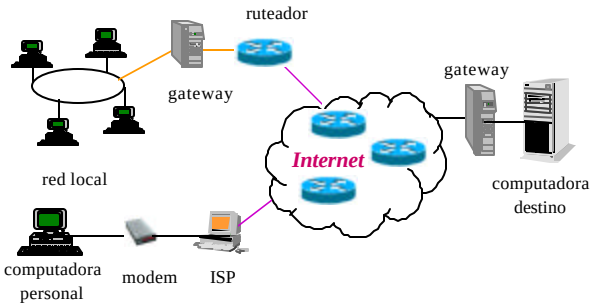
12a. Reunión de Otoño de Comunicaciones, Computación Electrónica y Exposición Industrial

Seguridad en Redes

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@campus.cem.itesm.mx
http://webdia.cem.itesm.mx/dia/ac/rogomez
(conferencias)

Antecedentes

- Las redes fueron diseñadas para el intercambio de información y compartir recursos.
- La seguridad no era un factor tomado en cuenta en el diseño de las redes.



Protocolos y sistemas operativos

- TCP/IP, Netbios, HTTP, SMTP, FTP
- Unix / Windows / NT
- No fueron pensados para ser seguros.
- Ni siquiera podemos contar con que sean correctos.
  - las implementaciones son diferentes

Haciendo cuentas ...

- Computación electrónica 50 años !
- Redes sólo tienen 30 años de vida !
- Seguridad 23 años !
- Internet 15 años !
- Web 6 años !
- Intranets 3 años...
- Extranets 2 años...

Algunos Ataques

- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Fuerza bruta
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio
- Hijacking (secuestro)

Ejemplo ataque negación servicio

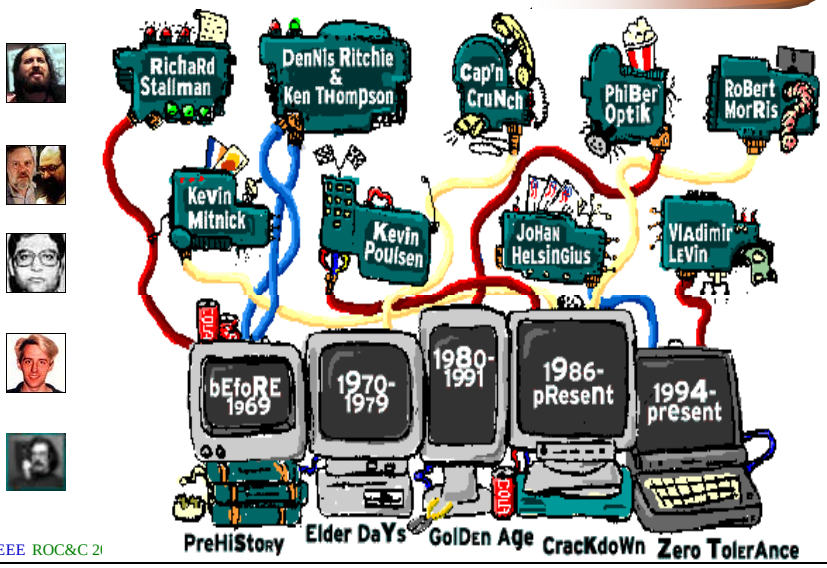
Hackers

Crackers

Script Kidies

Phreakers

¿Quien me ataca?



