Introducción a los Sistemas de detección de Intrusos (IDS) y monitoreo de Seguridad

Admon de Redes de Pc: Cristian Mutis Caez

Contenido de la charla

Parte I – Fundamentos de IDS

- Conceptos fundamentales de TCP/IP
- Teoría del ICMP (Internet Control Message Protocol)
- Teoría del servicio DNS (Domain Name Service)
- Teoría de fragmentación

Contenido de la charla

Parte II – Implementación y Administración de IDS

- Arquitectura de los sistemas de detección de Intrusos
- Introducción a los filtros y patrones
- Interoperatividad y correlación de eventos
- Escenarios de monitoreo de Seguridad
- Reacción automática o manual ante eventos de Seguridad
- Tendencias y proyección de los Sistemas de Detección de Intrusos

Contenido de la charla

Parte III - Factores Organizacionales

- Factores gerenciales
- Amenazas y vulnerabilidades Organizacionales
- Actividades relacionadas con la Implementación

Fundamentos de IDS

Conceptos de TCP/IP

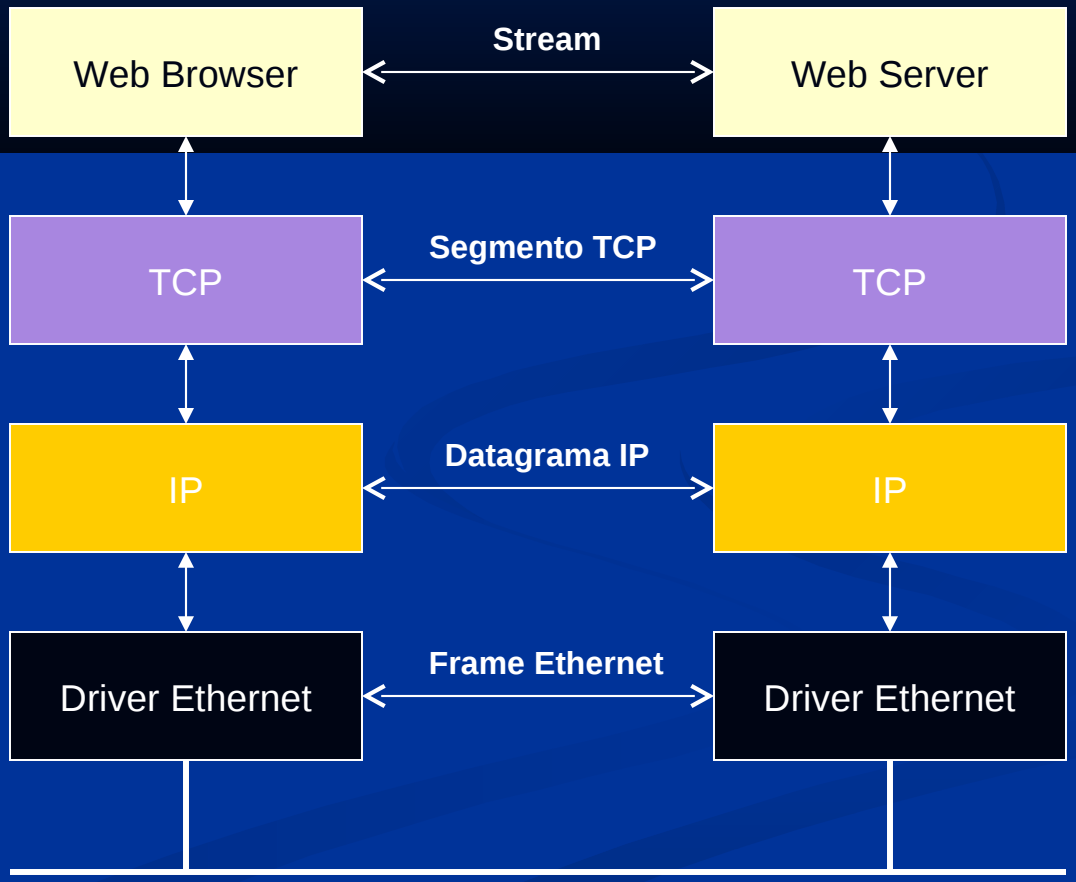
El modelo de Internet de TCP/IP

Capa de aplicación: Maneja la Implementación de aplicaciones de Usuario.

Capa de transporte: Maneja la conexión punto a punto entre equipos.

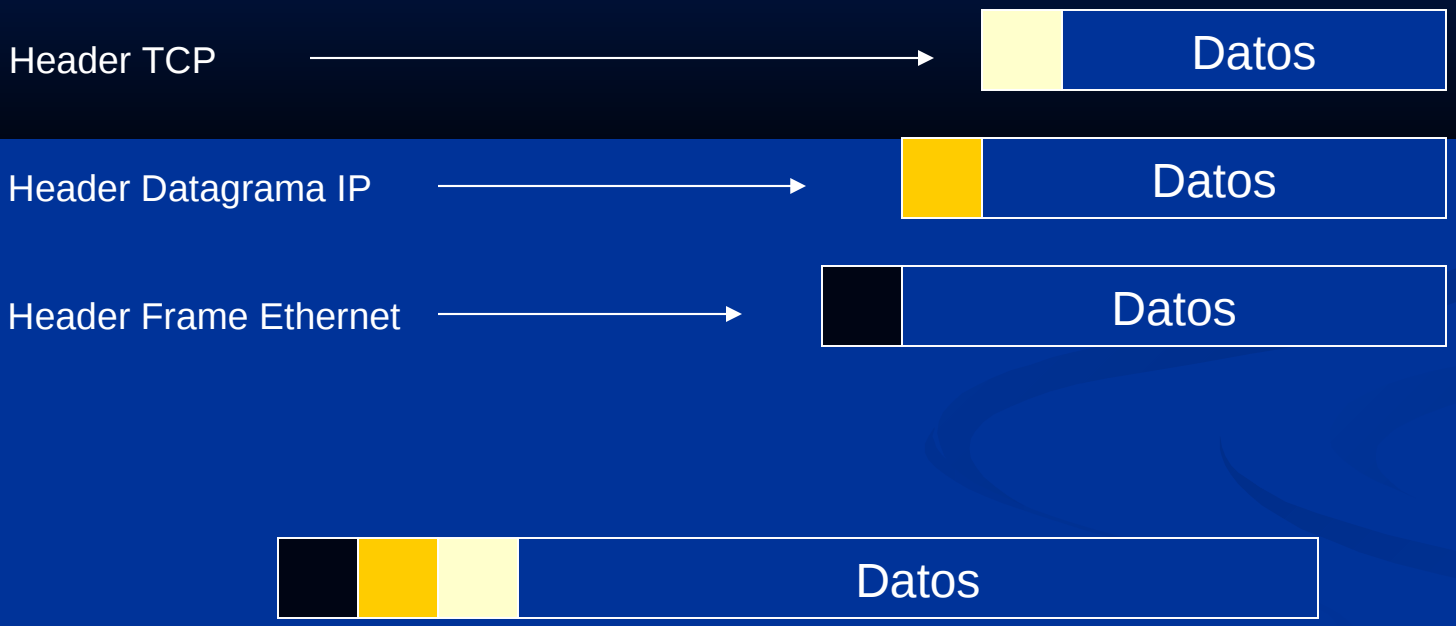
Capa de red: Mueve la información De fuente a destino.

