Ejecutivo	Opcional
Informe Técnico	Necesario
Descripción	Especificar la metodología es algo que permite al lector entender cuál fue el curso de acción durante la ejecución, así como también las consideraciones, técnicas y estándares que se utilizaron. Desde un punto de vista técnico permite al especialista repetir con la misma vara de medición las pruebas y entender la razón por la cual la anterior ejecución encontró aquellas vulnerabilidades y repetir las mismas pruebas o mejorarlas. Desde un punto de vista gerencial permite tener claridad sobre los estándares utilizados y el enfoque utilizado para buscar vulnerabilidades. En esta parte es fundamental realizar una separación en el estilo de escritura de ambos informes. El informe ejecutivo no debe contener ninguna declaración técnica más allá de estándares utilizados o metodologías. Debe explicar de manera clara desde donde se realizaron las pruebas y el objetivo de las mismas. En el informe técnico se pueden especificar más detalles, así como las pruebas a ser realizadas, las credenciales (¡sin contraseña!) entregadas, puntos de red, accesos IP, direcciones web y todo aquel detalle técnico que haga sentido a la evaluación.
Ejemplo	Objetivos del Servicio “Nuestro enfoque metodológico se basa en OWASP, un proyecto abierto de seguridad en aplicaciones Web que se encarga de identificar y documentar las vulnerabilidades más críticas y comunes en los sitios web. Para verificar la triada de seguridad (confidencialidad, integridad y disponibilidad) del sitio es necesario cubrir todos los aspectos que un hacker atacaría, por lo tanto, el análisis basado en OWASP [...]”

Sección: Hallazgos Detallados

Ficha	Hallazgos Detallados
Informe Ejecutivo	No
Informe Técnico	Necesario
Descripción	El hallazgo detallado es, sin duda alguna, la parte más importante del informe técnico. Es en dónde el lector puede analizar vulnerabilidad por vulnerabilidad, su respectivo detalle, identificación, la cantidad de activos que afectan la vulnerabilidad, la forma en la que fue detectada, la explotabilidad de la vulnerabilidad, el impacto técnico que tendría si un atacante la explotara, las condiciones que se deben dar para que la vulnerabilidad se materialice, su severidad técnica, la descripción de la vulnerabilidad, recomendaciones de mitigación, referencias, etcétera. La descripción detallada de como presentar estos hallazgos está en la siguiente sección de este documento.
Ejemplo	No aplica

Sección: Anexos

Ficha	Anexos
Informe Ejecutivo	No
Informe Técnico	Opcional
Descripción	La sección de Anexos es principalmente para adjuntar cualquier información, evidencia, tablas, datos extraídos, videos, etcétera que la persona elaborando el informe encuentre necesarios para contextualizar el reporte.
Ejemplo	No aplica

Sección: Control Documental

Ficha	Control Documental																																																														
Informe Ejecutivo	Opcional																																																														
Informe Técnico	Opcional																																																														
Descripción	El control documental permite llevar un seguimiento de las distintas modificaciones que se han realizado al documento. Esta sección evita que existan confusiones al momento de que dos partes conversen del mismo informe y cada uno tenga una versión distinta del mismo, también permite llevar seguimiento de las personas involucrados en la edición y aprobación del informe, así como clasificar la confidencialidad del mismo. Un control documental debiese presentar una identificación del documento, historial de ediciones, historial de aprobaciones y distribución del documento.																																																														
Ejemplo	Identificación <table><tr><td>ID</td><td>EHW-CLIENTE-0001</td></tr><tr><td>Nombre del Documento</td><td>Informe Ejecutivo Ethical Hacking Web [URL]</td></tr><tr><td>Nombre del Proyecto</td><td>Ethical Hacking Revisión Q3</td></tr><tr><td>Autor</td><td>Pentester 1 / Pentester 2</td></tr><tr><td>Versión</td><td>1.0</td></tr><tr><td>Clasificación</td><td>DOCUMENTO CONFIDENCIAL</td></tr><tr><td>Fecha de Elaboración</td><td>[FECHA]</td></tr></table> Historial de Ediciones <table><tr><td>Versión</td><td>Fecha</td><td>Adiciones/Modificaciones</td><td>Preparado/Revisado por</td></tr><tr><td>0.1</td><td>[FECHA]</td><td>Redacción inicial de informe</td><td>Pentester 1</td></tr><tr><td>1.0</td><td>[FECHA]</td><td>Redacción lista para ser enviada</td><td>Gerente</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table> Historial de Aprobaciones <table><tr><td>Fecha</td><td>Nombre</td><td>Organización/Puesto</td><td>Comentarios</td></tr><tr><td>[FECHA]</td><td>GERENTE</td><td>[PROVEEDOR]</td><td>Aprobado con correcciones</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table> Distribución del Documento <table><tr><td>Nombre</td><td>Organización/Puesto</td></tr><tr><td>CLIENTE 1</td><td>[EMPRESA_CLIENTE]</td></tr><tr><td>CLIENTE 2</td><td>[EMPRESA_CLIENTE]</td></tr><tr><td></td><td></td></tr></table>	ID	EHW-CLIENTE-0001	Nombre del Documento	Informe Ejecutivo Ethical Hacking Web [URL]	Nombre del Proyecto	Ethical Hacking Revisión Q3	Autor	Pentester 1 / Pentester 2	Versión	1.0	Clasificación	DOCUMENTO CONFIDENCIAL	Fecha de Elaboración	[FECHA]	Versión	Fecha	Adiciones/Modificaciones	Preparado/Revisado por	0.1	[FECHA]	Redacción inicial de informe	Pentester 1	1.0	[FECHA]	Redacción lista para ser enviada	Gerente									Fecha	Nombre	Organización/Puesto	Comentarios	[FECHA]	GERENTE	[PROVEEDOR]	Aprobado con correcciones													Nombre	Organización/Puesto	CLIENTE 1	[EMPRESA_CLIENTE]	CLIENTE 2	[EMPRESA_CLIENTE]		
ID	EHW-CLIENTE-0001																																																														
Nombre del Documento	Informe Ejecutivo Ethical Hacking Web [URL]																																																														
Nombre del Proyecto	Ethical Hacking Revisión Q3																																																														
Autor	Pentester 1 / Pentester 2																																																														
Versión	1.0																																																														
Clasificación	DOCUMENTO CONFIDENCIAL																																																														
Fecha de Elaboración	[FECHA]																																																														
Versión	Fecha	Adiciones/Modificaciones	Preparado/Revisado por																																																												
0.1	[FECHA]	Redacción inicial de informe	Pentester 1																																																												
1.0	[FECHA]	Redacción lista para ser enviada	Gerente																																																												
Fecha	Nombre	Organización/Puesto	Comentarios																																																												
[FECHA]	GERENTE	[PROVEEDOR]	Aprobado con correcciones																																																												
Nombre	Organización/Puesto																																																														
CLIENTE 1	[EMPRESA_CLIENTE]																																																														
CLIENTE 2	[EMPRESA_CLIENTE]																																																														