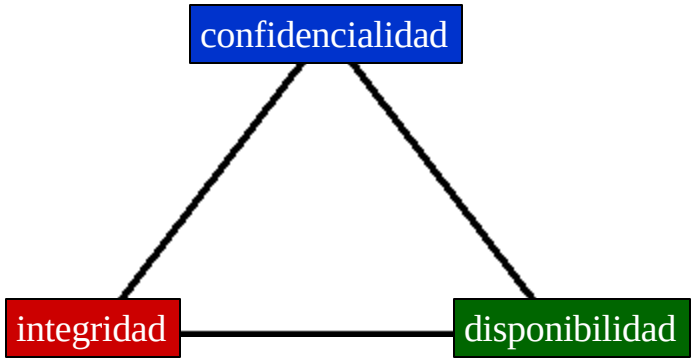




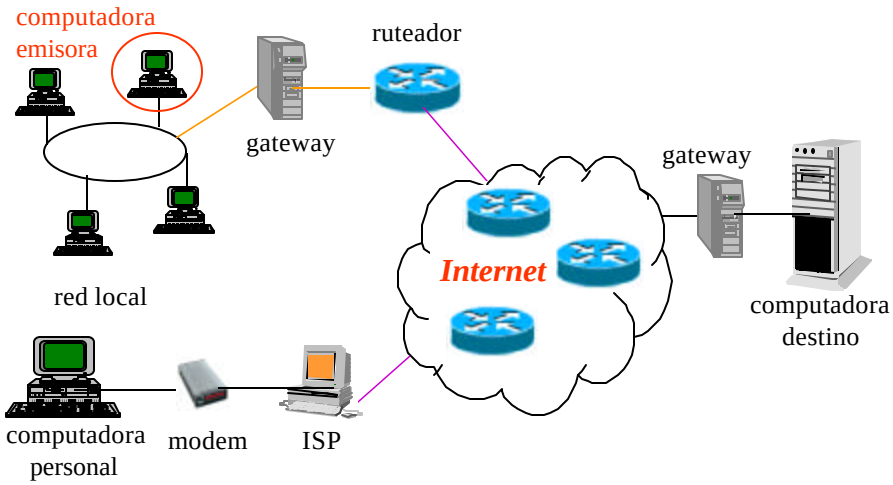
La seguridad computacional

- Conjunto de políticas y mecanismos que nos permiten garantizar la ***confidencialidad***, la ***integridad*** y la ***disponibilidad*** de los recursos de un sistema.

Elementos seguridad computacional



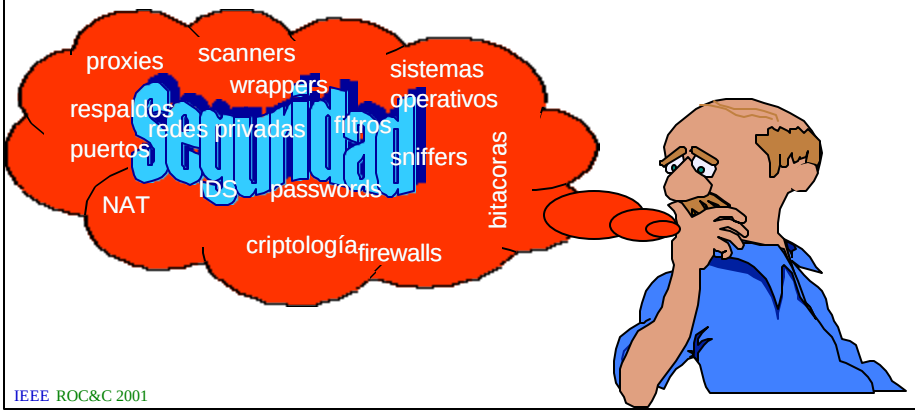
Comunicando dos computadoras



El principio básico

Protegiendo las redes

- Son varios aspectoa a tomar en cuenta
- No es una sola herramienta



Passwords

- Es el primer paso a probar dentro de un ataque.
- Para Ripley:
  - hay que decirle a algunas gentes que pongan passwords en sus equipis
- Existen diferentes reglas para passwords
  - El 7 de julio, se compro la máquina

Password: E7dj,sclm

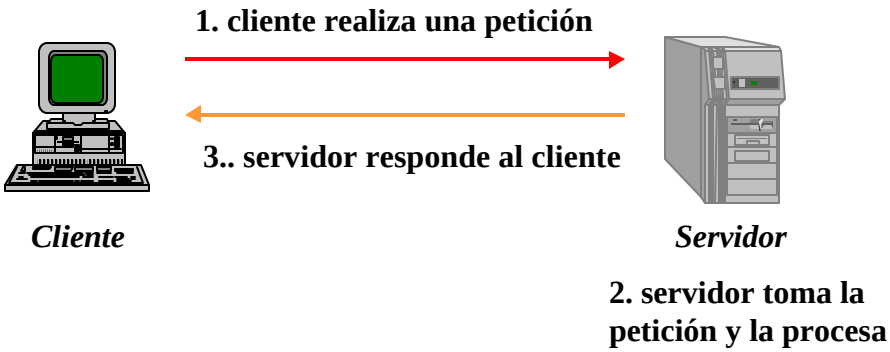
Filtros

- Examinar los paquetes que van hacia afuera o vienen entrando a la red.
- Se definen reglas que permiten dejar pasar el paquete o descartarlo.
- Las reglas se fijan en función de las direcciones, protocolos y puertos, básicamente.
- Programación del ruteador para filtrar paquetes.
- Ejemplos: IPFilter, Iptables, netfilter, ipchains e ipfwadm

