Detección y contención de incidentes de seguridad de red en la UCM

Luis Padilla
UCM

Puerto de la Cruz, 12-13 Abril 2007

RedIRIS

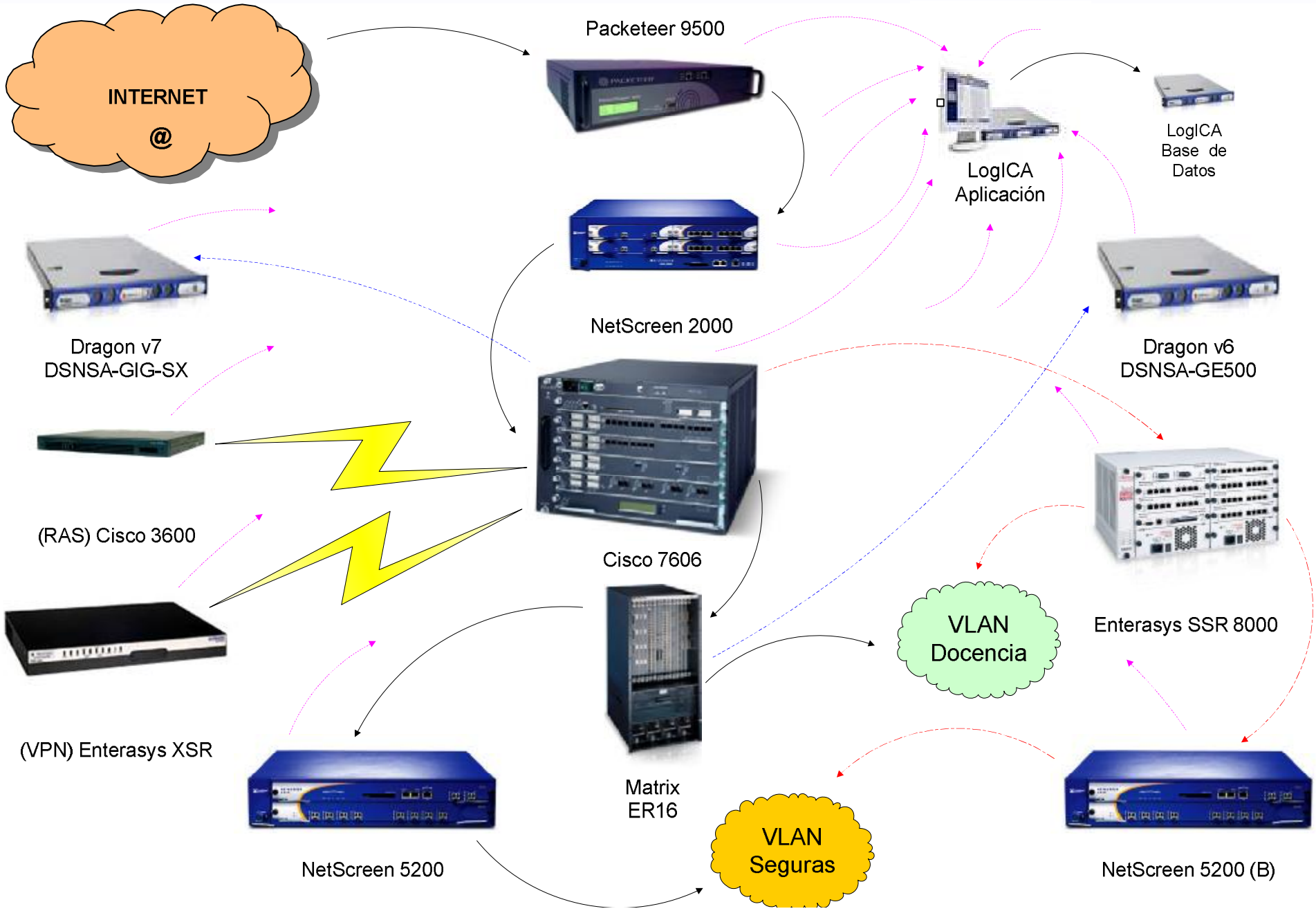
Contenido

- La UCM
- Arquitectura
  - Técnica
  - Humana
- Estrategia
  - Diseño
  - Configuración
- Operación
  - Primer nivel
  - Segundo nivel
- Detección
- Actuación
- Contención
  - Preventiva
  - Reactiva
- Resultados
- Problemas
- Soluciones y pruebas
- Ejemplos de incidentes
- Reglas de IDS más útiles

