Investigación en ciberseguridad en un año de pandemia

Javier Díaz, Paula Venosa, Nicolás Macia, Einar Lanfranco, Alejandro Sabolansky, Mateo Durante, Damián Rubio, Jeremías Pretto

Laboratorio de Investigación de Nuevas Tecnologías Informáticas (LINTI).
Facultad de Informática. Universidad Nacional de La Plata
50 y 120 La Plata
{jdiaz, pvenosa, nmacia, einar, asabolansky, mdurante, drubio, jpretto}@linti.unlp.edu.ar

RESUMEN

El grupo de investigación en ciberseguridad de la UNLP forma parte del LINTI[1] y participa e impulsa en forma ininterrumpida desde el año 2000 distintos proyectos nacionales e internacionales en relación a la temática. Entre los autores de este artículo se encuentra el equipo de CERTUNLP[2], primer CSIRT académico de la Argentina creado en 2008.
En el presente artículo se describe el trabajo que el equipo lidera en relación a detección de vulnerabilidades, detección de ataques, mitigación de ataques y gestión de incidentes.
Un pilar fundamental para el crecimiento del equipo es trabajar en proyectos vinculados a la formación de recursos humanos en estas temáticas, es por ello que también se incluye la experiencia de este último año en relación a la organización de CTFs los cuales propician un ámbito de formación para la comunidad, de una forma innovadora y motivadora.

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

CONTEXTO

La línea de investigación “Ciberseguridad” presentada en este trabajo, 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 y financiado por partidas del presupuesto nacional. De dicha línea participan docentes investigadores del LINTI de la Facultad de Informática de la Universidad Nacional de La Plata (UNLP).

1. INTRODUCCIÓN

La detección de malware y ataques mediante el análisis de tráfico de red continúa siendo un desafío para los responsables del monitoreo de seguridad de una red de datos y de la gestión de los incidentes de seguridad[4]. Aunque existen varios mecanismos de detección bien conocidos para diferenciar con precisión los comportamientos maliciosos de los normales, todavía es extremadamente difícil contar con sistemas de detección eficientes.
Desde hace algunos años, los sistemas de detección de intrusiones han incorporado paradigmas inteligentes como las técnicas de aprendizaje automático. Hoy en día existen también algunas propuestas para implementar algoritmos de Ensemble Learning[5][6], a fin de combinar múltiples clasificadores para lograr una mejor precisión en la detección.
Además de los mecanismos y herramientas, para implementar una defensa eficaz, las organizaciones necesitan contar con información sobre los posibles atacantes, como sus técnicas, tácticas y procedimientos. Esta metodología, denominada inteligencia de amenazas, ayuda a las organizaciones a

comprender mejor su perfil de amenazas. Las fuentes de inteligencia permiten obtener indicadores que luego podrían ser utilizados por dispositivos como firewalls o sistemas de detección de intrusos para disponer de una reacción oportuna a las amenazas emergentes.
Si se logra combinar la información de inteligencia con los mecanismos de detección de malware y detección de tráfico anómalo, permitiría gestionar los incidentes de seguridad de manera integral mejorando la mitigación de los ataques a los que estamos expuestos.
La gestión de incidentes de seguridad no debe ser un proceso separado de los procesos de monitoreo de seguridad y detección de incidentes a partir del uso de fuentes de información o feeds. Es por esto, que los sistemas de detección de incidentes utilizados, deben poder interactuar de manera fluida con otros procesos para poder automatizar dicha gestión, lo máximo posible.
En búsqueda de una evolución constante, y para no depender exclusivamente de fuentes externas de información para la gestión de incidentes, se requiere implementar herramientas de relevamiento continuo de información, que permitan identificar las fortalezas y debilidades de los servicios prestados a Internet por nuestra comunidad objetivo, manteniendo un historial que permita realizar consultas históricas y poder implementar análisis evolutivos.
Para poder llevar a cabo todas estas actividades, es necesaria la formación continua de recursos humanos tanto para el grupo de investigación como para la sociedad en general. En esta línea, es necesario generar marcos de capacitación formal a través del dictado de materias y cursos en el ámbito académico además de fomentar la formación a partir de un contexto lúdico a través del desarrollo de eventos de tipo 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.

