Departamento de Tecnología Electrónica

INTRODUCCIÓN A LA SEGURIDAD EN REDES DE COMPUTADORES

Tecnologías Avanzadas de la Información

v19.2

Objetivos

- Definir la problemática de la seguridad informática.
- Definir el papel de la seguridad informática en las redes de computadoras.
- Mostrar los peligros a los que se enfrentan las redes de computadores y formas de protegernos ante ellos.
- Mostrar el concepto de seguridad perimetral y el papel juega.

Bibliografía

- Inside network perimeter security: The definitive guide to firewalls, VPNs, routers and intrusion detection systems. Stephen Northcutt. New Riders, 2005
- Unixsec 2.1. Antonio Villalón. GNU Free Documentation License 2002

Índice

- Parte I:
  - Conceptos generales de seguridad: Gestión de la seguridad, análisis de riesgo y seguridad en redes
  - Peligros amenazas y defensas: modos de ataque, atacantes y métodos de defensas
- Parte II:
  - Seguridad Perimetral: Firewalls, dispositivos, políticas y topologías

Introducción

- Seguridad informática:
  - Es más que un producto o conjunto de ellos
  - Es más que una o varias tecnologías
  - Es un proceso, que hace intervenir a todas las tecnologías, todos los productos y, especialmente, el sentido común de los seres humanos que la gestionan.

Definiciones

- Vulnerabilidad: Debilidad
- Amenaza: Posibilidad de que una vulnerabilidad sea aprovechada
- Ataque: Llevar a cabo una amenaza
- Riesgo: Posibilidad de que ocurra un ataque

Definiciones

- Enfoques en el ámbito de la seguridad:
  - Seguridad Física
  - Seguridad Lógica
  - Gestión de Seguridad
- En esta asignatura nos centraremos en la Seguridad Lógica

Principios de la seguridad informática

- Acceso más fácil: La cadena es tan fuerte como su eslabón más débil
- Caducidad de la información: Los datos confidenciales deben protegerse sólo hasta que el secreto pierda su valor
- Eficiencia:
  - Deben funcionar en el momento oportuno.
  - Deben hacerlo optimizando los recursos del sistema.
  - Deben pasar desapercibidos para el usuario normal, es decir, ser transparentes.

Sistema seguro

- Para considerar sistema seguro se persiguen 4 objetivos:
  - Autenticidad
  - Confidencialidad
  - Integridad
  - Disponibilidad

Sistema seguro

Actos

Autenticidad	→	Falsificación
Confidencialidad	→	Revelación
Integridad	→	Modificación / Destrucción
Disponibilidad	→	Denegación de servicio

Activos a proteger

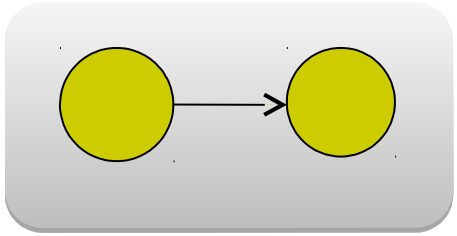
- Información
- Equipos:
  - Software: Bugs publicados y no reparados, malas configuraciones, backups
  - Hardware: Fallos eléctricos, Seguridad física en general
- Usuarios: Necesaria formación en el ámbito de la seguridad

Triángulo de debilidades

Clasificación de ataques

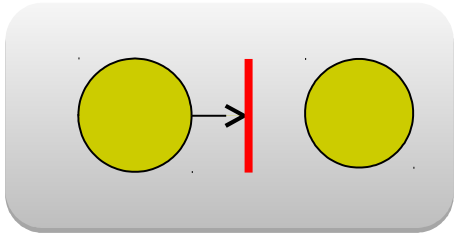
- Origen
  - Externos
  - Internos
- Complejidad
  - No estructurados: Usan herramientas típicas
  - Estructurados
- Objetivo
  - Interrupción del servicio
  - Interceptación
  - Modificación
  - Invención / Generación

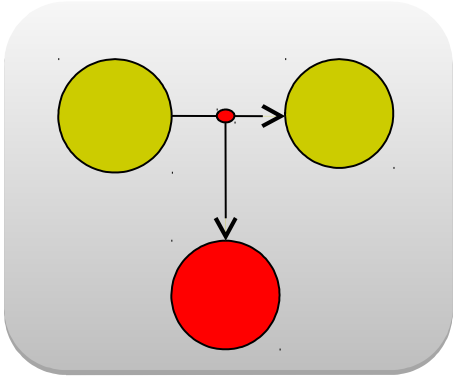
Clasificación según objetivo



Flujo normal de comunicación

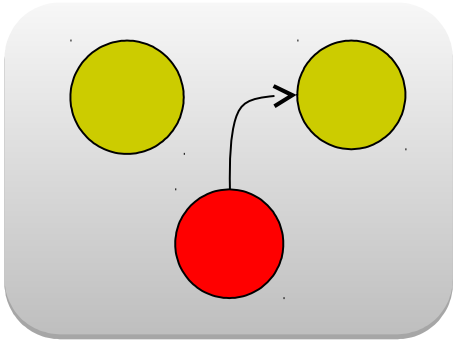
Ataque de Interrupción





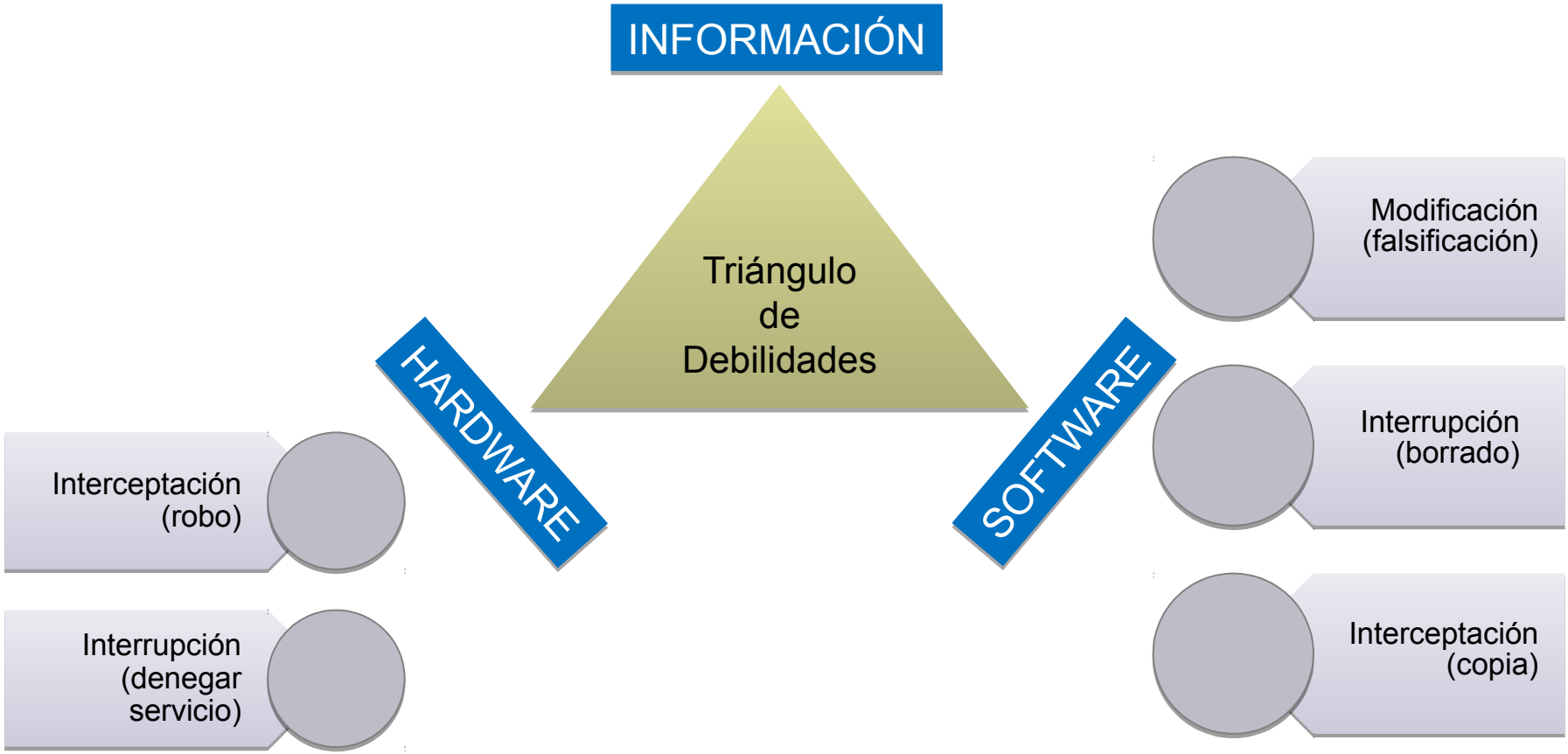
Ataque de Interceptación

Ataque de Generación



Amenazas


Interrupción (pérdida)
Interceptación (acceso)
Modificación (cambio)
Generación (alteración)


INFORMACIÓN
Triángulo de Debilidades
HARDWARE
SOFTWARE
Interceptación (robo)
Interrupción (denegar servicio)
Modificación (falsificación)
Interrupción (borrado)
Interceptación (copia)

Gestión de la Seguridad

- Ejemplos de ataques:
  - 5 de septiembre de 2016
  - 23 de abril de 2013
  - 9 de junio de 2016
  - 6 de junio de 2016
  - 15 mayo 2017
- Bases de datos de comprobación:
  - Leakedsource, https://haveibeenpwned.com
  - 2019: 617 millones de contraseñas por 20.000$

Gestión de la Seguridad

- Sistemas de gestión de la seguridad de la información (SGSI)
- Políticas básicas de seguridad:
  - Prohibitiva: Por defecto se deniega todo
  - Permisiva: Por defecto se permite todo
- ISO-27001: Estándar para la seguridad que define líneas de actuación.