Sección: Hoja de Ruta estratégica

Ficha	Hoja de Ruta estratégica
Informe Ejecutivo	Opcional
Informe Técnico	Opcional
Descripción	La hoja de ruta es la recomendación de alto nivel sobre la estrategia que la empresa debiese tomar para mitigar estas vulnerabilidades. Esta sección debe permitir entender al cliente cuales son las prioridades que debe colocar sobre las acciones en Corto, Mediano y Largo Plazo.
Ejemplo	Hoja de ruta: • En el corto plazo, analizar la posibilidad de actualizar el sistema operativo a [versión actual] y a IIS [versión actual] • En el mediano plazo Ajustar la implementación de SSL a los estándares actuales de seguridad. • En el largo plazo, encontrar un software de reemplazo para [software sin soporte]. [...]

Sección: Información de Contacto

Ficha	Información de Contacto
Informe Ejecutivo	Opcional
Informe Técnico	Opcional
Descripción	Esta sección permite al lector comunicarse con los especialistas, altos mandos, responsables que realizaron la actividad en caso de que exista alguna pregunta específica a la ejecución. Esto permite dar continuidad a los informes a lo largo del tiempo, permitiendo a futuras ejecuciones mantener contacto entre las partes.
Ejemplo	Información de Contacto “Los profesionales detrás de esta evaluación pueden ser contactados a la siguiente dirección: contacto@empresa.com”

Sección: Narración de la evaluación

Ficha	Narración de la evaluación
Informe Ejecutivo	No
Informe Técnico	Opcional
Descripción	La narración de la evaluación es una historia acerca de cómo el pentesting web fue realizado. Esta historia debe contener la línea de tiempo de la actividad, indicando cuales fueron las pruebas que resultaron y cuáles no, así como también el orden en la cual fueron ejecutadas. Esta narración permite al lector entender cuál fue la línea de pensamiento de los profesionales que pusieron a prueba el sistema y por donde pudieron penetrarlo. Esta sección permite darle repetitividad a la evaluación a lo largo del tiempo, e incluso permite a futuras ejecuciones explorar rincones que tal vez se dejaron de lado con anterioridad. Esta sección pertenece no debe estar presente en el informe ejecutivo, ya que tiene detalles una gran cantidad de detalles técnicos.
Ejemplo	Narración de la evaluación “Para esta actividad, [CLIENTE] entregó poca información acerca del objetivo, tan solo el sitio web [URL]. Antes de comenzar con la inspección del sitio web se realizó un escaneo de puertos utilizando NMAP para entender la cantidad de servicios funcionando en el servidor. - IMAGEN EVIDENCIA - Los resultados indican que el mismo servidor está corriendo varias instancias de NGINX y APACHE, por lo que es posible que [...]”

Sección: Explicación de Explotación

Ficha	Explicación de Explotación
Informe Ejecutivo	No
Informe Técnico	Opcional
Descripción	La sección explotación plantea un escenario ficticio o real de lo que pudiese haber ocurrido con la empresa en caso de que las vulnerabilidades hayan sido explotadas por los profesionales. Esta es una decisión que se toma antes de realizar la actividad, en donde se especifica si las vulnerabilidades encontradas, en caso de que se pueda, son o no explotadas. Esto permite conocer la real extensión de los resultados de la evaluación y hasta donde se puede llegar. En esta sección se expresan esos resultados.
Ejemplo	Explicación de Explotación “[...] en caso de que la vulnerabilidad EHW-CLIENTE-VULN-097 pueda ser explotada permitiría a un atacante pivotar la conexión utilizan la plataforma web como proxy para tener acceso a la red interna. Además, si se combina con la vulnerabilidad EHW-CLIENTE-VULN-083 es posible extraer [...]”

Presentación de las vulnerabilidades

Tal como se explicó en la sección anterior, presentar cada vulnerabilidad de manera fácil y concisa permitirá un mejor entendimiento de cada una de las desviaciones de seguridad que se encuentren presentes en el sitio web.

A continuación, se encuentra la Tabla 4 - Identificadores de un Hallazgo que contiene los identificadores necesarios y opcionales que cada presentación de vulnerabilidad debiese tener. Cada autor puede agregar sus propios identificadores, sin embargo, es necesario al menos considerar ciertos campos mínimos para cada reporte.

Tabla 4 - Identificadores de un Hallazgo. Fuente: Elaboración Propia

Necesario	Opcionales
1) Identificador Único	a) Tipo de vulnerabilidad
2) Nombre de Vulnerabilidad	b) Explotabilidad
3) Severidad	c) Condiciones
4) Riesgo	d) Referencias
5) Ubicación	
6) Descripción	
7) Recomendación	

Identificadores Necesarios

Identificador Único

El identificador único permite al lector poder hablar con facilidad sobre una vulnerabilidad en particular, este identificador debe permitir diferenciar una vulnerabilidad de otra dentro del mismo informe y de posteriores ejecuciones. Con la finalidad de mantener compatibilidad entre evaluaciones es necesario definir en el informe la manera en que se construye el identificador. Si la evaluación está considerando una ejecución anterior es necesario continuar con la misma nomenclatura que la ejecución original.

Nombre de la Vulnerabilidad

Este identificador es simplemente un nombre referencial de lo que la vulnerabilidad representa. Puede ser un nombre genérico o específico a la vulnerabilidad.

Severidad y Riesgo

La severidad y el riesgo de una vulnerabilidad fueron términos discutidos en la sección 3.3.1. Sin embargo, es importante destacar que el indicador de severidad debe ser calculado utilizando el CVSS2.0 o el CVSS3.0 presentado por FIRST (Ver ²¹).

Ubicación

Con la finalidad de que el área técnica sepa cual activo (Sitio web, URL, Servidor, *Plugin*, etcétera) es afectado por la vulnerabilidad señalada es importante señalar el alcance completo de la vulnerabilidad. En caso de que la vulnerabilidad esté presente en varias secciones del sitio web es necesario apuntarlas todas o crear una entrada en la sección de anexos.

Descripción

La descripción permite al lector entender a mayor profundidad la vulnerabilidad y cuál es su potencial impacto. Esta puede ser una narración del funcionamiento de la vulnerabilidad en conjunto con el impacto que tuviese si un atacante la explotaría. En esta parte se recomienda indicar pasos para reproducir la vulnerabilidad en caso de que sea posible y adjuntar toda la evidencia gráfica posible (si es video se debe mencionar el nombre del archivo y adjuntarlo en el reporte).