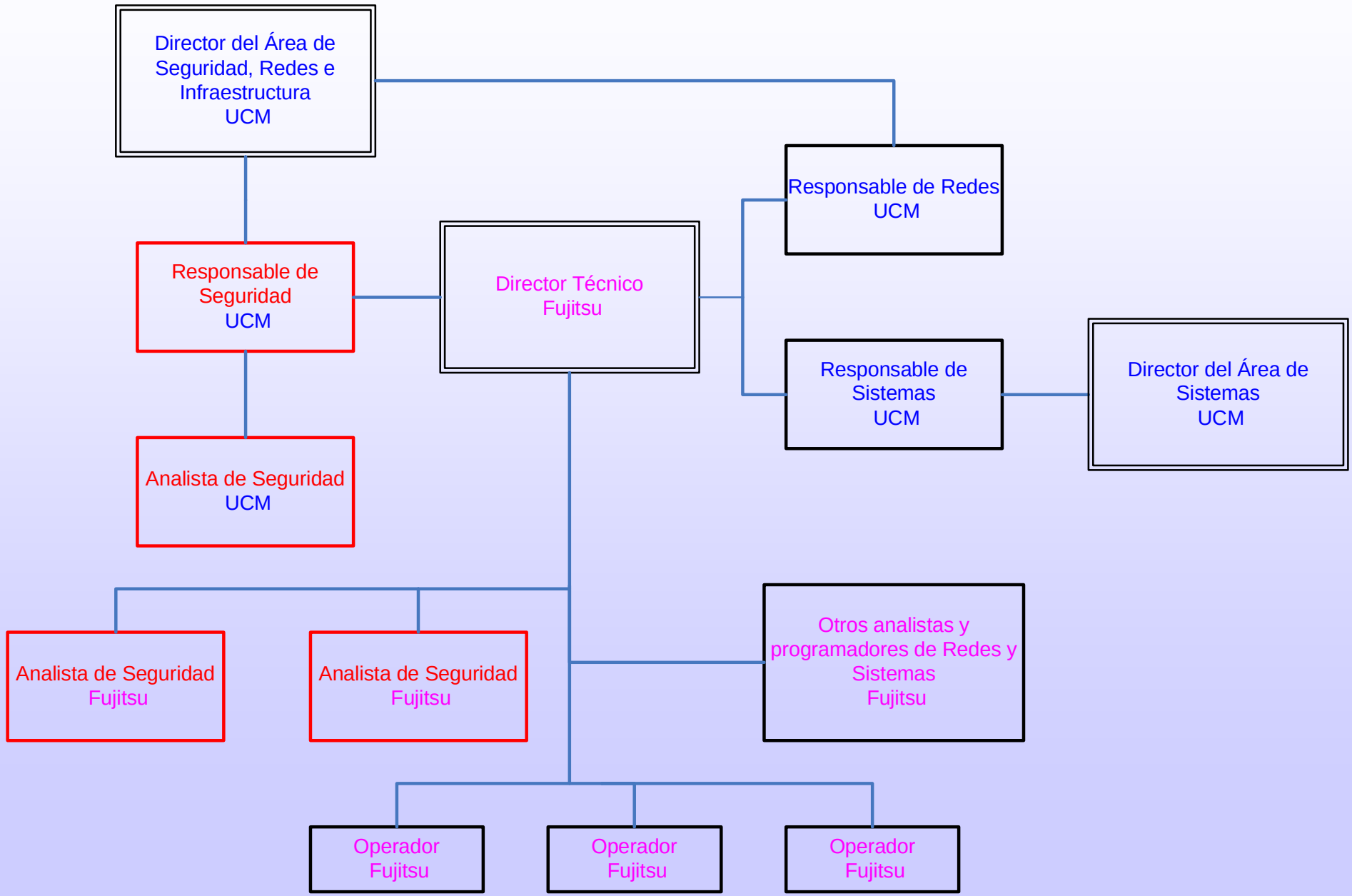
Los números de la Universidad

- 35 edificios en 2 campus + 5 centros remotos
- Estudiantes: > 100.000 (sólo títulos oficiales de primer, segundo y tercer ciclo)
- Personal: ~ 10.000 (PAS y PDI)
- Puntos activos de red: ~ 20.000 (+ 2.000 por año)
- Puntos de acceso Wifi: ~ 200 (+ 120 en verano 2007)
- Tráfico de red (picos habituales de entrada y de salida):
  - VLAN de servidores: ~ 500 Mbit/s
  - Internet: ~ 200 Mbit/s

