Experiencias de análisis forense en México

Departamento de Seguridad en Cómputo / UNAM-CERT
UNAM, México

Jornadas de Análisis Forense. Madrid, España. Septiembre 2005

UNAM-CERT

- UNAM-CERT es el equipo de respuesta a incidentes de seguridad de la Universidad Nacional Autónoma de México
- Atiende incidentes del dominio .unam.mx
- Al ser el único CERT de México reconocido oficialmente ante FIRST es, de hecho, el punto de contacto para los incidentes en el dominio .mx
- Colabora con entidades del sector gobierno, privado y financiero del país

Los comienzos (1994-2000)

- El Área de Seguridad en Cómputo, se encargaba de atender incidentes que reportaban los administradores de sistemas y de redes de la universidad.
- Virus/gusanos en Windows
- Intrusiones en sistemas Unix.
  - Se acudía y revisaba el equipo ingresando y haciendo uso de comandos del sistema (o copiados de otro similar) y de algunos scripts sencillos.

Los comienzos (1994-2000)

- No había capacitación formal en el área de atención a incidentes y análisis forense
- Los análisis resultaban en hallazgos en el sistema de archivos de material que los intrusos habían dejado visible
- No se tenía una metodología ni se tomaban precauciones necesarias para un forense.

Los comienzos (1994-2000)

- Era difícil detectar intrusiones "sofisticadas"
- Cosas como los LKM Rootkits (adore, knark) resultaban complejas para analizar
- Empezaba un auge global del análisis forense y se tenían las limitaciones propias de un área en surgimiento y evolución constante

Primeras experiencias

- Falta de experiencia
- Análisis basados en conocimientos y metodologías limitadas en la materia
- Pocos casos con implicaciones más allá de la prevención

Siguiente etapa: UNAM-CERT

- En 2001, se registra oficialmente UNAM-CERT ante FIRST
- Los incidentes que se atienden son cada vez más importantes
- Primeras experiencias con la iniciativa privada

Experiencias en la UNAM

- Se observa la necesidad de capacitarse en materia de análisis forense
- Se atiende una mayor cantidad de incidentes
- Atención de algunos casos en secretarías de Estado (ministerios)

Casos frecuentes en la UNAM

- Abuso de recursos para afectar a otras redes
- Envío de correo spam
- Sospechas de personas que acceden a archivos personales a los que no tienen permiso

Experiencias con entidades de Gobierno

- Forense en secretaría de estado a un Solaris "crackeado"
  - El sistema no había sido crackeado
  - Se había perdido información
  - Intento de ocultar omisiones de administración pretextando una intrusión

Experiencias con la iniciativa privada

- En una empresa privada
  - Se sospecha de accesos no autorizados
  - Se acude a atender el incidente
  - Se realizan las primeras investigaciones
  - La investigación es truncada por parte de la empresa
  - La empresa va a arreglar internamente el asunto

La etapa más reciente (2002-2005)

- Incidentes con implicaciones más importantes dentro de la Universidad
- Colaboración con entidades gubernamentales encargadas de la investigación de delitos informáticos.
- Se participa ahora de monitoreos mundiales sobre actividad maliciosa
- Se trabaja de manera coordinada con instituciones financieras afectadas por problemas de fraudes

La etapa más reciente (2002-2005)

- Las distintas policías tienen ahora entidades dedicadas a la atención de delitos informáticos con las que UNAM-CERT ha colaborado en análisis forense
- Las empresas más grandes han empezado a destinar más recursos a la atención a incidentes de seguridad informática
- Algunas procuradurías estatales cuentan con peritos en seguridad informática que realizan investigaciones forenses

Experiencias en la UNAM (2002-2005)

- Muchos administradores de sistemas aún no tienen claro para qué sirve el análisis forense
- En algunos casos sigue siendo difícil la respuesta al incidente
- Se ha tenido que clasificar los incidentes y definir adecuadamente los recursos para la atención y análisis de los casos

Algunos casos (UNAM)

- Trabajador asiduo a sitios pornográficos en las horas de trabajo
  - Luego de los resultados del análisis, se le despidió
  - El trabajador entabló una demanda para que se le restituyera en su puesto
  - El responsable del UNAM-CERT ha tenido que asistir a declarar en el juicio.

Algunos casos (UNAM)

- Difusión de correos difamatorios sobre autoridades de la universidad
  - Envío de correos a directivos de la universidad y a contactos en diarios de circulación nacional
  - El remitente cometió el error de enviar un archivo adjunto de Word
  - El responsable está hoy fuera de la UNAM

Algunos casos (UNAM)

- Phishing
  - Han ocurrido varios casos de máquinas en las que se encuentran sitios destinados al phishing relacionado con instituciones financieras de otros países

- Botnets
  - Muchas de las intrusiones recientes están relacionadas con botnets que muchas veces no son detectadas hasta que se reciben intentos de escaneos a otras redes

Casos en México

- Fraudes. Transferencias bancarias a través de sistemas de banca en línea
- Presidencia de la República. Ataque de negación de servicio
- En algunos casos se pudo castigar a los culpables
- UNAM-CERT ha colaborado con las agencias gubernamentales de investigación con análisis forenses en diversos casos