Recomendación

La recomendación es una explicación de alto nivel sobre una posible mitigación de una vulnerabilidad. Esta debe ser lo suficientemente explicativa para que el lector que está revisando el informe pueda realizar la respectiva acción correctiva. En caso de que la remediación pueda tener algún impacto en la funcionalidad y operatividad del activo afectado es importante señalarlo de manera especial. Si la recomendación es amplia o se apoya en documentos externos es necesario indicarlos.

Identificadores Opcionales

Tipo de vulnerabilidad

El tipo de vulnerabilidad debe clasificar la vulnerabilidad en una de las categorías indicadas por la *National Vulnerability Database*²².

Es necesario indicar su respectivo CVE²³ en caso de que sea una vulnerabilidad registrada en la base de datos mantenida por la organización MITRE. El tipo de vulnerabilidad también debe identificar en que sección del OWASP Testing Methodology Guide fue detectado y de ser posible, a cuál del TOP10 de vulnerabilidades OWASP pertenece.

²¹ <https://www.first.org/cvss>

²² <https://nvd.nist.gov/vuln/categorie>

²³ Common Vulnerabilities and Exposures - Mitre

Explotabilidad y Condiciones

El identificador de explotabilidad indica que tan probable y complejo es explotar la vulnerabilidad. En esta descripción se pueden colocar los pasos para replicar la vulnerabilidad o simplemente indicar que existe un exploit disponible. Este indicador va de la mano con el indicador de condiciones, que tiene por objetivo describir cuales son las condiciones técnicas necesarias para que esta vulnerabilidad pueda ser explotada.

Referencias

Finalmente, el identificador referencias permite al lector profundizar más aún en el detalle de la vulnerabilidad o su respectiva mitigación.

¿Cómo utilizar el Framework?

Si bien se ha propuesto una serie de definiciones, consideraciones y lineamientos a seguir es necesario contar con una guía sobre cómo utilizar este framework en la práctica. A continuación, se establecen los siguientes pasos:

1.- Preparación con el cliente.

Durante la sección de análisis de entregables y estilos de reporte capítulo 3 se acordaron 4 definiciones fundamentales (DEF-1, DEF-2, DEF-3 y DEF-4). En aquellas definiciones se busca acordar con el cliente lo necesario antes de realizar la evaluación. Estas definiciones ayudarán con lo siguiente:

- **DEF-1:** El cliente entenderá que se entregarán dos informes distintos, uno técnico y uno ejecutivo por separado.
- **DEF-2:** Acordar con el cliente si necesita separar el informe en distintas partes. Es necesario explicar las ventajas y desventajas de cada separación.
- **DEF-3:** El cliente entenderá la separación entre Severidad y Riesgo.
- **DEF-4:** El cliente podrá elegir, con la guía del profesional, las secciones que necesita en cada uno de los reportes a entregar.

2.- Ejecución de la actividad

Una vez acordado todos los puntos anteriores es posible ejecutar la actividad. Esto tiene dos enfoques principales. En primera instancia, el profesional sabe lo que el cliente espera, lo que permite coordinar los tiempos invertidos de mejor forma y orientar la ejecución de la consultoría acorde a lo que el cliente necesita, en segunda instancia el cliente ya fija las expectativas de lo que va a recibir al finalizar la consultoría.

3.- Preparación de los Informes

Este paso considera tomar los informes anteriores que se hayan realizado sobre los mismos activos, esto permite reconocer de manera rápida si ya se ha realizado alguna entrega de reportes utilizando este framework, en caso de que sea positivo, es necesario considerar las estrategias (identificadores necesarios, secciones, metodología de redacción, etc.) que haya utilizado el profesional anterior. En caso de que no exista informe previo es necesario diseñar el informe desde el principio colocando énfasis en las secciones presentadas en esta propuesta.

4.- Redacción de los Informes Técnicos

Utilizando la información del paso anterior, se redactan los informes. Escribiendo las secciones solicitadas por el cliente y ordenándolas de manera adecuadas.

5.- Chequeo cruzado con el Cliente y cálculo del Impacto

En este paso se presentan los resultados encontrados durante la evaluación utilizando el informe técnico. En conjunto con el cliente se explica a grandes rasgos las vulnerabilidades encontradas y presentando los riesgos cibernéticos a los que la empresa y/o el activo está expuesto. Durante esta actividad se calcula el impacto organizacional con la finalidad de calcular el riesgo de las vulnerabilidades (Recordar la DEF-3 del paso uno). Esto permite al cliente priorizar de mejor forma las remediaciones y al profesional redactar de mejor forma las recomendaciones.

6.- Redacción de los Informes Ejecutivos

Una vez llegado a este paso, el profesional ya se debiese tener completa claridad sobre las apreciaciones del cliente y el gran escenario de la evaluación. Con esta información ya es posible redactar el informe ejecutivo y finalizar la evaluación.

7.- Presentación y cierre

Una vez redactados los informes, los entregables debiesen estar listos para ser presentados al cliente. En este paso se propone utilizar un formato de slides en conjunto con los documentos para presentar de manera más acorde al cliente.

Utilizando estos 7 pasos, se propone entregar al cliente y al profesional una forma ordenada, cooperativa y asertiva los procedimientos y pasos para realizar una correcta evaluación de seguridad de un Pentesting web.

En el siguiente capítulo se presentará los resultados de ejecutar estos siete pasos, utilizando lo propuesto por el estándar y recopilando las apreciaciones de profesionales y un cliente voluntario involucrado en la memoria.

CAPÍTULO 4

VALIDACIÓN DE LA SOLUCIÓN

Acuerdo de Evaluación con el Cliente Voluntario

Para validar la propuesta se realizó un Pentesting Web sobre un cliente voluntario, quién entregó la autorización para publicar los resultados si y solo si se cumplían las siguientes condiciones:

- No se mostraba la evidencia de los hallazgos en formato gráfico.
- Todo nombre relacionado a la evaluación que permita identificar al cliente debe estar correctamente censurado.
- Completo anonimato al momento de mencionarlo en la memoria dado que es un cliente de un sector de retail importante.

El cliente voluntario puso a disposición de la memoria la aplicación web por la cual sus clientes pueden conocer el estado de avance de sus pedidos y comprar en línea. Según los antecedentes entregados la plataforma fue desarrollada por un alumno en práctica el año 2010 sin mayores conocimientos en seguridad, por lo que actuará como buen ejemplo para realizar un reporte de vulnerabilidades web.

