TECTZAPIC
Revista Académico-Científica

Revista de divulgación científica y tecnológica. ISSN: 2444-4944
Tecnológico Nacional de México Campus Ciudad Valles

IMPLEMENTACIÓN DE UNA ESTRATEGIA DE PENTESTING CON SOFTWARE LIBRE.

IMPLEMENTATION OF A PENTESTING STRATEGY WITH FREE SOFTWARE.

Recibido: 15 de septiembre del 2020.
Aceptado: 29 de septiembre de 2020.

J.M. Salazar Mata[1]
A.V. Balderas Sánchez[2]
H. García Aldape[3]
C. Cruz Navarro[4]

RESUMEN

En la actualidad las Tecnologías de la Información y Comunicación (TIC's) son un bien necesario para toda organización, así como lo es también la seguridad de su información; la confidencialidad, la integridad, y la disponibilidad de esta. Obtener esquemas que aseguren todo lo anterior; es un gran reto, ya que al hacer uso de las TIC's siempre se corre el riesgo de ataques o intrusiones por hackers o crackers; quienes pueden acceder desde cualquier punto donde se tenga conexión a la Internet.

De acuerdo con el informe de la Policía Federal Cibernética, México ocupa el tercer lugar mundial en delitos cibernéticos; donde destaca que el 83% de los adultos mexicanos ha sido víctima de algún delito asociado a las nuevas tecnologías; y un 71% de los usuarios de tecnología informática ha sido infectado por lo menos alguna vez con un virus. Así mismo, el 11% ha declarado ser víctima de fraude; y 10% ha sufrido phishing (robo de identidad). En este sentido, las Instituciones de Educación Superior no están exentas de estas problemáticas; a inicios del año 2016 en los meses de enero y febrero, Institutos Tecnológicos pertenecientes a Tecnológico Nacional de México, se han visto expuestos a ciber-delitos y se han vulnerado los sistemas informáticos, principalmente en el Sistemas que Administran Información Escolar (SII). Ante la problemática planteada y dada la fragilidad de los sistemas informáticos en uso hoy en día, en este proyecto se pretende implementar una la metodología OWASP como una estrategia de Pentesting con herramientas de Software Libre como KALI Linux, para fortalecer la seguridad informática del sistema de información escolar (SII), realizando las pruebas de intrusión de acuerdo al modelo de seguridad elegido, con la finalidad de elaborar un plan de monitoreo, prevención y control en la seguridad informática para estos sistemas.

PALABRAS CLAVE

Hacker, Cracker, Pentesting, Linux, Seguridad.

ABSTRACT

At present, Information and Communication Technologies (ICTs) are a necessary good for every organization, as is the security of your information; confidentiality, integrity, and availability of the same. Have schemes that ensure all of the above; It is a great challenge, since when using ICTs there is always the risk of attacks or intrusions by hackers or crackers; who can access from any point where you have an-Internet connection.

According to the report of the Federal Cyber Police, Mexico ranks third in the world in cyber-crimes; where it stands out that 83% of Mexican adults have been the victim of some crime associated with new technologies; and 71% of computer technology users have been infected with a virus at least once. Likewise, 11% have declared to be victims of fraud; and 10% have suffered

[1] Profesor de Tiempo Completo. Tecnológico Nacional de México, Campus Ciudad Valles, juan.salazar@tecvalles.mx
[2] Profesor de Tiempo Completo. Tecnológico Nacional de México, Campus Ciudad Valles, alba.balderas@tecvalles.mx
[3] Profesor de Tiempo Completo. Tecnológico Nacional de México, Campus Ciudad Valles, horacio.garcia@tecvalles.mx
[4] Profesor de Tiempo Completo Tecnológico Nacional de México, Campus Ciudad Valles, claudia.cruz@tecvalles.mx

phishing (identity theft). In this sense, Higher Education Institutions are not exempt from these problems; At the beginning of 2016 in the months of January and February, Technological Institutes belonging to Tecnológico Nacional de México, have been exposed to cyber-crimes and computer systems have been violated, mainly in the Systems that Manage School Information (SII). Given the problems raised and given the fragility of computer systems in use today, this project intends to implement an OWASP methodology as a Pentesting strategy with Free Software tools such as KALI Linux, to strengthen the computer security of computer systems. school information (SII), performing intrusion tests according to the chosen security model, in order to develop a plan for monitoring, prevention and control of computer security for these systems.

