PED: Red de máquinas trampas de la red académica

cert@rediris.es

1 de noviembre de 2001

- Detección lenta de nuevos ataques (exploit, scripts, worms...).

- Dificultad para analizar ataque reales en condiciones optimas.

- Falta de información en las instituciones afiliadas sobre como análizar estos incidentes.

Objetivo:

- Establecer una red de sistemas operativos vulnerables controlados , que simule el comportamiento normal de los sistemas en uso las instituciones. Analizar los ataques que se

PeD: HoneyNet en la red academica.

- Disponibilidad de diversas clases B (130.206., 155.54, 147.83....)
- Colaboración mediante PTYOC con las Universidades.
- Uso de direccionamiento IP sobrante de las Universidades.
- Instalación y mantemimiento en RedIRIS de uno de los nodos de la red.

PED: Equipos.

- Dos equipos o más equipos.
  1. Equipos victima.
  2. Equipo de monitorización.

- El sistema se instala dentro de la red de la institución, de una forma transparente a los demás equipos de la red

PED: Victima.

- Equipo para poner en rack , procesador intel
- Posibilidad empleo del puerto serie como consola
- Todo el tráfico de este equipo es filtrado por el equipo de monitorización

Es posible instalar más equipos tras el sistema de control, de forma que sea posible ampliar el número de sistemas trampa sin tener más equipos de captura.

PED: Monitor.

- Equipo con Linux, con posibilidad de instalación en rack
- Funciona como un puente ethernet con filtrado de tráfico
- Puede bloquear en cualquier momento el tráfico con origen y/o destino una de las máquinas victimas
- Captura y almacena todo el tráfico de las máquinas victima

PED: Coordinación

Tres tipos de tareas:

- Administración de la red y equipos
- Creación herramientas y modificación de los sistemas.
- Análisis de los ataques, establecimiento de guias de actuación,etc.

Creación de una lista de coordinación proximamente.

Informaremos en IRIS CERT cuando tegnamos más información