Arquitectura del equipamiento de seguridad



"Arquitectura" del equipo de seguridad



Estrategia de diseño

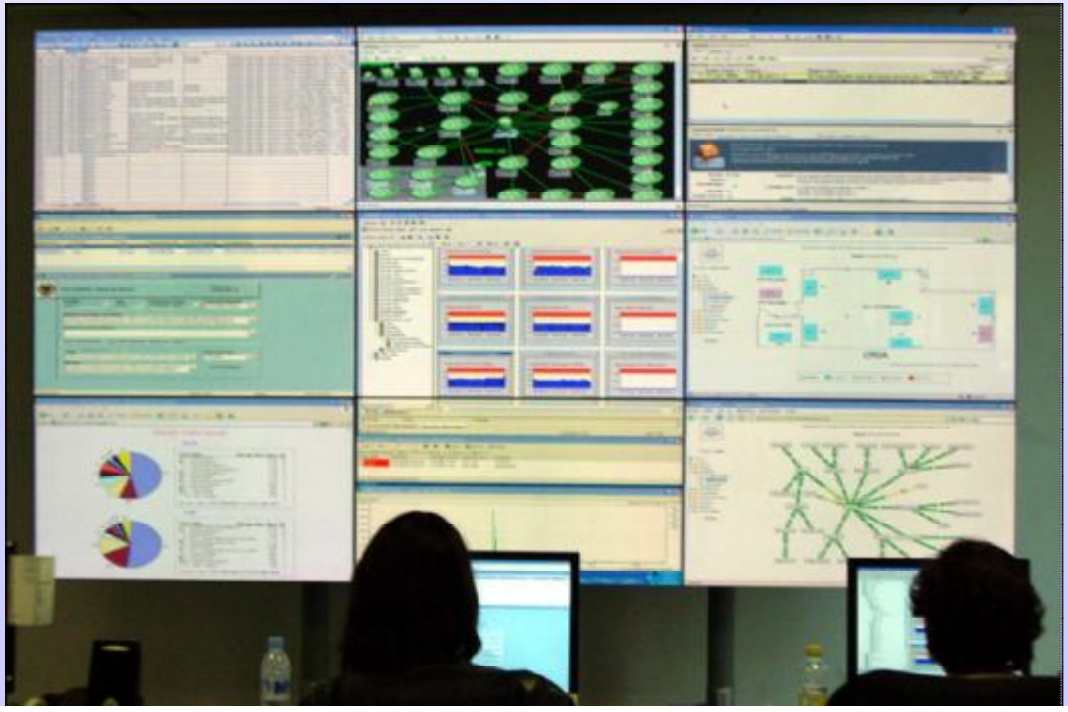
- Gestor de ancho de banda + FW + IDS en la conexión con Internet
- FW + IDS en el acceso a VLAN protegidas (servidores, administración, etc.)
- Control de flujos, políticas (cuarentenas) y MAC *locking* a nivel de puerto de red (electrónica Enterasys)
- Centralización y correlación de *logs* de *routers*, FWs, IDSs, AVs, sistemas, aplicaciones, etc. en una consola de seguridad (SIM/SEM/SIEM)

Estrategia de configuración

- Dos aproximaciones para la detección de incidentes:
  - Paranoica, del todo al máximo útil
    - Ventaja: obtiene el máximo partido de la información
    - Inconveniente: agobiante y consume mucho tiempo al principio
    - Usada con nuestros IDSs
  - Precavida, de cero al máximo efectivo
    - Ventaja: apenas hay falsos positivos, se ahorra tiempo
    - Inconveniente: se pueden perder eventos importantes
    - Usada con nuestra consola de seguridad (correlaciones)