KEY WORDS:

Hacker, Cracker, Pentesting, Linux, Security

INTRODUCCIÓN

El despunte en el desarrollo y crecimiento de las Tecnologías Informáticas han obligado a que todas las empresas apliquen en sus procesos de producción, industrias, educación, entre otras, el uso de internet, sobre todo el Internet de las Cosas "*IoT*", por sus siglas en inglés. Esto ha obligado a los desarrolladores de aplicaciones a que generen soluciones, en ocasiones dejando de lado o simplemente ignorando aspectos claves en la seguridad en los sistemas y aplicaciones.

Lo anterior, deja un área de oportunidad para los ciber-delincuentes que atacan a las computadoras o a los servidores, buscando y encontrando los huecos o vulnerabilidades de estos dispositivos y realizan los ataques, conocidos como hacker, La firma KPMG (junio 2020) publicó en su artículo el impacto de los delitos financieros en México, la lista de los ciber-delitos más comunes: falsificación, fraude, pornografía *infantil*, violaciones de la propiedad intelectual, derecho a la intimidad y el ciberterrorismo.

Por otro lado, en la revista Contenido (2020) indica que, la Policía Federal en el 2013, menciona que la información más vulnerable es: las cuentas bancarias, tarjetas de crédito, identidades completas, cuentas de subasta en línea, direcciones de correo electrónico y contraseñas. Además, que los sectores más afectados, son Instituciones académicas (39%); gobierno (31%); sector privado (26%). Al igual se indica que México ocupa el tercer lugar mundial en delitos cibernéticos. En donde el 83% de los adultos mexicanos ha padecido algún delito asociado a las nuevas tecnologías; y que un 71% de los usuarios de tecnología informática ha sido infectado por lo menos alguna vez con un virus. Un 11% ha declarado ser víctima de fraude. El 10% ha sufrido phishing (robo de identidad). Además, KPMG (junio, 2020) menciona que, las entidades con más delitos cibernéticos son: Nuevo León, Ciudad de México, Estado de México y Baja California.

El Sistema Nacional de Tecnológicos de México, no ha sido excluido de estos ataques. En el 2016, tecnológicos como Querétaro y Ciudad Victoria en gran escala y en el de Ciudad Valles en menor grado. Sin embargo; no deja de ser un delito grave. Sufrieron ataques en sus aplicaciones de escolares (Sistema Integral de Información “SII”); debido a la vulnerabilidad de su infraestructura informática o a la falta de personal capacitado en seguridad dejando abierta la puerta para los ciber-criminales.

En la publicación de El Horizonte (2016), en el banner de Yahoo.com, Youtube.com y en el noticiero televisivo de Televisa, explicaron que en algunos tecnológicos sucedió la intrusión o penetración al Sistema Integral de Información (SII), el cual contiene

principalmente las bases de datos del historial académico de los alumnos; en la cual los intrusos vía acceso remoto alteraron calificaciones propiciando que los estudiantes se involucren en acciones no éticas y no legales. El Tecnológico Nacional de México Campus Ciudad Valles no quedo exento de este ataque, ya que, con una entrevista realizada al exjefe del Centro de Cómputo, mencionó que, en el 2016, también fueron atacadas las bases de datos para alterar calificaciones en esta institución.

En la actualidad, los hackers intensifican la búsqueda de las vulnerabilidades para acceder a estos sistemas por las personas maliciosas. Principalmente en sistemas que administran información escolar, realizando acciones de intrusión, por ello, el Tecnológico está en una constante implementación de acciones de mejora como el monitoreo, prevención y control, pero a la fecha no han sido suficientes.

Por lo anterior, se estableció una estrategia para implantar una guía de prácticas de *Pentesting* con herramientas de Software Libre para fortalecer y prever la seguridad informática de los diferentes dispositivos y por consiguiente a los sistemas de información escolar.

El "*pentesting*" o "test de penetración" consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos. Esto es con autorización documentada por el dueño de la empresa o de los dispositivos, para no incurrir en un delito informático.