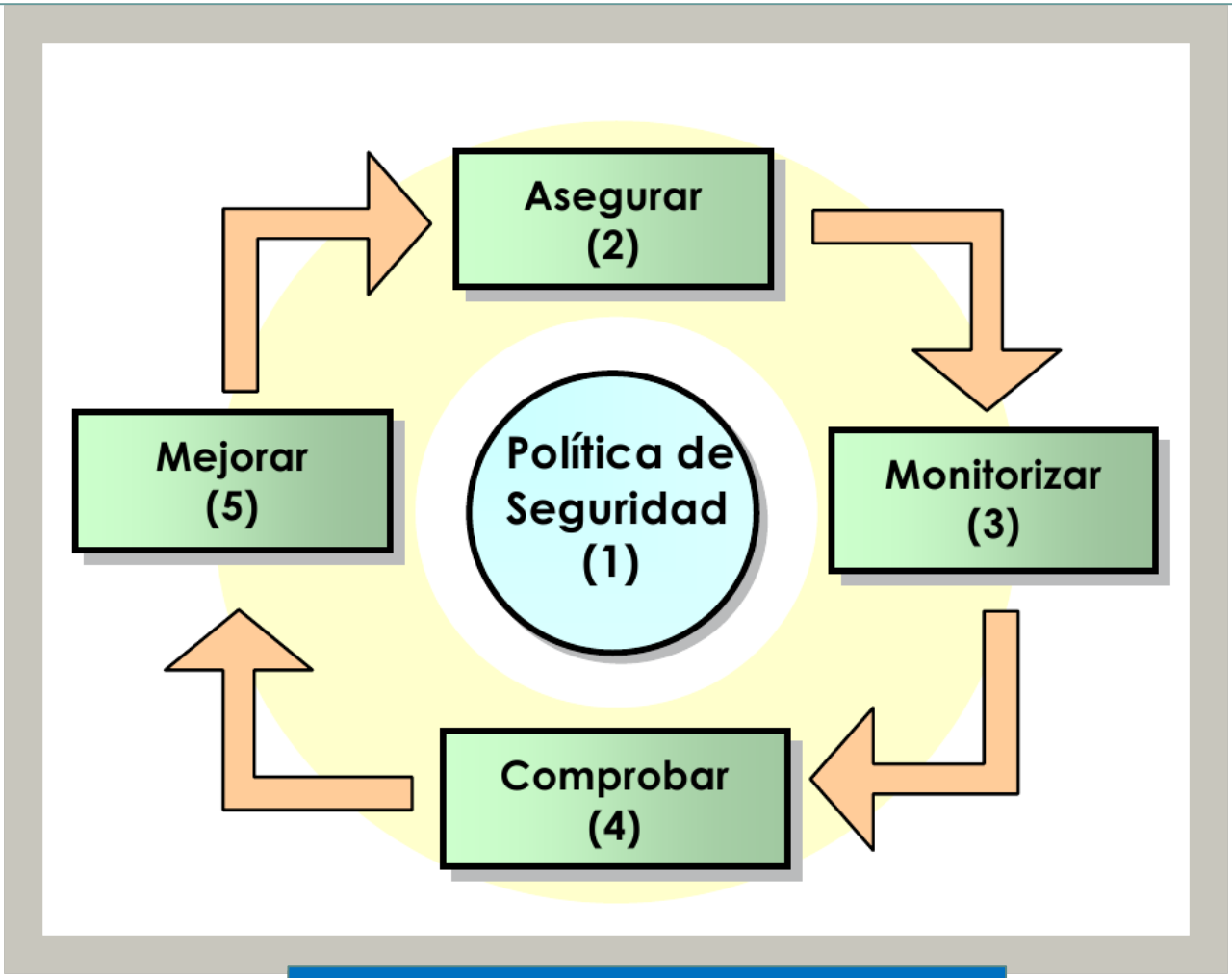
ISO-27001

- Seguridad organizativa
- Clasificación y control de activos
- Seguridad del personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Controles de acceso
- Desarrollo y mantenimiento de sistemas
- Gestión y continuidad del negocio
- Requisitos legales

Normas generales

- Una buena política de seguridad debe cumplir una serie de normas generales:
  - Debe poder implantarse, entenderse y cumplirse
  - Debe definir responsabilidades
  - Debe permitir que siga realizándose el trabajo normal
  - Debe ser exhaustiva (tener en cuenta todos los componentes que ha de proteger)
  - Debe incluir mecanismos de respuesta
  - Debe tener mecanismos de actualización

Metodología



La rueda de la seguridad

Metodología

- Fases de la metodología propuesta:
  1. Política de seguridad
  2. Asegurar: PKI, Firewalls, IPSec, VPN, etc.
  3. Monitorizar: IDS (Intrusión Detection System), Honeypots (señuelos)
  4. Comprobar
  5. Gestionar y mejorar: Analizar resultados
- Proceso iterativo

Análisis de riesgo

- En España existe una metodología para el análisis de riesgos denominada MAGERIT
  - http://administracionelectronica.gob.es/
- A nivel europeo:
  - Agencia Europea de Seguridad de las Redes y de la Información: https://www.enisa.europa.eu
- Ecuación básica del Análisis de Riesgo: RIESGO vs CONTROL vs COSTE

$$B < P \times L$$

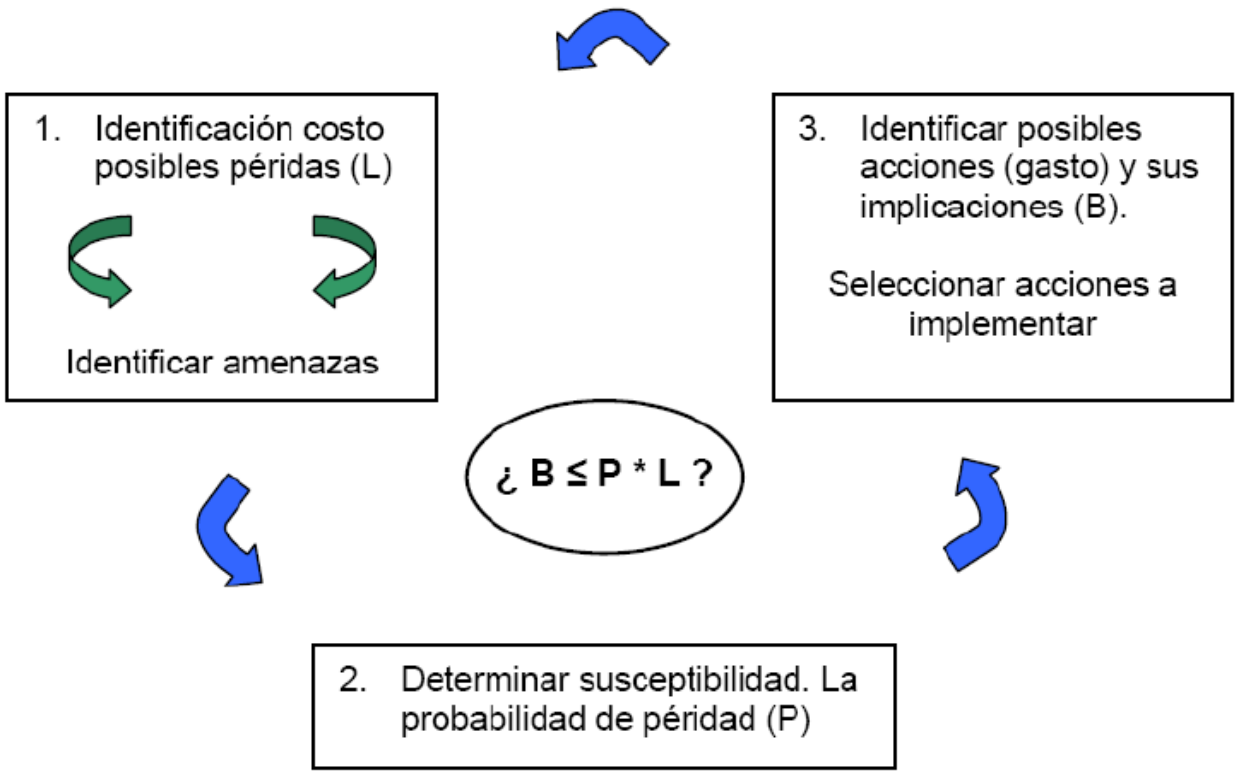
B: Coste de implantación
L: Coste en pérdidas tras un ataque
P: Probabilidad de ocurrencia

Análisis de riesgo

- El coste necesario para implantar las medidas de prevención ha de ser menor que el coste que supone perder el activo que se protege:
  - Si B ≤ P x L: El coste que supone perder el activo es mayor que el coste que supone implantar una medida de prevención. Hay que implementar una medida de prevención o mejorar la existente.
  - Si B > P x L: No es necesaria una medida de prevención ya que el coste de implantarla es mayor que el coste que supone perder el activo que se quiere proteger.

Análisis de riesgo

- ¿Cómo estimar el coste de implantación?



Peligros y modos de ataque

- Los ataques son cada vez mas sofisticados, y a la vez se requieren menos conocimientos técnicos para llevarlos a cabo
- Taxonomía de vulnerabilidades:
  - Ataques a la confidencialidad.
  - Ataques a la autenticidad.
  - Ataques a la disponibilidad.
  - Ataques a la integridad.

Ataques a la confidencialidad

- Objetivo: Obtener información privilegiada.
- Métodos:
  - Basados en ingeniería social.
  - Basados en técnicas informáticas de obtención de información.

Ataques a la confidencialidad

- Ingeniería social:
  - Uso de técnicas psicológicas y/o habilidades sociales para la obtención de información de terceros.
  - No implica necesariamente el uso de tecnología
- Principios establecidos por Kevin Mitnick
  - Todos queremos ayudar.
  - El primer movimiento es siempre de confianza hacia el otro.
  - No nos gusta decir No.
  - A todos nos gusta que nos alaben.
  - ¿Quién es Kevin Mitnick?