Capa de enlace: Maneja la Transferencia de datos desde y hacia Medio físico.



Conceptos de TCP/IP

Encapsulamiento



Los encabezados de una capa, se convierten en datos para la siguiente

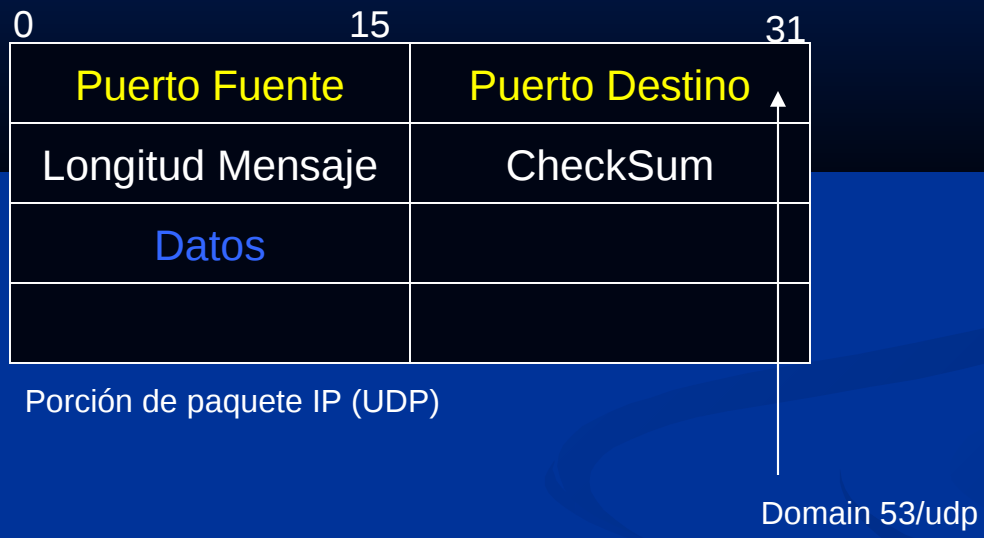
Conceptos de TCP/IP

Estructura del Encabezado IP

Total: 20 bytes

Conceptos de TCP/IP

Puertos de Servicios



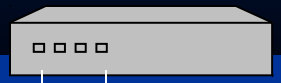
La longitud del campo es 16 bits, por lo que se Permiten 65535 puertos diferentes.

Conceptos de TCP/IP

Enrutamiento

IP Fuente: 172.20.41.2 MAC
MAC Fuente: 0f:00:20:1f:b0:0f
IP Destino: 172.21.19.8
MAC Destino: 0f:00:20:51:ab:47

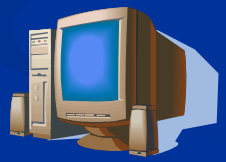
Enrutador



172.21.19.1
00:00:0c:00:8f:3c

172.20.41.1
00:00:0c:03:00:de

172.20.41.2
0f:00:20:1f:b0:0f



172.21.19.8
0f:00:20:51:ab:47

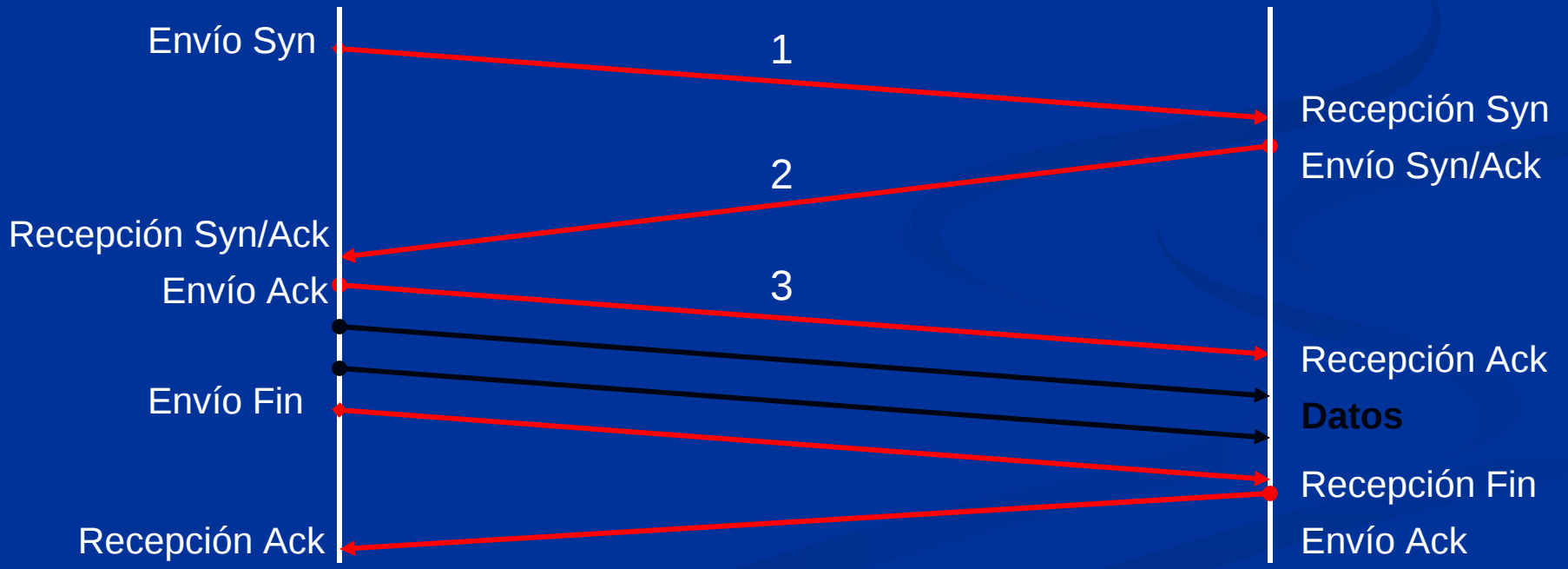
IP Fuente: 172.20.41.2 MAC
MAC Fuente: 00:00:0c:00:8f:3c
IP Destino: 172.21.19.8
MAC Destino: 0f:00:20:51:ab:47

Conceptos de TCP/IP

Establecimiento de conexiones TCP (1)