Utilización del Estándar para los entregables

Contexto de la Evaluación

La evaluación está dentro de la revisión anual de visibilidad de la empresa voluntaria. La actividad realizada tuvo por objetivo apoyar la constante transformación tecnológica de la empresa, procurando que sus sistemas se encuentren debidamente protegidos.

La consultoría completa se realizó entre los días 28 de agosto de 2017 y 13 de septiembre del 2017, en donde hubo distintas sesiones en que se evaluaron los activos del cliente y se realizaron reuniones para conversar, evaluar y presentar los resultados.

Metodología de Evaluación

Para la evaluación se utilizó la metodología OWASP según lo propuesto en el capítulo 3 de esta memoria.

La primera instancia para realizar los entregables propuestos por la memoria es realizar las cuatro definiciones iniciales, en las que se trabaja codo a codo con el cliente:

- **DEF-1:** Se separa los entregables en dos informes distintos: Uno ejecutivo y uno técnico en base a lo necesario para comprender los resultados de la evaluación.
- **DEF-2:** El cliente no necesita separar el informe técnico en distintas partes, ni el ejecutivo. Por lo que se acuerda entregar un solo un ejemplar por cada sección.
- **DEF-3:** Se explica al cliente que las vulnerabilidades se presentan con la severidad técnica y luego se acordará el impacto organización con él. Esto tiene por finalidad calcular el riesgo.
- **DEF-4:** Se orienta al cliente en las secciones que pueden incluir los reportes. Una vez orientado el cliente solicita sólo las selecciona las que necesita.

La DEF-4 es la más importante a realizar con el cliente, ya que determinará la cantidad de esfuerzo y tiempo que será necesario invertir para redactar los entregables solicitados por el cliente. De la Tabla 3 (Capítulo 3), se acuerda lo siguiente con el cliente:

Tabla 5 - Secciones solicitados por el cliente. Fuente: Elaboración Propia

Sección	Ejecutivo	Técnico
Introducción	Incluido	Incluido
Alcance del Trabajo	Incluido	Incluido
Hallazgos Generales	Incluido	Incluido
Acuerdos	Incluido	Incluido
Conclusiones	Incluido	Incluido
Recomendaciones Generales	Incluido	Incluido

Sección	Ejecutivo	Técnico
Objetivos del Servicio	Incluido	Incluido
Riesgo Consolidado	Incluido	Incluido
Metodología		Incluido
Hallazgos Detallados		Incluido
Anexos	Incluido (Sólo evidencia)	Incluido (Sólo evidencia)
Control Documental	Incluido	Incluido
Hoja de Ruta	Excluido	Excluido
Información de Contacto	Incluido	Incluido
Narración de la Evaluación		Excluido
Explicación de la explotación		Excluido

Como es posible ver en la Tabla 5, por el lado del reporte ejecutivo el cliente solicitó 11 de los 12 disponibles. Y en el caso del reporte técnico solicitó 13 de los 16 disponibles.

Durante la reunión, el cliente explica que la sección **Hoja de ruta** prefiere dejarla fuera ya que él no es el encargado final de los sistemas y quería saber la aprobación de sus superiores antes de planificar la remediación del sistema, sin embargo, sí tenía la autorización para realizar las pruebas. Con respecto a la **Narración de la Evaluación** y la **Explicación de la explotación** tampoco fueron incluidas dado que se acordó dejar la explotación del servidor base fuera del alcance, y tan solo limitarse a comprobar las vulnerabilidades encontradas, pero no ir más lejos. El resto de los puntos fueron incluidos en el reporte final entregado.

El informe se puede encontrar al final de esta memoria en la sección de Anexos.

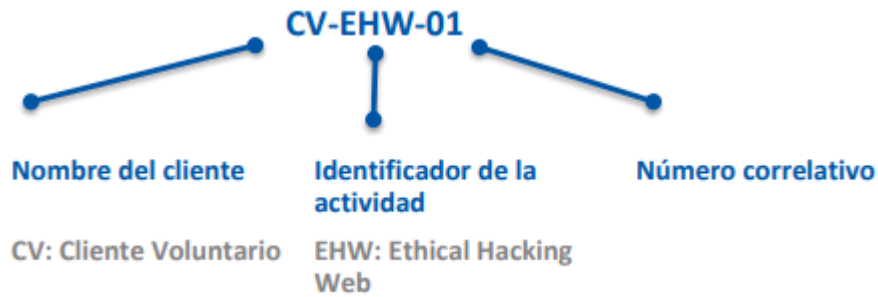
Una vez acordadas las 4 definiciones iniciales es posible comenzar la ejecución de las actividades.

Para realizar la actividad, se ejecutaron las herramientas automáticas, se realizó la limpieza de falsos positivos y comenzó la parte más larga de la evaluación: La evaluación manual.

Redacción de los entregables

En primera instancia se escribe el informe técnico, en donde de manera organizada se escriben todas las vulnerabilidades encontradas. Para ello el memorista las ordenó por severidad y acordó una forma de identificarlas según como lo define la sección de identificadores necesarios.

La forma acordada por el memorista fue la siguiente:



Utilizando la nomenclatura CV-EHW-#NUMERO. Esto permite identificar la vulnerabilidad por cliente, la actividad realizada y el número correlativo.

Una vez escrito este informe se presentó al cliente en forma de slides y se calculó el impacto organizacional con la finalidad de estimar el riesgo y reordenar las vulnerabilidades por Riesgo y luego por Severidad.

Una vez actualizado el informe técnico y teniendo completa claridad del escenario de seguridad en que el activo de cliente se encuentra se procede a lo siguiente:

- Redactar las secciones solicitadas por el cliente (Tabla 5)
- Colocar portadas e imágenes de autoría
- Se revisa por última vez para asegurar que las vulnerabilidades y su numeración sea congruente.

Una vez redactado el informe técnico, se redacta el informe ejecutivo, en donde de manera resumida se explican las vulnerabilidades encontradas sin entrar en mucho detalle y se presentan escenarios de riesgos en los que el activo se pueda ver involucrado. Esto permite dar una clara visión sobre los potenciales riesgos de la empresa. En este informe se utilizó mucho de lo redactado en el informe técnico eliminando todos aquellos tecnicismos.

Finalmente, se presentan ambos informes al cliente y se responden las preguntas necesarias.