Ataques a la confidencialidad

- Depende en gran medida de la formación del usuario
  - Desde el punto de vista tecnológico: uso de firma digital.
  - Desde el punto de vista humano: formación en seguridad y “sentido común”.
- Herramientas de aprendizaje: Social Engineering Toolkit SET [Enlace]

Ataques a la confidencialidad

- **Sentido común**: *Apps que piden ~70 permisos ¿Para encender la linterna? [Fuente Avast]:*
  - *Ultra Color Flashlight, 77 permisos, 100.000 descargas*
  - *Super Bright Flashlight, 77 permisos, 100.000 descargas*
  - *Flashlight Plus, 76 permisos, 1.000.000 descargas*
  - *Brightest LED Flashlight — Multi LED & SOS Mode, 76 permisos, 100.000 descargas*
  - *Fun Flashlight SOS mode & Multi LED , 76 permisos, 100.000 descargas*
  - *Super Flashlight LED & Morse code, 74 permisos, 1.000.000 descargas*
  - *FlashLight – Brightest Flash Light, 71 permisos, 1.000.000 descargas*
  - *Flashlight for Samsung, 70 permisos, 500.000 descargas*
  - *Flashlight – Brightest LED Light & Call Flash, 68 permisos, 1.000.000 descargas*
  - *Free Flashlight – Brightest LED, Call Screen, 68 permisos, 500.000 descargas*

Técnicas informáticas de obtención de información

- Escaneo de puertos
  - Herramientas: NMAP
  - Contramedidas: Filtrado de puertos, análisis de logs y alarmas
  - Múltiples métodos: se resumen en la documentación de NMAP
    - TCP Connect Scan
    - TCP SYN Scan
    - TCP FIN Scan
    - TCP Fragmentation Scan

Técnicas informáticas de obtención de información

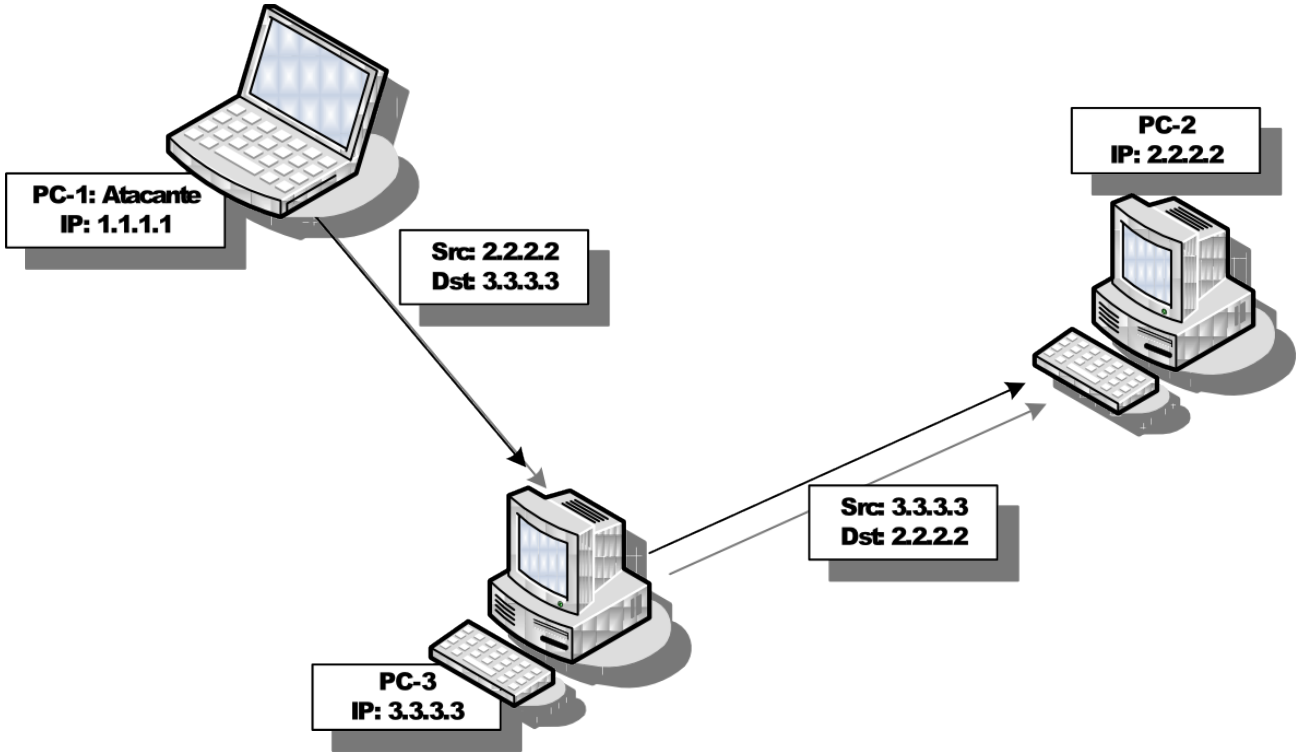
- Sniffing interceptación pasiva o escucha
  - Herramientas: tcpdump, Dsniff, Darkstat, Ethercap, Cain & Abel, WinDump, Airodump-ng
  - Contramedidas: mecanismos de autenticación y cifrado.
- Snooping downloading
  - Objetivo: Obtener documentos, mensajes, correos, etc. Para análisis posterior por curiosidad espionaje o robo.

Ataques a la autenticidad

- Objetivo: Engañar al sistema de la víctima para ingresar al mismo como usuario privilegiado
- Tipos
  - Spoofing: Suplantación de identidad
  - Hijacking: Secuestro de sesiones
  - Backdoors: Puertas traseras
  - Fuerza bruta

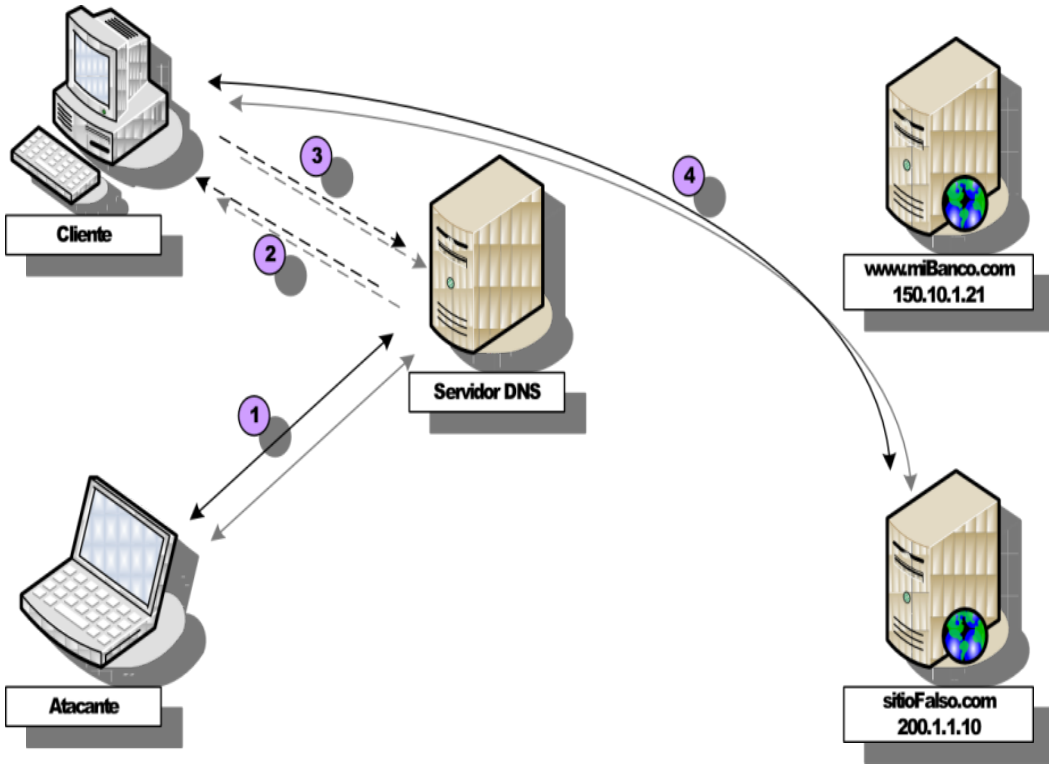
Ataques a la autenticidad

- IP Spoofing: Usurpación de una dirección IP, debe estar en la misma red local



Ataques a la autenticidad

- DNS Spoofing:
  - Interno: Manipular los paquetes UDP para comprometer el servidor DNS
  - Externo: Vulnerabilidad en los routers [Ejemplo]
  - ICANN urge a usar DNSSEC a todos los proveedores [Enlace]



Ataques a la autenticidad

- Phishing: Envío de falsos e-mails es una forma de spoofing, mails a nombre de otra persona o entidad. También utilizado con mensajería instantánea.
- Web Spoofing: El atacante crea un sitio web completo, falso y similar al que la víctima desea entrar.
- ARP Spoofing: Se redirecciona el tráfico hacia el atacante. El atacante falsifica los paquetes ARP

Ataques a la autenticidad

- HIJACKING - Secuestro de sesiones: Se roba una conexión después de haber superado con éxito el proceso de identificación
- BACKDOORS: Trozos de código dentro de un programa que permiten, a quien las conoce, saltarse los métodos usuales de autentificación.

Ataques a la autenticidad

- Fuerza bruta: Obtención de claves para ingresar en sistemas, aplicaciones, cuentas, etc, probando todas las posibilidades.
  - Uso de diccionarios
  - Uso de clústers
- ¿Cómo se almacenan las contraseñas en los sistemas informáticos?
  - Uso de funciones HASH – Huellas digitales
  - Se profundiza en el siguiente tema

Ataques a la autenticidad

- Otros ejemplos:
  - Stingrays/IMSI cátcher: Repetidores de red móvil falsos. [Ejemplo]
  - SIM swap: Duplicado de tarjeta SIM para usarlo contra la autenticación en 2 pasos. [Ejemplo]
  - Scambot: Parece un ataque a la autenticidad pero realmente es ingeniería social

