Enseñar y aprender Seguridad y Privacidad en Redes en la UNLP: SyPeR

Francisco J. Díaz
Paula Venosa Nicolás Macia Alejandro Sabolansky Joaquín Bogado

jdiaz@info.unlp.edu.ar
(pvenosa,nmacia,asabolansky,jbogado)@linti.unlp.edu.ar

Laboratorio de Nuevas Tecnologías Informáticas (LINTI)
Facultad de Informática
Universidad Nacional de La Plata - Argentina.

Resumen

Este artículo cuenta la experiencia del equipo de la cátedra de Seguridad y Privacidad en Redes, materia optativa de las actuales carreras de Licenciatura en Informática y Licenciatura en Sistemas, de la Facultad de Informática de la Universidad Nacional de la Plata [1].
Seguridad y Privacidad en Redes forma a los alumnos en el análisis de problemas de seguridad de sistemas, redes y servicios así como en el diseño e implementación de soluciones a los mismos.
El estudiante aprende normas, protocolos y herramientas que aplicará para implementar mecanismos de seguridad en los sistemas que él mismo desarrolle y/o en las redes y servicios que él administre, así como para analizar el nivel de seguridad de sistemas, redes y servicios.
En el transcurso del último lustro, la materia ha tenido que ir ajustando los contenidos mostrados año a año, para que estos reflejen lo mejor posible no sólo la situación actual en el área, sino también las tendencias por venir.
Para ello, resulta de suma importancia el permanente perfeccionamiento del plantel docente. Esto permite que año tras año se incorporen nuevos ejercicios prácticos, que se adopten nuevas metodologías y se utilicen herramientas de última generación.

Palabras clave: Seguridad, Privacidad, Redes, Lihuen [2], Software Libre.

Motivación

Desde la aparición del Gusano Morris en 1988 [3][4] se puso de manifiesto que el uso indebido de las redes de computadoras puede producir daños monetarios importantes a una organización. Un graduado en carreras de Informática, Sistemas o afines no sólo debe ser capaz de identificar y mitigar problemas de seguridad basados en amenazas conocidas, sino también prevenir, detectar y reaccionar ante ataques basados en amenazas nuevas. Por ello consideramos esta materia, no como una mera colección de contenidos estáticos e invariantes con el correr del tiempo, sino como un desafío donde cada año es necesario aprender y comprender en profundidad nuevas amenazas para poder incorporar técnicas de detección, prevención y mitigación al plan de estudios de la materia.

Un poco de historia

A partir del año 2001, siguiendo la tendencia de América Latina respecto a la creación de asignaturas dedicadas 100% a la seguridad de la información en el marco de carreras de grado [5], comenzó a dictarse en nuestra Facultad la materia "Seguridad y Privacidad en Redes", como optativa de la carrera Licenciatura en Informática Plan 90, a cargo del Profesor Francisco Javier Díaz y la entonces Jefe de Trabajos Prácticos Paula Venosa. Dicha materia luego formó parte de la oferta de optativas de las carreras Licenciatura en Informática Plan 2003 y Licenciatura en Sistemas Plan 2003, dentro del área Arquitectura, Redes y Sistemas Operativos.

Desde sus comienzos, estuvo presente el objetivo de darle a la asignatura un enfoque práctico. Los primeros laboratorios realizados en las prácticas incluían el armado de topologías con máquinas reales; por ejemplo el caso de un servidor vulnerable (que la cátedra instalaba sobre una máquina real con determinada versión de sistema operativo) para que los alumnos pudieran experimentar respecto a cómo detectar amenazas de seguridad y cómo mitigarlas.
Esta alternativa generaba una inversión de tiempo muy importante para la cátedra, ya que debía instalar y mantener las máquinas reales, además de tener que dedicar recursos de hardware de la Facultad para este fin. A su vez, si algún grupo a partir de alguna prueba dejaba el servicio no disponible, el resto de los grupos se veía imposibilitado de avanzar con sus pruebas.
Cuando se armaban pequeñas topologías reales, las dificultades con las que se enfrentaban los alumnos para poner a punto dichas topologías eran grandes, no siendo éste el objetivo de la materia sino la dedicación del tiempo y esfuerzo a la comprensión de los tópicos específicos de seguridad. Además se tornaba dificultoso el plantear actividades fuera del horario de la práctica porque en general los alumnos no contaban con los recursos para replicar las topologías en sus hogares.
Otra desventaja era la imposibilidad de establecer una configuración unificada sobre la que tanto los alumnos como los docentes pudieran trabajar y de esa forma contar con un único entorno de trabajo para la corrección y evaluación.