Resumen de los resultados de la evaluación

Durante la evaluación se encontraron 12 vulnerabilidades en total, de las cuales 3 eran de severidad alta, 5 de severidad media y 4 de severidad baja. El cliente estaba expuesto a 4 riesgos de seguridad:

Inyección de código

Se encontraron 3 vulnerabilidades de inyección de código en la plataforma. Estas vulnerabilidades podrían permitir a un atacante de manera directa o indirecta inyectar código malicioso en la aplicación, como inyectar malware o engañar a los usuarios para robarle los datos. Adicionalmente, dentro de esta categoría se encuentra una vulnerabilidad que permite al atacante extraer la información de las bases de datos, conocida como inyección SQL. Esta vulnerabilidad es de severidad ALTA, y debiese tratarse de manera inmediata.

- **Recomendación:** Para resolver estas vulnerabilidades es necesario intervenir el código fuente de la aplicación e idealmente implementar un Firewall de aplicación.
- **Riesgo:** Alto

Vulnerabilidad en el código

Se detectó 1 vulnerabilidad de vulnerabilidad en el código. El primer ataque utilizando esta vulnerabilidad permitiría a un atacante realizar múltiples ataques de fuerza bruta para adivinar las contraseñas de los usuarios del sistema. El sistema no tiene implementado un sistema de bloqueo para este tipo de ataques.

- **Recomendación:** Para resolver estas vulnerabilidades es necesario intervenir el código fuente o implementar algún control externo mitigatorio.
- **Riesgo** Medio (Impacto: Alto, Severidad: Media)

Configuración

Se detectaron 7 vulnerabilidades de configuración en el sistema. Estas vulnerabilidades son debilidades en cómo está configurando la plataforma o el servidor en sí. Estas vulnerabilidades permitirían a un atacante realizar diversos ataques, pero en general:

- Cargar archivos maliciosos al servidor (Riesgo alto)
- Extraer información de usuarios en la plataforma (Riesgo medio)
- Intervenir comunicaciones (Riesgo bajo)
- **Recomendación:** Para resolver estas vulnerabilidades se deben tomar múltiples estrategias, pero principalmente revisar las configuraciones del servidor donde está alojado el sitio web.

Mantenimiento

Se detectó 1 vulnerabilidad de mantenimiento. Esto quiere decir que uno de los componentes utilizados para la aplicación web ya no cuenta con soporte por parte del fabricante, por lo que cualquier vulnerabilidad de seguridad encontrada en esos componentes no tendrá forma de ser parchada adecuadamente.

- **Recomendación:** Revisar alternativas al componente mencionado y migrar el sistema.
- **Riesgo** bajo (Impacto: Bajo, Severidad: Media)

Para evaluar la propuesta se entrevistó al cliente y se recopilaban sus apreciaciones. De manera paralela se consiguió la opinión de tres expertos de seguridad y se realizó una serie de preguntas, se les presentó el informe debidamente censurado y se recopilaban sus comentarios.

Evaluación de las partes involucradas

El cliente

La primera evaluación, y una de las más importantes provenía por parte del cliente, quien debía entender a cabalidad el estado de seguridad de su sistema web.

Para la entrega de estos resultados se realizaron 6 fases:

1. Creación de los entregables utilizando el estándar.
2. Presentaciones a cliente final.
3. Co-revisión detallada con cliente del informe ejecutivo.
4. Co-revisión detallada con cliente (Informático) del informe técnico.
5. Entrega final de ambos informes a Cliente.
6. Entrevista de cierre.

La fase número 4 fue interesante, ya que era la primera evaluación que el cliente recibía de su sitio web y todo le sorprendía. En primera instancia se vio preocupado por los hallazgos y entender los riesgos a los que su sitio web estaba expuesto, sin embargo, logró concentrarse en lo más importante para priorizar su reparación.

El feedback por parte del cliente fue extremadamente positivo, destacando 4 puntos principales al momento de recopilar sus apreciaciones:

- **Cómoda estructura de reporte:** El cliente destaca la estructura del reporte, indicando que está organizado desde lo más global de la evaluación y los acuerdos realizados entre ambas partes, hasta llegar al detalle estratégico de las vulnerabilidades detectadas.
- **Un riesgo consolidado fácil de entender:** Indica que el riesgo consolidado está bien explicado y que a pesar de ser 12 vulnerabilidades pudo entenderlas correctamente sin necesidad de una experiencia técnica avanzada.
- **Identificación clara de los riesgos:** Sin una necesidad de leer las 12 vulnerabilidades involucradas en el sistema se entienden de manera rápida los riesgos leyendo la sección 5.2. Riesgo Consolidado del informe. Esto permite en una lectura rápida, entender la posición de seguridad de la aplicación web.
- **La evaluación va más allá de la vulnerabilidad:** Finalmente el cliente indica que en la sección 6. Conclusiones y Acciones Propuestas, las declaraciones del profesional

no se limitan a reparar sólo las vulnerabilidades, si no que a descubrir la causa raíz de algunas de las vulnerabilidades para que no se puedan repetir en otros sistemas.

Luego de revisar el informe ejecutivo con el cliente, se revisó al detalle el informe técnico con el personal informático. En este caso el personal técnico contaba con cero conocimientos técnicos de seguridad, por lo que hubo que explicarle punto a punto los hallazgos encontrados. Esto era de esperar, ya que, en las evaluaciones, según lo que comentaron los profesionales el personal técnico no sabe cómo reparar las vulnerabilidades en la mayoría de los casos. Por lo que en esta parte hubo asesoramiento caso por caso para que pudieran reparar las vulnerabilidades.

Los profesionales

Luego de realizar las evaluaciones con el cliente, se desarrolló la parte más importante de la validación, la que considera la evaluación profesional de expertos dedicados en el tema y con varios años de experiencia. Para esta evaluación se consideraron tres personas de tres empresas distintas enfocadas a los servicios de Ciberseguridad:

- Entel CyberSecure
- Aiuken Solutions Chile
- E-Sign LATAM

A los evaluadores se les presentó el estándar en un formato resumido y luego los informes que fueron emitidos al cliente correctamente anonimizados.

A cada uno de estos profesionales se le realizaron 11 preguntas específicas sobre la memoria y 1 pregunta abierta para que pudieran agregar y/o modificar aspectos del estándar que encuentren pertinentes.

En cada una de las preguntas se colocará una conclusión consolidada de las respuestas de los profesionales con respecto a la memoria

1) ¿Consideran utilizar el pentesting anterior antes de realizar el siguiente? ¿Los leerían si tuvieran este estándar?

Los profesionales indican que en general no por diversas razones. La primera de ellas es por que usualmente tienen clientes que jamás han tenido una experiencia previa con respecto a este tipo de evaluaciones o simplemente no tienen disponibles los documentos del pentesting anterior. En las ocasiones que si tenían acceso al pentesting anterior simplemente lo ignoraban ya que les pasaban un documento de 400 páginas. Indican que un estándar más ordenado como el presentado por el memorista sería más fácil de leer y de comparar con futuras evaluaciones.

