fs2007
V Foro de Seguridad RedIRIS

Detección de Intrusiones

Toni Pérez
Universitat de les Illes Balears

toni.perez@uib.es

RedIRIS

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

¿Cómo somos?

- Alumnos + Personal = 20.000
- 14 Edificios + 26 Centros remotos
- Presencia en todas las islas
- 4000 Equipos conectados a la red
- 3366 Direcciones IP públicas administradas

- Personal redes y comunicaciones: 8
  - Reciente incorporación: 4
  - Dedicados a Seguridad: ?
  - Muchos cambios: fw, lan, core, wifi, voip,…

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

Elementos de seguridad

- Firewall perimetral
  - Perímetro: internet, wifi y vpn
  - Funciones de IDS/IPS
  - Centralización de logs
- ACLs routing entre vlans
- Control de ancho de banda del perímetro
- Protección contra intrusos IPS

Elementos de seguridad

- IDS: Snort-Base y Dragon
- Honeypots: KFSensor

- Sniffers
  - Ethereal/Wireshark y Netasyst
- Analizadores de vulnerabilidades
  - Nmap, Nessus y Retina

- Políticas 802.1x/UPN
- Antivirus/firewall para usuarios

Agenda

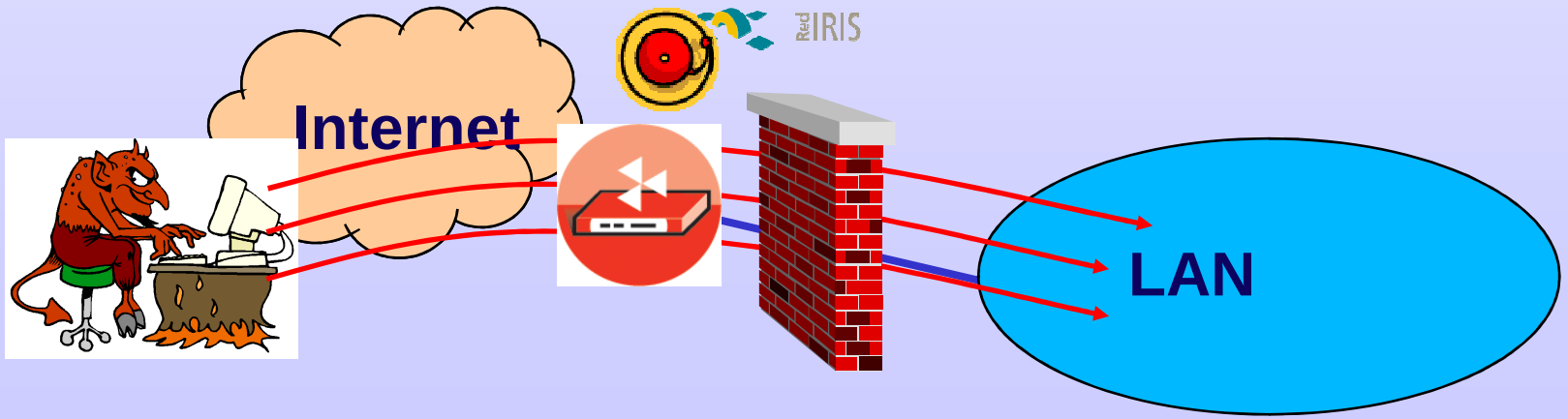
- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

Diseño: a tener en cuenta…

- Equilibrio seguridad-rendimiento
  - Minimizar la latencia
- Alta disponibilidad
  - Redundancia o bypass
- Equipos multifunción: ¿para qué fueron diseñados?
  - IDS/IPS
    - IPS, Firewall, controler wifi,…
  - Filtrado:
    - BW-MGR, IPS, switch/UPN,…
  - Control de ancho de banda:
    - BW-MGR, IPS, Firewall, …
- Cuatro frentes de batalla…

