UNIVERSIDAD AUTONOMA METROPOLITANA
Casa abierta al tiempo Azcapotzalco

Tema 1. Generalidades de la seguridad en redes

Arturo Zúñiga López
Departamento de Electrónica

Introducción

- Con la llegada de las computadoras personales, las LAN y la Internet, las redes de hoy tiene que ser más abiertas.

Introducción

- Fallos del sistema (bugs)
  - Bugs: es simplemente una propiedad no deseada de un sistema
- Todos estos bugs y vulnerabilidades hacen que sea difícil conseguir que un sistema, sea seguro.
  - Los sistema seguros son difíciles de obtener

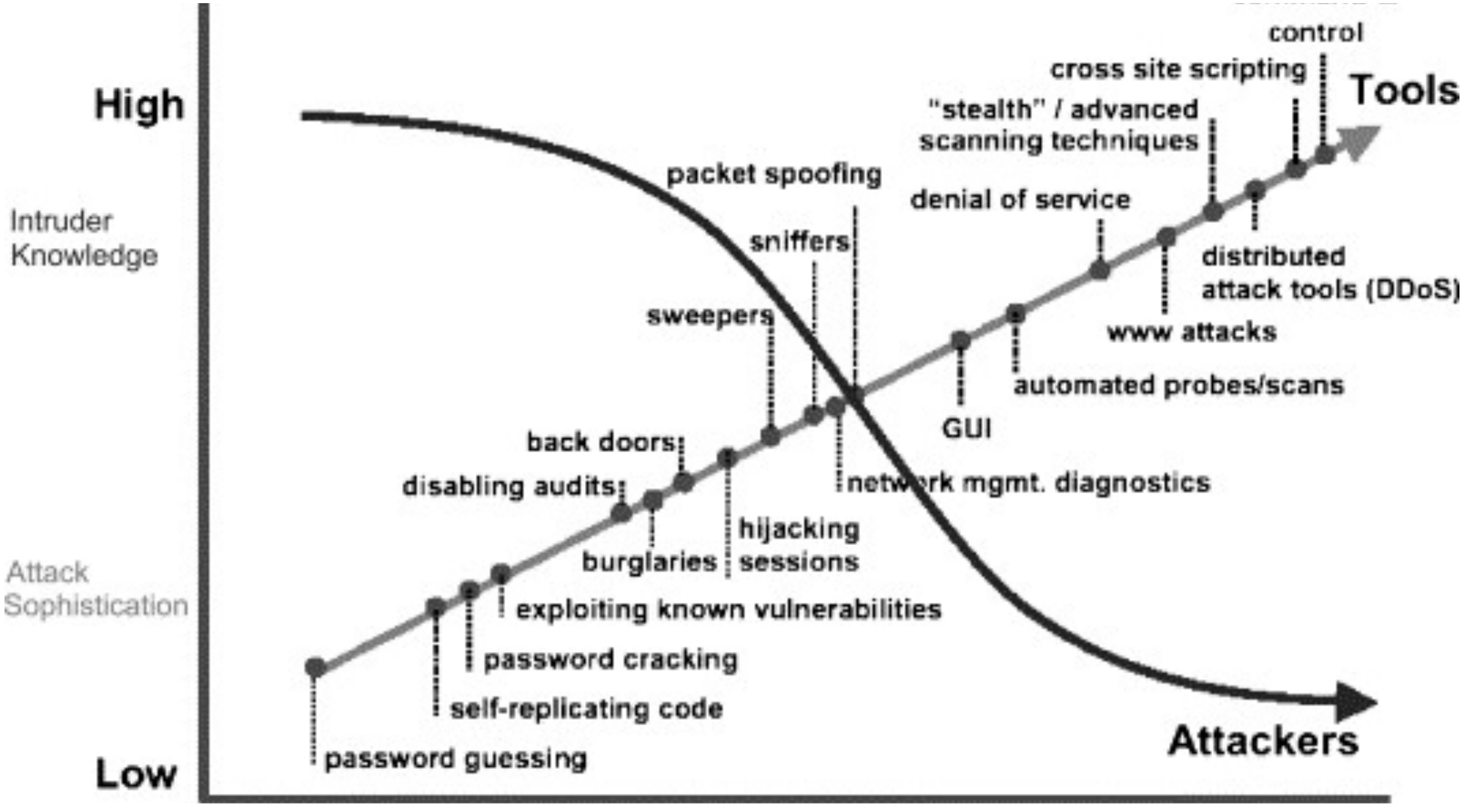
Preguntas relevantes

- ¿Que es lo que se quiere tener protegido?
  - Activos
- ¿Contra quien se quiere proteger?
  - Algunos Datos
    - 60% de los ataques se realizan desde el interior de la organización.
    - 60% de los ataques son mediante conexiones desde la red Internet.
    - 70 a 80 % de las empresas en México han sido hackeadas.
  - Los actores principales
    - Empleados
    - Defensores de los derechos civiles (extremistas)
    - Hacker
    - Un caso especial es Anonymous

