Propuesta de Arquitectura para Emulación de Adversarios

Trabajo Terminal No. 2019-B102

Alumnos: Ramirez Gibbs Jorge Alberto, *Sánchez Cruz Víctor Iván
Directores: M. en C. Saucedo Delgado Rafael Norman, Ing. Sandoval Delgado Raúl
Turno para la presentación del TT:
*email: vsanchezc1404@alumno.ipn.mx

Resumen – El presente trabajo terminal busca proponer una arquitectura para emulación de adversarios. Así mismo, se probará dicha arquitectura desarrollando software sobre la misma, esto permitirá emular adversarios de manera automatizada pudiendo realizar evaluaciones de seguridad periódicas abatiendo tiempo y costos para las organizaciones.

Palabras clave – Ciberseguridad, Redes de Computadoras, Sistemas Operativos, Simulación.

1. Introducción

Actualmente los riesgos informáticos representan una amenaza a entidades públicas, privadas, gubernamentales y al entorno digital en general. En cifras del 2018, México es el segundo país más atacado de la región de América Latina, sólo después de Brasil.
Para las organizaciones, (empresas, gobierno, educativas, etc) las evaluaciones de seguridad de sus activos es un reto mayúsculo al demandar entre otras cosas, tiempo y costos en recursos materiales, humanos y económicos. Así mismo, realizar evaluaciones periódicas o recurrentes implica una inversión aún mayor.

A continuación, se enlista una serie de taxonomías necesarias para contextualizar .

- **Vulnerabilidad** – Una falla o debilidad en los procedimientos de seguridad del sistema, diseño, implementación o controles internos que podrían ejercerse (activarse accidentalmente o explotarse intencionalmente) y dar como resultado una violación de seguridad o una violación de la política de seguridad del sistema [1].
- **Adversario** – Individuo, grupo, organización o gobierno que realiza o tiene la intención de realizar actividades perjudiciales [2].
- **Prueba de Penetración (Pentesting)** – Son un tipo especializado de evaluación realizada en sistemas de información o componentes individuales del sistema para identificar vulnerabilidades que podrían ser explotadas por los adversarios. Dichas pruebas se pueden usar para validar vulnerabilidades o determinar el grado de resistencia que los sistemas de información organizacional tienen ante los adversarios dentro de un conjunto de restricciones específicas (por ejemplo, tiempo, recursos y/o habilidades) [3].
- **Red Team** – Grupo de individuos organizados y autorizados para simular un potencial ataque de un adversario o su capacidad de explotación en contra del nivel de maduración en seguridad informática de una organización [4].

El mecanismo de evaluación más utilizado en México son las pruebas de penetración o *pentesting* sin embargo, por su alcance, puede llegar a ser insuficiente para evaluar las

amenazas actuales; cada vez éstas son más complejas. Por esta razón, se ha ido introduciendo ejercicios de *Red Team* para simulación de adversarios. Al tener un alcance más profundo, los resultados son más cercanos a la realidad. En contraste, los recursos invertidos en un ejercicio de *Red Team* son mayores. Como resultado, se ha diseñado soluciones para emular (simulación automatizada) a los adversarios siguiendo marcos de trabajo y metodologías.

SOFTWARE	**CARACTERÍSTICAS**
ATOMIC RED TEAM [5]	Atomic Red Team es una biblioteca de pruebas simples que los equipos de seguridad puede ejecutar para probar sus defensas. Las pruebas están enfocadas, tienen pocas dependencias y se definen en un formato estructurado que puede ser utilizado por los marcos de automatización.
CALDERA [6]	CALDERA es un sistema automatizado de emulación de adversarios, funciona al unir habilidades a un adversario y ejecutar al adversario en una operación.

2. Objetivo

Implementar un sistema de emulación de adversario, siguiendo las tácticas y técnicas documentadas en la matriz ATT&CK de MITRE sobre la arquitectura propuesta.

2.1. Objetivos Específicos

- Desarrollar del software basado en la arquitectura propuesta.
- Construir laboratorio para ejecutar las pruebas del desarrollo.
- Generar manuales técnicos de la arquitectura y del software desarrollado

3. Justificación

El presente trabajo encuentra justificación en tres frentes:

- Social
- Económico
- Académico

Como se mencionó anteriormente, de acuerdo a cifras de la Encuesta de Delitos Económicos del 2018 se puede destacar que:[7]

- México es el segundo país más atacado de la región de América Latina, el primer lugar lo ocupa Brasil.
- El 49% de las empresas se han enfocado principalmente en evaluar sus vulnerabilidades y riesgos de ciberataques.
- El 56% de las empresas encuestadas, indicaron haber sido víctimas de ciberataques, causando en la mayoría grandes pérdidas para las organizaciones.