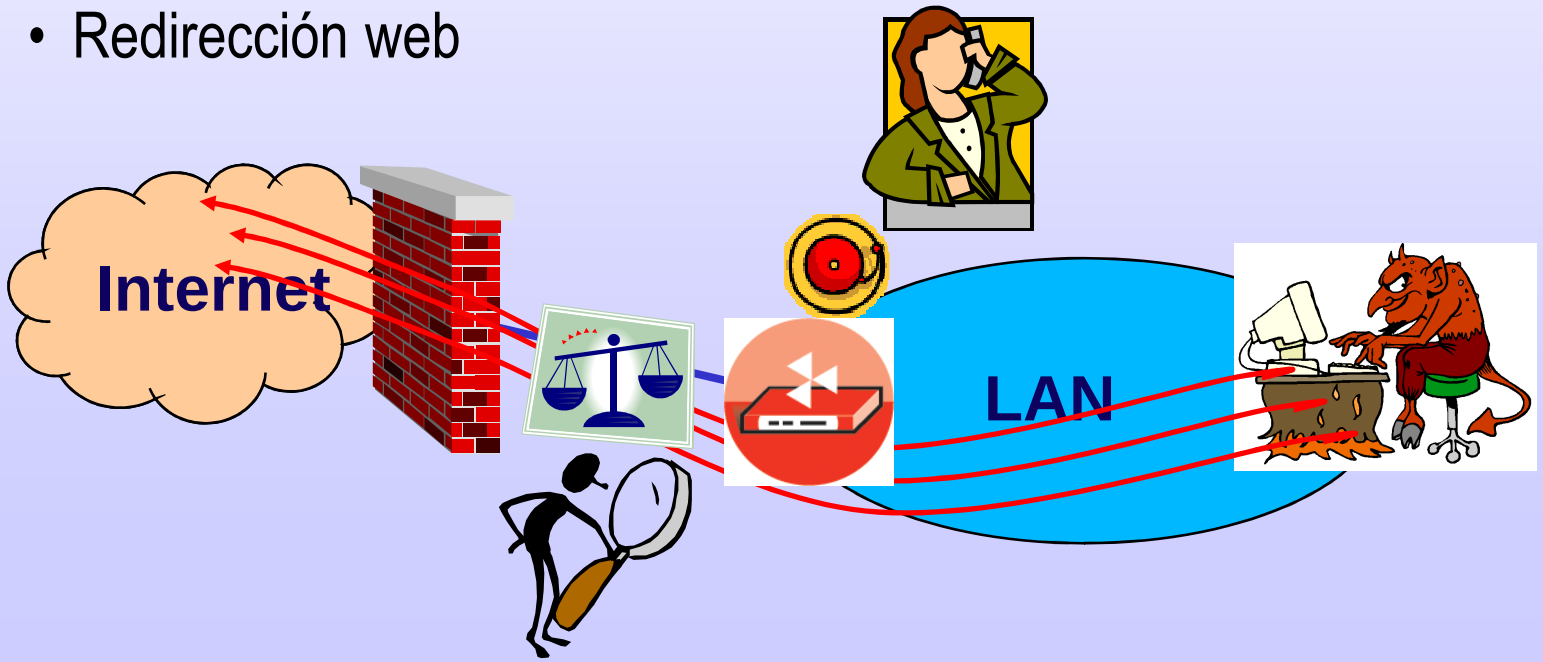
Internet hacia LAN (1/4)

- Externo – Interno
  - Constantes scans y DoS “típicos” contra el rango público
    - Origen RedIRIS y origen no-RedIRIS
  - Bloqueo “despreocupado” con IPS
    - Cuarentena de IPs, patrones de lógica difusa (estado de la red)
  - IDS más específico