Operación de primer nivel

- 3 operadores de Fujitsu atienden alarmas y vigilan anomalías de 8 a 20 horas en el CPD de la UCM
- Vigilancia remota 24x7 desde Fujitsu de anomalías graves, con servicio de *standby*



Operación de segundo nivel

- 2 analistas de Fujitsu de 8 a 19:
  - Atienden alarmas escaladas por los operadores
  - Analizan eventos complejos que requieren investigación
  - Configuran los dispositivos y crean nuevas reglas
- 2 analistas de la UCM de 9 a 18:
  - Apoyan a Fujitsu en la atención e investigación de eventos
  - Apoyan a Fujitsu en la configuración y creación de reglas
  - Coordinan con el resto de departamentos: Sistemas, Apoyo al Puesto de Trabajo (APT), Aulas, etc.

Detección de incidentes (manual)

- Anomalías en el tráfico de red en *routers* y gestor de ancho de banda: volumen y clases de tráfico, nivel de *broadcast*, número de sesiones, consumo de CPU en los *routers*, etc.
- Eventos conocidos de alta efectividad en IDSs, FWs, *routers*, SEM (correlación) y aquellos que muestren un crecimiento anómalo
- El resto de eventos son “ruido” investigado según el tiempo disponible

Actuación (manual) ante incidentes

- *Escaneo* equipo/s interno/s implicado/s => puertos indicativos
- Vigilancia conexiones IP/s implicada/s (locales y remotas)
  => puertos indicativos
  => otros equipos comprometidos
- *Escaneo* red UCM puertos indicativos => otros equipos comprometidos
- Investigación forense IP/s implicada/s en IDSs y SEM
  => otros equipos comprometidos
  => eventos que pasan de ser “ruido” a ser efectivos
  => posible creación de reglas de correlación
- Incidencia (*ticket*) al equipo de soporte: APT, Aulas, Sistemas => otros equipos comprometidos

Contención de incidentes (I)

- Preventiva:
  - Cierre de puertos peligrosos en FW de Internet (Netbios, MS SQL, SMTP, etc.)
  - Limitación en el gestor de ancho de banda del tráfico no clasificado y del clasificado como P2P, IRC y NNTP, a nivel de ADSL casero
  - Políticas de tráfico entre VLANs en FWs de *core*
  - Limitación del número de flujos a nivel de puerto de red a 700/s y bloqueo automático del puerto al sobrepasar 1000/s
  - Antivirus corporativo perimetral de correo, de servidor y de puesto de trabajo (Trend Micro)
  - Vigilancia automática anti-*defacement web* institucional

Contención de incidentes (II)

- Reactiva (manual):
  - Bloqueo a nivel de puerto de red de equipo/s interno/s implicado/s si incurre alguna de estas circunstancias:
    - IP duplicada o IP *spoofing*
    - Protocolos permitidos en la política de cuarentena
  - En otro caso, política de cuarentena a nivel de puerto de red de equipo/s interno/s implicado/s, que sólo permite:
    - DNS y navegación HTTP y HTTPS
    - Correo por POP, IMAP y SMTP
    - Actualización del antivirus
  - Bloqueo temporal a nivel del FW de Internet de IP/s externa/s implicada/s

Resultados

- Bastante buenos:
  - Disminución del número de incidentes, principalmente de los dirigidos, ejemplo:

Año \ Mes	enero	febrero
2005	431	305
2006	145	106
2007	268	25

  - Gran disminución del tiempo de respuesta, debido a:
    - Más personal
    - Eventos bien identificados
    - Personal dedicado (operadores)

Problemas (I)

1. No hay contención de incidentes fuera de horas laborables => Ya se ha observado la tendencia a que los ataques dirigidos se produzcan fuera de este horario
2. Difícil identificar ataques dentro de una misma VLAN => Ya se ha observado la tendencia en los ataques dirigidos a evitar *escaneos* de la red de servidores
3. Las cuarentenas se aplican al puerto de red => Los usuarios detectan un problema y se cambian de roseta

Problemas (II)

4. Difícil localizar e informar al usuario de su situación (aunque el usuario puede llamar al CAU y éste consulta la BD de cuarentenas) => cabreos
5. Políticas poco flexibles en puerto de red => limitaciones

- Difícil crear reglas de correlación complejas en LogICA
- Multitud de ataques externos (al menos *escaneos*) => si se aplica bloqueo en FW, ¿nos quedaremos solos?