Para la realización de este proyecto, se vincularán trabajos de investigación y prueba con el Laboratorio de Software Libre (LabSol) del Centro Zacatecano de Ciencia y Tecnología (COZCyT). En los últimos tiempos, la participación del TecNM en ANUIES en el área de la Seguridad de la Información en sus diferentes comisiones, a tomando más importancia por parte de las instituciones de educación superiores (IES), principalmente en los tecnológicos y la participación en las comisiones de formación, investigación y vinculación.

Tabla1. Número de instituciones de educación superior (IES) en México

Tipo de IES	No. Instituciones
Universidades públicas	56
Institutos Tecnológicos	194
Otras públicas	56
Universidades Tecnológicas	60
Instituciones Particulares	693
Educación Normal	457
Total	**1,516**

METODOLOGÍA

La investigación será de tipo aplicativo, partiendo de un análisis contextual de la situación actual, para la preparación del escenario para la implementación de las pruebas,

para ello se utilizará la metodología propuesta en su investigación por Gaviria Valencia en su trabajo de tesis, ya que utiliza como sustento de aplicación de las pruebas de penetración, teniendo como base la guía OWASP v3.0 y la metodología OSSTMM v2.1., considerando la herramienta Kali Linux misma en este proyecto (Valencia, 2015).

Las fases son las siguientes:

1. **Identificación del contexto**
   a) Área. Establecer el área de trabajo para la realización del pentesting, así como las áreas o equipos que serán testeados.
   b) Responsabilidades. Se establecerá el equipo de trabajo, los roles y las actividades para cada uno de los colaboradores del hackeo, así como los responsables del análisis, interpretación, evaluación y validación de la información obtenida.
   c) Alcance. Identificar claramente el alcance de aplicación de las pruebas considerando áreas, equipos, sistemas, procesos o enlaces.
2. **Elección y configuración de la herramienta**
   a) Configuración del equipo. Equipo asignado para la realización de las pruebas de Pentester.
   b) Instalación de la herramienta. Instalación y configuración del sistema operativo Kali Linux, así como todas sus herramientas aplicables para este caso de estudio.
3. **Determinación de las pruebas**
   a) Caja blanca. Se identificarán las pruebas que puedan ser aplicables mediante el conocimiento del funcionamiento interno del sistema, y con información que puede tener acceso uno o varios colaboradores del instituto.
   b) Caja gris. Se seleccionarán algunas pruebas de este tipo para aquellos aspectos del funcionamiento del sistema que pueden no ser conocidos.
   c) Caja negra. No se consideran como prioridad, sin embargo, se aplicarán solo en los casos que sea detectado vulnerabilidad que requiera ser explotada.
4. **Aplicación del modelo de penetración**
   a) Información. A través de la herramienta instalada, se iniciará la etapa de recolección de información sobre la empresa u objetivo meta establecido para el Pentester (archivos, IP, dominios, entre otros), todo esto de una forma pasiva, sin dejar rastro.
   b) Enumeración. Posterior a la identificación, se definirá el objetivo que se desea evaluar su vulnerabilidad, así como los puntos críticos de seguridad, en esta etapa se hace una recolección de información más específica de forma activa, entrando a los servidores para detectar equipos activos, sus sistemas operativos, los servicios que corren y sus respectivas versiones, rangos IP, DNS, detección de IDS y IPS, firewall, entre otros. En esta etapa se puede requerir el uso de otras herramientas para acceder a toda la información deseada.
   c) Análisis. En esta tercera fase se recopilará la información obtenida anteriormente para clasificar las posibles vulnerabilidades del sistema.

d) Explotación. La última fase es la más compleja del pentesting, aquí se utiliza la información obtenida en las fases anteriores, de las vulnerabilidades encontradas en el sistema se determina el tipo de prueba a aplicar para evaluar el grado de riesgo que existe en cada una de ellas.

5. Evaluación de resultados

a) Alcance de la herramienta utilizada. Se evaluará el alcance de la herramienta propuesta, así como la necesidad de incorporación de otras herramientas en el proceso.
b) Mejores Prácticas de Seguridad. Se identificarán los puntos de menor o nula vulnerabilidad para identificarlos como fortalezas y replicar su seguridad.
c) Áreas de mayor vulnerabilidad. Como se indica, se identificará las áreas de mayor vulnerabilidad para establecer acciones prioritarias para monitoreo y eliminación.