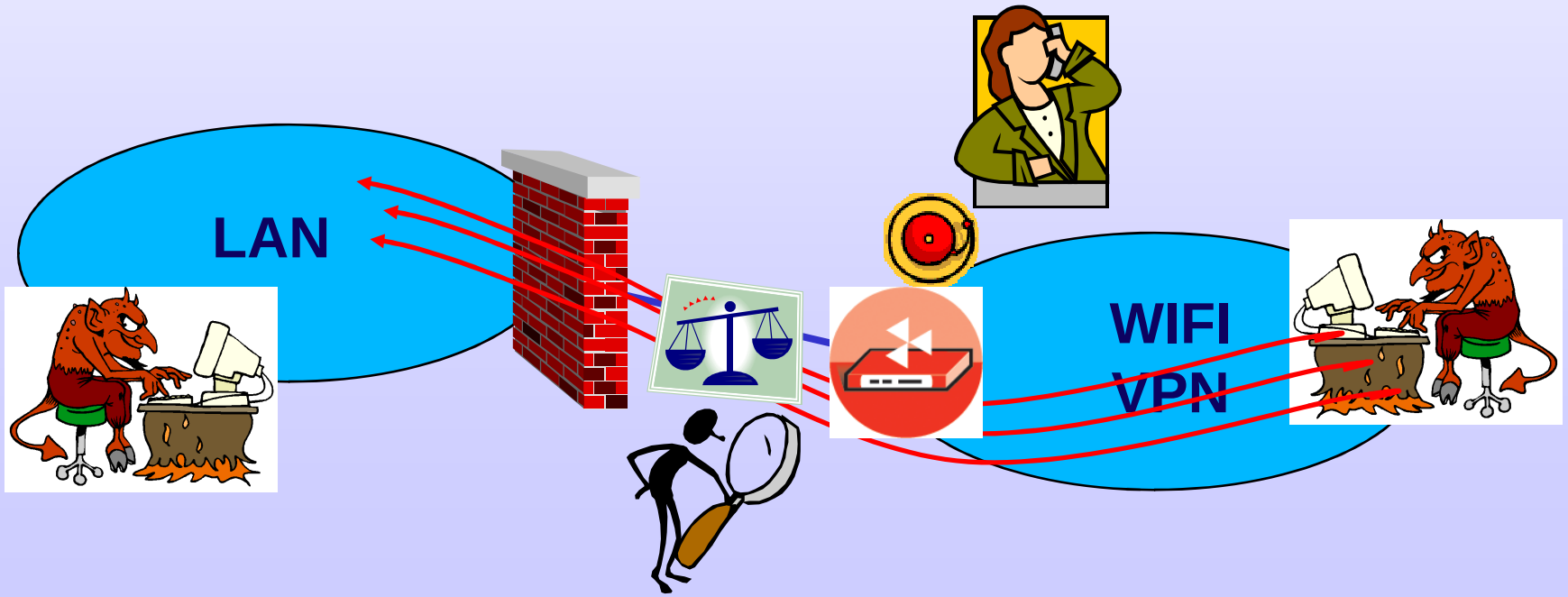
LAN hacia Internet (2/4)

- Interno – Externo: LAN-Internet
  - No volvemos a analizar el tráfico Externo-Interno
  - IPS con alarmas prioritarias
    - Podemos actuar sobre el origen
  - Control de ancho de banda
    - Redirección web



LAN – WIFI/VPN (3/4)

- Interno – Externo: LAN-wifi-vpn
  - Analizamos los dos sentidos
  - IPS con alarmas prioritarias
    - Podemos actuar sobre el origen
  - Control de ancho de banda



Comunicaciones Internas (4/4)

- Interno – Interno: LAN-CPDs
  - Complicado:
    - Enlaces malla 10Gbps
  - IPS-IDS con port-mirroring
  - Módulos IDS/IPS en el Core??

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

Arquitectura de seguridad

- IPS (Externo-Interno)
- Firewall perimetral
- Control de ancho de banda
- IPS (Interno-Externo)

- IDS (Externo-Interno y Interno-Externo): Port-Mirroring
- IDS (CPDs): Port-Mirroring
- IPS (IDS) (Interno-Interno): Port-Mirroring
- Honeypot
- Scanner: nmap + retina + nessus

Múltiples segmentos un IPS

Radware

Connect & Protect Table

Add | Delete

	S	Port	Networks	Intrusions	DoS/DDoS	SYN Floods	Anomalies	Anti-Scanning
0	☑		From any To Mail Servers	Mail Servers	DOS Inbound		Mail Protection	Mail scanning
1	☑		From any To Users Segment	Worms				scanning
	☐		From To					
	☐		From To					