2) ¿Cómo evalúa la estructura general de los reportes?

Los profesionales indican que los módulos indicados son los precisos, incluso algunos eran desconocidos y aceptaron bien la propuesta de utilizarlos en sus evaluaciones. Definen que la estructura de los módulos debe ser libre, sin embargo, las directivas propuestas por el estándar son fáciles de seguir y cumplen los objetivos de entregar de manera correcta la información al cliente.

3) ¿Está de acuerdo con las definiciones del Marco Teórico?

Esta pregunta fue una larga conversación y debate por alguno de los términos establecidos en la memoria, sin embargo, comentan que la diferencia se debe a que cada uno utiliza su propio vocabulario y forma de explicar a sus clientes. Los tres profesionales concuerdan que establecer un vocabulario como el planteado por el memorista es una

excelente iniciativa para diseñar un framework el vocabulario que usan los que brindan servicios y los que reciben este servicio.

4) ¿Cómo considera el nivel del informe ejecutivo?

El nivel del informe ejecutivo lo encuentran adecuado para que una persona sin conocimientos técnicos lo lea y evalúe. Indican los profesionales que el informe presentado al cliente es bastante largo en el contenido pero que en estructura es adecuada. Comentan que desde su experiencia los altos ejecutivos tienen poco tiempo para revisar un informe de 14 páginas y que ese tipo de reportes quedan archivados y que prefieren dar presentaciones vía slides. Sin embargo, para aquellas empresas que tienen procesos de auditoría está excelente el formato.

5) ¿Cómo considera el nivel de detalle del informe técnico?

En base a las respuestas de los profesionales, dos profesionales indicaron que el informe técnico tiene demasiadas secciones, el otro profesional indica que las secciones están bien, sin embargo, dejaría solo las marcadas como necesarias y dejaría afuera las opcionales. Finalmente, los tres indican que la sección Hallazgos necesarios debiese ser eliminada del informe técnico.

6) ¿Está de acuerdo con la separación del riesgo de la severidad?

La respuesta fue variada en esta sección. Uno de los profesionales indica que no hace una diferencia ya que en la mayoría de las herramientas automáticas de seguridad (dónde muchos clientes aprenden términos) hablan de la palabra “Risk” en inglés, la cual en español es traducida como Riesgo, por lo que hablar de severidad no es una buena estrategia. El otro profesional indicó que utiliza la palabra severidad, ya que hablar de riesgo significa involucrar al negocio en la evaluación y que no es una situación de un par de conversaciones para realizar una correcta evaluación de riesgo. El último profesional comenta que si realiza la separación y que deja el criterio de riesgo al cliente y que la severidad la coloca él. Esto indica que la necesidad de separación no está completamente clara. Finalmente, los tres establecen que la propuesta de separación y definición es una buena idea y que, desde una perspectiva educativa, estamos apoyando al desarrollo de la disciplina en el país.

7) ¿Este estándar le permitiría acordar mejor con el cliente los entregables?

Sin lugar a duda, esta fue la parte que más alabaron los profesionales con respecto a la propuesta de estándar, indicando que una de las problemáticas más comunes con respecto a la satisfacción de los entregables era que el cliente no tenía muy claro que es lo que iba a recibir, esto significaba que muchas veces había que editar mucho los informes finales para que se ajusten a las necesidades del cliente. Sin embargo, utilizando el estándar de manera ordenada y presentarlo así al cliente era posible para el profesional dimensionar la cantidad de trabajo y sólo realizar lo que realmente levanta valor al cliente.

8) ¿Considera que le ayudaría seguir esta estructura para futuras evaluaciones?

Los profesionales indican que más que la estructura de los informes les interesa utilizar las secciones y utilizar los mismos nombres. Que esto permitiría realizar un rápido seguimiento de los últimos informes y saber que secciones leer y cuales dejar para casos especiales.

Adicionalmente los tres indican que seguir esta estructura no sólo apoya al profesional en realizar los entregables, sino que también apoya a los clientes a no recibir múltiples informes con distintos formatos si es que la evaluación no la realiza el mismo profesional, así como también ayudarlo a realizar un seguimiento de las vulnerabilidades a lo largo del tiempo.

9) ¿Le gustaría recibir un informe previo con esta estructura?

En esta pregunta la respuesta fue unánime. Los tres entrevistados están completamente de acuerdo en que les gustaría recibir un informe con una estructura conocida y fácil de leer. Indican que cuando reciben un informe de herramientas automáticas como Nessus o Qualys, como conocen la estructura, les es fácil y rápido obtener los resultados, por lo que si se continúa con esta lógica es más fácil recibir informes previos y poder continuar desde ahí.

10) ¿Cree que está ajustado a la realidad chilena este tipo de informe?

Los profesionales comentan que en Chile la realidad está principalmente inclinado a ejecutar herramientas automáticas y enviar directamente el reporte de la herramienta, sin mucha interacción humana por detrás. Que si bien es algo necesario no es suficiente. Creen que esto se debe a que no entienden el real valor de realizar un pentesting a sus sistemas ya que están acostumbrado a recibir estos informes de 400 páginas, sin embargo, si se les presenta de esta forma quizás eso cambie.

11) ¿Cree que este pueda ser un estándar a seguir en la industria chilena?

La respuesta fue unánime. Los profesionales dicen que definitivamente esto puede llegar a ser un estándar para la industria chilena si se le presenta a las personas correctas. Que es una buena recopilación de información, estructura y definiciones, secciones, terminología y guías para que los tests de penetración web (más manuales y menos automáticos) tengan una mayor aceptación y sean más acertados a la realidad del país.

12) ¿Qué agregaría y/o modificaría?

Esta fue una pregunta abierta para los profesionales. De manera resumida indican que le quitarían la calidad de “Necesario” a algunas secciones de la parte técnica. Agregarían una presentación en formato slides para el reporte ejecutivo (como parte de los entregables) y finalmente proponen desarrollar un software o un modelo basado en XML que permita de manera colaborativa escribir estos informes manteniendo la estructura del estándar para así impulsarla más en el país, pero que sería tema para otro tópico de memoria.

En el siguiente capítulo 5 se conversará sobre los resultados y los impactos que tuvo esta propuesta de estándar sobre los actores involucrados, los potenciales resultados en la industria, la validez y las contribuciones que tuvo esta memoria.