6. Plan de acción

a) Plan estratégico de Pentesting para monitoreo y reacción en cuestiones de seguridad informática
b) Determinación de estándares aplicables en seguridad informática y formación del recurso humano.

RESULTADOS

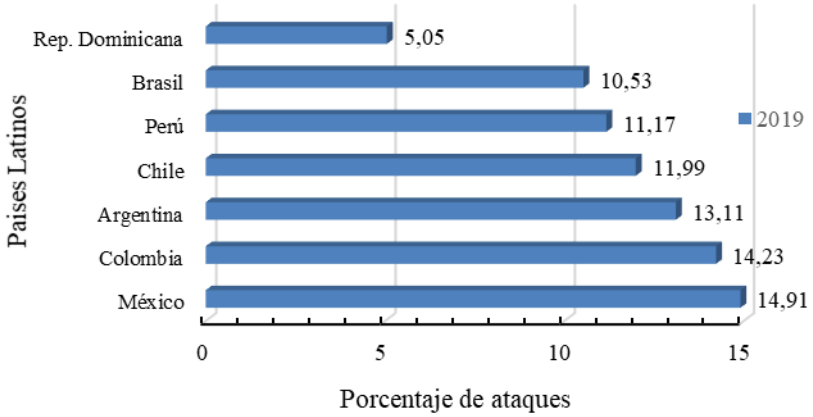
En sala de prensa, la firma KPMG (junio, 2020), proporciona datos muy importantes con el avance de la tecnología, los ataques cibernéticos se han convertido en un riesgo creciente para las organizaciones, ante el cual no siempre están preparadas. Por ejemplo, aunque 86% de las compañías afirman que utilizan un antivirus, así como firewalls internos o externos (71%), solo tres de cada diez han realizado evaluaciones de ciberseguridad, tales como pruebas de **penetración** "***pentesting***", a pesar de que estas son obligatorias para los bancos y otras entidades del sistema financiero. Otros hallazgos importantes en esta materia también revelan la vulnerabilidad de las organizaciones:

- 23% de los encuestados afirman que su empresa fue víctima de algún incidente de ciberseguridad en los últimos 12 meses; de ellos, el más popular es el malware (51%), seguido de la suplantación de identidad de proveedores y personas en los correos electrónicos corporativos (41%), y en tercer lugar el phishing (32%).
- A raíz de los ciberataques, la mitad de las empresas encuestadas sufrieron daños económicos, mientras que 22% sufrió daños legales, y 17% reputacionales.
- Para 47%, los costos de los ciberataques ascienden a menos de medio millón de pesos, mientras que 23% reporta que el costo fue de más de 2 mdp por incidente. En promedio, cada incidente de ciberseguridad representa un daño económico de 1.2 mdp.
- 52% de los encuestados manifiestan desconocer la fuente del ataque, lo que implica grandes retos en materia de las investigaciones de este delito, mientras que 36% de los ataques fueron realizados por grupos hacktivistas; 30%, por el crimen organizado, y 21%, por empleados o exempleados de la compañía

Según Shelley, citado en su publicación KPMG (junio, 2020) indica que "Hoy más que nunca, con la necesidad del trabajo a distancia y la dependencia en la tecnología, es fundamental que organizaciones e individuos estén alertas ante las amenazas que representa un entorno digital y las diversas formas de hacerles frente. Para ello, lo más importante es crear conciencia y capacitar a las personas para responder adecuadamente ante las amenazas, así como implementar controles tecnológicos preventivos y de investigación".