Settings

Intrusion Prevention Profiles

- Profiles
  - ☐ Ron
  - ☐ p1
  - ☐ Mail Servers
  - ☑ Worms

New Profile | Add | Delete | Edit Attack

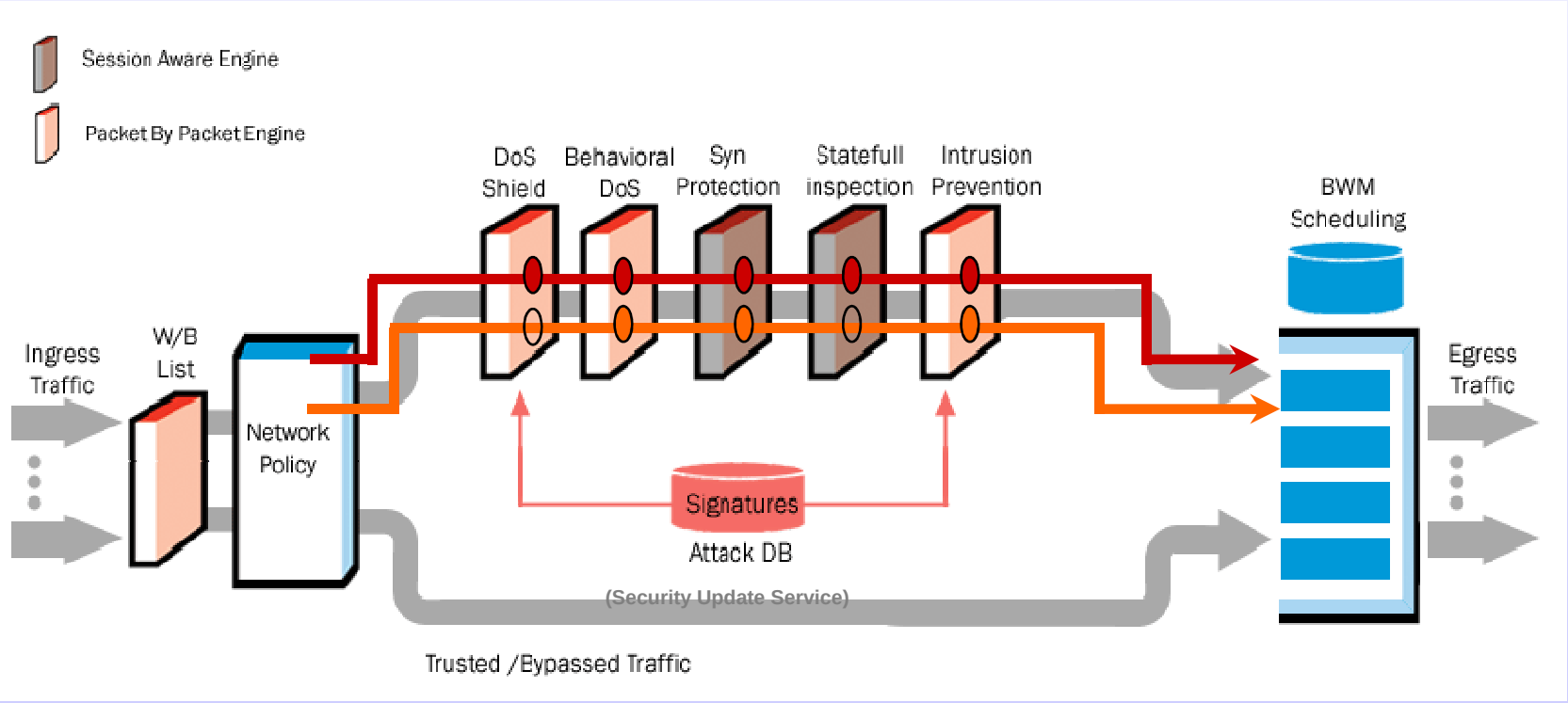
All Intrusion Attacks

- Attacks
  - unassigned_filters
  - standard
  - 0-dori-grp
  - worms
  - backdoors_inbound
  - backdoors_outbound