Análogamente en términos económicos, de acuerdo con el reporte Tendencias de seguridad en América Latina y el Caribe el cibercrimen le cuesta al país entre 3,000 y 5,000 millones de dólares al año. [8]
Por otro lado, el Sistema de Pagos Electrónicos Interbancarios (SPEI) fue víctima de un ataque de proporciones mayores, teniendo un impacto económico de aproximadamente 300 millones de pesos. Con esto podemos ver, que a pesar de ser el sistema financiero un sector crítico también ha sido vulnerado. [9]

La propuesta de una arquitectura no es una tarea trivial ya que requiere conocimientos de:

- Programación
- Ciencias de la computación
- Redes
- Sistemas Operativos
- Ingeniería de software
- Desarrollo de aplicaciones web
- Gobernanza de TI

Adicionalmente, en la formación necesaria para realizar el trabajo terminal se requirió de la asistencia de dos cursos de nivel posgrado:

- Ciberseguridad
- Análisis de Vulnerabilidades

4. Productos o Resultados Esperados

Los resultados esperados de este trabajo terminal son:

- La arquitectura sobre la cual se desarrollará el sistema.
- Desarrollo del sistema de emulación de adversario.
- Laboratorio para realizar pruebas.
- Documentación necesaria para agregar módulos.
- Reportes.

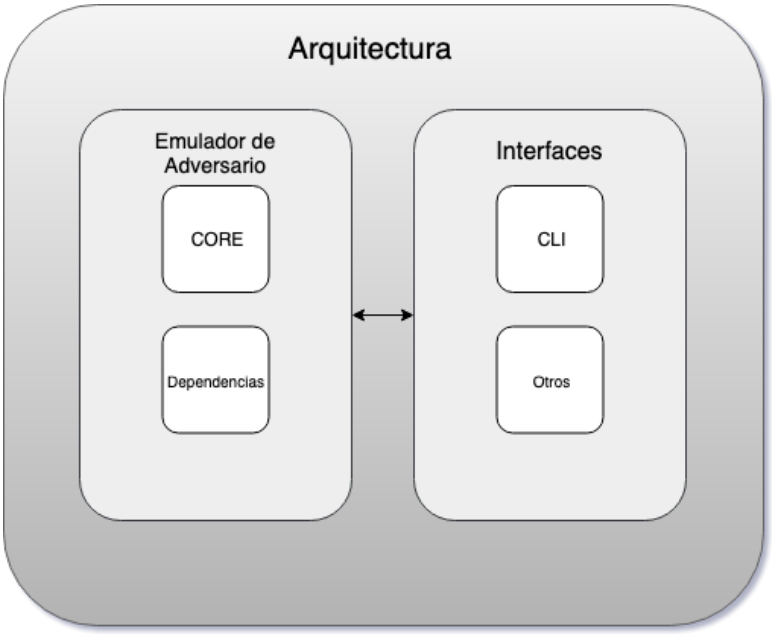

Figura 1. Arquitectura del sistema.

5. Metodología

Al requerir la redefinición e integración constante de requerimientos y módulos, las necesidades de desarrollo de la arquitectura se ajustan a las características de una metodología evolutiva, específicamente por prototipos de características selectas [10]. Siguiendo la metodología , se propone el desarrollo de 3 prototipos mediante los cuales se buscará llegar a la arquitectura final con las mejoras, adiciones y modificaciones requeridas.

El primer prototipo tiene el objetivo de definir los requerimientos y características básicos de la arquitectura, adicionalmente, familiarizarnos con la metodología y definir un esquema de trabajo para el resto del tiempo de desarrollo. El segundo prototipo se propone como uno funcional de la arquitectura, con los requerimientos propuestos para esta etapa funcionales. El tercer prototipo se designa como el prototipo final , una arquitectura con módulos funcionales.

6. Cronograma

Cronograma 1

Ramírez Gibbs Jorge Alberto

Actividad	Ene	Feb	Mar	Abr	May	Jun	Ago	Sep	Oct	Nov	Dic
Redacción del reporte de Trabajo Terminal.											
Análisis de requerimientos generales.											
Análisis de requerimientos del primer prototipo.											
Diseño del primer prototipo.											
Documentación del primer prototipo.											
Elaboración del primer prototipo.											
Entregable I.											
Retroalimentación de los resultados de desarrollo del primer prototipo.											
Análisis de requerimientos del segundo prototipo.											
Diseño del segundo prototipo.											