Algunos años más tarde, ante el auge de la virtualización [6], se comenzó a usar en las prácticas máquinas virtuales, lo que terminaba con algunas de las desventajas del escenario anterior [7].
Y además, aprovechando la experiencia de tener una distribución propia realizada en la Facultad de Informática, al igual que se ha implementado en la materia "Redes y Comunicaciones" [8] se creó una versión de Lihuen LiveCD con algunas herramientas útiles para la enseñanza de conceptos relacionados con la seguridad de la información.
El LiveCD es una versión de Lihuen [2], remasterizada con un conjunto de herramientas elegidas para poder resolver todos los ejercicios prácticos planteados.

Hoy en día, el equipo de trabajo se ha ampliado; los autores del presente artículo forman parte del mismo e impulsan y trabajan en el crecimiento de la enseñanza de la seguridad, donde también se lleva a la práctica también el concepto de mejora continua del conocido ciclo PDCA [9].

Los desafíos de enseñar Seguridad

Para aprender seguridad, es necesario conocer las características de los problemas y cómo estos pueden ser aprovechados por un

atacante. En relación a ello, son varios los desafíos al momento de abordar la materia. ¿Se encara el tema desde el lado del atacante? ¿Se da la visión del administrador? A veces "nos paramos en la vereda del atacante" y otras en la "vereda del administrador del servicio o de la red", es decir, mostrando las técnicas de ataque y las estrategias de defensa, dando así al alumno una visión integral de los distintos temas abordados.

A su vez, hay cuestiones de ética asociadas, que son inherentes a la forma descrita para tratar los temas, y que no deben descuidarse ya que no son menores, teniendo en cuenta que estamos formando profesionales responsables del desarrollo de aplicaciones, de la administración de servicios, de la seguridad de la organización. Muchas de las cuestiones éticas planteadas surgen de inquietudes de los mismos alumnos, que al momento de resolver algún ejercicio se encuentran ante dudas que no tienen solución desde la técnica. "¿Qué debo hacer si durante una auditoría mi jefe me pide que le encuentre algo malo a Bob por que lo quieren despedir?", "Si yo fuera un atacante también borraría la base de datos." o "¿Qué debo hacer si durante una auditoría logro el acceso a material ilegal?", son preguntas corrientes que el cuerpo docente debe estar preparado para discutir. Esto ha motivado el inicio de investigaciones relacionadas con temas de ética profesional que han permitido a los docentes de la cátedra participar de congresos relacionados a ésta temática [10]. Nuestra principal meta es transmitirles a los alumnos que lo aprendido debe aplicarse a la protección de la información de la organización, objetivo que no debemos perder de vista en ningún tramo del recorrido.

En el mundo de la seguridad de la información, surgen nuevas vulnerabilidades todo el tiempo, se crean nuevas formas de explotar las mismas permanentemente y también surgen nuevas metodologías y herramientas de defensa en consecuencia. Esto requiere una actualización constante de los contenidos de la materia, incorporando año a año los nuevos problemas de seguridad y las nuevas tácticas y herramientas que se pueden aplicar relacionadas con las distintas unidades temáticas. Un ejemplo de ello es el tema de seguridad de aplicaciones web, que se aborda siguiendo los lineamientos y utilizando el material disponible en OWASP [11], siendo el eje principal para abordar el tema el OWASP TOP TEN Project [12] que publica una lista de los 10 riesgos más críticos relacionados a la seguridad de las aplicaciones web, el cual se construye en forma consensuada. Esta lista, así como los criterios en los que se basa la misma, el conocimiento asociado, las herramientas que surgen, las metodologías de trabajo, los proyectos asociados, se han ido actualizando a medida que dichos contenidos han aparecido. En la materia se ha trabajado con las versiones OWASP Top Ten 2007, 2010 y más recientemente con la versión 2013 durante la última cursada.

