Seguridad de Redes de Computadores

Redes de Computadores

FIEC04705

Sesión 26

Agenda

- Terminología
- Seguridad operativa:
  - Firewalls
  - IDSs y
  - DMZs

Terminología

Terminología

- **Intrusion**: un conjunto de acciones que tiene por objeto comprometer los *security goals*:
  - Integrity
  - Confidentiality
  - Availability

Firewall

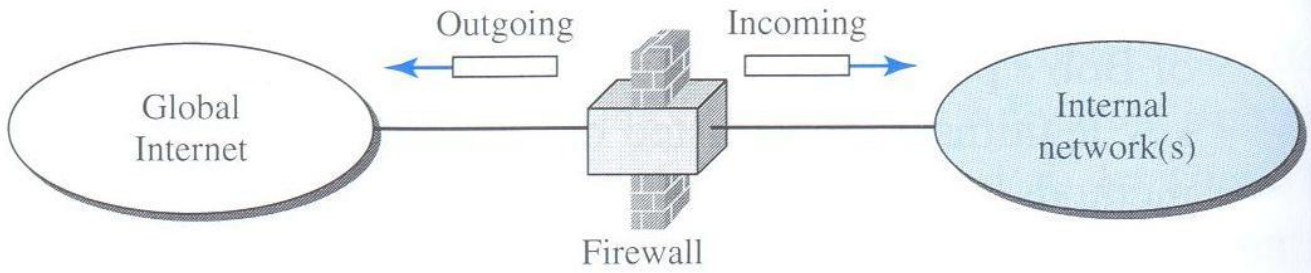
Firewall

- Un firewall es un dispositivo (usualmente un router o una computadora) instalado entre la red interna de una organización y el resto del Internet.
- Está diseñado para reenviar algunos paquetes y filtrar (no reenviar) otros.
- Los firewalls se clasifican como:
  - Packet-Filter Proxy
  - Proxy Firewall

Firewall

- Un firewall puede filtrar todos los paquetes entrantes destinados a un host o servidor.
- Un firewall puede ser utilizado para negar el acceso a un host o servicio específico dentro de la organización.

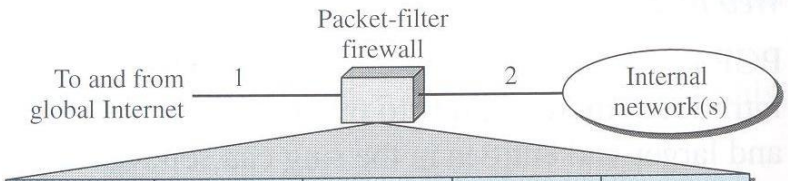
Figure 32.22 *Firewall*



Packet-Filter Firewall

- Un paket-filter firewall es un router que usa una tabla de filtración para decidir que paquetes deben ser descartados (no reenviados)