3. RESULTADOS OBTENIDOS Y ESPERADOS

Como principales objetivos se plantean:

- Desarrollar e implementar un método de detección de hosts infectados, basado en ensembling, que tenga en cuenta los resultados de detección de distintos clasificadores, que usen técnicas de aprendizaje automático y datos de Threat Intelligence y pueda funcionar con ventanas de tiempo y detección a lo largo del tiempo.

- Proponer una integración del mecanismo de ensembling para detectar hosts infectados, al servicio de monitoreo proactivo de seguridad de CERTUNLP [2], CSIRT Académico de la Universidad Nacional de La Plata.
- Desarrollar y mantener un sistema programable y configurable capaz de brindar soporte a la gestión de incidentes de seguridad en el ámbito de trabajo de un Computer Security Incident Response Team (CSIRT). Es deseable que dicho sistema sea integrable con otros componentes de software que son utilizados en la comunidad de CSIRTs
- Hacer posible la integración de los feeds al sistema de gestión de incidentes para así incorporar los enriquecedores de información que sirven para mejorar la base de conocimiento de un incidente y facilitar el intercambio de información con otros grupos.
- Capacitar al grupo de investigación y a terceros en distintas temáticas de ciberseguridad, mediante la implementación/organización y participación en CTFs con el objetivo de visibilizar, fomentar el interés e incorporar nuevas problemáticas y metodologías de resolución que puedan ser incorporadas y aplicadas en distintos ámbitos [7][8].
- Analizar la problemática y las alternativas de mitigación frente a ataques de denegación de servicio distribuidos en Internet con el objetivo de alcanzar una solución integral y abierta para que administradores de organizaciones con bajos recursos puedan acceder a una solución para mitigar este tipo de ataques utilizando un scrubbing center comunitario que permita captar y filtrar parte del tráfico relacionado con el ataque de DDoS.
- Implementar servicios reactivos que permitan contar con mayor visibilidad sobre los distintos recursos de nuestra organización para así mejorar las capacidades en la detección, prevención, gestión y análisis de incidentes de seguridad.
- Promover buenas prácticas en relación a la ciberseguridad que aplican en todas las etapas del ciclo de vida del desarrollo, de los servicios y de la gestión de las organizaciones.

Entre los resultados que se han obtenido en este último período se destacan:

- El diseño de una metodología para detectar hosts infectados en la red aplicando Ensemble Learning y la creación de un procedimiento asociado para testear la misma través de experimentos usando datasets reales y sus resultados.
- El diseño y propuesta de implementación del módulo de Ensembling integrado a Slips [9][10], en el marco de un trabajo de colaboración con el Laboratorio Stratosphere de la Universidad Técnica de República Checa de Praga.
- La actualización del sistema de incidentes NGEN integrando el mismo a IntelMQ con el fin de centralizar y normalizar la información obtenida de distintas fuentes de información las cuales se reciben por distintos canales de comunicación y en diferentes formatos.
- La implementación de un scanner de servicios activos de la UNLP. Este desarrollo hizo posible contar con una herramienta de relevamiento continuo que permite de manera centralizada, mantener actualizada en tiempo real y consultar información sobre los servicios brindados, los recursos de DNS usados, los productos de software, las

plataformas y las tecnologías utilizadas por la comunidad de la Universidad.