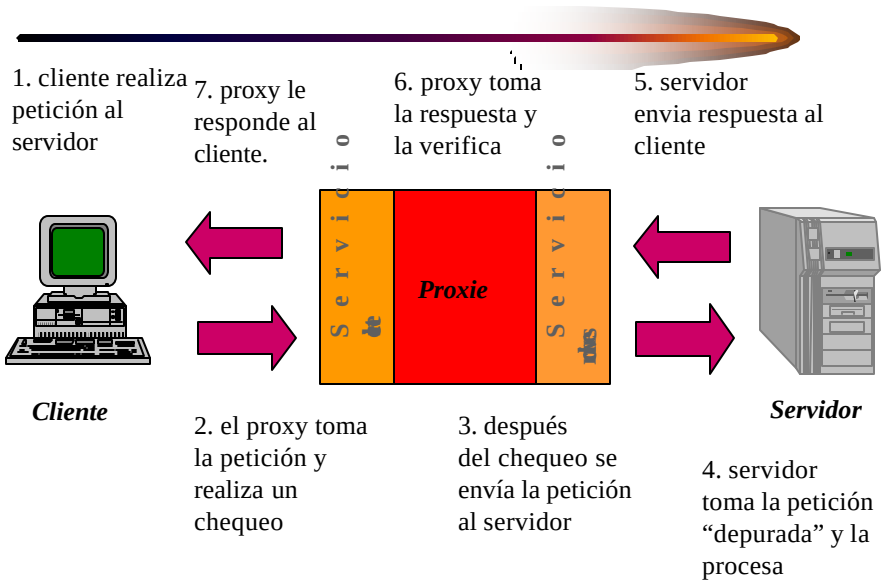
Los proxies

- Es un intermediarios entre cliente y servidor.
- Un servidor proxy realiza una conexión con un servidor de alguna aplicación, de la parte de un cliente.
- Desde el punto de vista del cliente, hace la conexión con el proxy, pensando que ésta es con el servidor.

Esquema cliente/servidor

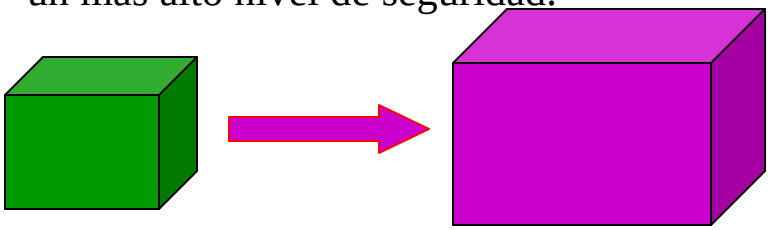


Cliente/servidor con proxy



Los wrappers

- Un programa para controlar el acceso a un segundo programa.
- El wrapper literalmente cubre la identidad del segundo programa, obteniendo con esto un más alto nivel de seguridad.



¿Por qué es útil?

- La lógica de la seguridad esta encapsulada en un sólo programa, los wrappers son fáciles de validar
- Es una unidad independiente se puede actualizar sin tocar el programa de aplicación
- Un solo wrapper puede controlar diferentes aplicaciones

Proxies vs Wrappers

- Proxie funciona como gestor o intermediario entre clientes y servidores.
  - permite que los clientes de la red se vean al exterior como una sola dirección IP
  - se convierte en un solo punto de control (y de fallas)

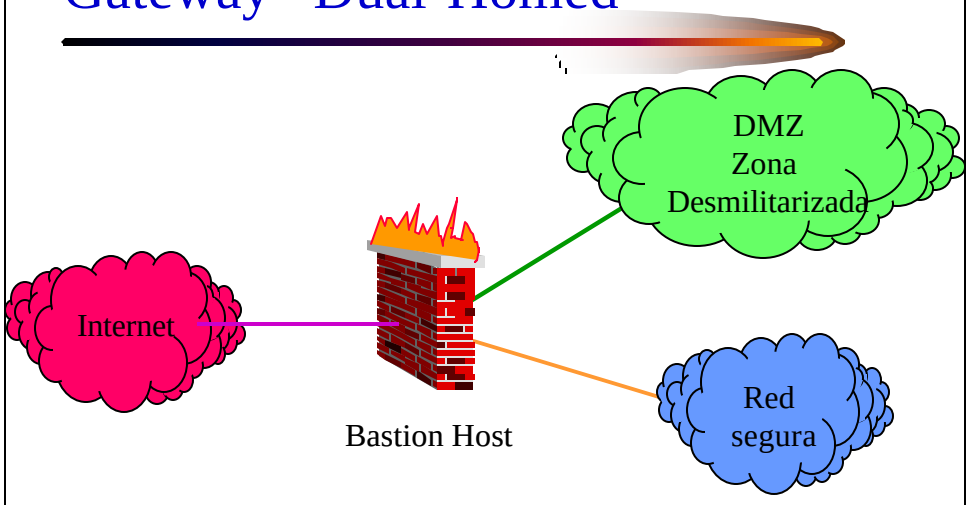
Proxies vs Wrappers

- Wrappers es un programa de envoltura para proteger un servicio
  - cuando se tienen un servicio que no es open-source y la respuesta del proveedor es lenta, se utlizan scripts para efectuar una asepsia de parametros (i.e. las validacines que el servicio original no prevee) o alguna otra operación que requiera la modificación del código fuente no disponible
    - p.e. añadir autenticación basada en biométricos para acceder pop3