Hacker

- La palabra hackers tiene una variedad de significados.
- El hacking comenzó en la década de los 60s con el phone freaking o phreaking.
- Ejemplos de ataques:
  - 1978 primer spam en ARPANET
  - 1988 virus Morris en internet
  - 1999 virus Melissa de correo electrónico
  - 2000 ataque DoS Mafiaboy, gusano Love Bug
  - 2004 Botnet ataca los sistemas militares de EUA
  - 2007 Storm botnet, filtrado de datos de tarjetas de crédito
  - 2013 Creció internacionalmente el uso ransomware
  - 2016 Ataque de DDoS (malware Mirai) a la empresa DyN
  - 2017 Ataque de phishing a usuarios de Gmail
  - 2017 WannaCry, el ransomware que sacudió al mundo

Hacker

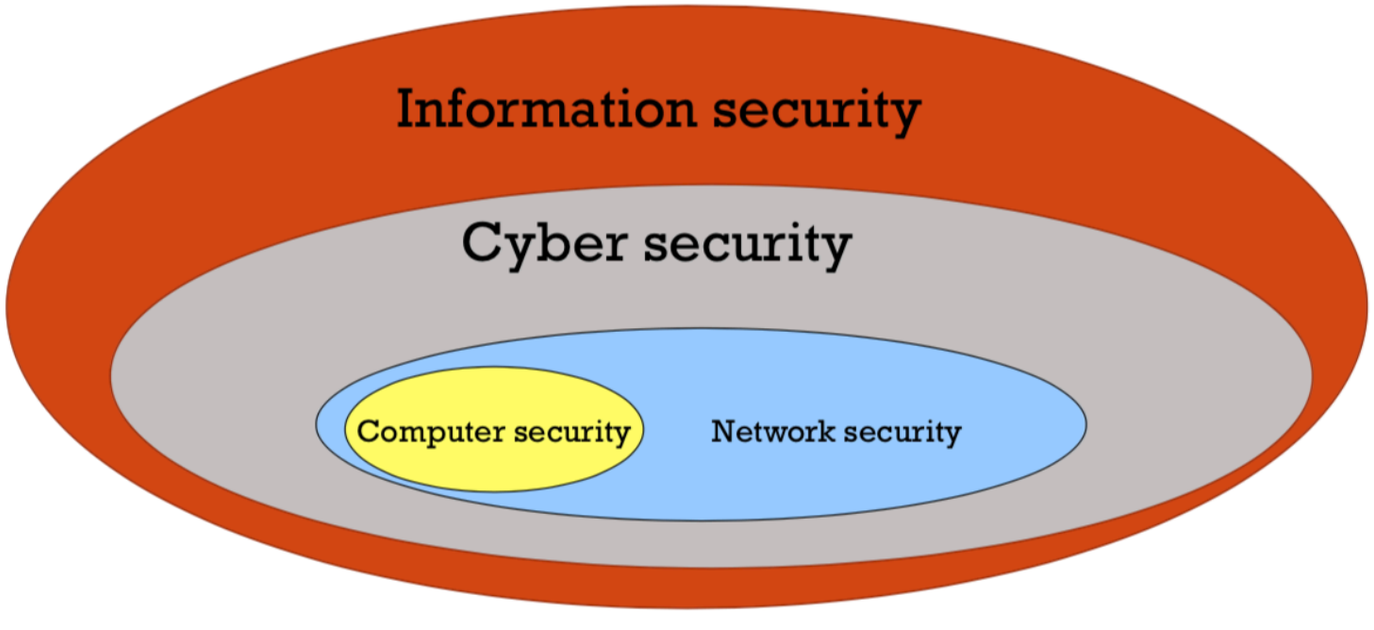

High
Intruder Knowledge
Attack Sophistication
Low
Tools
Attackers
control
cross site scripting
"stealth" / advanced scanning techniques
packet spoofing
denial of service
sniffers
distributed attack tools (DDoS)
sweepers
www attacks
automated probes/scans
GUI
back doors
disabling audits
network mgmt. diagnostics
hijacking sessions
burglaries
exploiting known vulnerabilities
password cracking
self-replicating code
password guessing

Preguntas relevantes

- ¿Cómo se quiere proteger?
  - Conocer los distintos tipos de ataques posible.
  - Conocer las distintas defensas posibles.
- ¿Cuanto dinero se puede emplear en implementar el proceso de seguridad?

