Tendencias en incidentes de seguridad atendidos por el CERT académico Cert-UNLP

Einar Lanfranco, Nicolás Macia, Paula Venosa, Lía Molinari, Javier Díaz

LINTI, Laboratorio de Investigación en Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad Nacional de La Plata, calle 50 y 120, La Plata, Buenos Aires, Argentina
{einar, nmacia, pvenosa, lmolinari, javierd}@linti.unlp.edu.ar

Resumen

El presente artículo describen los primeros pasos recorridos durante el primer año de funcionamiento del CERT[1] académico que funciona en el ámbito de la Universidad Nacional de La Plata Cert.-UNLP, proyecto que se define a partir de la necesidad de dar respuesta a los incidentes de seguridad que aumentan día a día. Durante dicho año, se recepcionaron diversos tipos de problemas de seguridad en diferentes unidades académicas de la UNLP, lo que permitió dar a conocer el trabajo del grupo por medio de la asistencia dada para la resolución de los problemas. Asimismo, cabe mencionar distintas tareas realizadas para permitir una mejor atención. Estas tareas comprenden el desarrollo de herramientas para la automatización de las tareas diarias, definición de procedimientos, capacitaciones en distintos temas e investigación sobre distintos problemas de seguridad. Se destaca como un importante valor agregado del proyecto el uso de herramientas open source para las actividades relacionadas con forensia, pentests y monitoreo proactivo.

Keywords: CERT, CSIRT, incidente de seguridad, pentest, forense, sensores.

Contexto

El siguiente trabajo trata sobre el aporte que implica tener un equipo de respuesta de incidentes de seguridad trabajando dentro del ámbito de la comunidad académica para el servicio de ésta.

La línea de investigación presentada está inserta en el proyecto de incentivos del LINTI "Redes, Seguridad y Desarrollo de Aplicaciones para e-educación, e-salud, e-gobierno y e-inclusión".

Las actividades realizadas están en el marco del Convenio ONTI – UNLP (2006-2009) en el cual se acordó poner en marcha un programa de trabajo on el objetivo de generar un ámbito de investigación, desarrollo, transferencia, cooperación y complementación en materia de seguridad informática, en particular en el desarrollo de la tecnología de firma digital, en la gestión y análisis de incidentes informáticos y en el desarrollo de acciones comunes para la protección de las redes de datos.

El trabajo operativo de CERT-UNLP es coordinado por el CeSPI de la UNLP.

1. Introducción

Un CERT, también conocido como CSIRT[2], es una organización que provee servicios y soporte para prevenir, manejar y dar respuesta a los incidentes de seguridad de la información que ocurren en el ámbito en el cual el CERT trabaja[1]. Presta los servicios necesarios para ocuparse de estos incidentes y ayudar a los damnificados a recuperarse después de sufrir uno de ellos.

Con la aparición de Morris, el primer gusano importante a fines de los '80 que se propagó rápidamente y logró infectar gran cantidad de equipos a lo largo de todo el mundo, los administradores de sistemas, y gestores de la tecnología de la información, vieron la necesidad de cooperar entre sí, y coordinarse de manera de poder enfrentarse a este tipo de casos. Sin duda, éste fue un paso decisivo para establecer un enfoque común y más organizado en el tratamiento de los incidentes relacionados a la seguridad de la información.

Poco después de este incidente, se crea el primer CSIRT: el CERT Coordination Center (CERT/CC), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania). Poco después el modelo se adoptó en Europa, y en

[1] CERT: Computer Emergency Response Team
[2] CSIRT: Computer Security Incident Response Team

1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnet-CERT. Desde entonces el número de equipos de similares características, ha ido en paulatino aumento, y su distribución ya incluye a muchos países del mundo.

CERT UNLP tiene como misión ser un Centro de Respuestas de Incidentes de Seguridad Académico en el ámbito de la Universidad Nacional de La Plata de manera tal de dar seguimiento y respuesta a incidentes que afectan activos de la Universidad como así también a incidentes originados dentro de nuestra red.

2. Líneas de investigación y Desarrollo

La función básica de todo equipo de respuesta a incidentes de seguridad es la atención y seguimiento de incidentes. Sin embargo, además de esta tarea, existen un conjunto de tareas adicionales que permiten tanto mejorar el servicio dado como así también planear contramedidas para mitigar las tendencias que presentan los incidentes recepcionados. En esta línea, se puede decir que CERT UNLP además de la atención y seguimiento de incidentes, ofrece servicios de forensia, tests de penetración y monitoreo proactivo de seguridad.

Para poder llevarse a cabo eficientemente estos temas de investigación suponen la comprensión, el análisis y el aprendizaje de nuevos conceptos. En lo que a forensia se refiere, éste aspecto es fundamental para en el caso de tratar un incidente grave causado por un host o servidor de la red de la Universidad, poder hacer un análisis en vivo y postmortem del dispositivo, que permita establecer como, cuando y de que manera se produjo la intrusión al host o servidor y como fue utilizado por el atacante una vez vulnerado.