Documentación del segundo prototipo.											
Elaboración del segundo prototipo.											
Entregable II.											
Preparación de presentación de TT1.											
Evaluación de TT1.											
Correcciones y análisis de resultados de TT1.											
Análisis y Diseño del tercer prototipo.											
Documentación del tercer prototipo.											
Elaboración del tercer prototipo.											
Entregable III.											
Preparación de presentación de TT2.											
Evaluación de TT2.											

Cronograma 2
Sánchez Cruz Victor Iván

Actividad	Ene	Feb	Mar	Abr	May	Jun	Ago	Sep	Oct	Nov	Dic
Redacción del reporte de Trabajo Terminal.											
Análisis de requerimientos generales.											
Análisis de requerimientos del primer prototipo.											
Diseño del primer prototipo.											
Documentación del primer prototipo.											
Elaboración del primer prototipo.											

Entregable I.											
Retroalimentación de los resultados de desarrollo del primer prototipo.											
Análisis de requerimientos del segundo prototipo.											
Diseño del segundo prototipo.											
Documentación del segundo prototipo.											
Elaboración del segundo prototipo.											
Entregable II.											
Preparación de presentación de TT1.											
Evaluación de TT1.											
Correcciones y análisis de resultados de TT1.											
Análisis y Diseño del tercer prototipo.											
Documentación del tercer prototipo.											
Elaboración del tercer prototipo.											
Entregable III.											
Preparación de presentación de TT2.											
Evaluación de TT2.											

7. Referencias

[1] National Institute National Institute of Standards and Technology, *NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems: NiST SP 800-47*. 2002.

[2] National Institute of Standards and Technology, *Nist Sp 800-30 Rev 1 Guide for Conducting Risk Assessments: September 2012*. Createspace Independent Publishing Platform, 2012.

[3] K. Dempsey, G. Witte, y D. Rike, “Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations”. 2014.

[4] National Institute of Standards and Technology, *Nist Sp 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. Createspace Independent Publishing Platform, 2015.

[5] “Using Atomic Red Team to test your security”, *Atomic Red Team*. [En línea]. Disponible en: https://atomicredteam.io/.

[6] mitre, “mitre/caldera”, *GitHub*. [En línea]. Disponible en: https://github.com/mitre/caldera.

[7] PricewaterhouseCoopers, “Delitos económicos 2018”, *PwC*. [En línea]. Disponible en: https://www.pwc.com/mx/es/servicios-forenses/delitos-economicos.html.

[8] “Estrategia Nacional de Ciberseguridad México”. 2017.

[9] Notimex, “Banxico confirma que ciberataque a SPEI fue por 300 millones de pesos”, *El Economista*, 16-may-2018. [En línea]. Disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Banxico-confirma-que-ciberataque-a-SPEI-fue-por-300-millones-de-pesos-20180516-0087.html.

[10] Kendall , Kenneth E. y Kendall , Julie E. 2011 *Análisis y diseño de sistemas.* , 8a ed., México: PEARSON EDUCACIÓN. Pág.156.

8. Alumnos y Directores

Sánchez Cruz Víctor Iván - Alumno de la carrera de Ingeniería en Sistemas Computacionales en Escuela Superior de Cómputo, Especialidad Sistemas, Boleta: 2015630461, Tel. 5543536699 e-mail: vsanchezc1404@alumno.ipn.mx

CARÁCTER: Confidencial FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública. PARTES CONFIDENCIALES: Número de boleta y teléfono.

Firma:_____

Ramírez Gibbs Jorge Alberto - Alumno de la carrera de Ingeniería en Sistemas Computacionales en Escuela Superior de Cómputo, Especialidad Sistemas, Boleta: 2016630318, Tel. 5549311847 e-mail: georgeramirezz97@gmail.com

Firma:_____

Norman Saucedo Delgado - Ingeniero en Sistemas Computacionales (IPN - ESCOM), Maestría en Ciencias de la Computación (UNAM).

Firma:_____

Raúl Sandoval Deglado - Ingeniero en Sistemas Computacionales (IPN - ESCOM), Fundador de Rogue Services, empresa especialista en consultoria sobre ciberseguridad, -con 6 años de experiencia en el campo Áreas de Interés: Pentesting, Secure Code Review, Ciberseguridad. Datos de contacto 5569378976, rulo@roguesecurity.io

Firma:_____