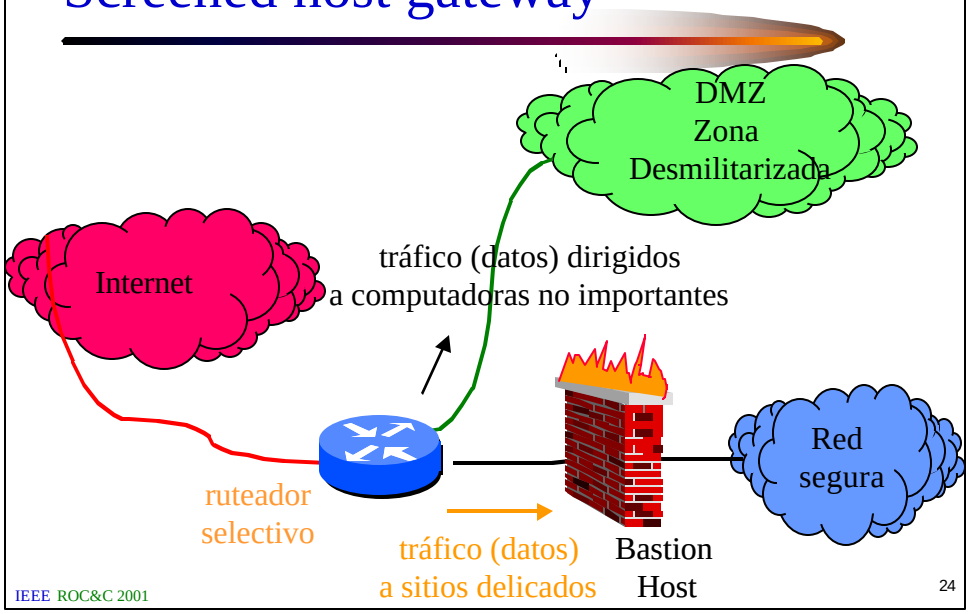
Firewalls

- Colección de componentes colocados entre dos redes, que en conjunto poseen las siguientes propiedades:
  - todo el tráfico de afuera hacia adentro, y viceversa, debe pasar por el firewall.
  - sólo tráfico autorizado, como establecido previamente en las políticas de la organización, puede pasar a través del firewall.

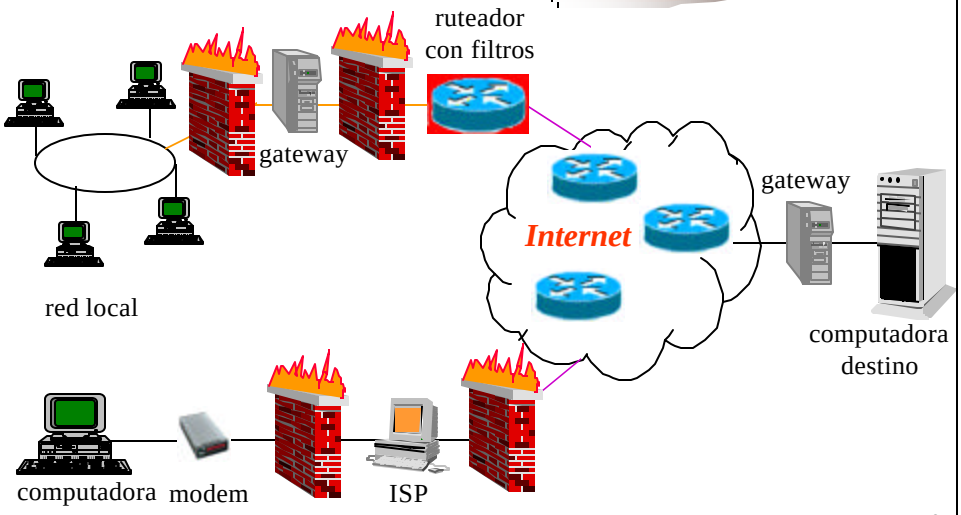
Gateway “Dual-Homed”



Screened host gateway



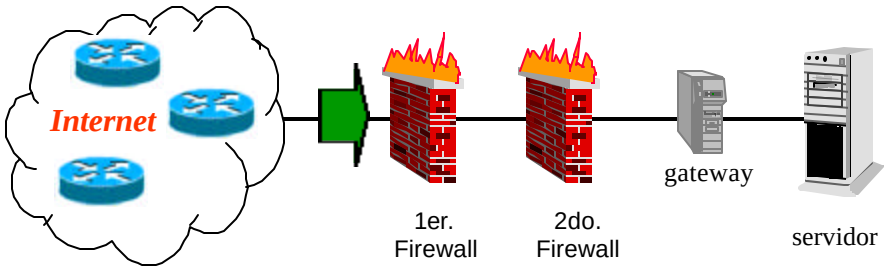
Integrando el firewall



Desventajas de los firewalls

- No adaptados a nuevos productos.
- Cuello de botella.
- Todos los huevos en la misma canasta.
- No nos proteje contra ataques internos.
- Es posible conocer la política de seguridad de la organización con una herramienta de ingeniería inversa
- Configuración
  - continuan los problemas de seguridad y no se puede hacer que lo antes se podía.

¿Y si uso dos firewalls?