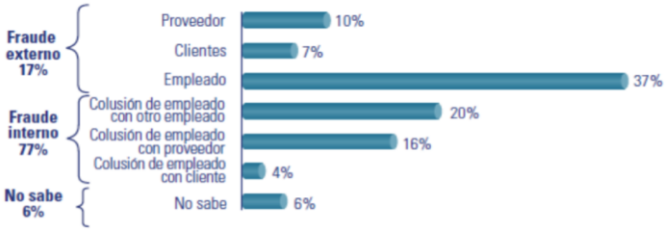
Es por eso que, aunque existan diversas tácticas efectivas para proteger los sistemas; como la puesta en marcha de buenas prácticas de seguridad o la instalación de una herramienta integral de alta tecnología; el Pentesting sigue representando un recurso vital para el equipo de seguridad de Tecnologías de Información pues contribuye a definir una estrategia de defensa que sea verdaderamente sólida y eficaz para cada caso en particular.

Otros datos importantes de KMPG obtenidos de Kaspersky, 2020 y, que a tomar en cuenta se representan en las siguientes imágenes. Donde en la gráfica 1, se observa que México es el país con mayor porcentaje de ataques cibernéticos fraudulentos, de los principales países latinos.



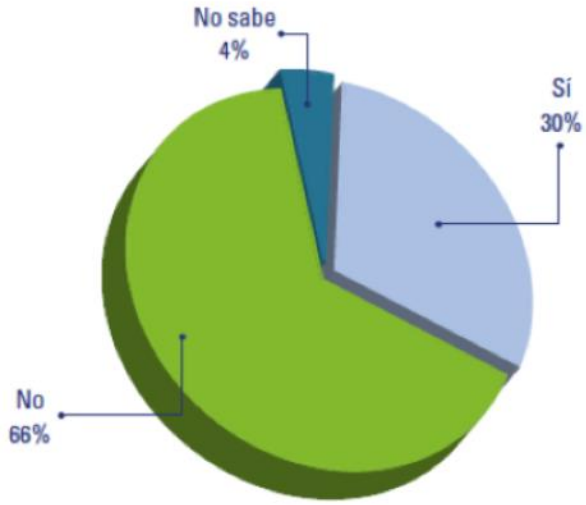
Gráfica 1. Incidencias de fraudes en America Latina.

Por otro lado, KMPG en la gráfica 2 se muestra que las empresas, el mayor porcentaje de los ataques cibernéticos son fraudes internos es de 77%, es cual es muy alto.



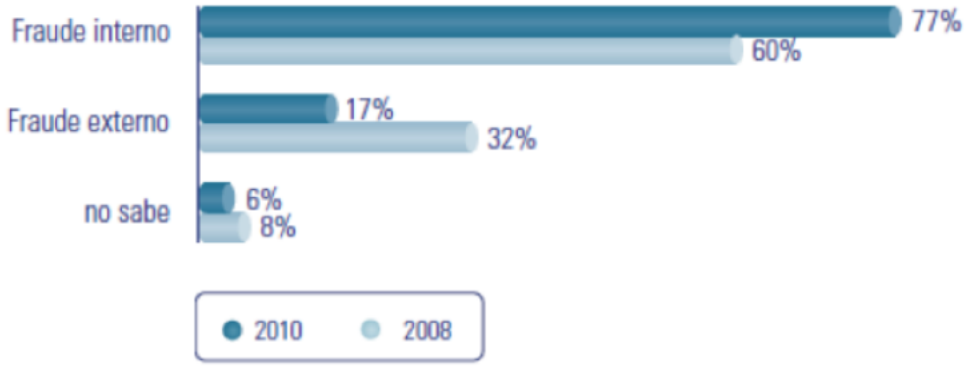
Gráfica 2. Tipos de fraudes por perpetrador del ilícito.

Además, KMPG indica que esto es debido a que, las empresas en un 66% no cuentan con alguna medida de prevención, lo cual es considerado muy elevado, el cual se muestra en la gráfica 3.



Gráfica 3. Porcentaje de empresas con medidas de prevención de fraudes.

Otra gráfica, donde se muestra el tipo de fraude que se ha incrementado a través del tiempo, es el interno de un 60% a un 77%, como se ve en la gráfica 4.



Gráfica 4. Comparativo de incidencias de fraudes.

Es por ello, que con estos datos; es de suma importación que las organizaciones como ANUIES y el TecNM lo tomen en cuesta, ya que ninguna organización o empresa está acepando los ataques cibernéticos. Y hacer conciencia en los directivos y personal general lo delicado y vulnerables los diferentes dispositivos con respecto al robo de la información.