Cliente

Servidor

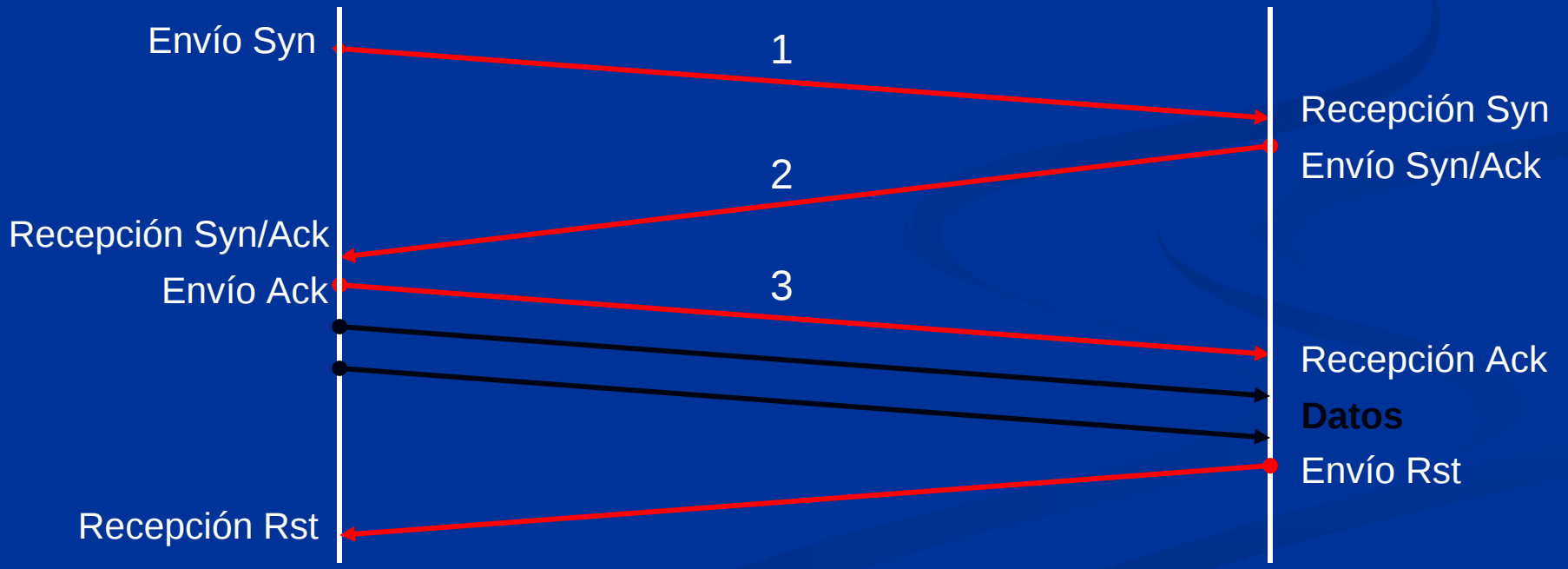


Conceptos de TCP/IP

Establecimiento de conexiones TCP (2)

Cliente

Servidor

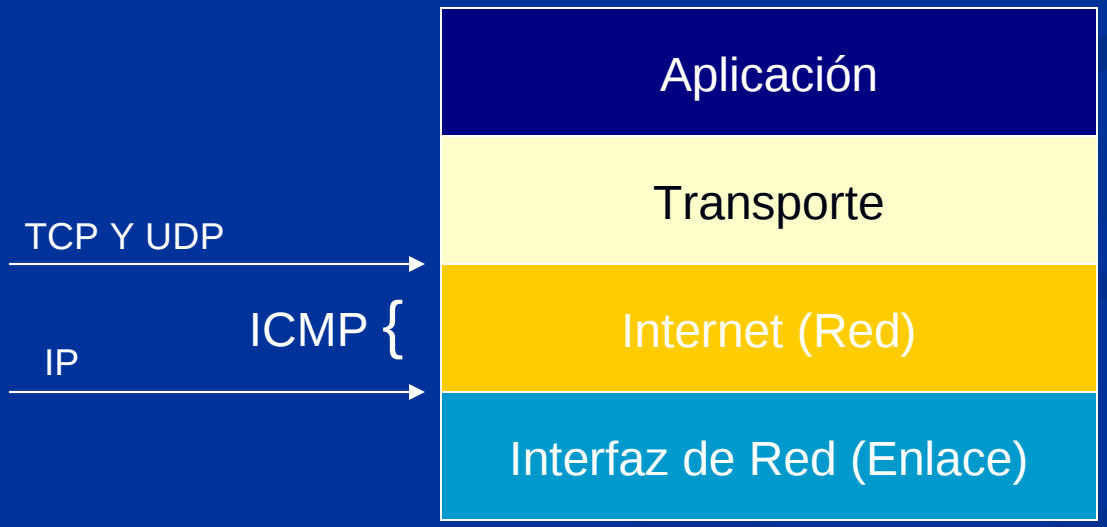


Teoría del ICMP

Orígenes y Utilización

Internet Control Message Protocol

- Fue concebido originalmente como un mecanismo de reportar condiciones de error y el envío y recepción de solicitudes simples.
- No utiliza puertos y va encapsulado en el Datagrama IP.



Teoría del ICMP

Funcionamiento

Teoría del ICMP

Actividad Maliciosa - Smurf

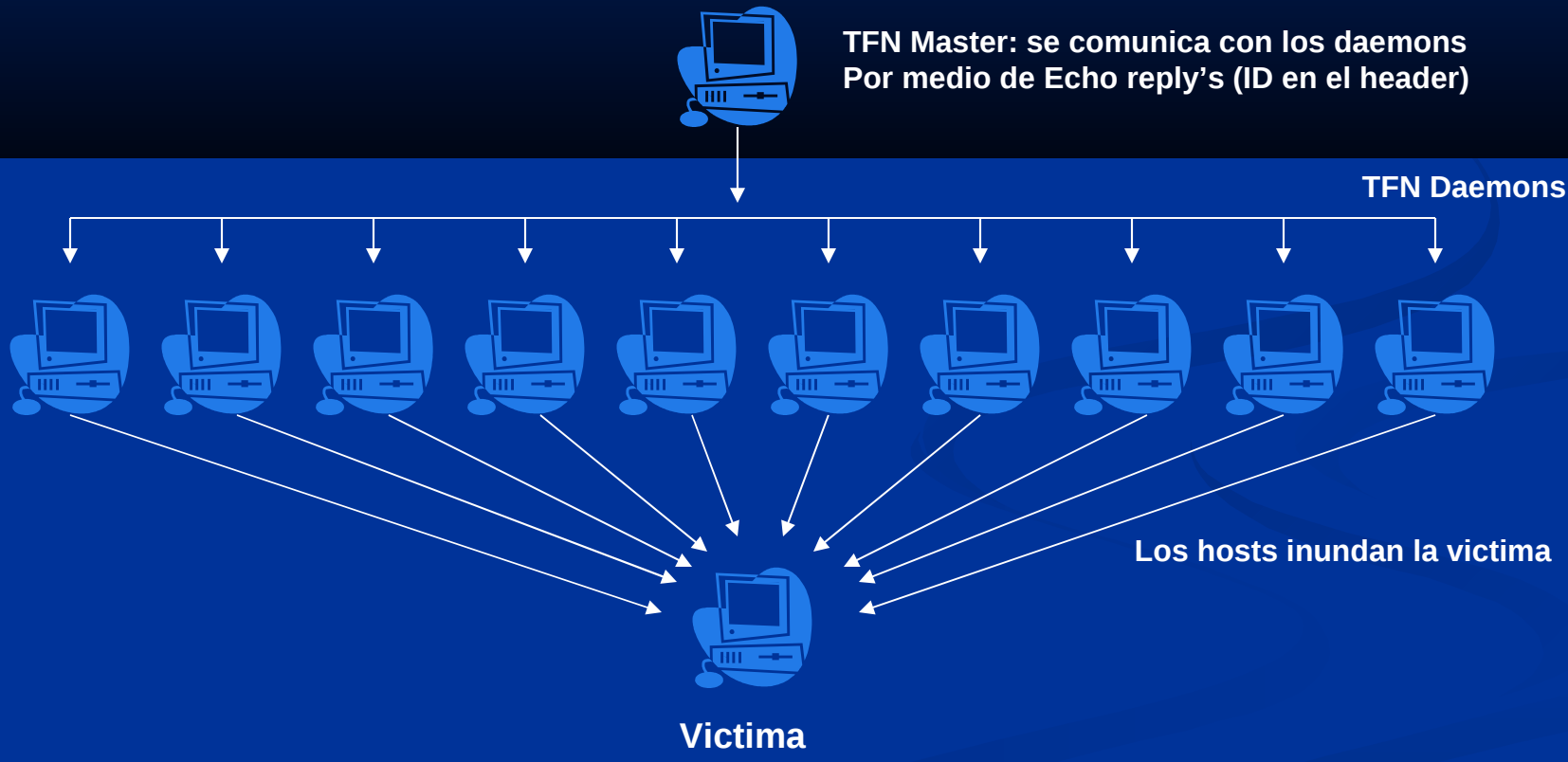
Paso 1: Se envía un Echo request a una dirección Broadcast con dirección fuente falsa de victima.com