Figure 32.23 *Packet-filter firewall*



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Packet-Filter Firewall

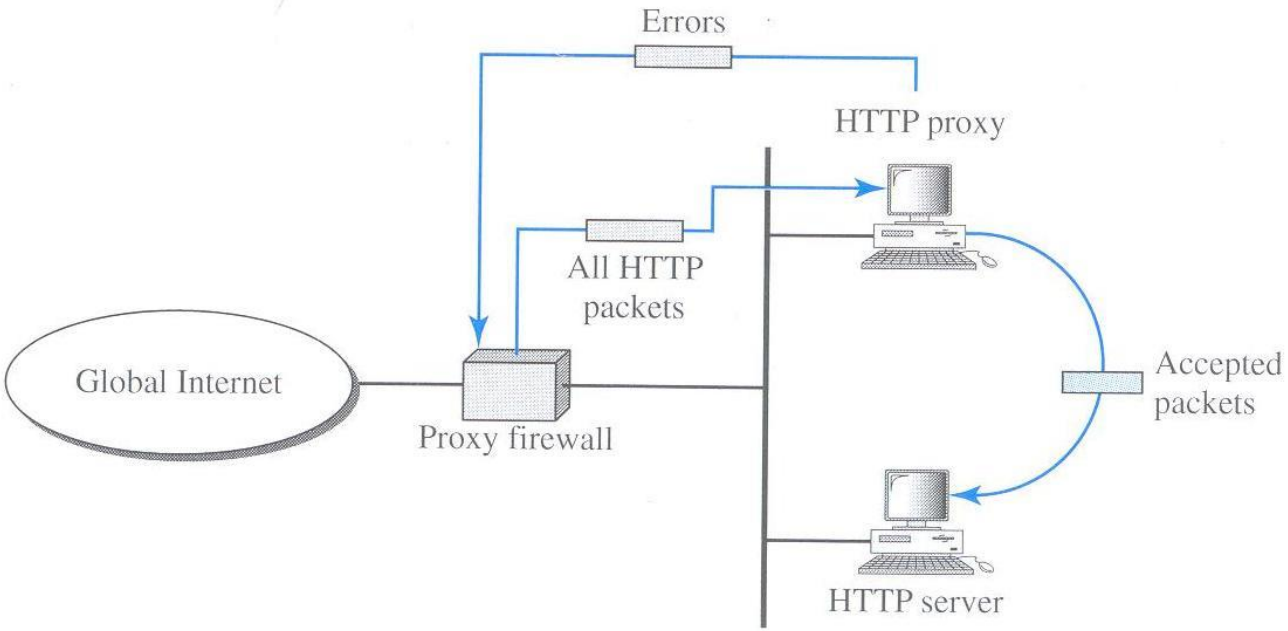
- Un packet-filter firewall filtra a nivel de capa de red o capa de transporte.
- Puede reenviar o bloquear paquetes basado en la información de las cabeceras de las capas de red y transporte:
  - IP origen y destino
  - Puertos origen y destino
  - Tipo de protocolo (TCP o UDP)

Proxy Firewall

- Un proxy firewall filtra a nivel de la capa de aplicación.
- Se implementa cuando se requiere filtrar un mensaje basado en la información disponible en el mismo.
- Un ejemplo clásico es el de filtrar los URLs para filtrar el acceso solo a ciertas páginas Web.

Proxy Firewall

Figure 32.24 *Proxy firewall*



Intrusion Detection System - IDS

IDS

- Un IDS es una aplicación que **detecta** y **responde** a intrusiones contra un sistema específico. Ejemplo: Snort
- Es un enfoque complementario a otros enfoques de seguridad:

Mecanismo	Enfoque
Prácticas de desarrollo seguro	Evitar
Firewall	Prevenir
IDS	Detectar

