Planificación detallada de un producto de software

Jorge Puente –Magister Informática

Definición del proyecto

Motivación: A pesar de la gran cantidad de ciber-ataques producidos hoy en día, no existe una herramienta, capaz de predecir la frecuencia de cada uno de ellos dentro de las organizaciones, basándose en análisis de la infraestructura tecnológica y permitiendo anticiparse directamente a las amenazas y daños potenciales.

Justificación del problema: Para llevar a cabo el desarrollo de una herramienta, basada en una arquitectura escalable de evaluación estocástica, que permita el análisis de vulnerabilidades asociadas a ciertos patrones de ataque, es necesario realizar una representación abstracta, tanto de explotación de dichas vulnerabilidades, como de los patrones de ataque existentes, a fin de realizar una automatización de prueba y diagnóstico que permita establecer una dualidad entre ambos.

Alcance: Como etapa inicial, el proyecto se centrará en la elaboración de un componente de software (Generador de ataques viables), interactuando con una interfaz mínima, capaz de analizar la infraestructura tecnológica en busca de dos vulnerabilidades existentes potenciales, que a su vez permitan establecer un patrón de ataque viable; determinando la probabilidad de ocurrencia.

Objetivo general: Elaborar y probar un componente de software capaz de analizar vulnerabilidades existentes en una infraestructura tecnológica y determinar si es posible establecer sus patrones de ataques asociados.

Objetivos específicos:

- Analizar la infraestructura tecnológica en busca de vulnerabilidades asociadas a puertos abiertos, en este caso puerto 23 con el servicio telnet activo y protocolos IP, en específico ICMP
- Determinar y diagnosticar patrones de ataques asociados a las vulnerabilidades del servicio telnet trabajando bajo el puerto 23 y el protocolo de control de mensajes ICMP
- Elaborar una primera versión del componente Generador de ataques viables, contenido dentro de la arquitectura del Pronosticador de ciber-riesgos.