Análisis de vulnerabilidades a la ETITC

SAPIENTIAM

Jose Trejos jtrejos@itc.edu.co (Director) Cristian Espinel (Coordinador)

caespinell@itc.edu.co

Introducción

Mas del 83% de las pequeñas y medianas empresas carecen de protocolos de respuesta a la violación de políticas de seguridad de la información, esto según el informe de seguridad que publico la CCIT, para periodo 2019-2020 [1]. La principal razón es porque las empresas en Colombia no conocen su infraestructura y ecosistema de ciberseguridad, aún más de sus vulnerabilidades y activos de valor en alto riesgo, por lo que realizar un Pentesting es el de vital importancia para brindar una visibilidad completa de los fallos en ciberseguridad que tiene cada empresa y con esto desprender un lineamiento especializado para cada entidad en ciberseguridad.

Objetivos

Objetivo General

Realización de un pentesting bajo estándares abalados y con las técnicas y herramientas apropiadas.

Objetivos específicos:

- Analizar las vulnerabilidades mediante herramientas técnicas.
- Divulgar los hallazgos encontrados en el proceso de explotación a los integrantes del equipo.
- Generar con los estudiantes del semillero, un proceso de reflexión pedagógica para dar a conocer aspectos fundamentales de las pruebas de penetración.

Planteamiento del Problema y justificación

La realidad que vive nuestro país en materia de seguridad informática es alarmante, de un número determinado de pequeñas y medianas empresas encuestadas se verifica que, en la gran mayoría, no cuentan con un equipo especializado de reacción en materia de ciberseguridad, la principal razón es por presupuesto o desconocimiento de la importancia de la ciberseguridad en la actualidad.

Los integrantes del semillero de investigación SAPIENTIAM, por su parte para poder suplir con estas necesidades en el ámbito laboral realizaran un pentesting a la misma institución ETITC, requiere como por ejemplo y para ser más específicos al realizar un test de vulnerabilidades y pruebas de penetración de una infraestructura tecnológica.

La información digital es un valioso activo del que dependen las organizaciones. Mantener su integridad, confidencialidad y disponibilidad, es esencial para alcanzar los objetivos de la institución.

El Pentesting permite identificar riesgos, vulnerabilidades y malas prácticas de configuración y manejo de información digital de las empresas. De esa forma estas, pueden tomar acción para corregir los fallos antes de que un ciberdelincuente se aproveche de ellos y genere afectaciones graves.

Marco teórico

El Pentesting o también llamado test de penetración está diseñado para determinar el alcance de los fallos de seguridad de un sistema. Asimismo, es una de las practicas más demandadas actualmente ya que gracias a estas pruebas, una empresa puede llegar a saber a qué peligros está expuesta y cuál es el nivel de eficiencia de sus defensas.

¿Cómo se realiza un Penetration Test?

Se utiliza una metodología de evaluación de seguridad informática que incluye cuatro grandes etapas:

1) Descubrimiento
2) Exploración
3) Evaluación
4) Intrusión

Si bien el orden de las etapas no es arbitrario, en muchos casos se paralelizan o adelantan tareas dependiendo de las características de la plataforma evaluada.

Metodología

La metodología seleccionada: “Aprender Haciendo”, es una investigación de tipo cualitativo, como un proceso permanente de producción de conocimiento, donde los resultados son momentos parciales, que de manera continua se integran dando lugar a nuevos interrogantes, abriendo nuevos caminos a la producción del conocimiento.
Aprender Haciendo, “learning by doing” en inglés, es una metodología de aprendizaje con enfoque del constructivismo donde el énfasis está puesto en el aprendizaje en contraposición a las metodologías de tipo conductistas donde el énfasis está puesto en la enseñanza.

En vez de la secuencia habitual que vá de la teoría a la práctica (Teoría → Práctica) se invierte el proceso (Práctica →Teoría). (Fuente: National Training Laboratories, 1977)

Se trabajan tres (3) pautas a seguir, a saber:

1. ¿Por qué?

Una realidad que no se puede obviar es que una persona aprende:

- El 20 % de lo que ve
- El 20% de lo que oye
- 2. Guía del Método

El método considera las siguientes etapas o proceso de aprendizaje:

- Experiencia/Vivencia.
- Análisis de la experiencia (¿Qué pasó?, ¿Cómo fue la experiencia?)
- Lecciones aprendidas. Construcción de conocimientos.
- Aplicación a futuro, generalización, proyección a futuro.

Actividades

Actividad	Fecha
Análisis de vulnerabilidades a la ETITC	27 de febrero al 3 de marzo
Divulgación de hallazgos y análisis de resultados con vicerrectoría y directivos de la ETITC	6 de Marzo
Hacking Day	29 de Marzo
Reunión interinstitucional de Semilleros Areandina	Abril
Consolidación y socialización del documento construido	10 de Mayo
Entrega de resultados	1 de junio

Resultados

1. Con el conocimiento adquirido se realizará un pentesting de calidad e informe completo con todas las vulnerabilidades presentadas para así dar mejores
2. recomendaciones logrando una mejor seguridad en nuestra escuela.
3. Se realizara el Hacking day su 9na versión.
4. Se realizara una reunión de semilleros con el AreaAndina para socialización de resultados

Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

References

[1] cámara colombiana de informática y telecomunicaciones. Tendencias de cibercrimen. , Disponible en https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/ ultimo acceso el 23/072020

[2] MinTic ley de protección de datos 1581 de 2012. Disponible en https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf ultimo acceso 22/07/2020

[3] Informe del C4 de la Policía, la CCIT y TicTac presenta el panorama en ciberseguridad del país. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790 ultimo acceso 23/07/2020

[4] Informe de ciberseguridad. Disponible en https://latam.kaspersky.com/ ultimo acceso 20/07/2020

[5] Que es un pentesting. Disponible en : https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting ultimo acceso 24/07/2020

[6] Tipos de pntesting. Disponible en : https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting ultimo acceso 24/07/2020