Paso 2: El enrutador permite trafico ICMP Echo Request a direcciones broadcast.

Paso 3: Todos los host responden con un Echo Reply a la direccion fuente real del mensaje.

Teoría del ICMP

Actividad Maliciosa – Tribe Flood Network (TFN)



Teoría de DNS

Domain Name Service

- Presta el servicio de conversión de nombres direcciones IP y viceversa
- Son probablemente el objetivo de la mayoría de ataques e intentos de Vulneración

Porque?

- Pueden proveer muchísima información sobre las maquinas de la red y ayudar a preparar ataques bien planeados

- Al ser vulnerados, pueden permitir la manipulación y redireccionamiento del trafico hacia otras redes

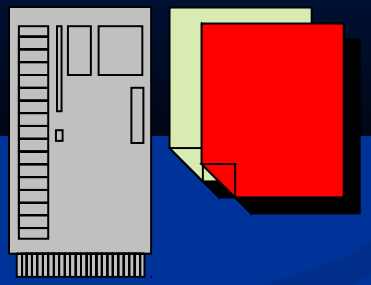
Teoría de DNS

DNS Poisoning

www.sitio1.com?

200.30.20.20

200.10.10.20

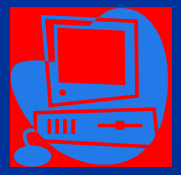


Servidor DNS

200.30.20.20

www.sitio1.com

200.10.10.20

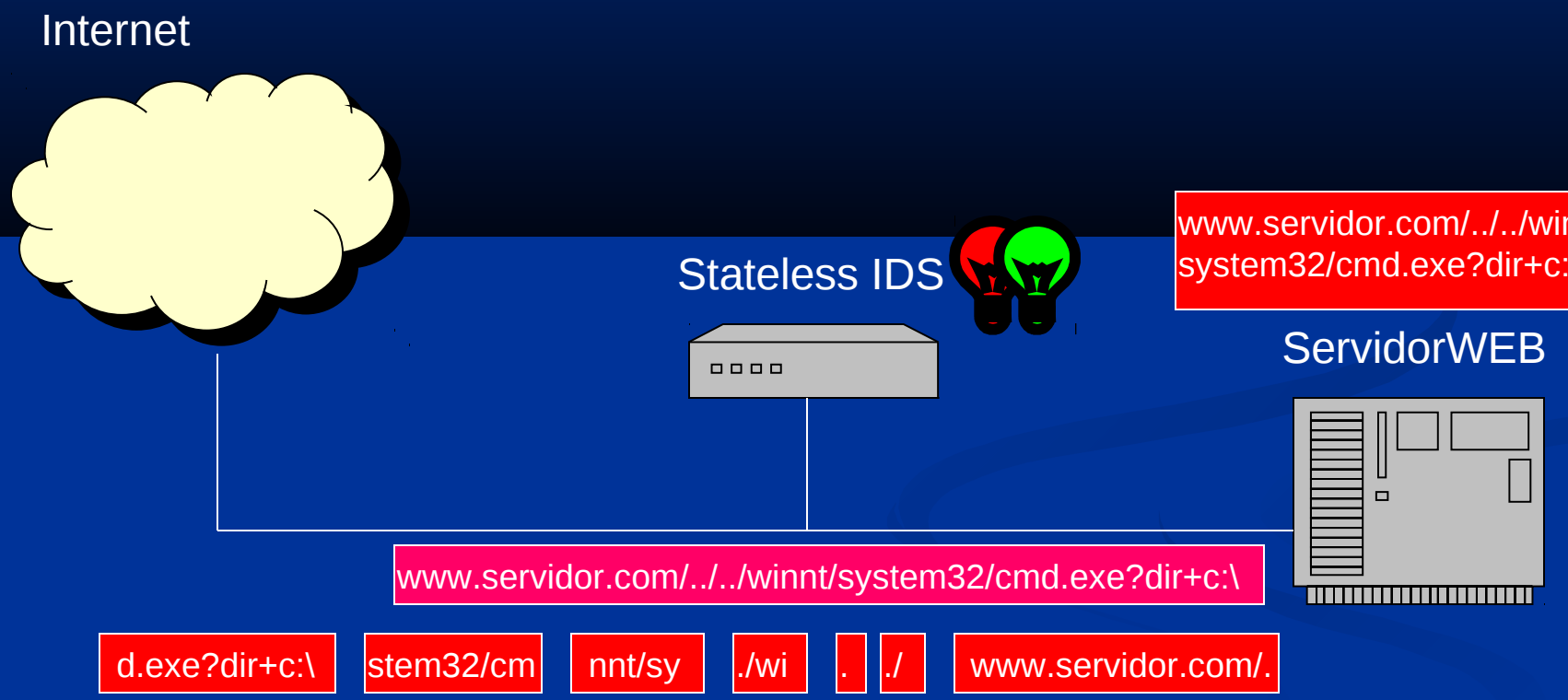


www.sitio2.com

Teoría de Fragmentación

- La fragmentación es necesaria para que los paquetes de datos puedan viajar de una red de ciertas características a otras.
- Aumentan la eficiencia en las transmisiones de datos, permitiendo adaptar los tamaños de los paquetes a las características de las redes por las que viajan.
- La fragmentación es utilizada para saltar los sistemas de detección de Intrusos que no “memorizan” el estado de las conexiones.