¿Qué es la seguridad?

- Seguridad se utiliza en el sentido de minimizar las vulnerabilidades de los bienes y recursos.
- Seguridad informática: La protección otorgada a un sistema de información para alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información (software, hardware, telecomunicaciones, etc.)
- Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red. A través de procedimientos basados en políticas de seguridad.



¿Qué es la seguridad?

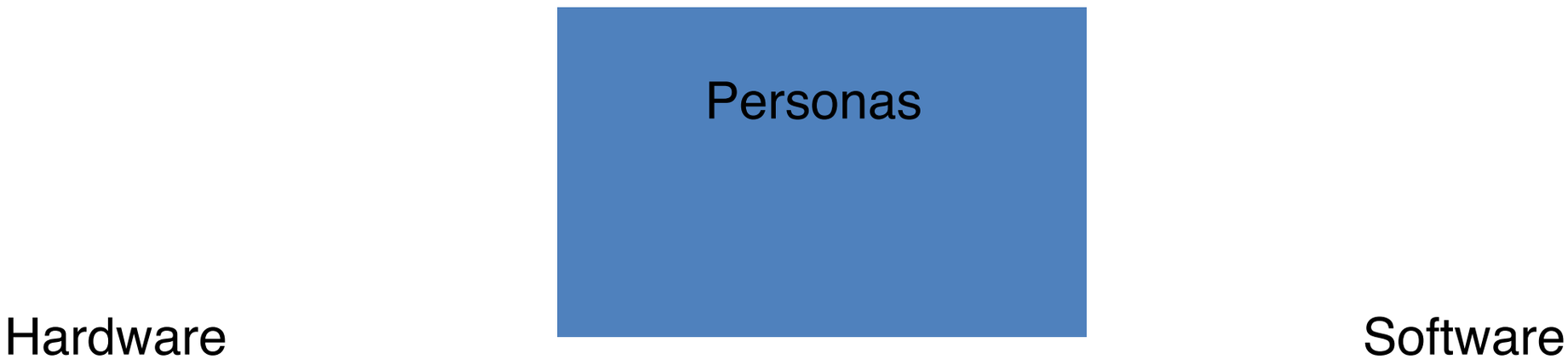
- Confidencialidad:
  - Confidencialidad de datos
  - Privacidad
- Integridad
  - Integridad de datos
  - Integridad de sistemas
- Disponibilidad

Elementos principales a proteger

- Hardware: Conjunto formado por todos los elementos físicos de una red.
- Software: Conjunto de programas que hacen funcionar el hardware.
- Datos: Conjunto de información lógica que maneja el software y el hardware.