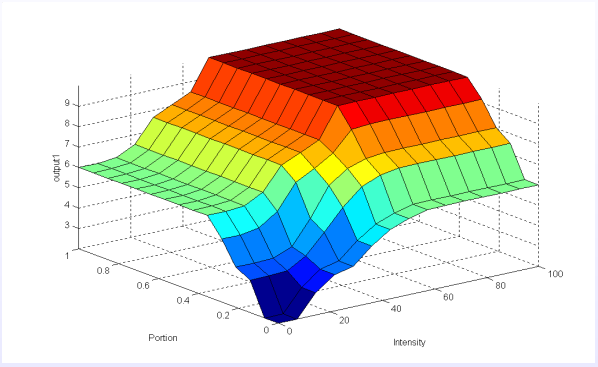
Custom Attack | Custom Group | Apply | OK

radware

Reglas aplicadas a cada segmento



Behavioural DoS

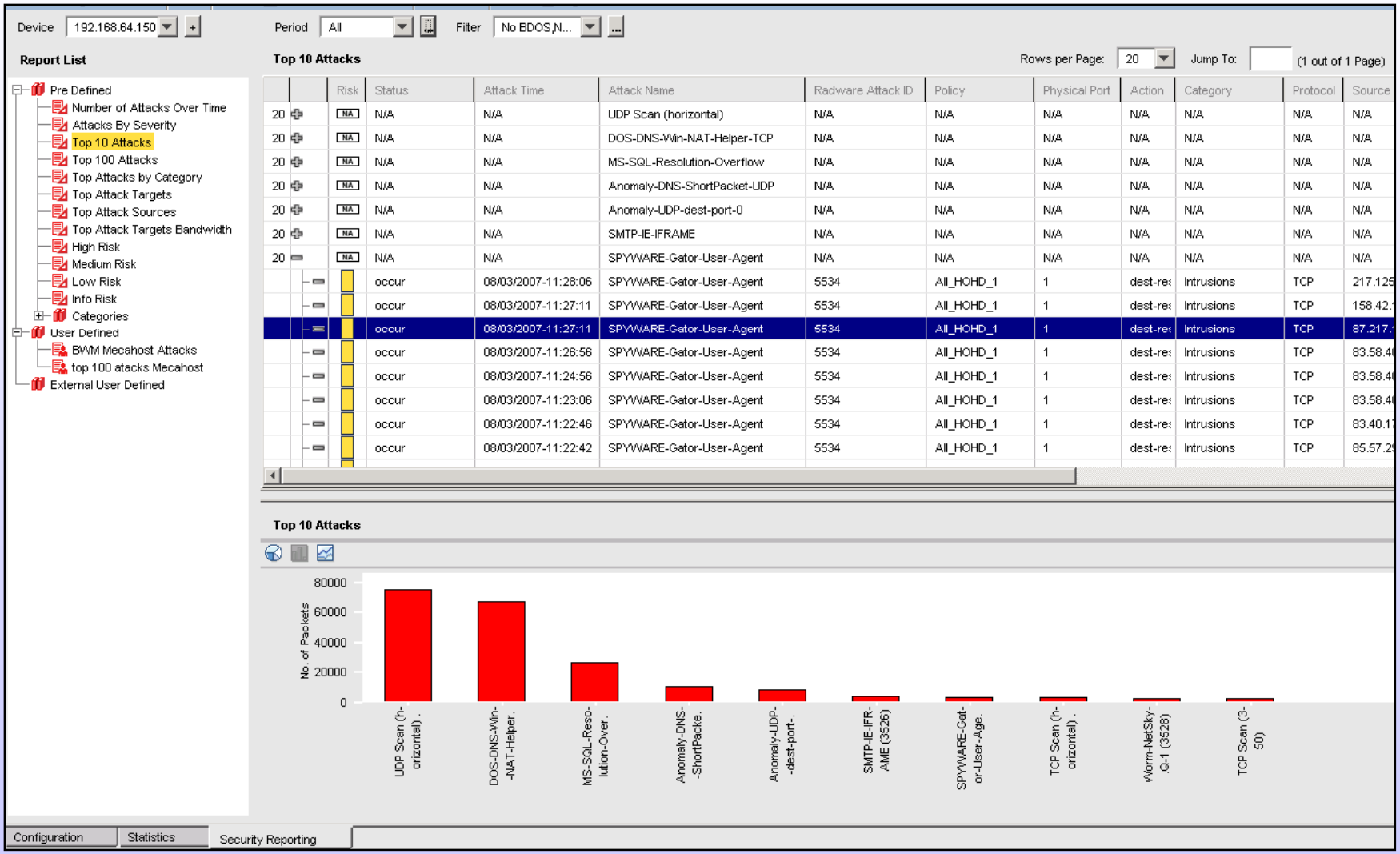


¿ Cómo Funciona ?