De lo anteriormente expresado, se desprende también el desafío del constante perfeccionamiento y actualización del plantel docente, lo cual genera un ámbito de estudio e investigación que nutre también al Laboratorio de Investigación en Nuevas Tecnologías en Informática, del cual forma parte dicho cuerpo docente. Todos los años, la cátedra hace una pausa que permite asistir al evento EKOparty , uno de los más prestigiosos encuentros de seguridad de nuestro país y que cuenta con renombrados expositores de nivel internacional. También se participa en eventos internacionales como LACNIC, Black Hat Trainings o SANS Security representando a la UNLP.

Desarrollo de la materia

Contenidos

De acuerdo al programa incluido en la propuesta pedagógica, actualmente la materia cubre siguientes temas:

- Conceptos básicos de seguridad y definiciones - Atributos de seguridad: confidencialidad, integridad, autenticidad, no repudio - Vulnerabilidad, Amenaza, Incidente- Tipos de amenazas
- Técnicas de descubrimiento (footprinting, fingerprinting, enumeración, escaneo de puertos, escaneo de vulnerabilidades).
- Sniffing
- Criptografía y aplicaciones de criptografía (PKI[13] , PGP[14], SSL[15], VPNs[16])
- Mecanismos de protección: firewalls[17], IDS[18], IPS, Honeypots[19].
- Seguridad en aplicaciones Web.
- Gestión de seguridad de la información

Metodología de trabajo

Para cada una de las unidades existen presentaciones teóricas, explicaciones prácticas que complementan el enfoque teórico y trabajos prácticos asociados. Todos los tópicos son abordados desde un enfoque práctico y experimental.

Se utiliza el ambiente educativo virtual Moodle [20] de libre distribución, tanto para gestionar los recursos asociados al curso (presentaciones de teoría, trabajos prácticos, imagen del live CD, apuntes complementarios, etc) así como para contar con foros de novedades y consultas, que resultan de suma utilidad al ser esta materia una asignatura correspondiente a los últimos años de la carrera.

A través de dicha plataforma también se realizan las evaluaciones al finalizar cada unidad del programa, las cuales han sido de carácter obligatorio en cursadas anteriores.

Prácticas y herramientas

La cátedra promueve la utilización de herramientas de Software Libre. Para cubrir el tema de criptografía y certificados se ha montado una autoridad de certificación mediante el uso de la herramienta *OpenCA* [21]. Los alumnos luego de realizar solicitudes de certificados digitales, realizan las prácticas enviándose mails firmados y cifrados entre ellos y con los docentes de la cátedra. Además en esta práctica se utilizan *GnuPG* [22] para gestión de claves PGP y su utilización como alternativa para realizar operaciones de cifrado. Y también *steghide* [23] como herramienta de esteganografía.

En la práctica de escaneo y descubrimiento, se utiliza la herramienta Nmap[24] la cual implementa la mayoría de las técnicas estudiadas, pero además se propone la utilización de hping3[25] y tcpdump[26] o wireshark [27] para realizar estas técnicas de una manera más manual y analizar los envíos y respuestas de los diferentes servicios de una manera más detallada. También se utilizan otras herramientas o recursos web como Netcraft [28], WebArchive [29] y Google para dar una idea de la cantidad de información pública que un sitio puede llegar a mostrar a veces sin que los administradores se den cuenta y cómo puede esta información ser utilizada en contra de dicho sitio.

Si bien las teorías son agnósticas respecto a las herramientas y se centran en mostrar los conceptos de los temas a desarrollar, la práctica de firewall se realiza sobre *iptables*[30]. Esto se debe a que es la opción por defecto en sistemas GNU/Linux, es Software Libre y su versatilidad permite aplicar los conceptos de una manera amplia y directa. En años anteriores se utilizó *Snort* [31] como IDS. Las actividades prácticas requerían que los alumnos generen reglas para detectar determinados ataques. Esto posteriormente fue reemplazado por un enfoque más teórico que

permitió dar lugar a nuevos contenidos que pueden ser resueltos sobre la plataforma CORE [32].