Teoría de Fragmentación



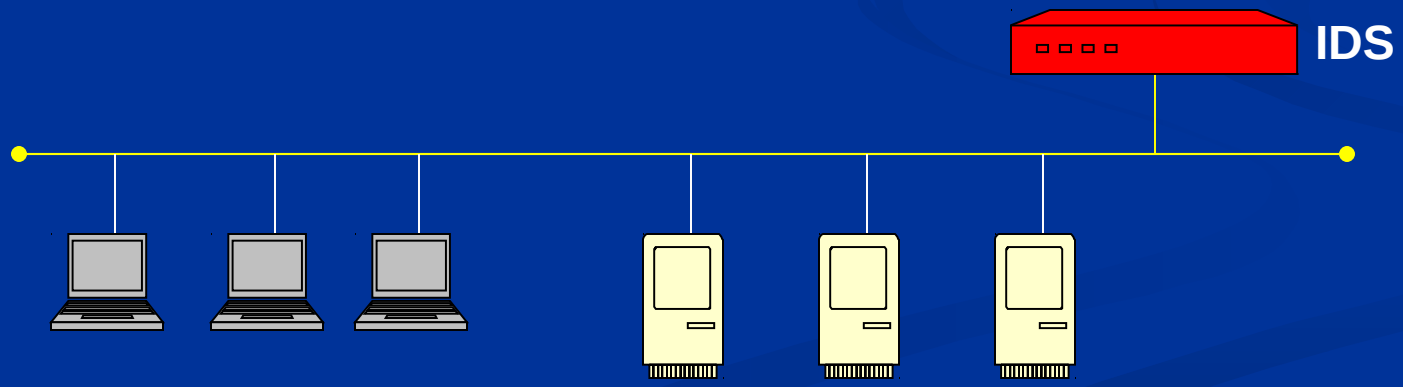
Implementación y Administración de IDS

Arquitectura de IDS

Básicamente existen dos tipos de detectores de Intrusos:

IDS basado en red

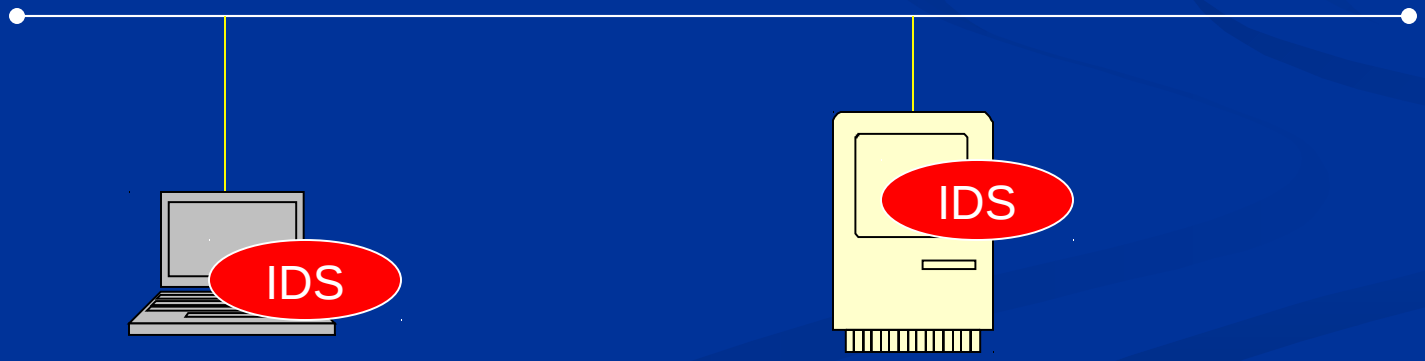
Un IDS basado en red monitorea los paquetes que circulan por nuestra red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el trafico (como un HUB o un enrutador). Este donde este, monitorizara diversas maquinas y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en host.



Arquitectura de IDS

IDS basado en maquina

Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión, los basados en maquina realizan su función protegiendo un único sistema; de una forma similar a como actúa un escudo antivirus residente en el sistema operativo, el IDS es un proceso que trabaja en background (o que despierta periódicamente) buscando patrones que puedan denotar un intento de intrusión o mala utilización y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado.



Filtros y Patrones

IDS

Filtros
Descartan paquetes de información que cumplen con ciertos criterios como IP fuente, protocolo, puerto, etc

Patrones
Comparan la información de los paquetes y los datos mismos para tomar acciones correctivas como desconexión, e-mail, almacenamiento en logs, etc.

Filtros y Patrones

Ejemplo de filtro:

Dirección IP	200.20.10.10
Mascara	255.255.255.0
Protocolo	TCP
Puerto	80, 443, 25, 23

Ejemplo de Patrón:

Dirección IP	cualquiera
Mascara	cualquiera
Protocolo	TCP
Puerto	80
Patrón	“cmd.exe”
Acción	Desconexión, e-mail (ids@miempresa.com), log

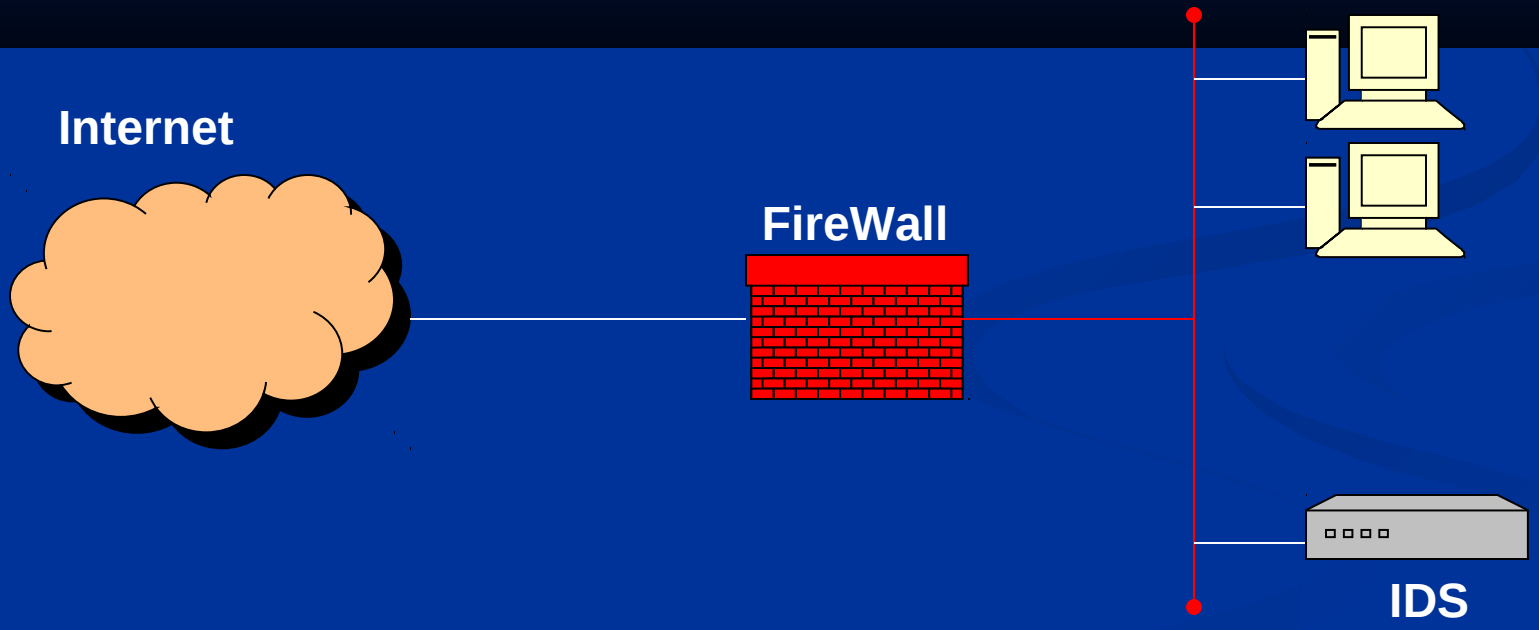
Interoperabilidad y correlación

La **interoperabilidad**, permite que un sistema IDS pueda compartir u obtener información de otros sistemas como Firewalls, Enrutadores y Switches, lo que permite reconfigurar las características de la red de acuerdo a los eventos que se generan. También permite que se utilicen protocolos como SNMP (Simple Network Management Protocol) para enviar notificaciones y alertas a otras maquinas de la red.