Ataques a la disponibilidad DoS

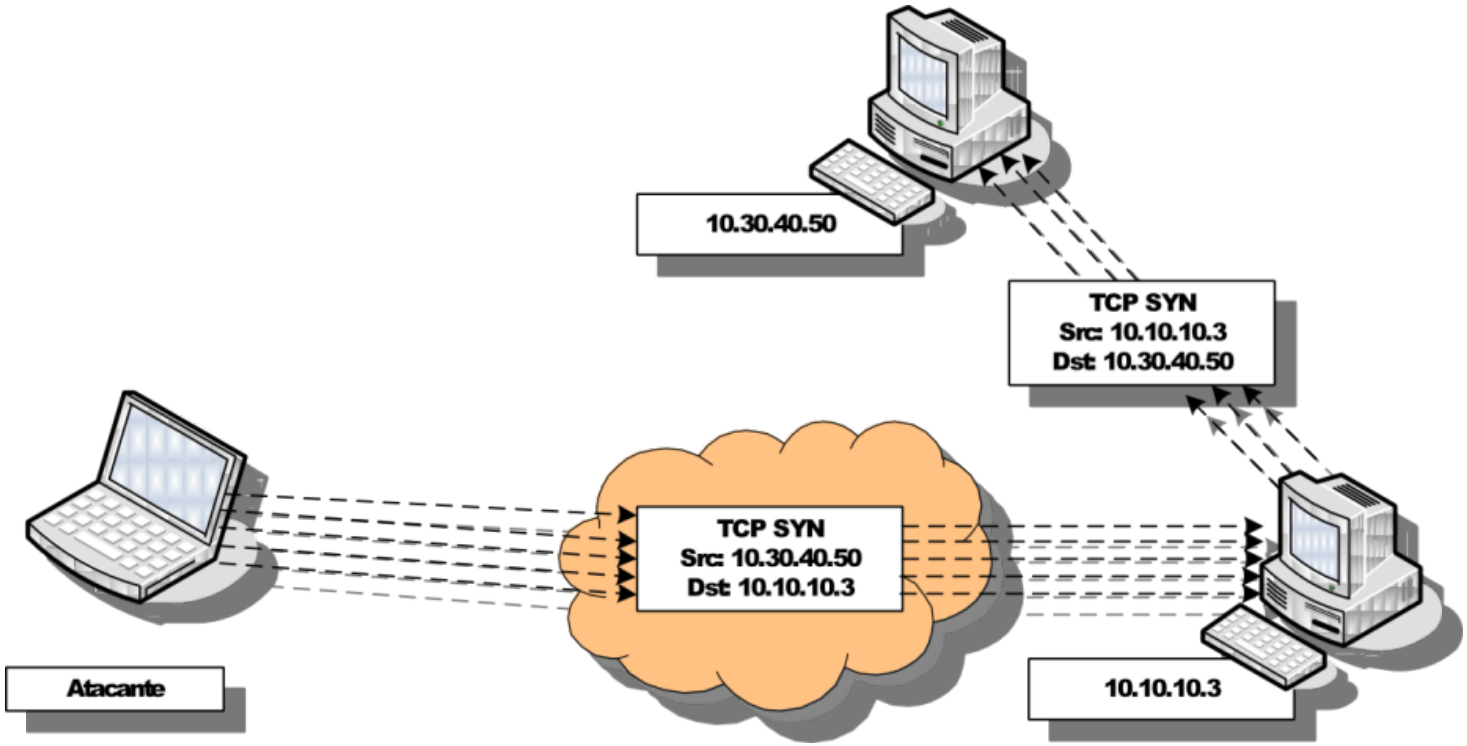
- Objetivo: Saturar los recursos del sistema víctima de forma que se inhabiliten durante algún tiempo los servicios ofrecidos por el mismo.
- Tipos de ataques DoS:
  - Denegación de servicio de aplicación
  - Denegación de servicio de red

Ataques a la disponibilidad DoS

- Flooding / Jamming: Saturar los recursos del sistema
  - Saturar la memoria
  - Saturar el disco
  - Saturar ancho de banda
- Ejemplos: Ping de la muerte, emails masivos

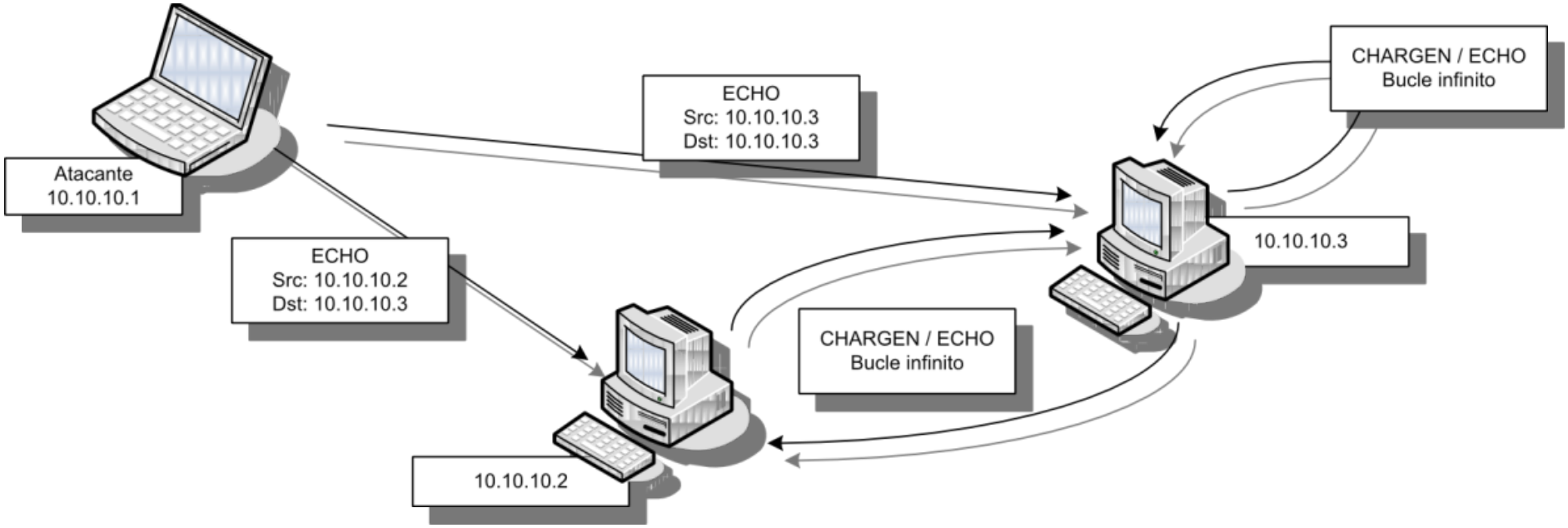
Ataques a la disponibilidad DoS

- Modalidades Flooding / Jamming
  - SYN Flooding: Dejar en la máquina objetivo un número elevado de conexiones TCP en espera.



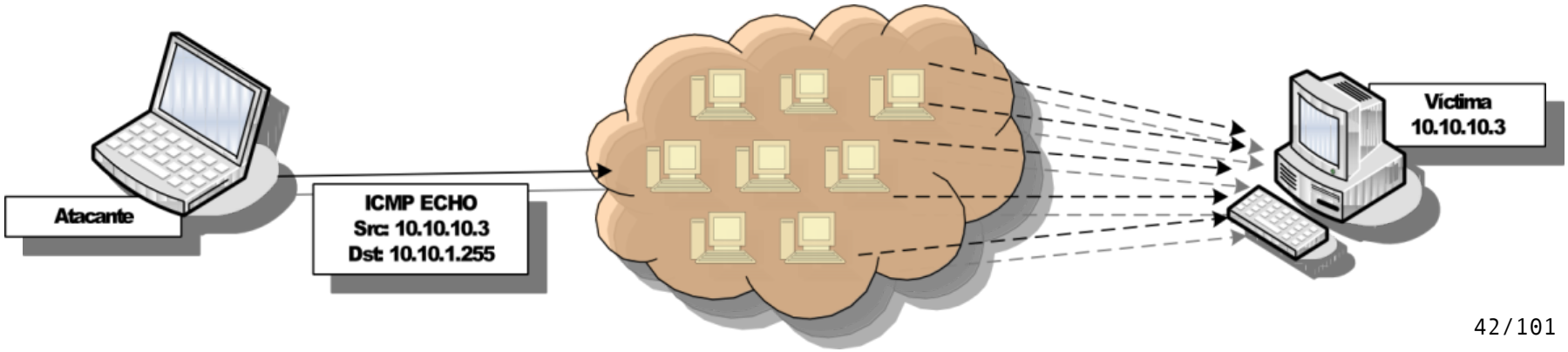
Ataques a la disponibilidad DoS

- Modalidades Flooding / Jamming
  - UDP Flooding: Inundación de paquetes UDP, UDP tiene prioridad sobre TCP



Ataques a la disponibilidad DoS

- Fragmentación de paquetes: Vulnerabilidad en la pila TCP/IP
  - Pequeños fragmentos
  - Superposición de fragmentos
  - Buscar Teardrop
  - IPv6 no permite la fragmentación
- Smurfing: Explotar ICMP.



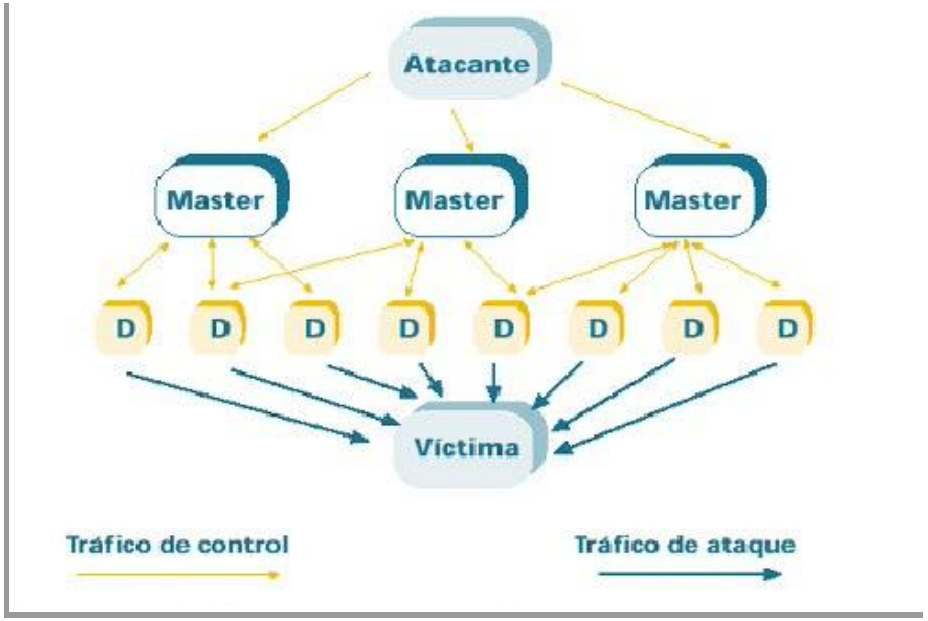
Ataques a la disponibilidad DoS

- Sockstress: Juega con la ventana TCP estableciéndola a 0.
  - Abre un puerto y envía un paquete con datos
  - Se responde indicando que la ventana es 0

```
syn    →    (4k window)
       ←    syn + ack (32k window)
ack    →    (0 window)
```

Ataques a la disponibilidad DoS

- E-Mail Bombing – Spamming
- Denegación de Servicio Distribuida (DDoS): Ordenadores zombies / botnets
  - Fase 1: Captura de nodos esclavos para el ataque
  - Fase 2: Ataque sincronizado desde los nodos esclavos