Conexiones remotas

- Es necesario conectarnos al servidor para cambiar la configuración?
  - la idea que se nos ocurrión a las 0:45 de la noche, ¿tiene que ser implementada en ese momento?
- ¿Es necesaria la administración remota?
- Si lo anterior es necesario utilizar un protocolo "seguro" de comunicación
  - SSH
  - SSL

Por cierto, ¿a quien voy dejar conectarse remotamente?
Restringir la conexión

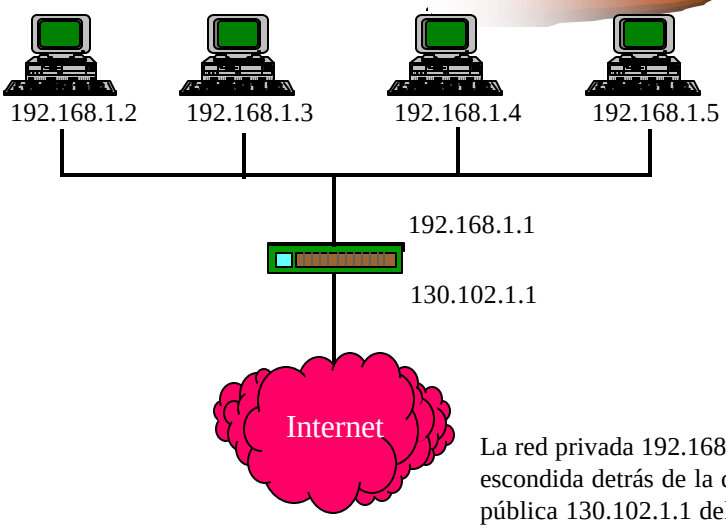
El protocolo DHCP

- Es fácil caminar en una oficina, encontrar la impresora, desconectarla y conectar una laptop en su lugar.
- DHCP se siente feliz proporcionando direcciones a un intruso
  - si es que el intruso no la obtiene a través de un sniffer
- Algunas herramientas nos permiten asegurar los puertos y prevenir que un hardware no-autorizado se conecte.

NAT: Network Address Translation

- Traducción de direcciones de red.
- Usos:
  - compartir una conexión internet (p.e. ISP)
  - expandir la red existente sin afectar los esquemas de IP existentes
  - reducir el requerimiento de direcciones publicamente asignadas
  - esconder un esquema de red interna de redes públicas

Ejemplo esquema NAT



La red privada 192.168.1.0 esta escondida detrás de la dirección pública 130.102.1.1 del ruteador NAT.

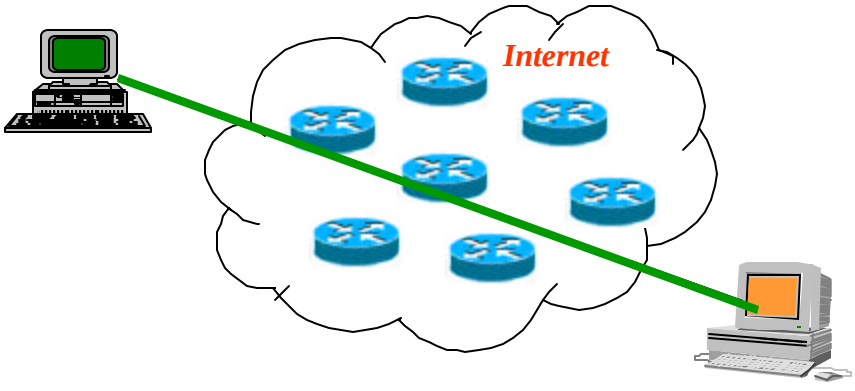
Servicios Internet

- ¿Es necesario tener todos los servicios activos?
  - conexión remota (telnet, 23)
  - transferencia de archivos (ftp, 21)
  - correo electrónico (smtp, 25)
  - página web (http, 80)
- Se tienen que cerrar los puertos de los servicios que no se usan
  - ¿óomo? depende del sistema operativo
  - herramientas permiten verificar puertos abiertos

Las VPNs

- Privacidad entre dos máquinas
  - comprar una línea dedicada ($$$)
  - utilizar el medio que se tiene (compartido con otros)
- Una VPN es una red privada virtual que actua sobre una ruta insegura.
  - ruta insegura: internet
- Tambien puede ser usada para definir diferentes intranets dentro de una internet
  - que pasa si dentro de un organismo se tienen grupos que no desean que la información de uno la vea otra

Esquema VPN



Problemas VPNs

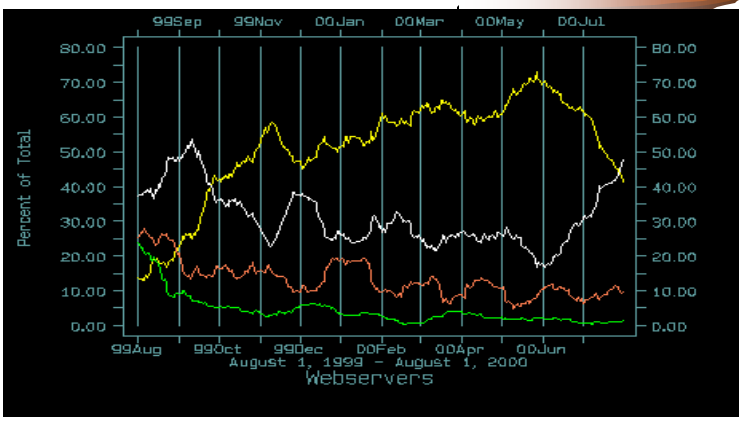
- Si no esta bien diseñada, una VPN puede representar un medio de entrar al sistema sin ser detectado.
- Un tunel encriptado no es una VPN
  - no tiene los elementos criptográficos para prevenir inyección de paquetes
  - los firewalls dejan pasar paquetes encriptados
  - un IDS no entiende de información encriptada

¿han oido hablar de inyección de paquetes?