En lo que a tests de penetración se refiere, son importantes para poder establecer de manera proactiva la seguridad de un servidor. Los mismos involucran conocer aspectos de seguridad de sistemas operativos, servicios, aplicaciones web, configuraciones, etc. En ocasiones, ante la ocurrencia de un incidente menor sobre un servidor y a pedido del administrador del mismo, se puede realizar este tipo de tests para determinar si es posible y cuan fácil es para un intruso concretar un ataque exitoso, por ejemplo tomando el control de un servidor. En general, este tipo de pruebas ayuda tanto para advertir sobre los peligros existentes actualmente a los administradores y desarrolladores, como para concientizarlos sobre buenas prácticas de seguridad.

Por último, en lo referente al monitoreo proactivo de seguridad, es una línea de investigación en la que se analiza diferentes formas de monitorear la red de forma tal de detectar en forma temprana la ocurrencia de un ataque. En tal sentido pueden ser útiles herramientas de monitoréo, HIDSs, NIDSs y honeypots, entre otros.

3. Resultados obtenidos/esperados

Durante esta primera etapa se realizaron diferentes tareas en distintas áreas. Estas tareas involucran temas de difusión, manejo de incidentes, automatización de tareas, capacitación, análisis forenses, tests de penetración, monitoreo proactivo y definición de procedimientos.

Difusión

Junto con el CERT, se creó el sitio público http://www.cert.unlp.edu.ar donde se brinda información a la comunidad, se ofrecen buenas prácticas de seguridad en diferentes aspectos y se atienden incidentes de seguridad internos y externos que afectan activos propios o foráneos.

El proceso de atención de incidentes en ocasiones implica interactuar con otros CERTs, razón por la cual en ocasiones se trabaja en forma conjunta con el ArCert.

Otras actividades como la de dar charlas de concientización dentro de la comunidad académica de la UNLP, entregar mousepads que incluyen el decálogo de la seguridad o realizar actividades en el marco de la semana de la seguridad informática, ayudan a dar difusón a este grupo.

Actualmente el grupo tiene cierto reconocimiento dentro de la UNLP, siendo referente de los administradores de red de distintos lugares sobre temas de seguridad, configuración e incluso monitoreo con honeypots.

Herramientas desarrolladas

Con el objeto de automatizar el chequeo de direcciones IP de la UNLP listadas en listas tipo blacklists, se desarrolló una herramienta llamada “Rainbow warrior”. La misma mantiene información básica de los diferentes administradores de las redes de la UNLP y permite realizar chequeos manuales y automáticos para verificar si los

servidores están listados en blacklists. En caso de encontrar algún problema de este tipo, envía mails automáticamente al administrador de la red correspondiente e inicia un caso en el sistema de manejo de incidentes.

Actualmente se está trabajando en ampliar el espectro de funciones que realiza esta herramienta. Estre estas nuevas funciones podemos mencionar el testeo de validez en certificados digitales de sitios web seguros y el testeo de validez en su cadena de confianza.

Procedimientos

Con el objeto de procedimentar la actividad desarrollada dentro del CERT, se definieron diversos procedimientos que establecen el plan de acción para distintas tareas llevadas a cabo. Entre los procedimientos desarrollados podemos mencionar:

- Procedimiento para tratamiento de SPAM recibido
- Procedimiento para tratamiento de SPAM enviado
- Procedimiento para tratamiento de BLACKLISTS detectados
- Procedimiento de tareas a realizar durante un análisis forense.
- Procedimiento para el almacenamiento de análisis forenses y pentests correspondientes a incidentes atendidos
- Procedimiento para el mantenimiento y versionado de procedimientos dentro del CERT.

Si bien actualmente, no todo está procedimentado, la idea es llegar a establecer procedimientos para todas las tareas involucradas.

Pentests y Forensia

Debido al desarrollo propio de incidentes atendidos, se realizaron en distintas ocasiones el análisis forense y en otras ocasiones un pentest del objetivo sospechoso de haber sido vulnerado. En ambos casos, se trabajo junto al administrador del servicio en cuestión y posteriormente se le entregó un informe de lo actuado.

Monitoreo proactivo y sensores de red (honeypots)

Dado que una de las amenazas principales con las que se trata diariamente la constituyen distintos problemas (Botnets, Spam, DOS, Scans) que tienen el origen en maquinas infectadas con algún tipo de malware, se instaló un honeypot para la detección de malware. Esta solución trabaja con sensores diseminados por las distintas redes de la Universidad. Actualmente se tiene solo dos sensores instalados y se espera la instalación de otros en redes de usuarios, de modo que estos problemas sean detectados por la dispersión del malware y no por la aparición de sintomas relacionados a la actividad de los mismos.

Resultados esperados

Quizás el mayor desafío es construir una cultura de colaboración para detectar incidentes y romper con el preconcepto que una organización no “tiene riesgos”, sino que el objetivo es mitigarlos, minimizarlos, y que el aprendizaje y el fortalecimiento es una tarea en conjunto.