- Principio de seguridad: mecanismos en capas

Redes con un IDS

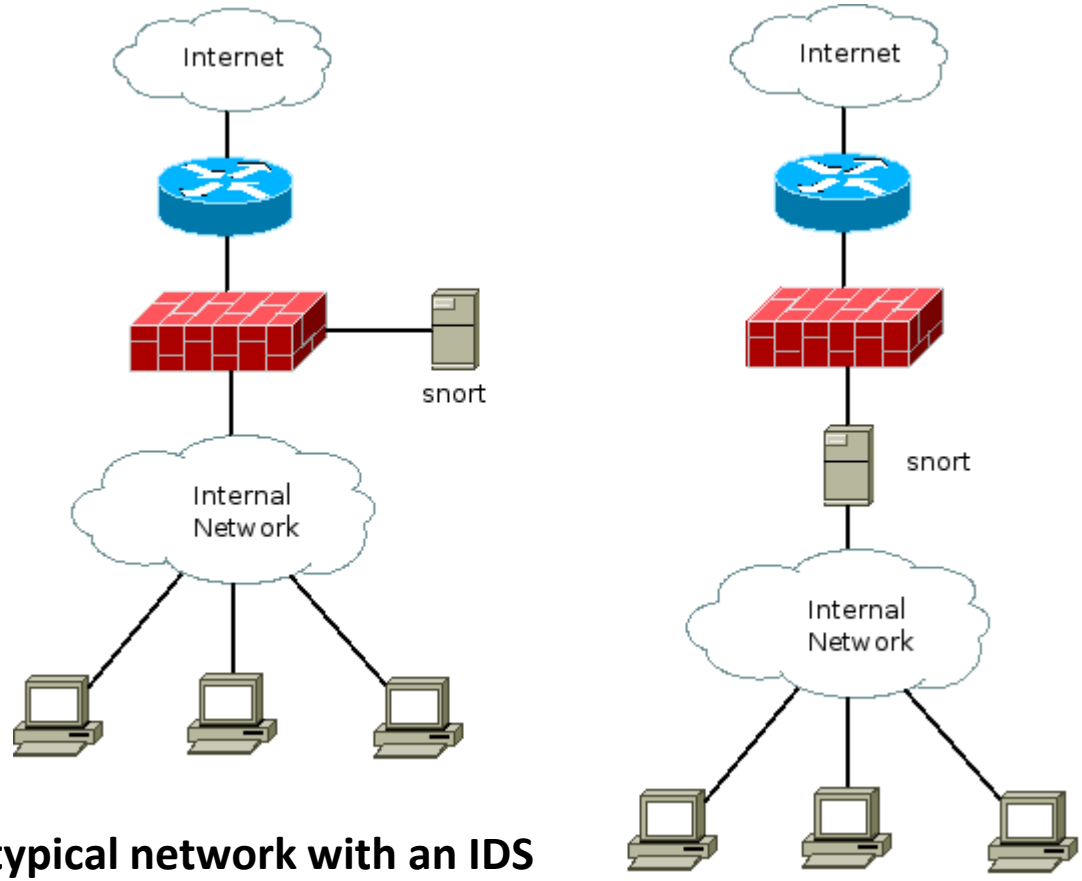
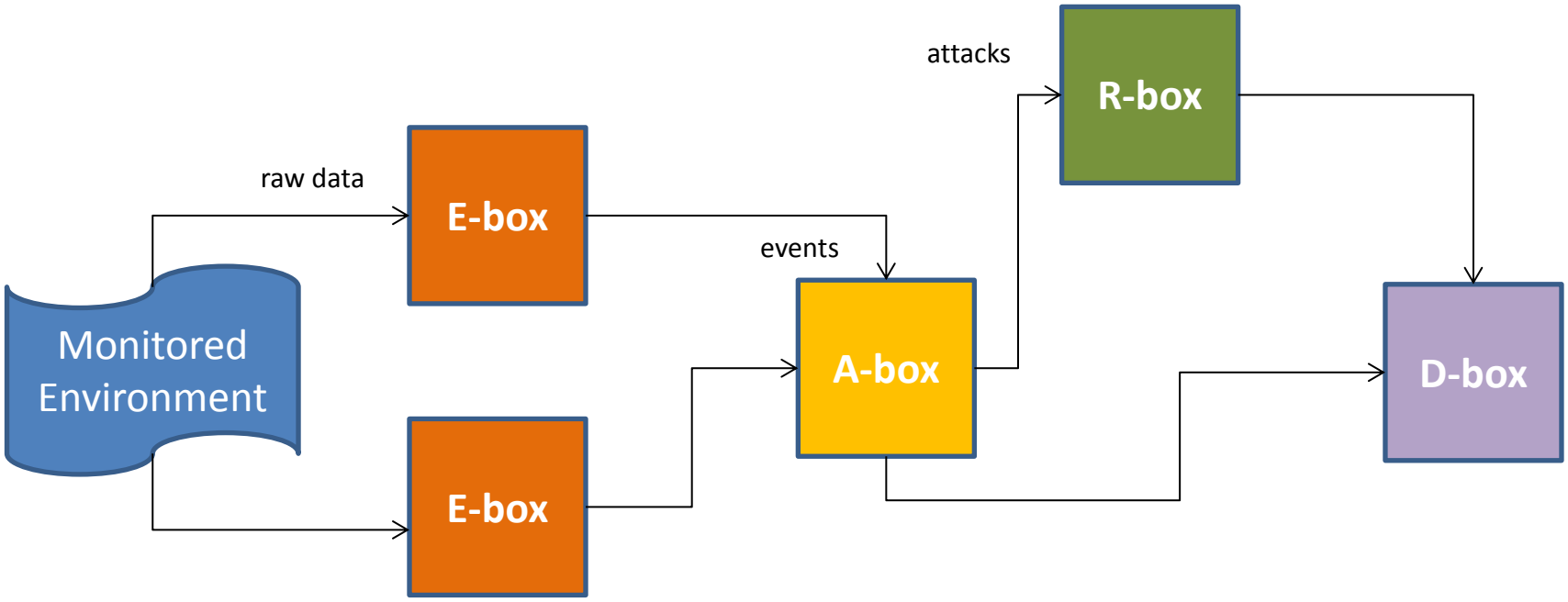