La **correlación** es una nueva característica que añade a los IDS la capacidad de establecer relaciones lógicas entre eventos diferentes e independientes, lo que permite manejar eventos de seguridad complejos que individualmente no son muy significativos, pero que analizados como un todo pueden representar un riesgo alto en la seguridad del sistema.

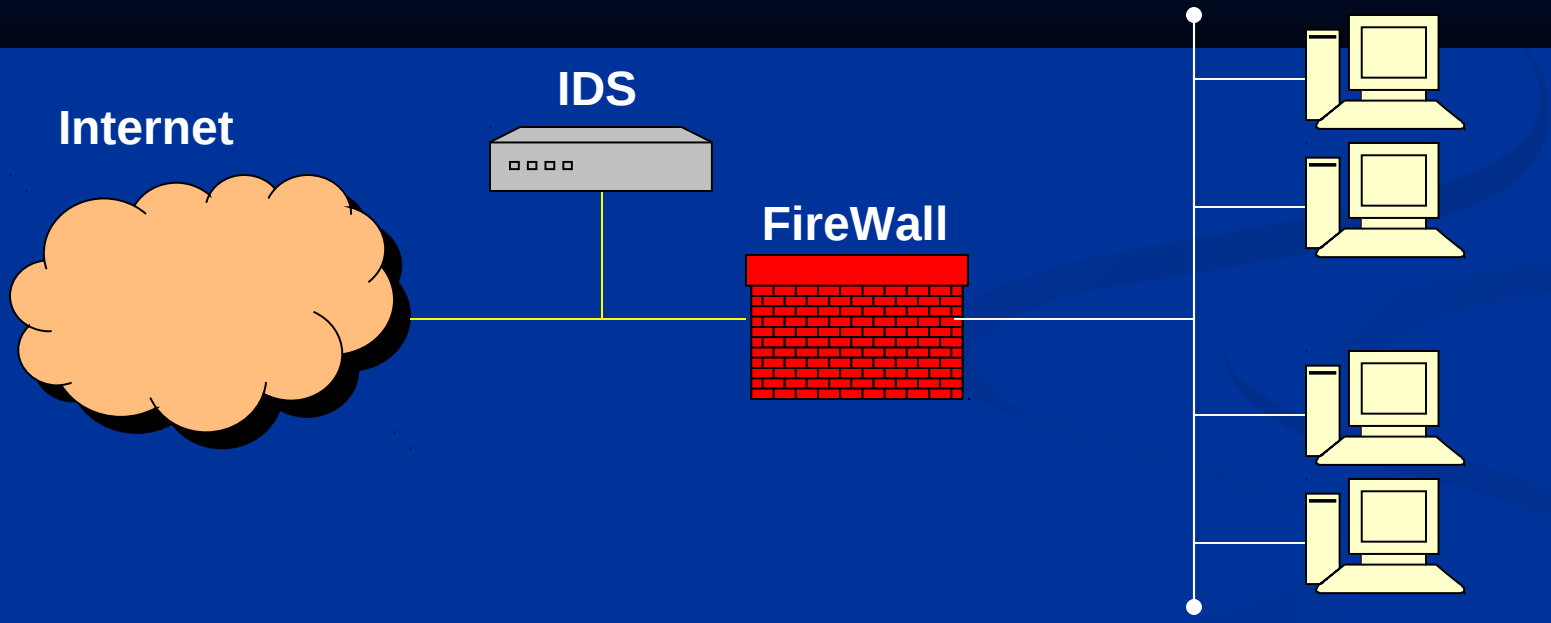
Escenarios de monitoreo de Seguridad

Sensor por dentro del FireWall



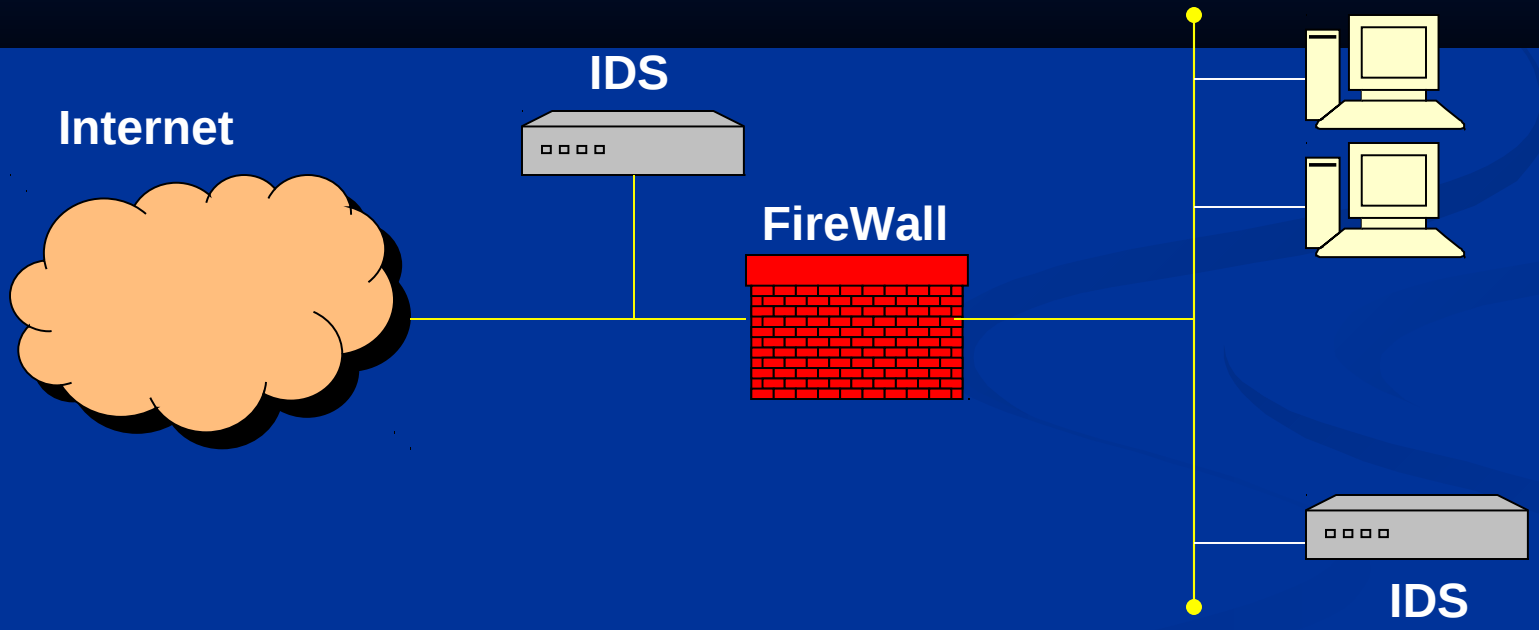
Escenarios de monitoreo de Seguridad

Sensor por fuera del FireWall



Escenarios de monitoreo de Seguridad

Sistemas híbridos



Reacción automática o manual

nismos de reacción automática:

rado de puertos y servicios en recursos perimetrales
lizar FireWalls internos para proteger redes internas
lizar IDS de maquina en los servidores críticos
moras en respuestas a escaneos de puertos en el FireWall
sechar conexiones por medio de IDS de red
oquear temporalmente todo el trafico de direcciones hostiles
lamiento automático de los dispositivos (apagado)
nulación de respuesta de puertos no abiertos en las maquina
plementación de Honeypots