¿Y los Sistemas Operativos?

- Redes funcionan sobre un sistema operativo.
- Ninguno es mejor que otro.
- Todos tienen sus ventajas y desventajas.
- El mercado utiliza principalmente dos: Unix y Windows NT.
- El sistema operativo es tan seguro como preparado este administrador y tan inseguro como deficiente sea el administrador.

Unix vs NT (ataques a Webservers)



Amarillo: NT, Blanco: Linux, Naramja: BSD, Solaris, Verde: tosdos los demás

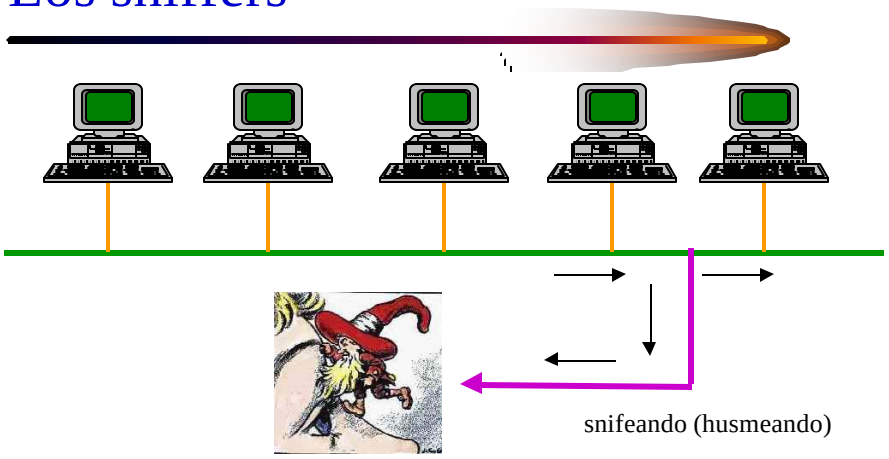
consejo tomar precauciones en instakación una nueva version de S.O.

Fuente: Attrition

El monitoreo de seguridad

- Se recomienda contar con herramientas que nos permitan ver que es lo que pasa en la red.
- Existen diferentes herramientas para eso
  - herramientas que toman una instantanea del sistema y buscan debilidades potenciales.
  - herramientas que monitorean el sistema periódicamente buscando cambios no autorizados.
  - herramientas que escudriñan la red buscando debilidades basadas en ella.
  - herramientas que monitorean el sistema y la red buscanco identificar ataques en proceso.

Los sniffers



computadora en
modo promiscuo

snifeando (husmeando)

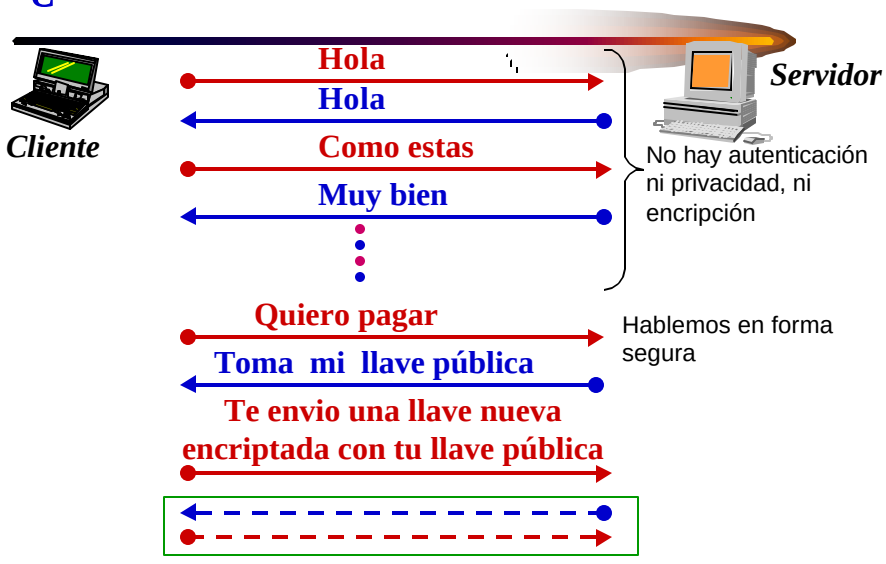
Previniendo sniffers

- Sniffers son difíciles de detectar y combatir ya que son programas pasivos.
- No generan bitacoras.
- Cuando se usan propiamente, no usan mucho disco ni memoria.
- Es posible localizarlos a nivel local
- A nivel red, algunos pueden localizarse mediante herramientas;
  - NEPED: Network Promiscous Ethernet Detector
  - Antisniff

Canales privados comunicación

- Protocolos criptográfico de propósito general para asegurar canales de comunicación bidireccionales
- Se utilizan comúnmente junto con el protocolo TCP/IP
- Sistema encripción usado por navegadores Netscape e Internet Explorer
- Basados en combinación de llaves asimétricas y simétricas

¿Cómo funciona?