La práctica de vulnerabilidades en aplicaciones Web se realizaba en un principio sobre aplicaciones reales cuyas versiones no actualizadas tenían errores conocidos. Estas se instalaban en un servidor implementado en una máquina virtual y se configuraban de manera que los alumnos debían buscar dichas vulnerabilidades y desarrollar ataques que cumplieran ciertos requerimientos (por ejemplo, obtener cierto nivel de privilegios o evitar que la víctima se de cuenta de la intrusión). Dada la complejidad en la selección no sólo de las aplicaciones sino también de versiones vulnerables, desde el año 2012 se utiliza la versión Live de Damn Vulnerable Web Application (DVWA)[33]. Esta herramienta incluye una serie de "pruebas de concepto" que cubren la mayoría de los tópicos relacionados con el desarrollo de aplicaciones web seguras.

Durante las explicaciones prácticas se hace referencia a una innumerable cantidad de herramientas (algunas muy específicas) animando a que los alumnos las prueben e investiguen por su cuenta, como ser *sqlmap*, *sqlninja*, *imsniff*, *httprint* o *sslstrip*.

Desde el año 2011, la cátedra ha adoptado el producto CORE como la herramienta de emulación de topologías de red. Esta herramienta ha sido incorporada en forma nativa en las sucesivas versiones del Live CD que la Cátedra ha ido liberando al comienzo de cada semestre de cursada.

La utilización de CORE permite que las actividades prácticas que en principio se hacían mediante máquinas físicas, puedan ser realizadas en forma sencilla utilizando el Live CD. Para cada una de las prácticas, la Cátedra facilita diferentes topologías preconfiguradas para que el alumno pueda resolver los ejercicios. Además, esta herramienta permite que el alumno pueda crear sus propias topologías y probar diferentes configuraciones de las mismas. A veces las soluciones propuestas por los alumnos exceden con creces las pautas iniciales y las investigaciones generadas por los mismos enriquecen los contenidos para la materia del siguiente ciclo lectivo.

Experiencia de la última cursada (2013)

En cursadas anteriores, el criterio para el orden de los temas consistía básicamente en presentar en la primer parte de la materia los temas asociados a problemas de seguridad y las formas existentes para descubrir o explotar los mismos (como ser por los temas sniffing o técnicas de descubrimiento) y luego en la segunda parte se presentaban las soluciones o formas de minimizar dichos problemas (criptografía, mecanismos de protección, etc).

Durante la cursada 2013, el plantel docente se propuso optar por un nuevo orden de los temas, intentando relacionar los temas en forma más directa, en los casos en que era posible, presentando el "problema" y luego la "solución asociada", por ejemplo: luego de presentar las técnicas de sniffing dar lugar a la criptografía.

En particular, en la práctica correspondiente a criptografía se incorporaron nuevos ejercicios relacionados con uso de la misma para asegurar la confidencialidad de la información en la transmisión de servicios en general (no sólo de correo electrónico como veníamos realizando hasta el momento) y hardening de servicios.

Por otra parte, se ha modificado la metodología de evaluación de la materia. Hasta el año 2012, las evaluaciones de cada una de las prácticas se realizaban a través de Moodle una vez finalizadas las actividades

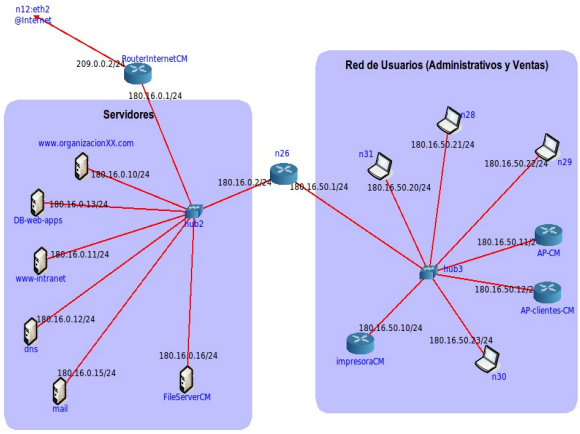
planteadas para dicha unidad. Si el alumno aprobaba la evaluación, dicho tema no era incluido en el examen parcial al finalizar la cursada. El año anterior (2013), se han eliminado dichas evaluaciones transformando las mismas en autoevaluaciones como una herramienta para que el alumno mida su nivel de conocimiento y no como una instancia de evaluación por parte de la cátedra. Este último cambio no dio resultados satisfactorios, ya que al no ser una instancia de evaluación los alumnos restaban importancia a su realización, aunque completarlas fuese de carácter obligatorio.