Figure 1: A typical network with an IDS

Figure 1 es una cortesía de http://www.digitalundercurrents.com

Arquitectura de un IDS



E-box genera eventos procesando raw audit data del sistema monitoreado [Audit source location]

A-box analiza eventos y genera alertas [Método de detección]

D-box almacena eventos para análisis post-mortem

R-box reacciona a ataques detectados [Comportamiento en detección]

Taxonomía de los IDSs

- Los IDSs difieren entre sí por la forma en la cual implementan cada una de las cajas del modelo abstracto:
- Método de detección
  - Cómo trabaja el A-box?
  - Cómo es desarrollado el A-box (manual vs. automático)
- Comportamiento en la detección
  - Cómo trabaja el R-box?
- Ubicación del origen de auditoria
  - De dónde leen los datos los E-boxes?

Detección: misuse-based

- Misuse-based IDSes contienen un conjunto de “firmas”, cada una de las cuales describe la manifestación de un ataque.
  - Las firmas son patrones de intrusiones
  - Si una secuencia de eventos es similar a una de las firmas, entonces es considerado como un ataque
- Modelo “*negativo*” o política de “*lista negra*”
  - Caracteriza actividad conocida como mala
- Ventajas:
  - Muy pocos falsos positivos
- Limitaciones:
  - Dificultad para generar el conjunto de firmas
  - No detecta nuevos tipos de ataques

Detección: anomaly-based

- Un anomaly-based IDS modela el comportamiento normal de eventos del sistema monitoreado.
  - Si una secuencia de eventos se desvía significativamente de estos modelos, los eventos son considerados evidencia de un ataque.
- Modelo "*positivo*" o política de "*lista blanca*"
  - Caracteriza actividad conocida como buena
- Beneficios
  - Puede detectar ataques desconocidos
- Desventajas
  - Puede generar falsos positivos (anomalías podrían ser nuevos tipos de actividades normales)

Misuse-based vs. Anomaly-based

Request	Tipo	Misuse-based	Anomaly-based
/view?page=balance	Normal	No alerta	No alerta
/view?page=../../etc/passwd	Ataque	Alerta	Alerta
/view?lang=aa[10kbytes]a	Ataque	No Alerta	Alerta
/view?id=1	Normal	No alerta	Alerta
/view?lang=OR 1=1	Ataque	Alerta	Alerta

Detección: generación del modelo

- Las firmas de los misuse-based IDS y perfiles de los anomaly-based IDS se generan de forma:
  - Manual
    - Inspeccionando ataques y extrayendo sus características
    - Usualmente misuse-based IDS
  - Proceso de aprendizaje
    - Analizando la actividad del sistema bajo monitoreo usando métodos estadísticos
    - Usualmente anomaly-based IDS

Comportamiento en la detección

- Pasivo
  - Cuando un ataque es detectado, la herramienta solo levanta una alerta
  - Existe un retraso significativo entre la detección y las acciones contra el ataque
- Proactivo
  - La herramienta reacciona contra ataques detectados (matar procesos, terminar conecciones, etc.)
  - Un intruso puede utilizar estas acciones para producir DoS

Ubicación del origen de auditoría

- Qué eventos son analizados por el IDS?
- Host-based IDS
  - Sistemas de información
  - Logs
  - Llamadas al sistema
- Network-based IDS
  - Sniffs la red para capturar tráfico
- Application-based IDS
  - Detecta ataques contra aplicaciones específicas

DMZ

DMZ

- DMZ es derivado del término “zona desmilitarizada”.
- DMZ es una subred física o lógica que contiene y expone los servicios externos de una organización a una red más grande no confiable, usualmente el Internet.
- El objetivo es agregar una capa de seguridad adicional a la LAN de una organización a fin que un intruso externo solo tenga acceso a los hosts en la DMZ.

DMZ

- Los hosts más vulnerables son aquellos que proveen servicios a usuarios fuera de la LAN, tales como los servidores de correo, Web y DNS.
- Por este motivo son ubicados en su propia subred para proteger al resto de la red en caso que un intruso tenga éxito al dirigir un ataque.
- Los hosts en la DMZ tienen conectividad limitada a hosts específicos en la red interna, pero la comunicación con otros hosts en la DMZ y hacia la red externa es permitida.

Puntos para recordar

- Clasificación de firewalls
- Características de los IDS
- Utilidad de una DMZ

Próxima Sesión

- Exámen II Parcial