Algunos protocolos

- S-HTTP.
- Ipsec e IPv6.
- SSH.
- PCT
- TCL
- SSL
- S/Key.

Cuidando integridad sistema

- Punto crítico: preservar un snapshot del sistema inmediatamente después de la instalación.
  - responder pregunta: ¿las cosas estan de la misma forma que las deje?
  - objetos pueden ser directorios, archivos, dispositivos y otros
  - necesario comparar estos objetos contra algún dato previo

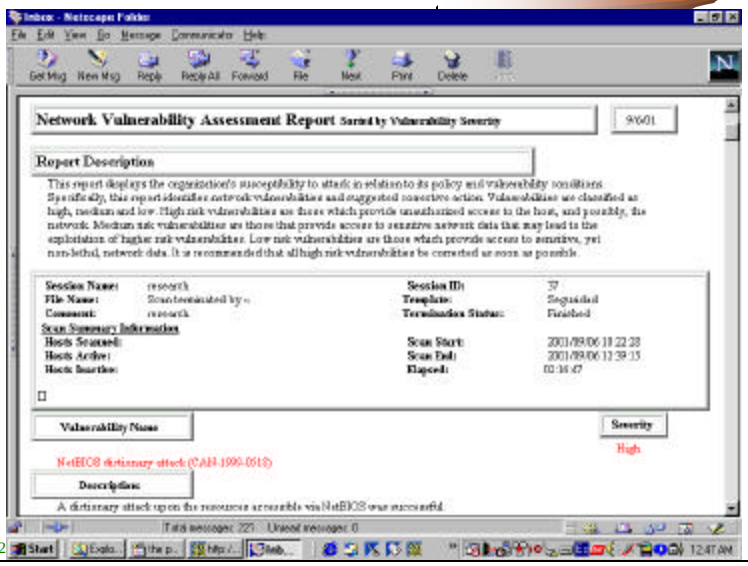
Comparando datos

- Es posible generar un checklist de todos los archivos y examinarlos despues para verificar cambios en:
  - la ultima fecha de modificacion
  - la fecha de creación
  - su tamaño
- Otro enfoque es utilizar checksums
- Utilizar herramientas más generales
  - tripwire

Scanners de vulnerabilidades

- Son herramientas para ayudar a los administradores a auditar sus redes para valorar y/o incrementar el nivel de seguridad
- La mayoría de las herramientas de seguridad disponibles hoy en dia se desarrollaron en universidades o las crearon especialistas independientes

Ejemplo scanner



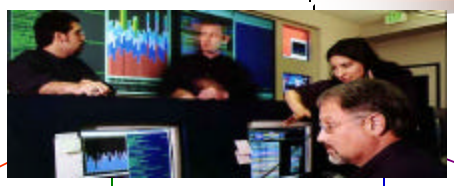
Scanners de Vulnerabilidades

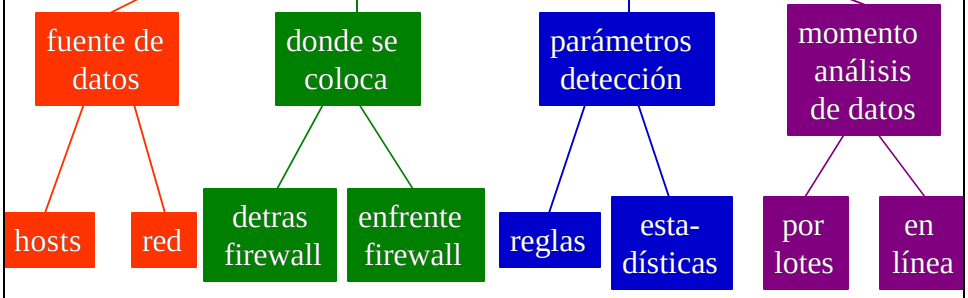
- COPS
- SATAN
- SAINT
- Nessus
- Whisker
- ISS Internet Security Scanner
- Cybercop
- SARA
- NAT
- Vetescan
- Retina
- Cerberus Internet Scanner

IDS

- Intrusion Detection Systems.
- Busca automatizar la detección y eliminación de intrusos.
- Asumen que un intruso puede detectarse examinando varios parámetros como:
  - -tráfico de la red, -ubicación del usuario,
  - -uso de CPU y E/S, -diferentes actividades usuario

Tipos IDS





Ejemplo IDS: snort

[**] IDS249/smtp-relay-denied [**]
09/10-12:13:49.774333 184.235.168.50:25 -> 184.241.75.146:2458
TCP TTL:237 TOS:0x0 ID:6164 IpLen:20 DgmLen:125
AP Seq: 0x371DC6E6 Ack: 0x10CDB3D Win: 0x8218 TcpLen: 32
TCP Options (3) => NOP NOP TS: 9281425 156264