Ataques a la disponibilidad DoS

- Ejemplos I:
  - 5/9/2016 (DOS): 150 Gbps Telefónica → OVH
  - 20/9/2016 (DDOS): 665 Gbps contra KrebsOnSecurity.com
  - 28/9/2016 (DDOS): más de 1 Tbps. Se detectaron más de 150.000 cámaras IP de videovigilancia.
  - 6/3/2018 (DDOS): Picos de 1.7 Tbps contra GitHub (Record actual) [Enlace]
- Estadísticas en tiempo real:

  http://www.digitalattackmap.com

Ataques a la disponibilidad DoS

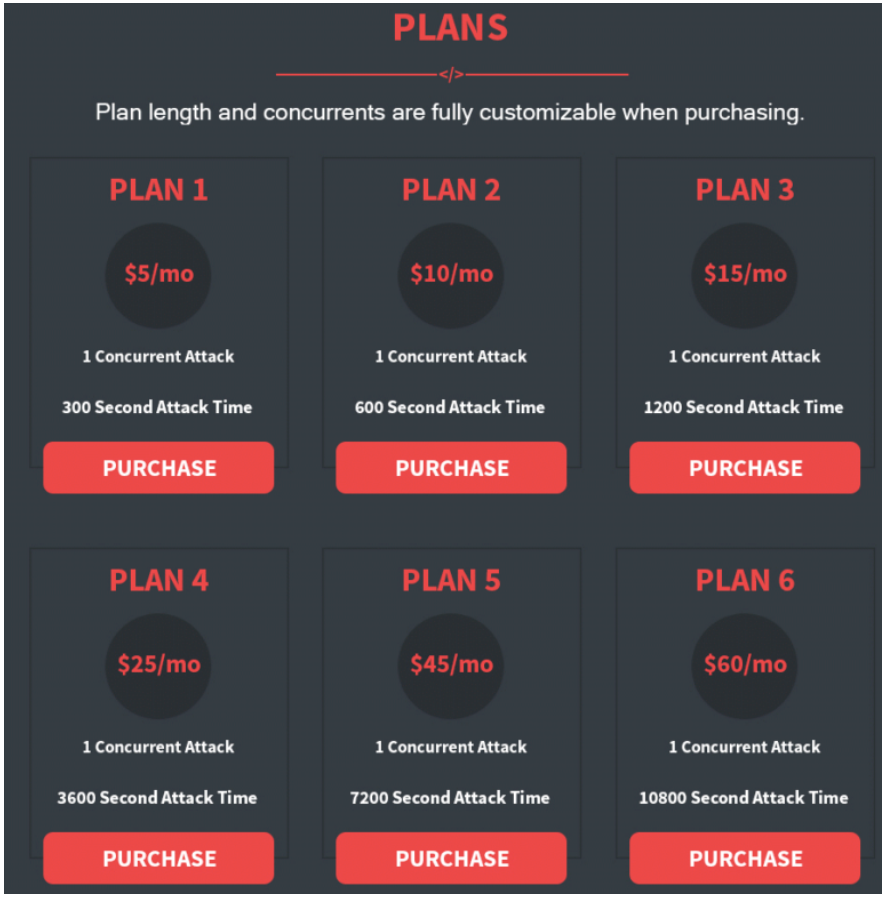
- Ejemplos II:
  - DoS disco duro con sonido.
  - Botnet envía 12 millones de correos (scarab botnet)
  - Resultado: Emails + Ingeniería Social + Poca formación + Poco sentido común = 99% of email attacks rely on victims clicking links [Fuente]

Ataques a la disponibilidad DoS

- Técnicas de mitigación:
  - Sync proxy
  - Eliminar conexiones enviando paquetes TPC/RST
  - Filtrado de IPs (Blacklists)
  - Otras: Análisis de cabeceras de conexión, detección de anomalías estadísticas

Ataques a la disponibilidad DoS

- Coste de realización de estos ataques
- Fuente: Trend Micro Russian Underground
- Precio por bloquear la red TOR ~20.000$/mes [Fuente, Estudio]



Ataques a la integridad

- Objetivo: Modificar o destruir información o aplicaciones.
- Modalidades:
  - Tampering / Data Diddling: Borrado
  - Borrado de huellas (Trazabilidad)
  - Ataques a aplicaciones
  - Exploits

Ataques a la integridad

- Ataques a aplicaciones:
  - El más común son vulnerabilidades en la navegación, Applets, JavaScript, Active-X.
  - Vulnerabilidad/Ataque día cero (zero-day)
- Origen:
  - Mala configuración
  - Bugs
  - Buffer overflow
  - Exploits

Ataques a la integridad

- Exploits: Programa preparado para atacar una debilidad existente.
  - Buffer overflow: Se sobrepasa la capacidad de almacenamiento de una variable.
  - Stack overflow: Desbordamiento de la pila.
- Prevención:
  - http://www.exploit-db.com
  - DEP, Data execution prevention (hardware)

Ataques a la integridad

- Ejemplos
  - Cajero automático con WinXP [Enlace]
  - Microsoft año 2004 en el manejo de imágenes JPG (GDI) de Microsoft [Enlace]
    - Impacto: Ejecución/inyección de código
  - Heartbleed: [Enlace]
  - ShellShock: [Enlace]
  - Spectre CVE-2017-5715 / Meltdown CVE-2017-5754
  - Broadcom BCM43xx (CVE-2017-9417)
  - BlueBorne afecta a bluetooth (CVE-2017-14315)
  - Herramientas: AutoSploit, ACsploit

Ataques a la integridad

- Ramsomware: secuestro de sistemas / datos.
- Ejemplos
  - WannaCry:12 de mayo de 2017, rescate en bitcoins
  - Erebus: 4.4 millones de dólares en bitcoins por rescatar los servidores de nayana.com.
  - Bloquean ordenadores de Apple y piden rescates.
  - 2017: La Oficina Europea de la Policía, afirma que "*el ransomware se ha convertido una de las amenazas más acuciantes para la sociedad*".
  - Oct-2019: Ayuntamiento de Jerez Paralizado [Fuente]

Ataques a la integridad

- Malware: Programas que se introducen en nuestros sistemas de formas muy diversas con el fin de producir efectos no deseados y nocivos.
- Tipos: troyanos, keyloggers, spywares, adwares, rootkits, gusanos, downloaders, crypto-minadores, etc.
- Características:
  - Pueden tener numerosas formas
  - Producen efectos diferentes según su tipo de intención

Ataques a la integridad

- Malware: Drive-by download:
  - Descarga no intencionada de software
  - Usuario involucrado:
    - Mientras el usuario navega, el sitio web le hace una petición de descarga.
    - Alega ser: una actualización de seguridad, un antivirus, u otro software no malicioso.
  - Usuario no involucrado:
    - El atacante puede instalar el malware en el terminal del usuario sin que este este involucrado.
    - Sitios webs que explotan bugs de determinados navegadores

Ataques a la integridad

- Malware. Ejemplos de funcionamiento:
  - Ejecución en aplicación: aplicación extensible (plugin malicioso)
  - Ejecución en interfaz gráfica: auto-arrance al inicio, contaminación de «mime-types»
  - Ejecución en el arranque del sistema: registro de windows
  - Arranque en el kernel: carga como módulo del kernel/driver
  - Javascript en navegadores

Ataques a la integridad

- Malware. Tipo de dispositivo:
  - Servidor: Ejemplo páginas web con minero javascript incrustado (ejecución en el cliente)
  - Driver de sistema operativo [Ejemplo]
  - UEFI: Infecta sistema de aranque (Rootkit UEFI) , ej:LoJax
  - Hardware USB: ej: BadUSB, USBNinja
  - Router: VPNFilter en marcas como MikroTik, Linksys, NETGEAR, TP-LINK o QNAP.
  - Placabase: Inserción de componentes [Enlace]
  - OnChip: Modificación del layout

Ataques a la integridad

- Ejemplos de malware:
  - Teclado GO de Android (keylogger)
  - Utorrent mina bitcoins
  - The Pirate Bay mina Monero en el Navegador
- Keylogger hardware
  - Teclado MatisTek Gk2: Keylogger
  - Cargador USB KeySeeper: Keylogger
  - Teclados y ratones Logitech CVE-2019-13053
- ¿Cuales son las diferencias entre?

  Malware, Virus, Gusanos, Troyanos, Adware y Spyware

Clasificación de atacantes

- Clasificación clásica:
  - Hacker
  - Cracker
  - Phreakers
  - Lammer
  - Copyhacker
  - Piratas
  - Newbie
  - Script Kiddie

- Existen otras clasificaciones
  - Hacker de sombrero blanco
  - Sniffers
  - Ciberterrorista
  - Carders
  - Programadores de virus
  - Etc.

¿Sirve de algo contratar un hacker? [Fuente]

Métodos de defensas

- El factor humano es fundamental
- Limitación de tráfico desde y hacia redes externas
- Para conexiones entrantes usar métodos de autenticación robustos
- Cifrado de la conexión para evitar ataques internos

Métodos de defensas

- Frentes de defensa:
  - Protección perimetral: Firewalls, Detección de intrusiones y VPN
  - Autenticación: Centro de Distribución de Claves (Kerberos)
  - Criptografía
- Discusión: ¿Qué es la Esteganografía?
  - *un troyano descubierto ahora utilizaba comentarios posteados en el perfil de Instagram de Britney Spears para localizar los servidores de control que le mandaban las instrucciones de ejecución y al que se enviaban los datos robados de los ordenadores infectados.*
  - Ejemplo para esconder el enlace http://bit.ly/2kdhuHX usaban la frase

#2hot make loveid to her, uupss #Hot #X

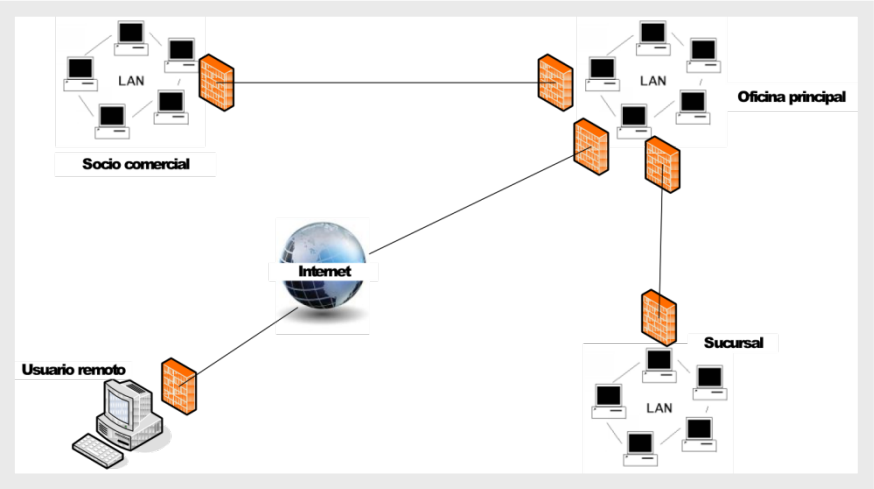
Parte II
Seguridad perimetral

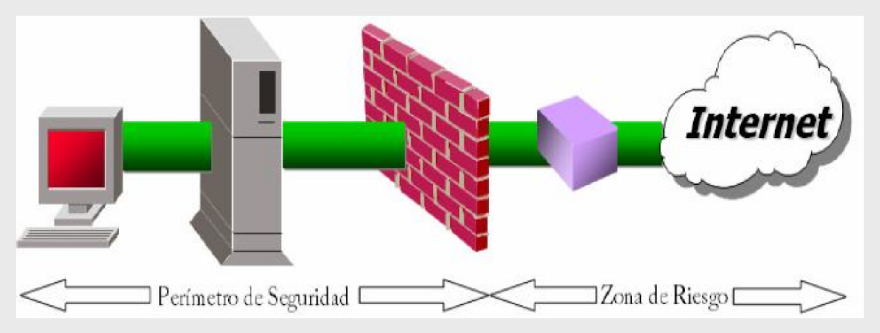
Seguridad Perimetral

- Conjunto de elementos y sistemas, encargados de:
  - Proteger perímetros físicos o lógicos.
  - Detectar tentativas de intrusión.
  - Expulsar intrusos del perímetro a proteger.