Reacción automática o manual

cedimientos de reacción manual:

eparación
- Recursos disponibles

entificación
- Herramientas y personas calificadas

ntención
- Congelar la escena física del incidente
- Transporte al sitio del incidente
- Forensica del sistema

radicación
- Herramientas y reinstalación de sistema si es necesario

cuperación
- Utilización de respaldos y copias de seguridad

render de las lecciones aprendidas en el incidente
- Llevar registro detallado de todos los incidentes y los procedimientos

Tendencias y proyección de IDSs

lidad:
os ataques están incrementando
as herramientas son cada día mas sofisticadas
yber-Terrorismo
tacantes Internos

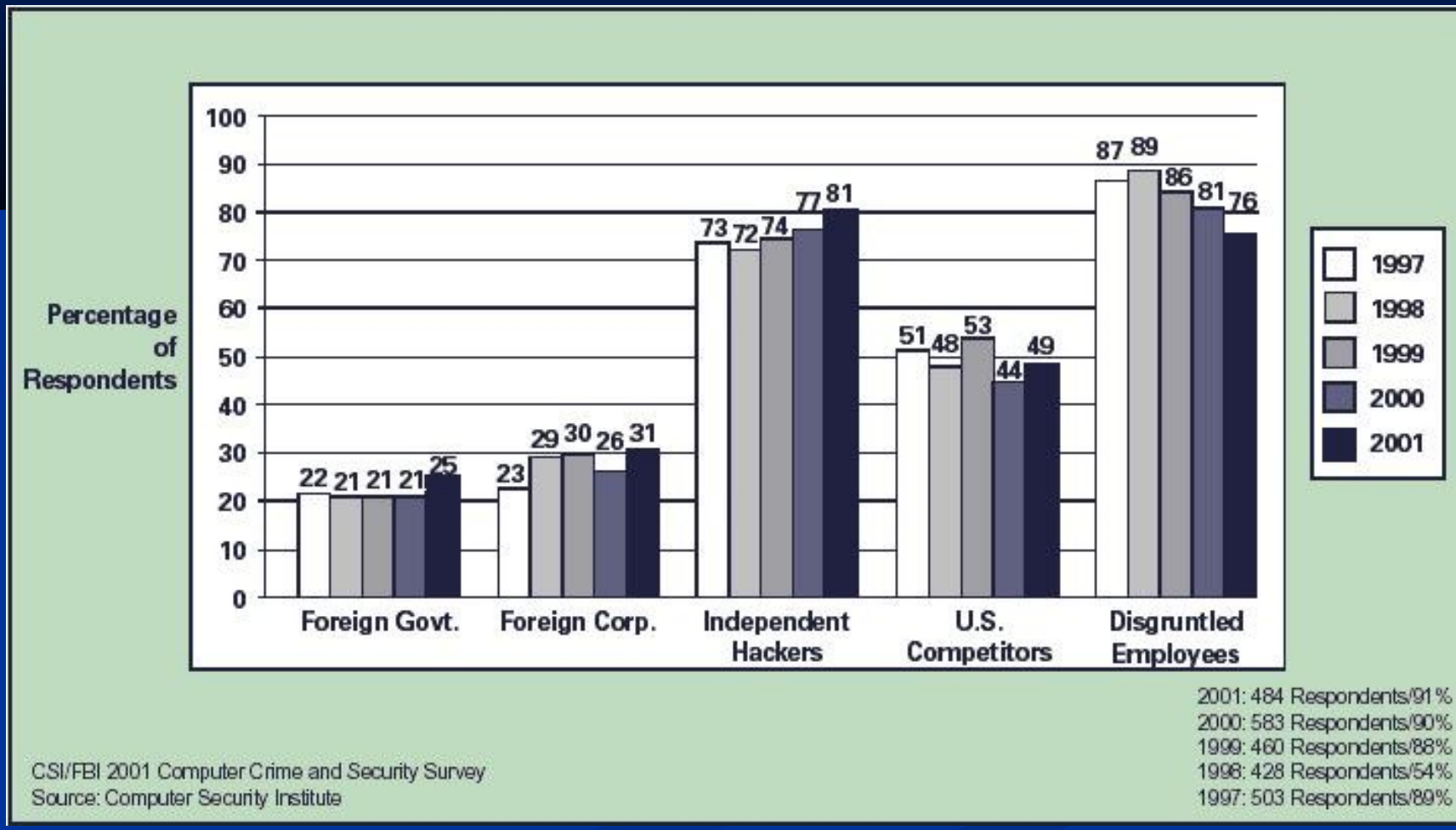
uciones a futuro:
tegración de Antivirus con IDSs y FireWalls
esencripcion del trafico encriptado para análisis de Seguridad
orrelación de eventos entre diferentes dispositivos en la red
etección de intrusos a nivel de aplicativo, como por ejemplo software de
ersonal mas calificado en temas de seguridad informática