CAPÍTULO 5

CONCLUSIONES

Sobre el alcances y limitaciones de la memoria

La memoria, al momento de ser presentada a la Universidad se declaró que tenía las siguientes limitaciones:

- Enfocado a Pentesting Web
- Limitado al ambiente nacional
- Limitado a lo que se pueda recopilar y analizar en un plazo de 6 meses

Estas limitaciones fueron planteadas en un comienzo y resultaron ser bastante acertadas. La recopilación de información estuvo limitada al tiempo disponible que tenían los profesionales a recibir al memorista, en conseguir un cliente voluntario para realizar un test de penetración web que esté de acuerdo en compartir los resultados de la evaluación y en escribir todas las definiciones y secciones que involucraba desarrollar una propuesta de estándar tomó mucho más del tiempo que estaba pensado en un comienzo. Pasó de una memoria de 6 meses a dura 1 año completo. Esto se debe a que el memorista también estaba trabajando laboralmente.

Sin embargo, se logró obtener un buen framework sobre cómo entregar reportes de test de penetración a aplicaciones web, teniendo una muy buena recepción por parte del cliente voluntario y los profesionales quienes apoyaron considerablemente la elaboración de este estándar, corrigiendo y aportando con sus conocimientos.

Con respecto al alcance (pentesting web) los estudios demostraron que fue acertado limitarlo a un solo aspecto de los tipos de pentesting, ya que unos de los mayores problemas identificados en los reportes propuestos por las distintas instituciones intentan abarcar muchos tópicos utilizando la misma estructura, dejando fuera muchas de las especificaciones que podría tener un informe enfocado a los tests de penetración web.

Sobre el impacto en los actores

Evaluar el impacto sobre los actores fue una tarea interesante, ya que el feedback recibido de ellos permitió, por una parte, validar que la propuesta tenía sentido y les ayudaba considerablemente tanto a los clientes que recibían este tipo de servicios como a los que lo entregaban.

Los comentarios recibidos y la evaluación crítica de los profesionales demostraron que la memoria tuvo un éxito en base a los objetivos planteados inicialmente, logrando entregar una pauta de lectura, una estructura y plantear una estandarización de vocabulario para este tipo de servicios.

Con respecto al impacto directo en las partes involucradas se concluye lo siguiente:

a) Cliente:

- Logró entender los riesgos relacionados a los que sus sistemas se veían expuestos.
- Pudo priorizar las actividades de reparación
- Logró identificar los responsables que deben estar involucrados en la mitigación de las vulnerabilidades.
- Entendió las ventajas de un pentesting web por sobre uno realizado automáticamente
- Está en vías de aumentar la seguridad de su plataforma web.

b) Profesionales:

- Marca una guía para los que están iniciando en la elaboración de informes de penetración web.
- Genera una rúbrica adecuada para evaluar si los reportes entregados son suficientes.
- Posee un documento formal para ser presentado en auditoría.
- Apoya a la rápida clasificación y entendimiento de evaluaciones previas.
- Mantiene una estructura para poder continuar con la misma

Este impacto demuestra que la memoria cumplió con los objetivos propuestos, esperando que esto pueda difundirse más allá de las personas involucradas en la investigación de esta memoria.

Parte del contexto de la memoria se pretendió presentar este estándar al comité interministerial de ciberseguridad de Chile²⁴, sin embargo, por disponibilidad de tiempo de ambas partes no se pudo presentar. Pero está planificado realizarlo fuera del contexto de la memoria para poder continuar con esta labor de expandir el conocimiento.

Sobre la validez de los objetivos formulados

Los objetivos formulados fueron producto de múltiples conversaciones con compañeros de trabajo, distintos profesionales de ciberseguridad y distintos clientes en conferencias de seguridad como la 8dot8²⁵ y la Ekoparty en donde se evidenciaron problemas durante los entregables o solicitudes de test de penetración web. Estos objetivos se lograron validar de sobremanera al momento de realizar las investigaciones relacionadas al tema, ya que al levantar el estado del arte se pudo apreciar que no existía una solución única a este problema y que se necesitaba un estándar lo suficientemente flexible para las diversas situaciones que se puedan presentar. Adicionalmente durante la entrevista con el cliente fue posible comprobar que efectivamente, sin una guía, es muy difícil para un profesional no dedicado al tema de ciberseguridad entender de qué se trata cada sección y que luego de explicar utilizando el estándar, el entendimiento de la misma fue mucho más ágil y comprensible para la persona que recibía la información. Dentro de las conversaciones con los profesionales comentaban lo complejo que también era pedirle a un profesional que estaba comenzando en la disciplina realizar un informe sin pasarle una “maqueta pre-hecha” pero que sin embargo utilizando el framework, el iniciado podría tener el material necesario para poder orientarlo.

Estas situaciones permiten comprobar la validez de los objetivos presentados y que estaban acordes a la realidad chilena de la ciberseguridad. En base a los comentarios de los profesionales (tanto clientes como proveedores de servicio) indican que es un verdadero aporte a la disciplina de ciberseguridad tanto como negocio, como desde el punto de vista educativo.

²⁴ <http://ciberseguridad.interior.gob.cl/>

²⁵ <http://8dot8.org/>

Sobre las contribuciones y aplicaciones del trabajo realizado

Contribución Educativa

Las contribuciones de este trabajo con respecto a la parte educativa se pueden evidenciar en el marco teórico presentado en el capítulo 3 en el cual se trató de abarcar la mayor cantidad de términos técnicos e incluso comerciales que fueron parte de los estudios y entrevistas realizadas durante esta memoria. Esta contribución apoyará a establecer un mismo lenguaje técnico al momento de diseñar y licitar estos servicios.

Continuando la perspectiva educativa, la memoria aporta con una estructura y conocimientos para entregar reportes de pentesting webs sin necesidad de “reinventar la rueda” por parte de los profesionales. Por otra parte, les permite tener argumentos para defender los puntos expuestos durante su evaluación y protegerlos al momento de diseñar servicios de pentesting web y aclarar los entregables que el cliente recibirá.

Contribución Comercial y de Negocio

Desde el punto de vista comercial tiene dos contribuciones importantes. La primera permite a los clientes solicitar de manera correcta el servicio que realmente necesitan para su organización, ya que siguiendo este estándar pueden entender la diferencia al momento de levantar su licitación y utilizar el lenguaje correcto y no sea confundible por parte de los proveedores de servicios. La segunda contribución es para los proveedores de servicio, quienes con esta memoria pueden levantar de manera más acertada los requerimientos de los clientes, pudiendo realizar entregables de servicios acorde a las necesidades de los clientes.

Aplicaciones del trabajo

Con respecto a las aplicaciones del trabajo, este pudiera ser utilizado como el motor inicial de estandarización de leyes por el comité interministerial de ciberseguridad, para exigir una calidad, estructura y contenido mínimo que debe tener un reporte de pentesting web como servicio a las empresas chilenas. Adicionalmente se puede utilizar directamente el anexo de esta memoria para orientar a nuevos practicantes a realizar estos informes.