Trabajo final

Durante la última de cursada (2013), se desarrolló un trabajo final cuyo objetivo fue integrar los distintos temas vistos, aplicando los conceptos aprendidos en el análisis de un caso de estudio, buscando en el mismo problemas de seguridad y proponiendo soluciones posibles.

Se presentó a los alumnos el caso "prototipo" de una organización que ofrece servicios (relacionados a transacciones financieras), la cuál cuenta con una casa matriz y una sucursal, que cumplen determinadas características en cuanto a sus recursos humanos, sus tareas, los servicios que presta y la topología física y lógica de su red.

Junto al enunciado del trabajo, se presentó una topología en CORE que representaba la estructura actual de la red de la organización sobre la cuál se debía hacer el análisis de seguridad. A modo de ejemplo se muestra en la siguiente figura la topología definida para la red de la casa matriz:



Los alumnos podían realizar el trabajo en forma individual o con un compañero. El primer paso consistía en realizar un análisis la seguridad de la organización (como se haría en el contexto de una auditoría de seguridad), identificando posibles amenazas que puedan afectar la operación interna de la organización como así también el servicio ofrecido a los clientes.

A partir de ello debían proponer mejoras a fin de eliminar o reducir el riesgo de las distintas amenazas identificadas, indicando cuáles eran factibles de implementar como parte del desarrollo del trabajo, teniendo en cuenta lo aprendido en la cursada y las limitaciones de la topología (por ejemplo: configuraciones de firewall, configuraciones de IDS de red, configuraciones de IDS de host, configuraciones de VPN (site-to-site), cambios en la estructura de la red, cambios en el direccionamiento IP, etc).

Los resultados de dicho análisis debían reflejarse en un informe preliminar entregable, el cual fue revisado por la cátedra, que en este caso actuó como supervisor y realizó una devolución a cada grupo indicando el camino a seguir (errores, ayudas para problemas no descubiertos, pistas para soluciones posibles no planteadas).

Como parte de las pautas, se planteó a los alumnos que usaran una metodología de mejora continua, es decir que luego de haber propuesto controles para mitigar o minimizar

amenazas, debían identificar nuevas amenazas en el contexto modificado por el control. De esta manera también se invitaba a trabajar siguiendo el modelo de mejora continua propuesto en la ISO 27001 [34]

Durante el desarrollo del trabajo la cátedra asumió el rol de Gerente General de la Organización, estando disponible para cualquier decisión que cada alumno/grupo necesitara tomar.

La entrega final consistió en la entrega de un informe, incluyendo amenazas descubiertas y controles propuestos, y la entrega de la topología en la cual debían haberse implementado los controles propuestos indicados como factibles de llevar a la práctica en este contexto.

Como última instancia, cada uno de los grupos expuso los resultados de su trabajo, para lo cual la cátedra definió el alcance de cada presentación (de acuerdo a lo que era más rico de cada trabajo para que esto también constituyera una instancia de aprendizaje para todos). Dicha exposición simuló lo que podría constituir en la vida real la presentación de los resultados de una auditoría de seguridad o la presentación de una solución implementada (dependiendo el caso de cada grupo según lo asignado para la exposición)

De los grupos que realizaron el trabajo, hubo algunos que siguieron un enfoque más gerencial, planteando problemas y posibles soluciones a alto nivel, mientras que otros le dieron un enfoque más práctico, centrándose en los aspectos técnicos de las soluciones.

Un aspecto que vale la pena resaltar es que al momento de la presentación, cada grupo compartió las experiencias positivas y negativas con las cuales se habían enfrentado durante la realización del trabajo, desde su óptica y presentando argumentos para sus afirmaciones, tal cual ocurre en el mundo "del trabajo" a la hora de presentar las tareas que se hicieron y las dificultades encontradas en el camino.

En relación a los informes presentados, se observa una falta de experiencia en la redacción y presentación de los mismos, siendo este un ítem que debe ser revisado por parte de la Cátedra.