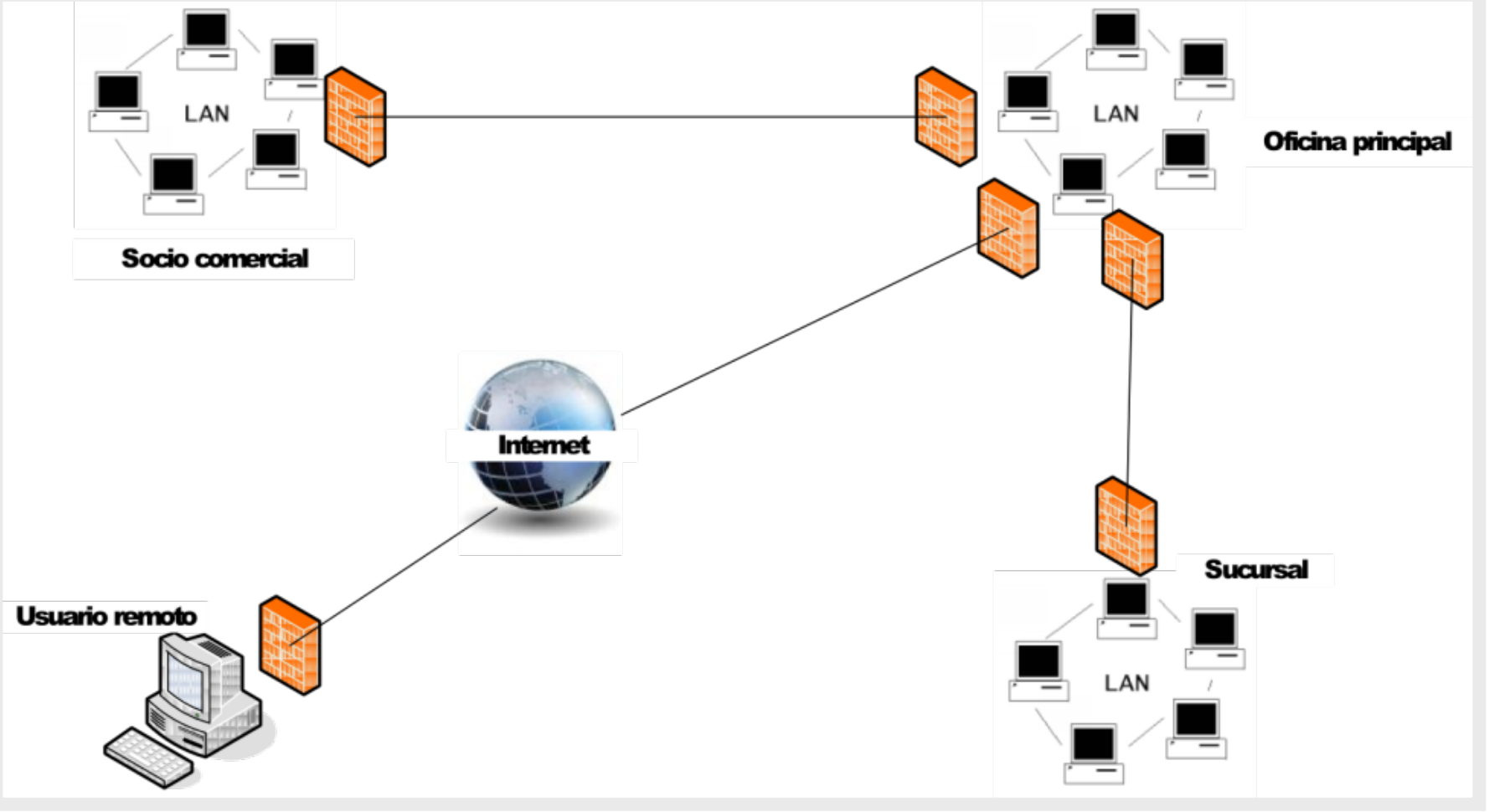
Seguridad Perimetral

- Perímetro de seguridad:
  - Separado de la red externa o zona de riesgo.
  - Suele ser propiedad de la misma organización que lo forma.





Seguridad Perimetral



Seguridad Perimetral

- Cometidos de la seguridad perimetral:
  - Rechazar conexiones ilegítimas a los servicios.
  - Permitir solo cierto tipo de tráfico o entre ciertos nodos.
  - Proporcionar un único punto de interconexión con el exterior.
  - Redirigir el tráfico entrante a los sistemas adecuados, dentro de la red interna.
  - Ocultar sistemas o servicios vulnerables que no son fáciles de proteger.
  - Auditar el tráfico entre el exterior y el interior.
  - Ocultar información: nombres de sistemas, topología de red, tipos de dispositivos de red, cuentas de usuarios internas, etc.

Seguridad Perimetral
Elementos

- Routers
- Firewalls
- Sistemas de detección de intrusiones (IDS)
- Redes privadas virtuales (VPNs)
- Software y servicios
- Zonas desmilitarizadas (DMZ) y subredes controladas

Seguridad Perimetral
Objetivos

- Buenas prácticas
  - Diseñar la red considerando y planificando la seguridad
  - Separación de servicios
  - Separación en subredes
- Elementos de protección
  - Dispositivos de control: Firewalls, Proxys
  - Dispositivos para monitorización: IDS, IPS, Honeypots
  - Túneles cifrados: VPN
- Señuelos (Honeypots):
  - Digital Attack Map
  - Cyber Threat Map

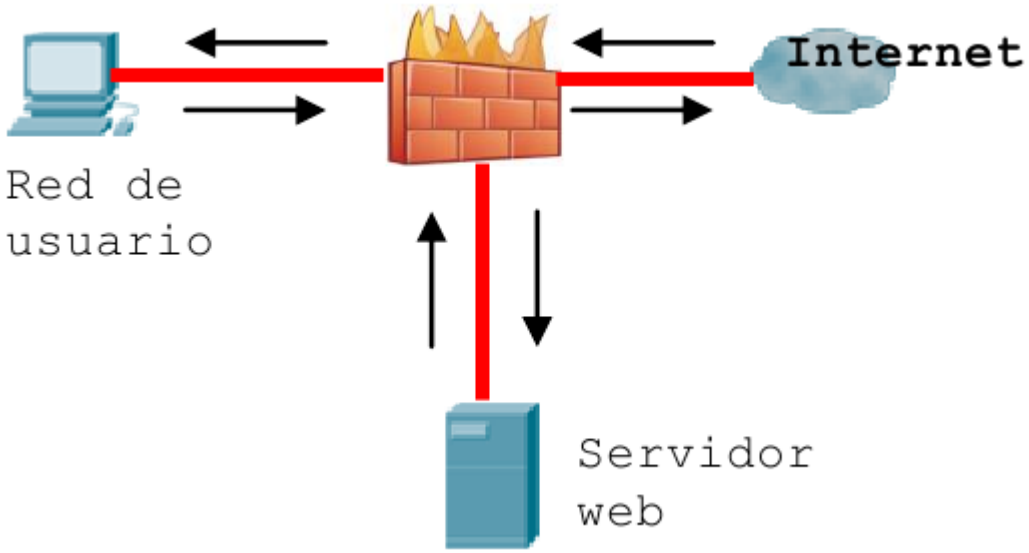
Protección perimetral
Firewalls

- Firewall: Sistema(s) capaces de separar una máquina o una subred (zona protegida) del resto de la red (zona de riesgo)

Nota: Se suele considerar firewall como el elemento encargado de filtrar paquetes, consideraremos otros elementos como los proxies parte del firewall.

Protección perimetral Firewalls

- Objetivo: Aislar zonas peligrosas
  - Protegen una red del mundo exterior
  - Filtran el tráfico entre dos redes
  - Fuerza una política de control



Protección perimetral
Firewalls

- Un firewall no puede proteger de:
  - Ataques cuyo tráfico no pase a través de él.
  - Amenazas producidas por ataques internos.
  - No puede controlar a espías corporativos localizados dentro del perímetro de seguridad.
  - Ataques de ingeniería social.
  - Virus informáticos.
  - Fallos de seguridad en servicios y protocolos.

Protección perimetral
Firewalls

- Mecanismos:
  - Filtrado de paquetes: Examina la cabecera de los paquetes y decide en base a reglas si los acepta o rechaza
  - Pasarela de aplicaciones (Proxy): Diferentes tipos de operación: caché, analizador, control.

Firewalls
Filtrado de paquetes

- Se suele implementar en routers
- Funcionamiento:
  - Los paquetes se examinan en la capa de red.
  - Se usa como primera línea de defensa.
  - Toman decisiones de aceptar o rechazar una conexión.
  - No realiza comprobaciones en niveles superiores de la pila.

Firewalls
Filtrado de paquetes

- Las reglas se basan en:
  - Dirección IP origen.
  - Dirección IP destino.
  - Puerto TCP/UDP origen.
  - Puerto TCP/UDP destino.
- Tipos de filtros:
  - Filtrado estático o Stateless
  - Filtrado dinámico o Stateful

Firewalls
Filtrado de paquetes estático

- Se analiza la cabecera de cada paquete y en función de la misma se acepta o rechaza
- No se establece relación alguna entre anteriores o sucesivos paquetes
- Funcionamiento:

  1.- Los paquetes entrantes se comparan con las reglas definidas: se aceptan o deniegan

  2.- Si es aceptado:

  2.1.- Si está destinado al firewall se propaga a la pila de red para su futuro procesado.