Finalmente, un cliente de estos servicios puede utilizar lo expuesto en esta memoria para realizar sus licitaciones y exigir directamente en ellas que se utilice el estándar y especificar, utilizando los términos técnicos, que es lo que necesita y como necesita que se lo entreguen.

Invitación a nuevas investigaciones relacionadas

Definitivamente una de las conclusiones más marcadas de esta memoria fue que quedó mucho tema sin abarcar debido a las limitaciones de alcance y de tiempo de desarrollo. Quedan oportunidades de mejores en el mismo estándar y para seguir desarrollando nuevos módulos o investigaciones que deriven de esta memoria.

Se invita al lector a continuar con los siguientes temas propuestos:

Elaboración de un modelo XML de reporte: Se invita a desarrollar un modelo XML que soporte la creación de reportes de penetración web que respeten el estándar acá mencionado. Existe un proyecto parecido llamado THE COMMON VULNERABILITY REPORTING FRAMEWORK (CSVRF²⁶) el que cumple el mismo objetivo, pero sólo para el reporte de vulnerabilidades y no del reporte completo. Se invita a realizar una extensión o seguir la misma idea.

Formato de auditoría: Las evaluaciones de seguridad permiten conocer el estado de seguridad de una compañía, sin embargo, las auditorías permiten a un ente externo tener una certificación auditada de un estado de seguridad. La consultoría a diferencia de una auditoría debe presentar los resultados proponiendo mejoras e identificando fallas para ser mitigadas, una auditoría debe actuar de manera imparcial ante lo auditado y debe entregar la visión del estado actual sin emitir ningún juicio. Se invita a realizar una forma estandarizada de los entregables que debe tener una auditoría de seguridad considerando normas internacionales como la PCI-DSS, HIPPA, NERC.

Expandir el estándar a otros tipos de tests de penetración: La memoria se limitó a realizar sólo el estándar especializado para los tests de penetración web, sin embargo, aún está abierta la brecha con los tests de penetración de redes corporativas, servidores, aplicaciones de escritorio y servicios *cloud*. Se invita a colaborar desarrollando la misma iniciativa y proponer nuevos estándares especializados en las demás disciplinas de la seguridad y llevarlo más lejos.

Mejora continua: La mejora continua es una de las labores más importantes de la ingeniería, y no podemos dejarla jamás de lado. Ningún sistema está a prueba de fallas ni es infalible. Se invita a futuros tesis o memorias a seguir contribuyendo con este estándar, modificando, agregando o quitando nuevos campos, definiciones o secciones que permitan aumentar aún más la calidad de servicio y la satisfacción de cliente de los servicios de test de penetración web y sus entregables.

²⁶ <https://www.icasi.org/cvrf/>

REFERENCIAS BIBLIOGRÁFICAS

- Alharbi, M. A. (18 de 09 de 2016). *Writing a Penetration Testing Report*. Obtenido de <https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343>
- Armerding, T. (23 de 10 de 2016). *Self-taught hackers rule*. Obtenido de <http://www.csoononline.com/article/2146363/security-leadership/self-taught-hackers-rule.html>
- Centre, N. C. (24 de 06 de 2017). *Scheme Penetration Testing*. Obtenido de <https://www.ncsc.gov.uk/scheme/penetration-testing>
- Chile, G. d. (19 de 10 de 2016). *Comité Interministerial de Ciberseguridad - Ejes*. Obtenido de <http://ciberseguridad.interior.gob.cl/ejes/>
- Deloitte. (01 de 01 de 2014). *Cambiar el juego en riesgo cibernético*. Obtenido de <https://www2.deloitte.com/sv/es/pages/risk/articles/changing-the-game-on-cyber-risk.html>
- INFORMATICA, B.-O. (s.f.). *La Triada CID Seguridad informatica*. Obtenido de <https://b-one-informatica.blogspot.cl/2016/02/la-triada-cid-seguridad-informatica.html>
- Ivy Wigmore, M. R. (24 de 09 de 2016). *Whatis.com - Offensive Security*. Obtenido de <http://whatis.techtarget.com/definition/offensive-security>
- Offensive, S. (18 de 09 de 2016). *Offensive Security*. Obtenido de Sample Penetration Testing Report: <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>
- OWASP. (10 de 04 de 2016). *Web Application Penetration Testing*. Obtenido de https://www.owasp.org/index.php/Web_Application_Penetration_Testing
- Rapid7. (01 de 10 de 2016). *How to Justify Your Security Assessment Budget*. Obtenido de http://informationsecurity.report/Resources/Whitepapers/75509947-78c3-484d-b1d0-b4c6b272f27d_How%20to%20Justify%20Your%20Security%20Assessment%20Budget.pdf
- Rouse, M. (18 de 10 de 2016). *Los 12 requisitos PCI DSS*. Obtenido de <http://searchdatacenter.techtarget.com/es/definicion/Los-12-requisitos-PCI-DSS>

- SANSInstitute. (24 de 09 de 2016). *About SANS Institute*. Obtenido de <https://www.sans.org/about/>
- Schneider, B. (18 de 09 de 2016). *Is Penetration Testing Worth it?* Obtenido de https://www.schneier.com/blog/archives/2007/05/is_penetration.html
- Security, R. (01 de 01 de 2016). *Vulnerability Quick View*. Obtenido de https://pages.riskbasedsecurity.com/2016-ye-vuln-quickview?portalId=614666&hsFormKey=cfc948dd2509430f38cbb4f0af83ea19&submissionGuid=5ed6cc5f-2d5e-49ba-a5ef-54bf762c1e19#module_13885068285937553
- Sheward, M. (19 de 03 de 2017). *The Art of Writing Penetration Test Reports*. Obtenido de <http://resources.infosecinstitute.com/writing-penetration-testing-reports/>
- Smith, E. (18 de 09 de 2016). *Reporting*. Obtenido de <http://www.pentest-standard.org/index.php/Reporting>
- Standard, I. (28 de 10 de 2016). *ISO27000 - Overview and Vocabulary*. Obtenido de [http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip)
- Tecnológico, C. d. (03 de 01 de 2017). *Registro de Empresas Certificadas*. Obtenido de <http://www.registrocdt.cl/registrocdt/www/admintools/registroEmpresa/index.asp>
- Wright, D. (18 de 10 de 2016). *Is Penetration Testing Now a Must for My Business?* Obtenido de <https://www.pcicomplianceguide.org/is-penetration-testing-now-a-must-for-my-business/>

ANEXOS A - Reporte Ejecutivo Anonimizado

ANEXO B - Reporte Técnico Anonimizado