- La organización de diversas competencias de tipo CTF. En el último tiempo, el grupo de investigación organizó, desplegó y diseñó competencias de tipo CTF, desde la instalación de la infraestructura requerida hasta la creación de los retos de la competencia. Entre los eventos destacados se encuentran:
  - Etapa Argentina (segunda etapa) del CTF Internacional MetaRed 2020. Esta etapa contó con la participación de 342 equipos de 37 países distintos. [11]
  - CTF OWASP LATAM@Home 2020 organizado en el marco del OWASP LATAM TOUR 2020. Este CTF contó con 525 usuarios registrados de la comunidad internacional, representando a 181 equipos participantes [12].
  - 2 CTFs con alumnos de escuelas secundarias en el marco del Proyecto de Extensión "Vínculos con Escuelas Secundarias" de la Facultad de Informática de la UNLP. Uno de ellos en el marco del evento Chicas en TICs y el otro auspiciado por la embajada de Estados Unidos. Para ello se adaptó la plataforma creada en la Tesina de grado "Capture the flag aplicada a la enseñanza de ciberseguridad en escuelas secundarias" realizada por los alumnos Patricio Bolino y Gabriela Suárez [8] creando nuevos desafíos para esta instancia.

4. 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 [2], 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)[13].
También 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". Esta tesis, está íntimamente ligada al desarrollo y evolución de NGEN, el sistema de gestión de incidentes actualmente usado en CERTUNLP y liberado como software libre para su uso y contribución por parte de la comunidad.
Además, 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.
Y como ocurre hace unos años, continuamos con la consolidación del equipo de CTF, denominado SYPER[14], formado por alumnos y docentes. Teniendo participación en distintos eventos, tanto nacionales como internacionales durante el 2020.

5. REFERENCIAS

[1] LINTI: Laboratorio de Investigación en

Nuevas Tecnologías Informáticas www.linti.unlp.edu.ar
[2]CERTUNLP. Sitio institucional https://www.cert.unlp.edu.ar (accedido en febrero de 2021).
[3] Proyectos I+D - 11/F028 (2020/2023)- "De la Sociedad del Conocimiento a la Sociedad 5.0: un abordaje tecnológico y ético en nuestra región http://secyt.presi.unlp.edu.ar/Wordpress/wp-content/uploads/2020/03/DISPOSICION-130.pdf
[4] Emmanouil Vasilomanolakis et al. Taxonomy and survey of collaborative intru-sion detection. ACM Computing Surveys (CSUR), 47:1–33, 2015.
[5] Emna Bahri et al. Approach based ensemble methods for better and faster intrusion detection. Computational Intelligence in Security for Information Systems, pág. 17–24, 2011.
[6] Emna Bahri et al. A survey of intrusion detection systems based on ensemble and hybrid classifiers. Computers Security, 65:135–152, 2017.
[7]Francisco Javier Díaz et al.(2018). WICC 2018 (Workshop de Investigadores en Ciencias de la Computación). UNNE, Corrientes, Argentina. Abril de 2018. Libro de Actas XX Workshop de Investigadores en Ciencias de la Computación. pp1056-1060. ISBN 978-987-3619-27-4.
[8]Francisco Javier Díaz et al. Participación y despliegue de CTFs como herramienta para fortalecer la formación en ciberseguridad WICC 2020 (Workshop de Investigadores en Ciencias de la Computación). UNPA, Santa Cruz, Argentina. Abril de 2020. Libro de Actas XX Workshop de Investigadores en Ciencias de la Computación. pp1056-1060. ISBN 978-987-3714-82-5.
[9]Stratosphere Lab. Stratosphere IPS https://www.stratosphereips.org/stratosphere-ips-suite.2
[10]Repositorio donde se encuentra la versión de SLIPS con el módulo Ensembling https://github.com/pvenosa/StratosphereLinuxIPS
[11]Sitio del evento de Metared https://eventos.metared.org/55909/detail/ctf-internacional-metared-2020.html
[12]Sitio del evento OWASP LATAM https://owasp.org/www-event-2020-latam-at-home/
[13]Stratosphere Thesis Projects homepage https://www.stratosphereips.org/thesis-projects.
[14] Perfil del equipo SYPER https://ctftime.org/team/2003