UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

TÍTULO: Automatizando la resolución de problemas en competencias de Seguridad Informática

AUTORES: Basso Facundo – Pretto Jeremías

DIRECTOR: Venosa Paula

DIRECTOR: Lanfranco Einar

ASESOR PROFESIONAL: -

CARRERA: Lic. En Sistemas – Lic. En Informática

Resumen

Actualmente se llevan a cabo múltiples competencias internacionales de Seguridad Informática conocidas como Capture The Flag (CTF), donde distintos equipos distribuidos a través del planeta compiten resolviendo desafíos de distintas categorías. Nuestra motivación principal al ser participantes habituales de dichas competencias, consiste en generar herramientas las cuales automaticen las tareas repetitivas que suelen requerirse para la resolución de dichos desafíos persiguiendo la idea de reutilizar las soluciones o mecanismos ya empleados y evitando de esta forma "reinventar la rueda" en cada nuevo evento. La tesina se basa en el desarrollo de dos herramientas: RSolver, que ayuda a automatizar la resolución de desafíos de criptografía RSA. Y SYPER CTF Tools, la cual provee una plataforma web para equipos de CTF que permite disparar una batería múltiples herramientas de forma intuitiva y amigable.

Palabras Clave

Capture The Flag, CTF, automatización, RSA, DRY, criptografía, esteganografía, RSolver, SYPER CTF Tools, Seguridad Informática, Jeopardy, Ataque-Defensa, explotación web, plaintext, ciphertext, algoritmos asimétricos, clave privada, algoritmos de factorización, ataque de Wiener, ataque de Hastad, ataque de texto plano común, ataque de texto plano relacionado, ataque a instancias con exponente público bajo, ataque de mensaje estereotipado, esteganografía en bit menos significativos, OWASP Top Ten.

Conclusiones

Gracias al uso de las herramientas descritas en esta tesina, hemos podido lograr una significativa optimización del uso del tiempo en competencias del tipo CTF, el cual era nuestro objetivo principal al desarrollarlas. También logramos facilitar el aprendizaje de ataques al protocolo RSA ya que la herramienta además de automatizar la resolución de los problemas hace hincapié en el aspecto formativo de los mismos. Por otra parte estas herramientas favorecen la integración de nuevos participantes ya que permiten un uso fácil e intuitivo.

Trabajos Realizados

Desarrollo de la herramienta RSolver para automatizar la resolución de problemas frecuentes en CTF de criptografía RSA.

Desarrollo de la herramienta SYPER CTF Tools para integrar y facilitar el uso mediante una interfaz web de una batería de aplicaciones CLI usualmente utilizadas en CTF.

Trabajos Futuros

RSolver
- Agregar nuevos ataques RSA
- Soporte multithreading de los ataques
- Agregar soporte AES, XOR, GPG
- Migración scripts Sage a Python

Syper CTF Tools
- Destacar ejecuciones mediante tags
- Filtrado de tags
- Incorporar nuevas herramientas
- Mejorar mecanismo de actualización

Fecha de la presentación: Diciembre 2019