Investigación en ciberseguridad en un año de pandemia

Javier Díaz - jdiaz@linti.unlp.edu.ar
Paula Venosa - pvenosa@linti.unlp.edu.ar
Nicolás Macia - nmacia@linti.unlp.edu.ar
Einar Lanfranco - einar@linti.unlp.edu.ar
Alejandro Sabolansky - asabolansky@linti.unlp.edu.ar
Mateo Durante - mdurante@linti.unlp.edu.ar
Damián Rubio - drubio@linti.unlp.edu.ar
Jeremías Pretto - jpretto@linti.unlp.edu.ar

LINTI
Laboratorio de Investigación de Nuevas Tecnologías Informáticas
Facultad de Informática
Calle 50 y 120- La Plata - Argentina
Universidad Nacional de La Plata

CONTEXTO

La línea de investigación "Ciberseguridad" presentada se desarrolla en el marco del proyecto de investigación "De la Sociedad del Conocimiento a la Sociedad 5.0: un abordaje tecnológico y ético en nuestra región"[3] del Programa Nacional de Incentivos. Este proyecto está acreditado por la UNLP (Universidad Nacional de La Plata) y financiado por partidas del presupuesto nacional. De dicha línea participan docentes investigadores del LINTI de la Facultad de Informática de la UNLP.

Palabras clave: ciberseguridad, monitoreo inteligente, threat intelligence, gestión de incidentes, CTF.

LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

En la actualidad, las principales líneas de trabajo en las que el grupo de investigación en ciberseguridad desarrolla sus actividades y consolida su formación son las siguientes:

:: Detección y análisis de vulnerabilidades en distintos tipos de dispositivos, protocolos y tecnologías.
:: Desarrollo de herramientas propias para la automatización de los procesos de gestión de incidentes de seguridad y escaneo de vulnerabilidades. Integración con otras existentes.
Pentesting de redes, aplicaciones y servicios.
:: Monitoreo de seguridad de red. Uso de herramientas de Machine Learning para un monitoreo inteligente.
OSINT. Uso de software libre para el uso, el procesamiento y la correlación de distintas fuentes de información de amenazas.
:: Formación y actualización a través del desarrollo de competencias mediante la continua participación en concursos de tipo Capture The Flag.

RESULTADOS Y OBJETIVOS OBTENIDOS

Objetivos:

Desarrollar una metodología para detectar hosts infectados basada en Ensembling que haga uso de técnicas de aprendizaje automático y datos de Threat Intelligence e integrar a los sistemas de monitoreo proactivo de CERTUNLP.

Integrar nuevos feeds al sistema de gestión de incidentes NGEN para enriquecer la información obtenida a partir de los sistemas internos y los datos intercambiados con otros grupos.

Implementar nuevos servicios reactivos para tener contar con mayor información sobre los recursos de nuestra organización.

Fortalecer las capacidades en ciberseguridad del grupo de investigación y diversos grupos de interés a partir de la organización y participación en competencias de tipo CTF.

Diseñar soluciones alternativas que aborden la problemática de los ataques de DDoS y puedan ser usadas por organizaciones de bajos recursos.

Promover buenas prácticas de seguridad en el ciclo de vida de desarrollo de software.

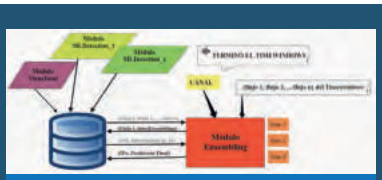
Resultados obtenidos:

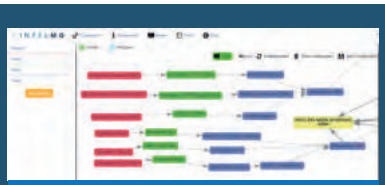
:: Diseño de metodología para detectar hosts infectados aplicando Ensembling Learning
:: Diseño y propuesta de implementación de un módulo de Ensembling para integrar a Slips, IPS desarrollado por Stratosphere Labs.
:: Integración de IntelMQ a NGEN, sistema de gestión de incidentes de CertUNLP.
:: Implementación de scanner de servicios activos de la UNLP.
:: Diseño y organización de diversas competencias de tipo CTF para equipos académicos, equipos de ciberseguridad y alumnos de escuelas secundarias.

FORMACIÓN DE RECURSOS HUMANOS

En esta línea de investigación trabaja un grupo de docentes/investigadores del LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas) de la Facultad de Informática de la UNLP (Universidad Nacional de La Plata). Parte de este grupo también forma parte de CERTUNLP, el CSIRT Académico de la Universidad Nacional de La Plata, ámbito en el cual aplican directamente las temáticas propuestas.
En el marco de estas actividades:
Se ha finalizado la tesis para obtener la Maestría en Redes de Datos: "Detección de ataques de seguridad en redes usando técnicas de ensembling" de la Lic. Paula Venosa. Esta tesis realizó aportes al proyecto SLIPS del Stratosphere Laboratory en República Checa, que funciona en el ámbito de la CVUT (Czech Technical University in Prague).
Se encuentra en su etapa final de desarrollo la tesina de grado de Damián Rubio "Evolución del sistema de gestión de incidentes de seguridad orientado a CSIRT de la UNLP - NGEN".
Se ha presentado la propuesta de la tesina de grado de Mateo Durante y Cristian Barbaro relacionada a la implementación de una herramienta para mitigar ataques de DDoS.

Además, se continuó con la consolidación del equipo de CTF, denominado SYPER, formado por alumnos y docentes. El mismo participó en distintos eventos, tanto nacionales como internacionales durante el 2020.


Arquitectura del módulo de Ensembling de Slips


Inicio de INTELMQ:


Panel de administración de NGEN:

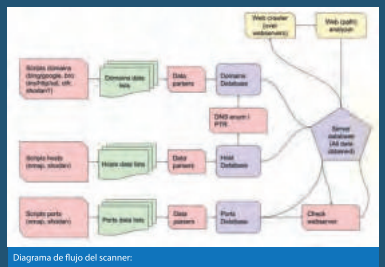
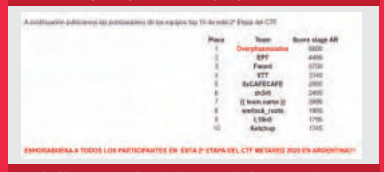


Diagrama de flujo del scanner:

CTF Internacional organizado por Metared - 2da etapa (Argentina)


Resultados del CTF Internacional organizado por Metared - 2da etapa (Argentina)

Performance del equipo SYPER en CTFs

	Argentina		Mundo		# CTFs
	Posición	# Equipos	Posición	# Equipos	Competidos
2018	1	4	141	18235	21
2019	1	13	221	24551	15
2020	1	30	150	35997	22

Participación en CTFs por parte del equipo integrado por docentes y alumnos.