- Adaptando las características base de la red, a través de análisis estadísticos
- El sistema adapta periódicamente los algoritmos de decisión a las características base de la red protegida
- Correlación del análisis y de la decisión a través del **algoritmo de Lógica Difusa**
- Prevención automática a través del análisis del impacto de las firmas y **retroalimentación** (refinado de las firmas)

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Reports tiempo real



Dashboard


APSolute Insite - Top Attacks Dashboard
radware
Device 192.168.64....
Port 1
Date 24.02.2007 16:17:24
Display 1 Hour/s
Total Active Attacks 27,594,025
Map Top 12
TCP Scan (350)
Anomaly-DNS-ShortPacket-UDP (3662)
UDP Scan (horizontal) (351)
MS-RPC-DCOM-Interface-BO (4294)
Ping Sweep (352)
network flood UDP (70)
TCP Scan (horizontal) (350)
L4 port zero (16)
UDP Scan (351)
MS-SQL-Resolution-Overflow (4726)
SPYWARE-Gator-User-Agent (5534)
Anomaly-DNS-Z-Flag-UDP (
Top Sources
82.159.204.29
496 (46.62%)
62.81.199.32
266 (25%)
62.81.199.29
146 (13.72%)
82.159.210.21
83 (7.8%)
82.159.210.31
73 (6.86%)
Attacks by Risk
high
27,419,294 (99.93%)
medium
17,413 (0.06%)
low
445 (0%)
Top Targets
62.81.199.225
98 (37.4%)
82.159.210.31
46 (17.56%)
62.57.21.77
42 (16.03%)
82.159.210.21
39 (14.89%)
82.159.210.10
37 (14.12%)
Attacks by Group
Behavioral-DoS
27,575,528 (99.93%)
Anti-Scanning
17,280 (0.06%)
Intrusions
764 (0%)
Anomalies
464 (0%)
Last Event: UDP Scan, 0 Kbit at 16:17:47
Device: 192.168.64.150
Total Traffic and Attacks

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

Operativa y procedimientos

- Alarma o incidencia
- Investigación: acotar una firma o patrón
- Localizar equipos con la misma firma o patrón
- Actuación…
  - Reinstalar el sistema comprometido
  - Concienciar a los usuarios

- Base de datos de información de red
- Futura correlación completa

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

Pros y contras

- IPS
  - Diseñado para ser un IPS
  - Filtrar las ataques masivos y prever comportamientos anómalos
  - No es crítico: modo bypass
  - Precio elevado… o no, por todo lo que hace.
- IDS
  - Dedicarlo a reglas más específicas
  - Económico

Pros y contras

- Firewall
  - Elemento crítico con funciones de routing
  - ¿Nos arriesgamos a sobrecargarlo con IDS/IPS?
- Electrónica de red / Backbone
  - ¿Añadimos módulos IDS/IPS?
  - Solución para DMZ no claramente definidas
  - Precio, estabilidad,…

Resultados

- Snort: Numerosos equipos Pubstro
  - ACRI
- IPS:
  - Desaparición de los constantes scans y descarga de proceso de firewall e IDS
- Incrementamos la complejidad
  - Aparece un problema… ¿Dónde estamos filtrando?
  - De que sirve hacer un ping o un telnet al puerto 80…

Agenda

- ¿Cómo somos?
- Elementos de seguridad
- Estrategias de diseño
- Arquitectura de seguridad
- Operativa y procedimientos
- Resultados y experiencias
- ¿Hacia dónde vamos?

¿Hacia dónde vamos?

- Adquirir el IPS?
- Automatizar y centralizar la gestión de alarmas
  - Correlación con la base de datos de información de red
- Ampliar las políticas de buen uso
- Control de admisión

Gracias!!!

Red IRIS

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Toni Pérez
toni.perez@uib.es