Soluciones en estudio y pruebas (I)

1. Automatización de acciones de contención usando consola de seguridad (en pruebas)

   Usar IDSs en modo IPS (ya posible pero en estudio)
2. Usar otros IDSs o sondas virtuales con VLAN *mirror* (en estudio)
3. Sentinel (Enterasys) para aplicar políticas por MAC y no por puerto de red (en pruebas)
4. Redirección de usuarios en cuarentena a *web* cautiva (en estudio)

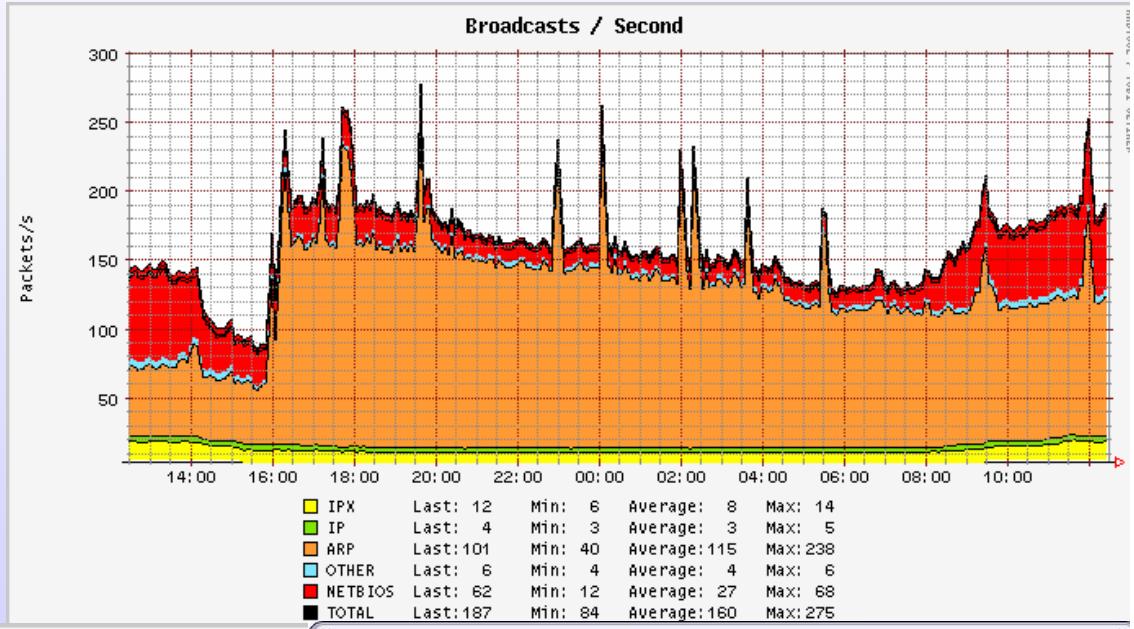
Soluciones en estudio y pruebas (II)

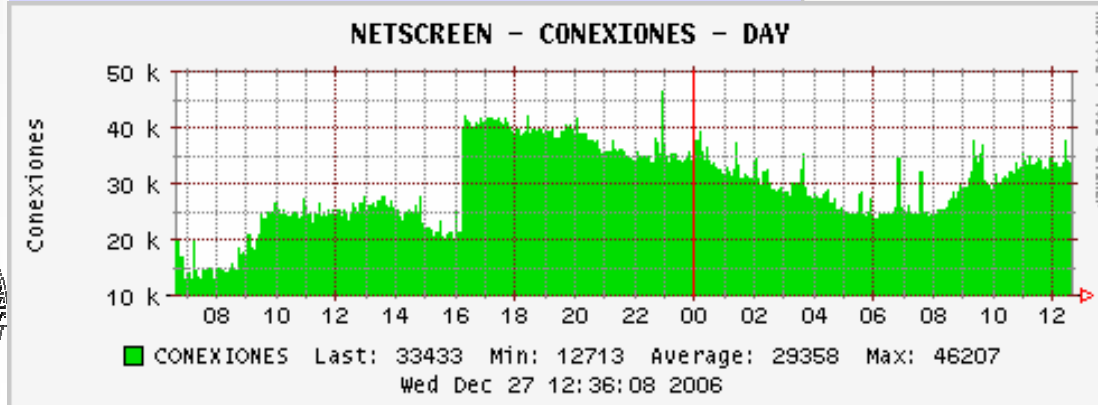
5. Actualización de la electrónica de red (habitualmente de manera continua)