Los objetivos iniciales que se plantearon para UNLP CERT, sobre los cuales se avanzó en mayor o menor medida desde el momento de su creación, se enumeran a continuación:

- Brindar atención, seguimiento y respuesta de incidentes de seguridad en el ámbito de la Universidad Nacional de La Plata.
- Monitorear la seguridad del Backbone de la red de la UNLP.
- Monitorear el uso de la red según políticas de uso razonable.
- Desarrollar una red de sensores de seguridad y Honeypots en distintos segmentos de red de la UNLP.
- Garantizar la continuidad de los servicios de red de las distintas unidades académicas de la UNLP.
- Realizar diagnósticos de seguridad proactivos, según pautas acordadas con cada dependencia.
- Entregar en forma oportuna y sistemática información sobre vulnerabilidades de seguridad, amenazas, prevención y resolución de incidentes de seguridad.
- Brindar capacitación sobre temas de seguridad y uso seguro de la tecnología.

Estadísticas

En base a lo observado en lo que se refiere a incidentes tratados, se presentan la siguiente distribución de incidentes observados.

Tipo de incidente	Cantidad
Blacklist	57
Spam total	36
Spam Enviado	18
Spam Recibido	18
Scans	17
Phishing	3
Bugs de seguridad	1
Virus	1
Spyware	1

Cabe destacar que los incidentes muchas veces están relacionados. Por ejemplo, un problema de virus/malware el cual puede ser parte de una botnet, puede ocasionar un problema de spam si el mismo no es tratado en tiempo y forma. En este sentido, se está trabajando en la instalación de una red de sensores, honeypots, que permita detectar problemas de virus/malware durante la propagación del mismo.

Otro objetivo a corto plazo es la de adaptar nuestros sistemas de incidentes y herramientas de testeo internas para que mantengan estadísticas de tipo de incidentes por unidad académica, de modo de poder contar con un mapa con los sectores mas conflictivos según el tipo de incidente de la Universidad. Dicha información sería de gran utilidad para poder implementar las contramedidas adecuadas, para el problema adecuado, en el lugar adecuado.

Tendencias en Incidentes

En base a lo observado en los incidentes recepcionados, los problemas recurrentes que requieren algún tipo de tratamiento son:

- Problemas de SPAM enviado. Se espera mitigar este problema mediante la instalación de honeypots de baja interacción para la detección de malware en las distintas redes de la UNLP.
- Problemas de Phishing. La recolección de datos personales por medio de técnicas de phishing es un problema en auge el cual que se deberá seguir atacando mediante concientización a usuarios.
- Problemas de seguridad en aplicaciones WEB. Si bien ésta no es la única vía de acceso que tienen los atacantes, el gran universo de aplicaciones existentes y la gran variadad de desarrolladores de aplicaciones web existentes, hace que sea necesario concientizarlos sobre técnicas de programación segura.

4. Formacion de recursos humanos

CERT-unlp empezó a funcionar en Marzo del 2009 y actualmente en trabajan en este proyecto 3 becarios, los cuales son dirigidos por 3 docentes especializados en el campo de la seguridad y las redes.

Una de los principales objetivos del grupo es la formación y la capacitación permanente de todos los integrantes del CERT de la UNLP. Por esta razón, los becarios se han capacitado en temas afines a redes (CCNA 1 y 2), seguridad de redes y aplicaciones y tratamiento y gestión de incidentes. También han asistido a conferencias de seguridad (ekoparty 2009) y han participado de diversos eventos de seguridad con la modalidad “capture de flag”.

Previo al nacimiento de este Proyecto y durante la primer etapa de funcionamiento del mismo, se visitaron otros CERTs de la región: UNAM CERT (México) en 2007, CERT.br (Brasil) en 2008 y CLCERT (Chile) en 2009, nutriéndose el equipo de la experiencia de Proyectos similares aplicables luego a la puesta en marcha y funcionamiento de CERT-unlp. Esta actividad permite también establecer los lazos de cooperación necesarios en una línea de trabajo de esta naturaleza.

En 2009 se participó también del evento anual de LACNIC llevado a cabo en Brasil.

Dentro de esta línea de trabajo se enmarca la tesina de grado actualmente en desarrollo “Integración de herramientas de seguridad para redes informáticas” de los Analistas en Computación Einar Lanfranco y Matías Pagano.

5. Bibliografía

- http://www.cert.org/, Carnegie Mellon University
- http://www.arcert.gov.ar/, Subsecretaría de TEcnologías de Gestión, Secretaría de la Gestión Pública
- Fundamentos de la Gestión de Servicios de TI. Basada en ITIL V3. ITSMF International.
- http://www.owasp.org - The Open Web Application Security Project (OWASP)
- Computer Networking: *A Top-Down Approach Featuring the Internet* - James F. Kurose and Keith W. Ross
- Hacking Exposed - Network Security Secrets & Solutions - Tony Bradley
- Forensic Discovery (Hardcover) - Dan Farmer y Wietse Venema