[**] IDS249/smtp-relay-denied [**]
09/10-12:16:04.704333 184.235.168.50:25 -> 184.241.75.146:2469
TCP TTL:237 TOS:0x0 ID:40468 IpLen:20 DgmLen:125
AP Seq: 0x3F2D3061 Ack: 0x10EF83B Win: 0x8218 TcpLen: 32
TCP Options (3) => NOP NOP TS: 9310686 157498

[**] IDS28/probe-nmap_tcp_ping [**]
09/10-12:44:02.724333 200.23.241.13:80 -> 184.241.91.18:21

Desventajas IDS

- Falsos positivos
  - No se detecto una instrusión, siendo que alguien intentó entrar
- Falsos negativos
  - Se dio una alarma siendo que se hizo una operación normal.

Si se cae un árbol y nadie oye (se percata que se cayó) entonces, ¿¿en realidad se cayó??

Bitácoras

- Muchos servicios permiten llevar una bitacora de sus actividades.
- Es posible configurar los sistemas de tal forma que los eventos:
  - se escriban en uno o en distintos archivos,
  - se envien a través de la red a otra computadora,
  - se transmitan a algún dipositivo

Ejemplo bitacora: logcheck

/etc/cron.weekly/2webalizerftp:

```
Webalizer V2.01-06 (Linux 2.2.19-7.0.8) English
Using logfile /var/log/xferlog (ftp)
DNS Lookup (15): Warning: Truncating oversized request field [3342]
Warning: Truncating oversized request field [3363]
Warning: Truncating oversized request field [3364]
Warning: Truncating oversized request field [3365]
Warning: Truncating oversized request field [3366]
Warning: Truncating oversized request field [3367]
Warning: Truncating oversized request field [3368]
111 addresses in 23.29 seconds, 4/sec
Using DNS cache file cachedns
Creating output in /usr/local/apache/htdocs/estadisticas/ftp
Reading history file... webalizer.hist
Generating report for February 2001
Saving history information...
10815 records (315 ignored) in 3.32 seconds, 3257/sec
```

¿Qué hacer con ellas?

- Las bitácoras del sistema reflejan lo que ocurre en el mismo.
- De nada sirve tenerlas si no son leídas.
- Ahí es donde pueden descubrirse ataques no exitosos perpetrados contra un sistema
- Es importante revisarlas periódicamente.
- Tarea tediosa, pero es posible auxiliarse a través de herramientas.

¿Y las redes inalámbricas?

- Emiten al aire,
  - alguien pueda tomar la señal y ver lo que se transmite
- La mayor parte de la configuración de las redes no ofrecen autenticación
  - basta con arrancar una computadora con una tarjeta inalambrica dentro de la covertura
  - implementar sistema autenticación en base a direccione físicas
- Protocolo RC4 ya fue roto
  - versión de 128 bits, se cree que se puede hacer lo mismo con la de 40 bits

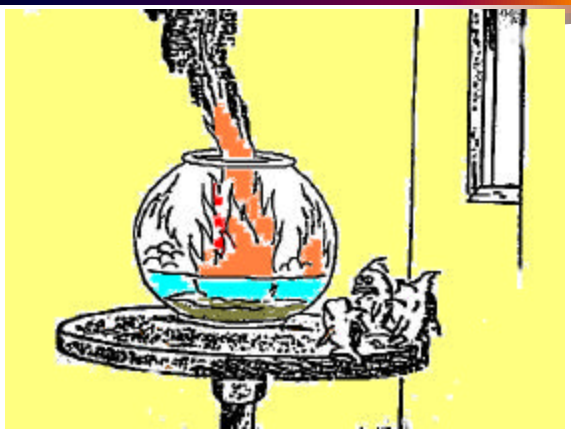
Plan de contingencia

- Acciones a tomar cuando un evento de seguridad se encuentra en progreso en una máquina, sitio o ambiente de red.
- Seguridad computacional clásica:

  evitar un ataque
- Contingencia:

  el ataque ya se presentó

¿Por qué es necesario un DRP?



Bueno, Gracias al Cielo salimos a tiempo . . . Y Ahora Qué? . . .

DRP = Disaster Recovery Plan

¿Y los respaldos?

Aspectos a considerar en un plan de contingencia

- Preservar vidas humanas.
- Notificar a las personas adecuadas
- Recuperar información.
- Preservar equipos e infraestructura.
- Cuidar la imagen de la empresa.
- Aplicar aspectos legales.
- Investigar cómo ocurrio el incidente.
- Adecuar la Política de seguridad.

Conclusiones

- El 100% de seguridad no existe.
- No hay una herramienta mágica
  - se requiere una estrategia global y usar cada herramienta para lo que fue diseñada
- El factor humano es primordial
  - capacitación y sensibilización
- El hecho de que todo funcione bien no significa que no tendremos problemas de seguridad
  - NO HAY QUE CONFIARNOS