  2.2.- Si está destinado a un host remoto se reenvía hacia éste.

Firewalls
Filtrado de paquetes estático

- Ejemplo

Regla	Acción	IP Fuente	IP Destino	Protocolo	Puerto origen	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	TCP	Cualquiera	25 (smtp)
2	Aceptar	Cualquiera	192.168.10.3	TCP	Cualquiera	80 (http)
3	Aceptar	192.168.10.0/24	Cualquiera	TCP	Cualquiera	80 (http)
4	Denegar	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera

Firewalls
Filtrado de paquetes estático

- Ventajas
  - Consume pocos recursos
  - Fácil de implementar
- Inconvenientes
  - No mantienen información de contexto acerca del estado de la conexión, lo que los convierte en débiles desde el punto de vista de la seguridad, pues permiten aprovechar vulnerabilidades en protocolos y aplicaciones.
  - Sólo examina los paquetes a nivel de red.

Firewalls
Filtrado de paquetes dinámico

- Necesidad de uso:
  - La mayoría de las conexiones son admitidas en el nivel de transporte por el protocolo TCP
  - En este nivel se administran sesiones y hay que verificar que todos los intercambios se lleven a cabo de forma correcta.
- Ejemplo: el protocolo FTP abre puertos extra aleatoriamente

Firewalls
Filtrado de paquetes dinámico

- Características:
  - Se añaden y eliminan reglas al vuelo durante una sesión TCP
  - Se considera el estado de los paquetes previos para definir la nuevas reglas

Firewalls
Filtrado de paquetes dinámico

- Funcionamiento:

  1.- Los paquetes entrantes se comparan con las reglas estáticas definidas y son denegados ó aceptados.

  2.- En función de la información contenida en cada paquete, se asocia una información estática adicional.

  3.- Se añaden las reglas dinámicas en función del contenido del paquete y la información estática adicional.

  4.- Si el paquete pasa el filtrado toma una de estas dos rutas:

  4.a.- Esta destinado al firewall y se propaga a la pila de red

  4.b.- Está destinado a un host remoto y se reenvía.

  5.- Todos los paquetes asociados con una sesión de autenticación son procesados por una aplicación que se ejecuta en el host firewall.

Firewalls
Filtrado de paquetes dinámico

- Ventajas:
  - Sofisticado.
  - Control exhaustivo del tráfico.
  - Resuelve necesidades a nivel de transporte.
  - Mantiene información de contexto acerca del estado de la conexión.
- Inconvenientes:
  - Consumen más recursos.
  - Más difíciles de implementar.

Conclusiones del filtrado de paquetes en general

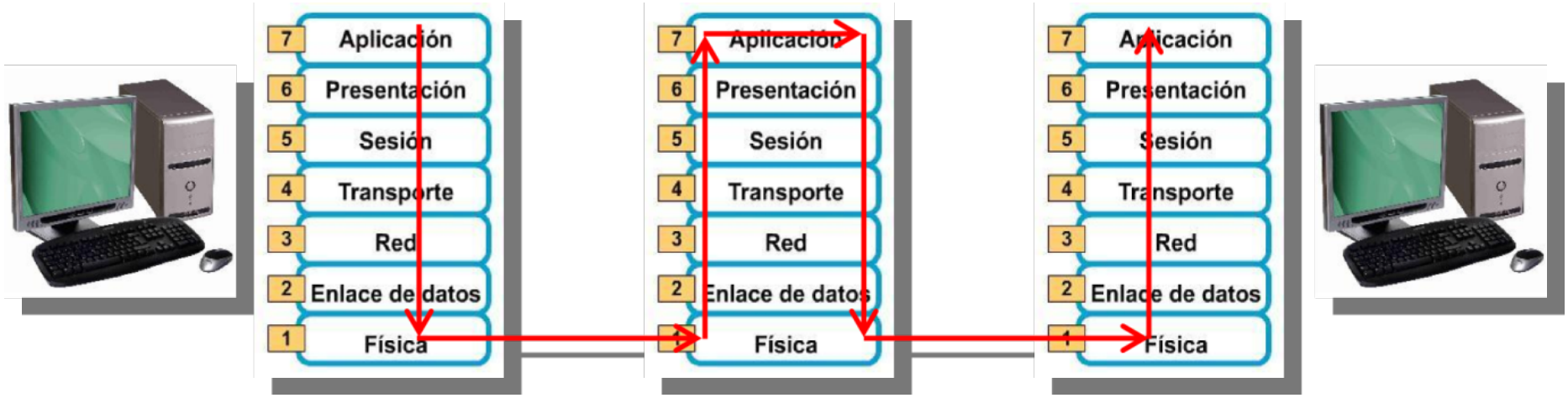
- Ventajas del filtrado de paquetes:
  - Alto rendimiento: Reglas simples, requieren poco procesado.
  - Escalabilidad: Poca sobrecarga, pueden manejar caudales altos de datos.
  - Transparencia frente al usuario
- Inconvenientes del filtrado de paquetes:
  - Vulnerables: Reducen el riesgo de los ataques, pero no los impiden.
  - Sólo impiden el acceso, una vez dentro no sirven.
  - El tráfico falsificado y fragmentado puede burlar el filtro de paquetes
- Algunos filtros de paquetes:
  - Listas de control de acceso (ACLs) en routers Cisco.
  - Netfilter de Linux.
  - OpenBSD Packet Filter.

Proxy / Pasarela de aplicaciones

- Proxy: Programa que realiza una acción en representación de otro.
- Funciones: Filtrar, reenviar, bloquear, balancear
- Es un intermediario entre dos redes interconectadas
- El filtrado es de nivel superior al filtrado de paquetes

Proxy

- Los paquetes se examinan a nivel de aplicación.
- Permiten el filtrado de contenidos y comandos de aplicación



Proxy

- Ventajas
  - Seguridad. Controlan el inicio y cierre de sesión.
  - Integridad. Conocen el nivel de aplicación.
  - Ocultación de información. Los hosts no necesitan dar información propia al exterior para que puedan comunicarse con hosts externos.
  - Reducen la complejidad en las reglas de filtrado.
  - Aumentan la velocidad de la navegación web gracias a que cuentan con una caché de contenidos.

Proxy

- Inconvenientes:
  - Se limitan a ciertas aplicaciones. En ocasiones se necesita un proxy para cada servicio.
  - Agilidad limitada dado el número de protocolos y la necesidad de compilar para cada plataforma.
  - Reducido rendimiento. Requiere muchas instancias (buffering) y conmutaciones de los datos para su proceso.
  - Limita la conectividad y la transparencia.

Proxys

- Clasificación

  a.- Proxy a nivel de aplicación: Proxy dedicado

  b.- Proxy a nivel de circuito: Proxy genérico

  c.- Proxy HTTP Directo

  d.- Proxy HTTP Inverso

Proxy a nivel de aplicación

- Usos:
  - Hacen de caché
  - Filtran comandos del nivel de aplicación
  - Registro de sucesos
- Son de propósito específico para cada aplicación:
  - Entiende en interpreta los comandos en el protocolo de aplicación
- Ejemplos: TCPWrapper, SQUID, BlueCoat

Proxy a nivel de circuito - Proxy genérico

- No interpreta el contenido del protocolo de aplicación, sólo determina si una conexión es permitida.
- No son específicos para cada protocolo de aplicación, es genérico.
- Permiten implementar mecanismos de control de acceso elaborados, incluyendo autenticación e intercambio de mensajes de protocolo entre proxy y cliente.

Proxy a nivel de circuito - Proxy genérico

- Características:
  - Crea un circuito entre el cliente y el servidor.
  - No interpreta el protocolo de la aplicación que hace uso del circuito.
  - Determina si una conexión entre dos puntos es permitida, de acuerdo con un determinado conjunto de reglas.
  - Mantiene el estado de la conexión a lo largo de la transmisión, agrupando los paquetes que pertenezcan a la misma conexión.
  - Proveen servicios para un amplio rango de protocolos diferentes.
  - Pueden implementar mecanismos de control de acceso y autenticación elaborados.
  - Requieren software de cliente especial.

Proxy HTTP Directo

- Gateway genérico para el navegador del cliente.
- Oculta el direccionamiento de la red interna
- Permite establecer reglas de acceso a la Web desde el perímetro de seguridad.

Proxy HTTP Inverso

- Actúa en el back-end de servidores cliente.
- Características:
  - Se centralizan los accesos ofreciendo un punto único a proteger. Facilita el acceso a los servicios.
  - Se facilita la gestión de cambios en la granja de servicios. Cualquier cambio en ésta es reflejado en la política de mapeo del proxy inverso.
  - Redirecciona http y https. Permite que podamos acceder a las páginas en formato URL.

Software vs Hardware

- Soluciones Software: Operan sobre una instalación de un S.O.
  - Microsoft Internet Security and Acceleration (ISA) Server
  - Novell BorderManager
  - Netfilter / Iptables
- Soluciones hardware: Dispositivos con el software preinstalado en una plataforma hardware especializada.
  - Cisco PIX / ASA
  - NetScreen
  - SonicWALL
  - WatchGuard
  - Fortigate

Software vs Hardware

- Comparativa:

	Software	Hardware
Tiempo de instalación	☹	☺
Escalabilidad	☺	☹
Estabilidad	☹	☺
Flexibilidad hardware	☺	☹