Los principales problemas

- Muchos administradores de sistemas aún no tienen claro para qué sirve el análisis forense
- En algunos casos sigue siendo difícil la respuesta al incidente
- Los afectados muchas veces quieren venganza y pueden actuar de forma imprudente

Las herramientas para el forense

- Conforme UNAM-CERT ha evolucionado en la atención a incidentes y el análisis forense, también se ha evolucionado en el uso de herramientas para el análisis forense
- En un principio, las herramientas se limitaban a las utilerías de los sistemas operativos analizados
- Scripts propios desarrollados de acuerdo a la experiencia encontrada

Las herramientas para el forense

- Se empezaron luego a utilizar herramientas libres y gratuitas
- Algunas herramientas diseñadas para análisis forense, como TCT
- La mayoría de las herramientas son para administración o monitoreo de sistemas Unix y Windows

Las herramientas para el forense

- Actualmente se usan herramientas más adecuadas para el análisis

- Herramientas libres y gratuitas como
  - Sleuthkit
  - Autopsy
  - Foremost
  - Chkrootkit
  - RKHunter
  - www.sysinternals.com
  - www.foundstone.com
  - OllyDbg

Las herramientas para el forense

- Herramientas comerciales para el análisis forense y análisis de binarios
  - Encase
  - IDA Pro
  - SoftICE
- UNAM-CERT desarrolla en la actualidad algunas herramientas para el análisis forense

La legislación

- Se han tipificado algunos delitos informáticos en el Código Penal Federal y algunas otras legislaciones relacionadas
- Es posible castigar intrusiones a sistemas informáticos
- No es claro el mecanismo de presentación de pruebas en un juicio sobre un acceso no autorizado a un sistema

La legislación

- Las personas y las organizaciones no saben qué deben hacer para denunciar un delito de este tipo
- Muchas organizaciones no tienen definidas políticas de uso permitido de sus recursos de cómputo
- La policía federal, a través de tratados internacionales, puede investigar más allá de las fronteras

Lecciones aprendidas

- El análisis forense se ha vuelto cada vez más importante en nuestra universidad y en México.
- Es importante cuidar la metodología y, sobre todo, los reportes que se generan de los análisis pues las implicaciones pueden ser severas.
- Capacitar a los administradores de red/sistemas en la detección de intrusiones y en la respuesta a incidentes

Lecciones aprendidas

- Hacer más eficiente la labor de atención a incidentes
- Tener mecanismos para clasificar los incidentes y definir límites de recursos materiales y tiempo dedicado a cada caso
- Capacitación constante de quienes hacen análisis forense

Lecciones aprendidas

- Algunas personas tienen una idea equivocada del análisis forense e intentan utilizarlo como mecanismo de venganza
- Existen algunas cosas poco claras en la legislación
- Los especialistas en forense debemos conocer el proceder legal para una investigación de este tipo

Proyectos relacionados

- Honeynet DSC/UNAM-CERT
  - Se monitorea el tráfico en dos segmentos de RedUNAM
  - Honeypots con diversos sistemas operativos y servicios
  - Imágenes para el Reto Forense v.2.0
  - Captura de malware para Windows, Linux

Proyectos relacionados

- Código Malicioso
  - Almacenamiento del código malicioso encontrado en los análisis.
  - Mecanismos de clasificación
  - Sistema de consultas sobre el código malicioso almacenado para determinar novedades o variantes

Proyectos relacionados

- Reto Forense
  - El objetivo es difundir y compartir conocimiento sobre cómputo forense entre la comunidad de seguridad en cómputo en Iberoamérica
  - Organizado en conjunto con RedIRIS
  - Colaboraron especialistas de España, Brasil y México
  - Mayor complejidad que el primer reto
  - Participantes inscritos de varios países
  - Trabajos entregados sólo de 4 países distintos

Proyectos relacionados

- Reto Forense (Retos)
  - Conformar un mecanismo útil de difusión sobre la materia
  - Abarcar aspectos menos explorados del análisis forense
  - Colaborar en la generación de recursos humanos mejor capacitados en la materia a través del intercambio de información

Proyectos relacionados

- Plan de Becarios en Seguridad en Cómputo
  - Formación de personal capacitado en la materia
  - Personas que están terminando una carrera afín a la informática.
  - 14 meses de cursos sobre diversos aspectos de la seguridad informática
  - Ha egresado la primera generación y está en curso la segunda
  - Egresados capaces de entender los problemas de seguridad y plantear y desarrollar soluciones adecuadas

Lo que esperamos a futuro

- Cada vez habrá más casos de análisis forense, en la universidad y en los sectores público y privado.
- Se requiere capacitación para los administradores en cuanto a la atención a incidentes
- Se necesitan mecanismos de colaboración para tener retroalimentación y capacitación sobre cómputo forense

Lo que esperamos a futuro

- Los casos más frecuentes estarán relacionados con fraudes y botnets.
- Cada vez encontraremos con mayor frecuencia casos de fuga de información, sobre todo en instituciones gubernamentales y empresas privadas
- Tendrá que actualizarse la legislación vigente pues la actual es insuficiente.

¡ Gracias !

Rubén Aquino Luna
raquino@seguridad.unam.mx

http://www.seguridad.unam.mx
http://www.unam-cert.unam.mx