Conclusiones

Es indiscutible en la actualidad la importancia de la seguridad de la información y su gestión en las organizaciones, motivo que hace imprescindible la formación de futuros graduados en este área, siendo sumamente útil la misma si los contenidos, metodología y herramientas se actualizan permanentemente, acompañando los cambios tecnológicos.

Como se ha mencionado a la largo del presente artículo lo anteriormente expresado conlleva a la actualización permanente del plantel docente de la cátedra y al reflejo de dicha actualización en el dictado de la materia.

Un resultado que muestra interés en el área por parte de los alumnos y satisfacción respecto a lo aprendido es el incremento de la cantidad de tesinas en temas relacionados con seguridad de la información.

Respecto a la metodología de trabajo, el uso del Live CD basado en Lihuen y la herramienta CORE han roto la barrera de la dificultad del "armado del ambiente de trabajo" que se presentaba en los primeros tiempos del dictado de las materia. El trabajo coordinado entre teoría, explicaciones y trabajos prácticos, hitos en que los docentes muchas veces "se mezclan" participando indistintamente de las diferentes actividades, resulta exitoso a la hora de llevar adelante la materia de manera integral.

Respecto a las evaluaciones, ha resultado más efectivo la evaluación por tema utilizando Moodle, porque permite que los alumnos lleven las prácticas al día y facilitan el seguimiento por parte del cuerpo docente.

Las innovaciones en la metodología permiten sacar este tipo de conclusiones y no sólo quedarse con una modalidad clásica y estancada que genera rutina para todos los actores (docentes y alumnos).

Respecto al trabajo final, este año se va a presentar al principio de la cursada, para ir analizando el caso a medida que se va incorporando conocimiento e ir aplicando los distintos conceptos que se van trabajando en la resolución del mismo, de manera tal que la solución se vaya encarando en forma modular e incremental.

Referencias

[1] Oferta de optativas del año 2014 de las carreras Licenciatura en Informática Plan 2012 http://www.info.unlp.edu.ar/articulo/2012/2/22/optativas2014_lic_informatica_plan2012 y Oferta de optativas del año 2014 de las carreras Licenciatura en Sistemas Plan 2012 http://www.info.unlp.edu.ar/articulo/2012/2/22/optativas2014_lic_sistemas_plan2012

[2]http://lihuen.linti.unlp.edu.ar

[3]http://es.wikipedia.org/wiki/Gusano_Morris

[4]http://www.symantec.com/connect/articles/brief-history-worm

[5]http://www.criptored.upm.es/descarga/ActasCIBSI2011.pdf

[6]http://www-07.ibm.com/solutions/in/education/download/Virtualization%20in%20Education.pdf

[7] http://dl.acm.org/citation.cfm?id=1352181

[8][Integración de herramientas de software libre para enseñar redes con un enfoque práctico Alejandro Sabolansky, Einar Lanfranco, Nicolas Macia, Paula Venosa Jornadas de Software Libre JAIIO 2012

[9] http://www.iso-9001-checklist.co.uk/iso-9001-training.htm

[10]Reflexiones iniciales sobre la validez ética de la utilización de técnicas de minería de datos sobre datos personales en la búsqueda de terroristas. Joaquín Bogado, Beatriz García. Ethicomp Latinoamérica 2012.

[11] http://www.owasp.org]

[12]https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[13] http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica

[14]http://es.wikipedia.org/wiki/Pretty_Good_Privacy

[15]www.digicert.com/es/ssl.htm

[16]es.wikipedia.org/wiki/Red_privada_virtual

[17]http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

[18]http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

[19]http://es.wikipedia.org/wiki/Honeypot

[20]Moodle - sistema de gestión de cursos de código abierto. http://www.moodle.org

[21]http://www.openca.org

[22]steghide.sourceforge.net/

[23]http://www.gnupg.org/

[24]http://nmap.org/

[25]http://www.hping.org/hping3.html

[26]www.tcpdump.org/

[27]www.wireshark.org/

[28]http://www.netcraft.com/

[29]web.archive.org/

[30]http://www.netfilter.org/

[31]www.snort.org/

[32]CORE - Common Open Research Emulator.http://cs.itd.nrl.navy.mil/work/core/index.php.].

[33]http://www.dvwa.co.uk/

[34]www.iso27000.es/