ANÁLISIS DE VULNERABILIDADES INFORMÁTICAS A LA ETITC

Evaluacion de seguridad a los sistemas informaticos de la Escuela Tecnologica Instituto Tecnico Central

AUTORES

Brian Ferney Rojas García
Cristian Andrés Espinel Londoño
Edinson Jair Yara Rueda
Javier Alberto Isaza Caicedo
Jenny Valentina Rojas Orjuela
Juan David Rueda Quiroga
Liliana Katherine Forero Vargas
Luis David Gil Martínez
Manuel Felipe pacheco Gutiérrez
Mily Alejandra Cordon Guzman

01. INTRODUCCIÓN

Se busca realizar un análisis de vulneravilidades informáticas a la ETITC con el fin de ayudar a la seguridad que tiene la infraestructura informática con la que cuenta la escuela.

Se explicará como se ha procedido en la realización de esta actividad, resultados alcanzados y los resultados que se esperan al siguiente semestre con la continuación de este proyecto.

02. OBJETIVOS

General: Realizar un pentesting a la ETITC.
Específicos:
Capacitar a los estudiantes que realizaran el pentesting a la ETITC identificar las aplicaciones y métodos que se utilizaran para el desarrollo del Pentesting hecho a la ETITTC
Presentar un informe sobre las vulnerabilidades encontradas en los servidores y pagina web de la ETITC

03. PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

Basándonos en las constantes actualizaciones tecnológicas que día a día se presentan en el mundo y el como esta afecta a la seguridad de la información se nos ha hecho necesario el identificar las diversas vulnerabilidades que presentan los sistemas de información, para saber como combatirlos y aplicar medidas de seguridad actualizadas que protejan los datos en este caso de la ETITC.

Es por esta razón que de manera periódica se es necesario aplicar pruebas de testing y generar un informe de los hallazgos en este testing.

08. RESULTADOS

En conjunto se realizó una búsqueda de herramientas lúdicas para el aprendizaje colectivo acerca del hacking ético como lo es Owasp Juice Shop entre otras, se invitó a expertos en el área de seguridad informática para que cuenten sus experiencias sobre seguridad informática y también para que nos retro alimenten en el proceso que se ha realizado, adicional a ello se realiza aprendizaje autónomo acerca del tema para reforzar conocimientos acerca del tema. Se realizó cotizaciones para capacitar al equipo acerca de "Capacitación de ethical hacking y red team" que dura aproximadamente 2 meses, esto con el fin de conocer de la mano de un profesional como se realiza estas actividades.

Se espera que el siguiente semestre que con los conocimientos adquiridos a lo largo de la investigación realizada durante el semestre y con la capacitación que se espera realizar. Con el conocimiento adquirido se realizará un pentest de calidad e informe completo con todas las vulnerabilidades presentadas para así dar mejores recomendaciones logrando una mejor seguridad en nuestra escuela.

Basándonos en el pentesting ya realizado a la empresa 24 satelital, esperamos poder reforzar nuestros conocimientos y mejorar en la presentación de nuestros resultados obtenidos en el próximo análisis a la ETITC

BIBLIOGRAFÍA

- Red Team Guide.. Disponible en https://github.com/tanc7/hacking-books/blob/master/RTFM%20-%20Red%20Team%20Field%20Manual%20v3.pdf ultimo acceso el 11/06/2022
- BlueTeam Guide. Disponible en https://github.com/tom0li/collection-document/blob/master/Blue%20Team%20Field%20Manual.pdf ultimo acceso 11/06/2022
- 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 11/06/2022
- Informe de ciberseguridad. Disponible en https://latam.kaspersky.com/ ultimo acceso 11/06/2022
- Que es un pentesting. Disponible en : https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting ultimo acceso 11/06/2022
- Tipos de pentesting. Disponible en : https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting ultimo acceso 11/06/2022

05. MARCO TEÓRICO

Uno de los temas de mayor auge que tiene actualmente el mundo de la tecnología es la seguridad informática, ya que día a día somos testigos de los múltiples ataques a empresas y sistemas de información que se creían invulnerables a estos. Para favorecer empresas y usuarios, se ha creado una normatividad que tiene como finalidad reglamentar el cuidado de la información como el bien más preciado que tiene cualquier organización. Es así como existen varios tipos de Pentesting y métodos que se clasifican según el tipo de información que se tenga a la hora de realizar las pruebas:

- Pentesting de caja blanca "White Box": Análisis teniendo conocimiento de la infraestructura completa.
- Pentesting de caja negra "Black Box": Análisis sin tener algún conocimiento de la infraestructura.
- Pentesting de caja gris "Grey Box": Análisis teniendo conocimiento parcial de la infraestructura.
- Red Team y Blue Team: Equipo atacante y equipo defensor.
- Etapa de Descubrimiento: Se estudian los activos tecnológicos disponibles.
- Etapa de Exploración: Observar posibles vulnerabilidades blancos de ataque.
- Etapa de Evaluación: Se intentan vulnerar los blancos y evaluar su seguridad.
- Herramientas de scanning de vulnerabilidades: Conjunto de programas para evaluar la seguridad.
- Búsqueda manual de vulnerabilidades: Búsqueda de información publica sin necesidad de scanneres.
- Etapa de Intrusión: Según la información recolectada en las etapas anteriores, se realizan los ataques.
- Escalación de privilegios: Intentar obtener la mayor cantidad de funciones restringidas posibles.
- Pentesting: Análisis de vulnerabilidades informáticas a un sistema para evaluar su seguridad

06. METODOLOGÍA

Se realiza entrevista a personal administrativo de la ETITC acerca de la necesidad de tener este análisis de vulneraviidades y así efectuarlo, paralelo a ello todo el grupo se debe capacitar acerca de hacking ético como lo son los métodos y herramientas para ello además para trabajar en equipo se debe entender la metodología de Red Team y Blue Team, todo lo anterior para poder hacer un análisis de vulnerabilidades efectivo y de calidad como paso final.

07. ACTIVIDAD

Semestre II-2022					
ACTIVIDAD	1	2	3	4	5
Instrucción a estudiantes y diseño de laboratorio de pruebas	x				
Análisis de metodología y vulnerabilidades		x			
Divulgación de hallazgos y análisis de resultados			x		
Reflexión ética/pedagógica con los semilleristas	x	x	x	x	x
Consolidación y socialización del documento construido				x	
Entrega de resultados					x