INTRODUCCIÓN

OBJETIVO

Incrementar la integridad, confidencialidad y disponibilidad de los recursos informáticos de RED-UNAM por medio de varios proyectos que desarrollé en la Subdirección de Seguridad de la Información de la DGTIC, los cuales han mejorado el servicio de respuesta a incidentes de seguridad en cómputo que la SSI/UNAM-CERT ofrece a las dependencias de la UNAM.

JUSTIFICACIÓN

De acuerdo al estándar ISO/IEC 27000 la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información.

El Equipo de Respuesta a Incidentes de Seguridad en Cómputo de la UNAM (UNAM-CERT) tiene como misión, para con la UNAM, proporcionar servicios de asesoría y atención a incidentes en materia de seguridad informática a cada una de las entidades que la conforman, satisfaciendo sus necesidades con base en la capacidad tecnológica que se disponga.

Asimismo, tiene como misión, para con su comunidad, proporcionar información clara, precisa y objetiva respecto a los problemas de seguridad informática que la comunidad universitaria afronta cotidianamente, así como auxiliar en la solución de estos problemas.

Hay dos tipos de actividades para cumplir estas misiones: las preventivas o proactivas y las reactivas. Estas últimas tienen como propósito actuar una vez que ha ocurrido un incidente de seguridad informática y consta de las siguientes fases: preparación, contención, erradicación, recuperación y lecciones aprendidas. Las preventivas, o proactivas, tienen como propósito tomar las acciones necesarias para reducir la probabilidad de que ocurran incidentes de seguridad.

De enero a agosto de 2009 realicé mi servicio social en el Proyecto Honeynet UNAM y después de mi servicio me incorporé al puesto de atención y respuesta a incidentes de seguridad en cómputo, en el cual he laborado desde agosto de 2009.

En la parte proactiva, realicé varios manuales de seguridad informática dirigidos a ayudar a los administradores de RED-UNAM a implementar acciones preventivas para reducir la probabilidad de ocurrencia de los incidentes de seguridad informática que observé con mayor frecuencia. La mayor parte de los casos que atendí en RED-UNAM, fueron provocados por el uso de contraseñas débiles en servidores LINUX y también por correos fraudulentos enviados a usuarios de CORREO-UNAM.

En el primer capítulo defino la visión y misión de SSI/UNAM-CERT, describo su historia y los servicios que proporciona a la comunidad. Además, detallo los servicios que proporciona el Departamento de Respuesta a Incidentes y Detección de Intrusos, el cual es responsable del Área de Respuesta a Incidentes, de la cual soy miembro.

En el segundo capítulo de este informe, se describen algunos proyectos que desarrollé en la SSI/UNAM-CERT con el fin de prevenir o supervisar incidentes de seguridad en equipos de RED-UNAM.

El primer proyecto descrito en el segundo capítulo tiene el objetivo de reducir la incidencia del robo de credenciales de acceso de usuarios de *Correo UNAM* por medio de mensajes fraudulentos de correo electrónico, así como indicar a los usuarios cómo notificar estos incidentes a UNAM-CERT. El segundo proyecto descrito tiene el propósito de incrementar la seguridad de las contraseñas en sistemas basados en la distribución GNU/LINUX Debian, mediante el uso de las bibliotecas `pam_unix` y `pam_cracklib`, con el fin de proveer a los administradores de RED-UNAM una alternativa para reducir una de las causas más comunes de incidentes en la UNAM, el uso de contraseñas débiles.

El tercer proyecto descrito se concibe para mejorar la supervisión y reducir el tiempo de respuesta a incidentes de modificaciones no autorizadas en sitios web que pertenecen al dominio de RED-UNAM, por medio de un programa automático de supervisión desarrollado en lenguaje bash shell. Después de identificar una modificación no autorizada, el programa notifica el incidente a los miembros de respuesta a incidentes, a fin de que ellos se pongan en contacto con el responsable del sitio web y se resuelva el incidente.

El cuarto y último proyecto de este capítulo tiene el objetivo de incrementar la seguridad de las contraseñas en sistemas operativos GNU/LINUX mediante el uso de la biblioteca `pam_passwdqc`, la cual permite mayor funcionalidad que `pam_cracklib`. Se proveen indicaciones generales de instalación y configuración de esta herramienta, así como indicaciones para distribuciones específicas para facilitar a administradores de RED-UNAM la instalación de esta herramienta.

En el tercer capítulo de este trabajo se describe el propósito, instalación, configuración, administración, actualización, documentación y uso del whois de UNAM-CERT cuyo propósito es brindar a los miembros de respuesta a incidentes una forma rápida de obtener los datos de los administradores de redes de RED-UNAM y así reducir el tiempo de respuesta a incidentes, minimizando el impacto causado por el incidente de seguridad.

En el último capítulo se describen los resultados obtenidos del proyecto descrito en el tercer capítulo.