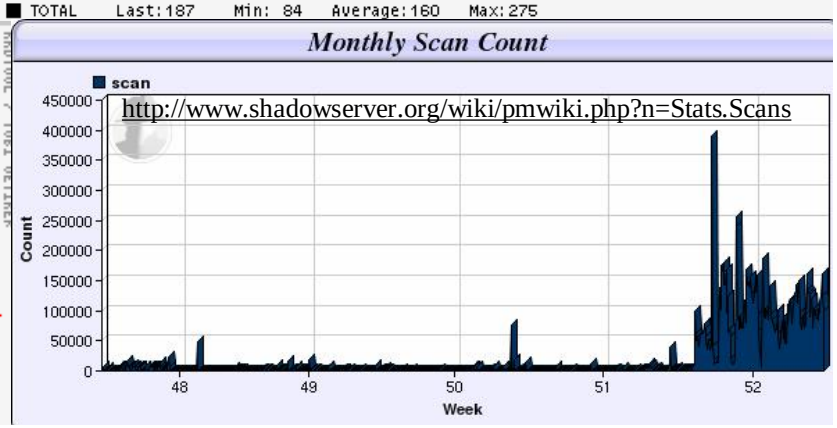
- *Honeypot* (en pruebas)
- Análisis de vulnerabilidades (Nessus) => base de datos para correlacionar con los ataques (en pruebas)

Incidente 26/12/2006 (externo)

- Aumento súbito del *broadcast* ARP
- IDSs no detectan nada anormal
- Idéntico aumento en flujos Internet
- *Honeypot* muestra *scan* ICMP lento:
  - 4 *echo request*, 1 por segundo
  - 5 segundos de pausa entre IPs
- Se crea regla en IDS con ejecución de bloqueo automático en el FW
- En una sola noche se detectan 4500 IPs externas distintas







Incidente 08/01/2007 (interno)

- Precursor el martes 2 de enero (durante vacaciones de Navidad):
  - La línea de un centro remoto (2 Mbps) se acerca a la saturación
  - El IDS de Internet muestra un incremento de conexiones IRC por puertos fuera del estándar, la mayoría hacia un determinado servidor externo
  - Se vigilan las conexiones de un PC infectado y se ve que el ataque consiste en un *buffer overflow* contra el puerto 139 de nuestra subred probando unas 15.000 variantes con cada IP => mucho tráfico pero *escaneo* lento
  - Se filtra la IP del servidor IRC externo en el FW de Internet, se registra todo ordenador interno que intenta conectarse a él y se pone en cuarentena
  - La infección continua hasta el viernes 5 a un ritmo bajo, unos 5-10 PCs por día
- Estallido el lunes 8 de enero (vuelta de vacaciones de Navidad):
  - Se repiten los síntomas pero a mayor escala: líneas de centro remotos saturadas y el IDS de Internet muestra un gran incremento de las conexiones IRC por puertos fuera del estándar, la mayoría hacia **otro** servidor externo
  - Se repite el procedimiento filtrando el nuevo servidor IRC externo y poniendo en cuarentena los ordenadores internos que intentan conectarse a él
  - La infección se controla el martes 9, poniendo en cuarentena unos 100 PCs por día

Eventos de IDS más útiles

- *Escaneo* de puertos Netbios desde el interior => PC con virus
- *Escaneo* de puertos **no** Netbios desde el interior => PC comprometido
- Ataques de fuerza bruta desde el interior => PC comprometido
- Envío de *spam* => PC con virus
- Servidor FTP en puerto no 21 => PC comprometido
- Incremento conexiones IRC no estándar => Botnet

Gracias por su atención

E-mail:

Luis Padilla: lpadilla (at domain) pas ucm es

Joaquín Martín: jjmartin (at domain) pas ucm es