Diseño del firewall

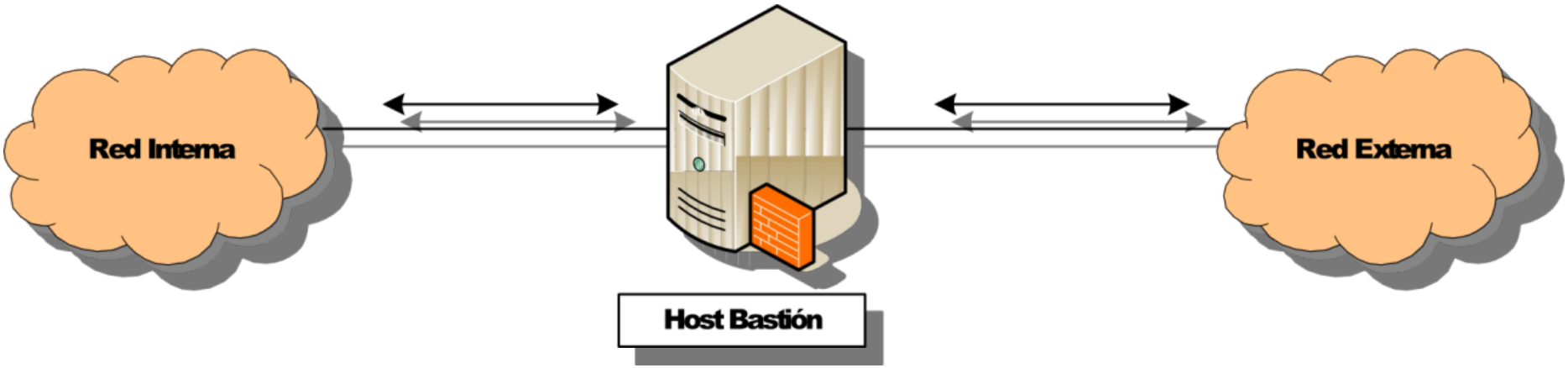
- Dos políticas básicas:
  - Permisiva
  - Restrictiva
- Topología / Configuración del perímetro:
  - Básica: Cortafuegos de filtrado de paquetes, Dual-homed Gateway, Screened host, Screened subset (DMZ).
  - Jerárquicas: Multinivel

Diseño del firewall

- Filtrado de paquetes:
  - Solución sencilla
  - Único dispositivo
  - Implementado en la mayoría de los routers

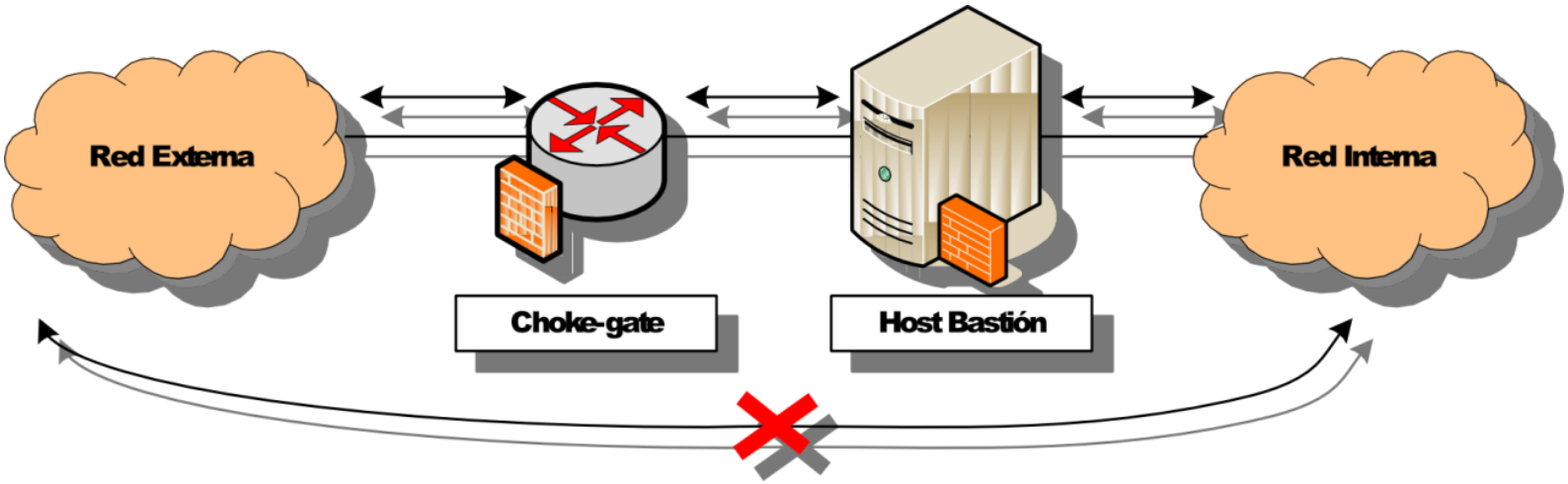
Diseño del firewall

- Dual-homed gateway
  - Máquinas con 2 o más tarjetas de red
  - El sistema implementa un proxy para cada servicio
  - Sólo implementan servicios mediante proxy's



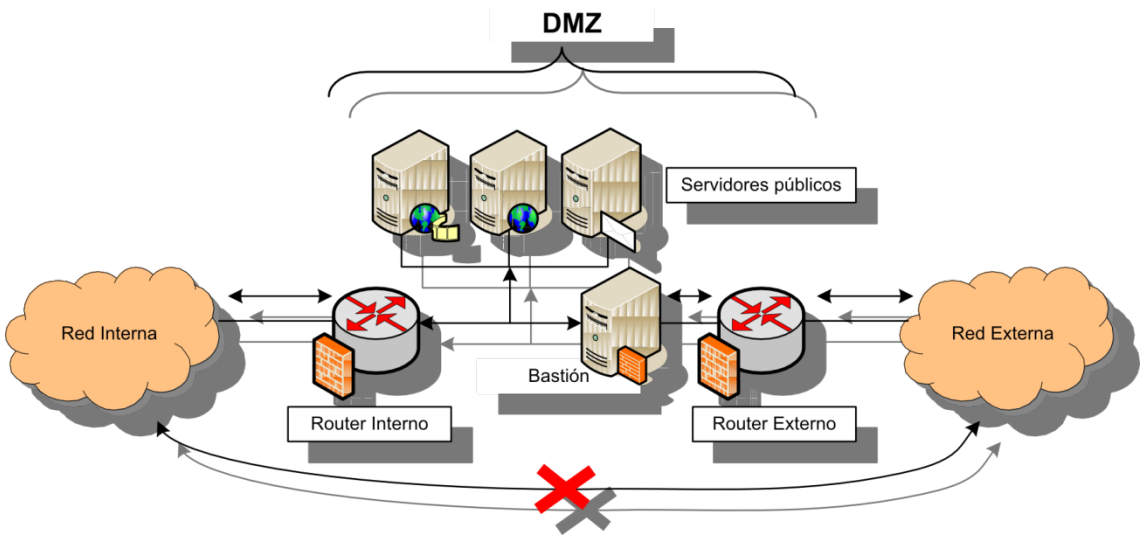
Diseño del firewall

- Screened host
  - Combina host-bastión + router
  - El router filtra paquetes
  - El host ejecuta los proxies

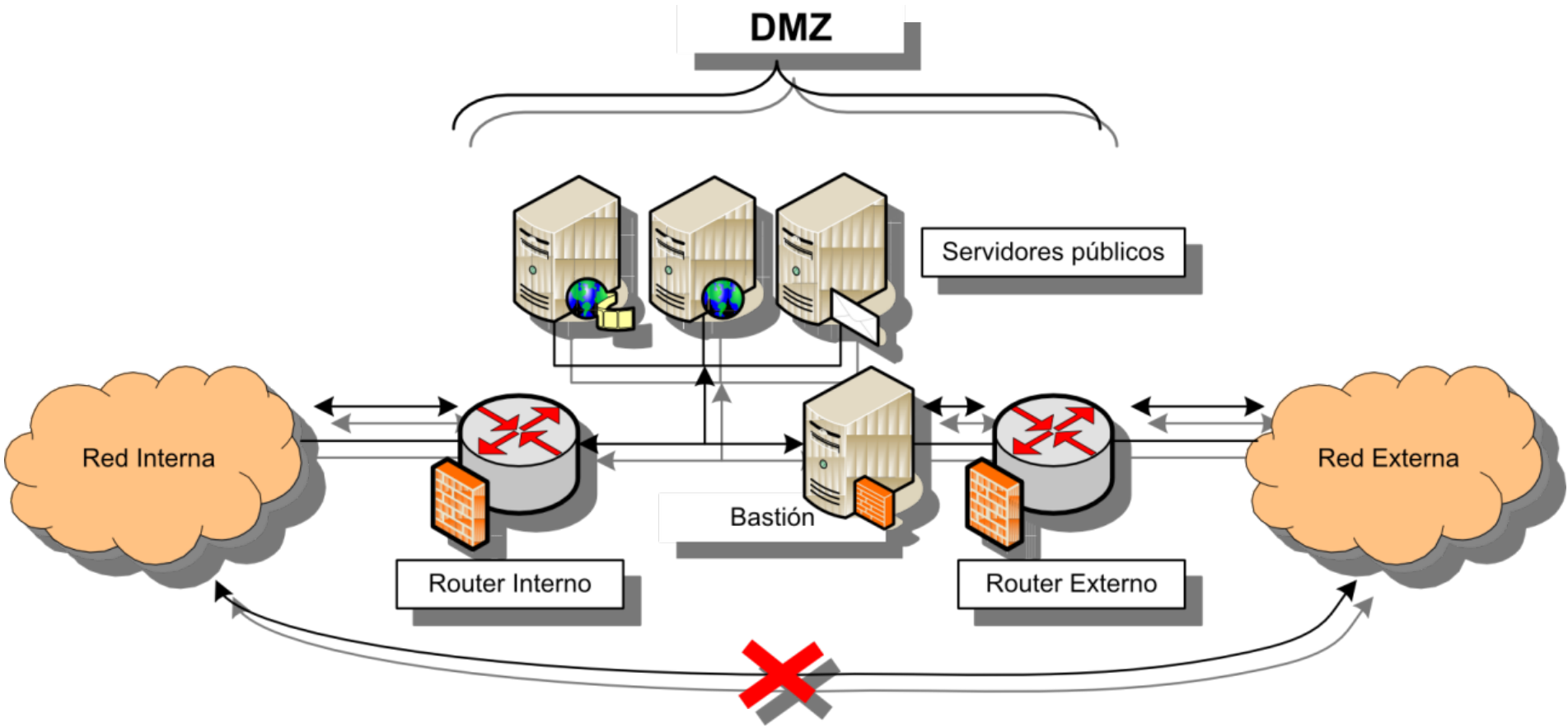


Diseño del firewall

- DMZ Screened Subnet
  - Es una de las más utilizadas
  - Se añade una subred entre la interna y externa
  - Si falla la seguridad del bastión no se compromete la red interna



Diseño del firewall



Diseño del firewall

- DMZ Screened Subnet Ventajas
  - Sólo se permiten conexiones hacia el bastión.
  - Soporta servicios mediante proxy (bastión).
  - Soporta filtrado de paquetes (routers).
  - Si el atacante entra en el bastión, todavía tiene un router por delante.
  - En ningún momento el exterior puede saturar la red interna, ya que están separadas.
  - En ningún momento se puede monitorizar (sniffer) la red interna en el caso de que el host bastión fuera saboteado.
- DMZ Screened Subnet Inconvenientes:
  - Complicada y cara de implementar