Factores Organizacionales

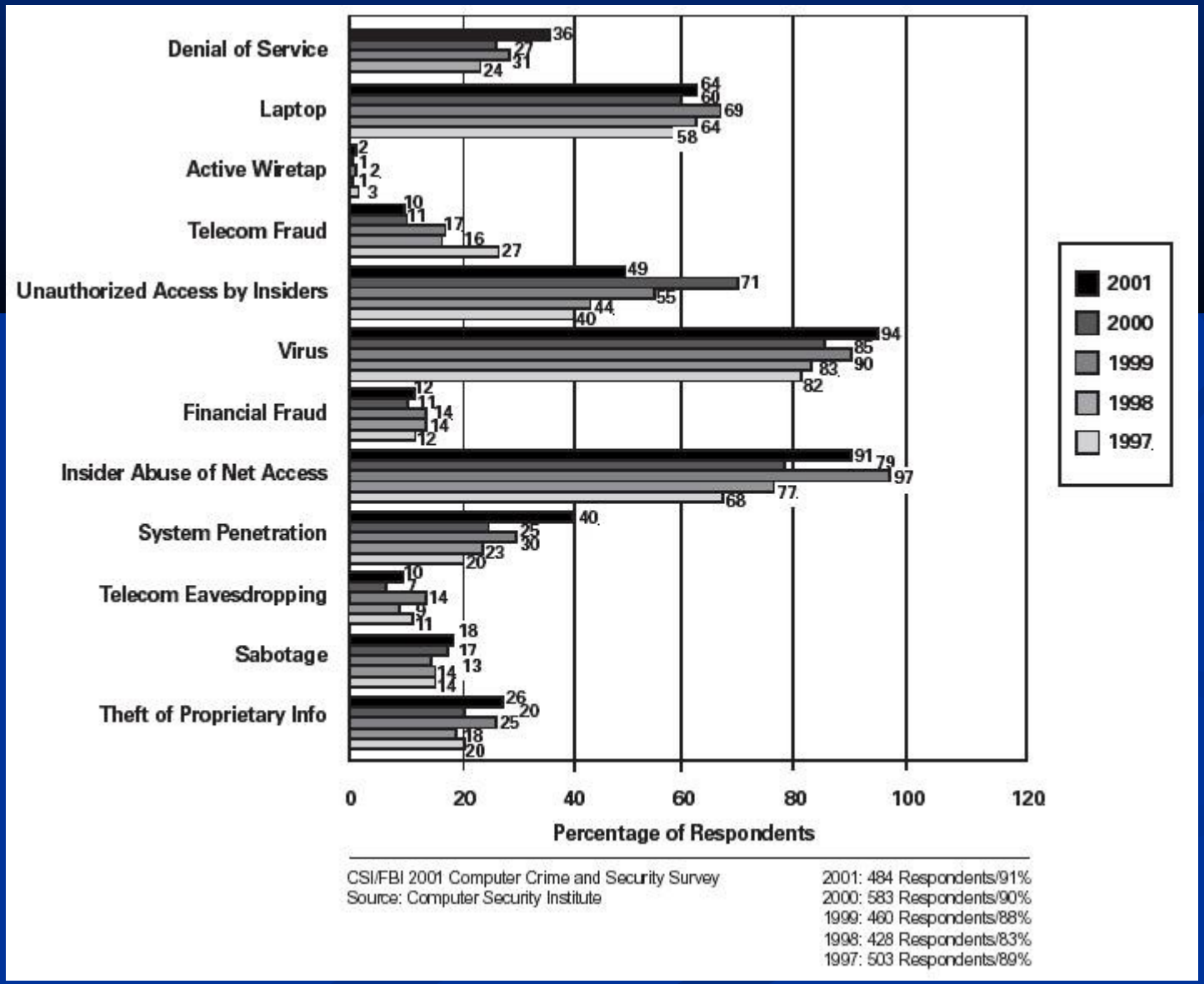
Factores Gerenciales

- POLITICA DE SEGURIDAD CORPORATIVA
- SEGUIR LAS MEJORES PRACTICAS DE LA INDUSTRIA
- CONTAR CON INFRAESTRUCTURA PARA SEGURIDAD
- IMPLEMENTAR CONTRAMEDIDAS SEGÚN LA PRIORIDAD
- REALIZAR REVISIONES PERIODICAS DEL ESTADO DE LA SEGURIDAD
- IMPLEMENTAR MECANISMOS DE REACCION ANTE INCIDENTES
- DEFINIR EL NIVEL DE RIESGO
- REDUCIR GRADUALMENTE EL NIVEL DE RIESGO
- DEFINIR LAS AMENAZAS Y SU IMPACTO (MATRIZ DE RIESGO)
- JUSTIFICAR LA INVERSION DE SEGURIDAD EN TERMINOS DE REDUCCION DE TARIFAS DE POLIZAS DE SEGUROS Y SERVICIOS RELACIONADOS

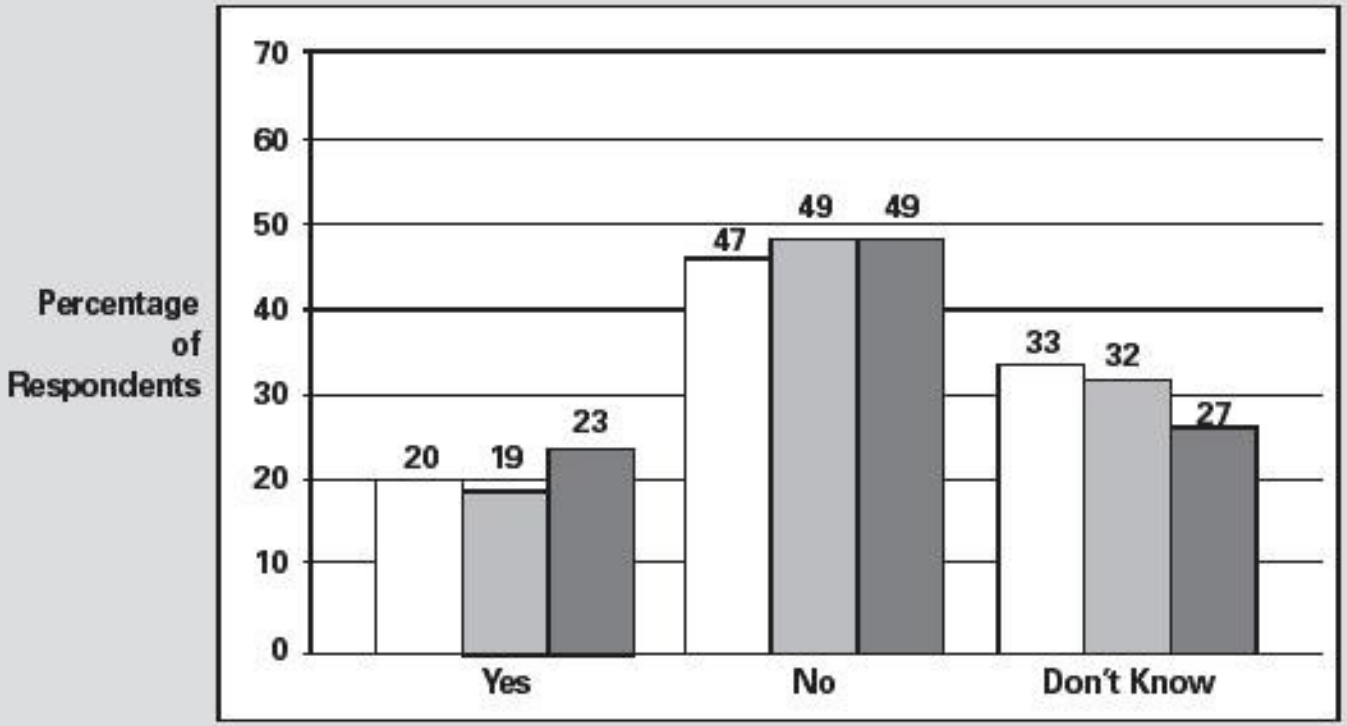
Amenazas y Vulnerabilidades



Amenazas y Vulnerabilidades



Amenazas y Vulnerabilidades



97% of respondents have WWW sites, 47% provide electronic commerce services via their WWW sites; only 43% were doing e-commerce in 2000.

1999
2000
2001

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 509 Respondents/95%
2000: 603 Respondents/93%
1999: 479 Respondents/92%

Actividades relacionadas con Implementación

- Definición de los recursos a proteger
- Análisis de la infraestructura de red
- Análisis especial para ambientes switcheados
- Análisis de estructura y disposición de FireWalls
- Sistemas Operativos a proteger
- Características geográficas
- Definición de los procedimientos de reacción
- Seguridad física y control de acceso a los recursos
- Definición de herramientas para pruebas de seguridad internas y externas
- Capacitación del personal en la utilización de las herramientas y en Seguridad en General