CONCLUSIONES

Un par de barreras a vencer son:1) la de involucrar a los diferentes actores del TecNM, como son directivos, estudiantes y personal; esto debido a la poca o nula importancia que se le da a esta rama de la "La Seguridad de la Información", en caso específico el Pentesting o Hacker Ético; y 2) la otra es la falta de un plan de seguridad que involucre la capacitación continua del recurso humano que apoye en el manejo de la información. Aun sabiendo que en ciertos campus se ha intentado ataques o accedido las bases de datos de algunos sistemas, no se les ha dado la importancia y el apoyo a las áreas responsables de la seguridad de los Tecnológicos, solo se han realizados acciones aisladas al respecto. Inclusive, hay cierta indiferencia por parte de las autoridades federales (TecNM). Otro aspecto a considerar adicional a las dos principales barreras es el apoyo económico que se tiene que invertir en capacitación, certificaciones, infraestructura, laboratorios equipados, entre otros para generar una cultura de seguridad en las instituciones tecnológicas.

Es por ello por lo que, en analizando los resultados de esta revisión documental y propuesta de plan de acción, se emiten algunas recomendaciones para la mejora e implementación logrando ser competitivos en esta área de la seguridad:

1. Formar más recurso humano involucrando estudiantes.
2. Implantar y evaluar el manual de mejores prácticas elaborado bajo este contexto.
3. Plantear un programa de capacitación al personal encargado del Centro de Cómputo y a estudiantes, buscando el apoyo del COZCyT y de ANUIES.
4. Con los resultados positivos, realizar una divulgación del Manual en le TecNM.
5. Crear un laboratorio de seguridad, para este caso *Pentestin*g o Hacker Ético.
6. En la siguiente etapa (aún no contemplada en este trabajo), será un proyecto de Cómputo Forense; para poder cerrar el ciclo de seguridad, principalmente en temas de gran interés como el hackeo o robo de información.

BIBLIOGRAFÍA

Contenido, policía cibernética. Ella nos cuida en la red. Boletín 028. (2020). https://contenido.com.mx/2016/06/policia-cibernetica-nos-cuida-la-red/

El horizonte. (2016). Más de 100 alumnos en Querétaro son dados de baja por hackear calificaciones. https://d.elhorizonte.mx/nacional/mas-de-100-alumnos-en-queretaro-son-dados-de-baja-por-hackear-calificaciones/1692139

Fernando, V. S. (2013). Khali Linux y Beaglebone Black: Un sabueso de ARMas tomar. Revista de la Universidad Piloto de Colombia, 1-5.

Guardia, J. E. (2017). Pentesting "prueba de penetración" para la identificación de vulnerabilidades en la red de computadoras en la alcaldía en municipio de Cantón de San Pablo, Departamento de Chocó. QUIBDÓ-CHOCÓ: Universidad

Nacional Abierta y a Distancia- Escuela de Ciencias Básicas Tecnología e Ingeniería.

INTRIAGO, V. K. (2018). Propuesta de una Metodología de Pruebas de Penetración orientada a riesgos. Guayaquil: Universidad Espíritu Santo.

Jiménez, R. E. (2017). Pruebas de penetración en aplicaciones web. Revista Tecnológica, 13-19.

KPMG. (25 junio 2020). El impacto de los delitos financieros en México. https://home.kpmg/mx/es/home/sala-de-prensa/press-releases/2020/06/kpmg-presenta-el-impacto-de-los-delitos-financieros-en-mexico.html

LEMUS, W. E. (2017). Aplicación de pentesting a la red de la secretaria de Bogotá: Universidad Nacional Abierta y a Distancia UNAD.

Luis, R. R. (2013). Pruebas de penetración o Pentest. Revistas Bolivianas-Revistas Electrónicas en línea, 31-33.

Serrato, G. (2016). Metodología para el análisis de vulnerabilidades. TIA.

Valencia, R. A. (2015). Guía práctica para pruebas de pentest basada en la metodología Osstmm v2.1 y la guía Owasp v3.0. Pereira: Universidad Libre Seccional Pereira.

Veloz, J. (2017). Ethical Hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta Kali Linux. Revista de Tecnología de la Informática y las Comunicaciones, 1-12.