Triangulo de debilidades

Información



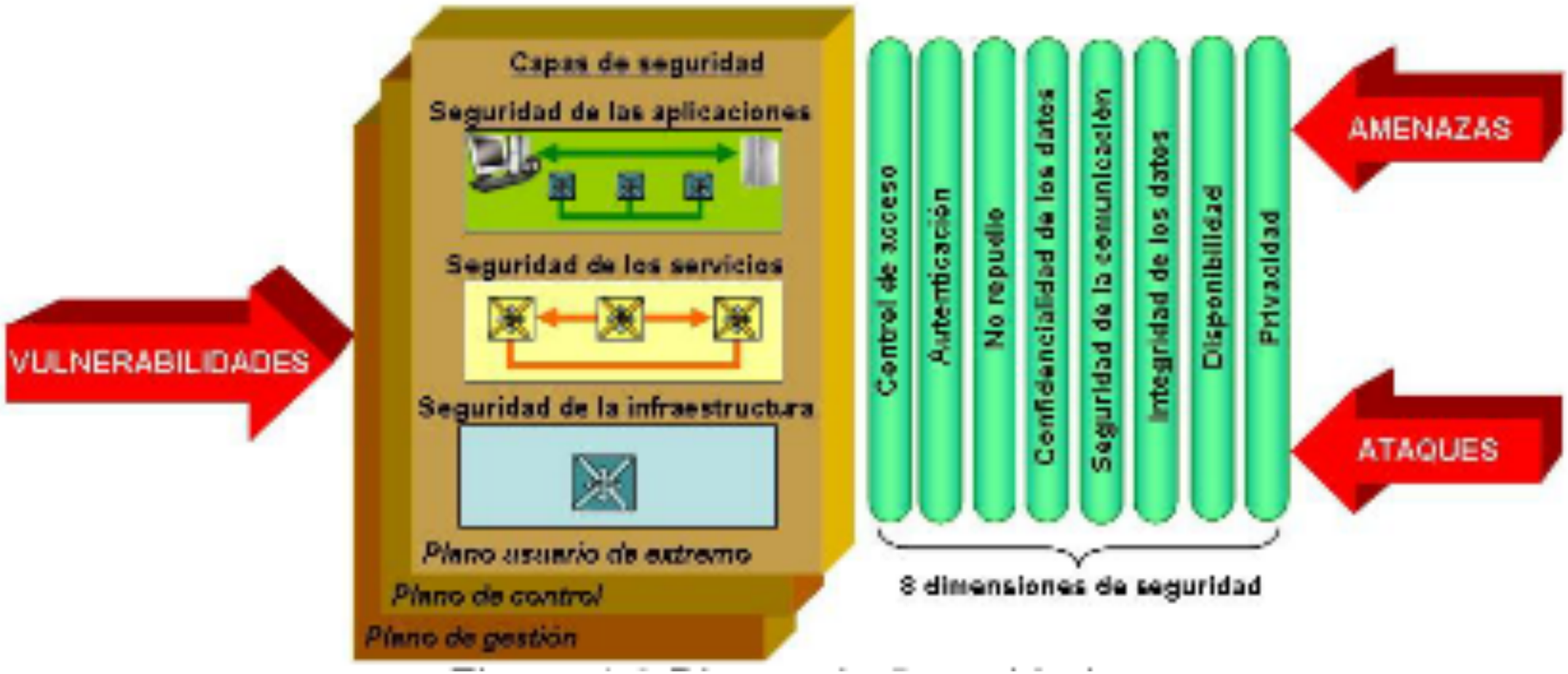
Definiciones

- Vulnerabilidad = Debilidad
- Amenaza = Probabilidad de que un hecho que pueda provocar un daño ocurra
- Ataque= Acción cuyo objetivo es provocar daño.
- Riesgo = Posibilidad de que, ante un ataque, nos veamos perjudicados

Arquitectura de seguridad para OSI

- Hay un estándar (ITU-T X.805)
- Integra las consideraciones de gestión, control y utilización de la infraestructura, los servicios y las aplicaciones de red.
- Integra tres consideraciones esenciales, para la seguridad extremo a extremo.
  - ¿Qué tipo de protección se necesita y contra qué amenazas?
  - ¿Cuáles son los diferentes conjuntos de equipos e instalaciones de red que se necesita proteger?
  - ¿Cuáles son las diferentes actividades de red que se necesita proteger?

Arquitectura de seguridad en redes



Dimensión de seguridad	Descripción	Ejemplo
Control de Acceso	Límite y control en el acceso a los elementos de red, servicios y aplicaciones	Password,
Autenticación	Garantía de la procedencia de la información	Password c digitales, et
No-repudio	Garantía de que no se puede negar cualquier tipo de actividad de red	Bitácoras, s digitales, et
Confidencialidad de los datos	Garantía de que la información solo es accesible por las entidades, sistemas o personas autorizadas	DES, AES,
Comunicación segura	Garantía de que la información fluye desde la fuente al destino	Frame Rela
Integración de los datos	Garantía de que la información no ha siso modificada o corrompida de manera alguna, desde su transmisión hasta su recepción	MD5, firma
Disponibilidad	Garantía de que los elementos de red, servicios y aplicaciones, se mantengan disponibles para los usuarios legítimos	IDS, IPS, re

Una red segura

- La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más delante de los hackers malintencionados.
- La complejidad de la seguridad en redes dificulta dominar todo lo que esta abarca.
- Todas las practicas de seguridad en redes están relacionadas con políticas de seguridad.
- Los virus, los gusanos y los troyanos son tipos específicos de ataque a las redes.

¿De qué nos queremos proteger?

- Los riegos se cuantifican en varios factores
  - Las amenazas existentes para los activos a proteger
  - La vulnerabilidad de estos activos
- Algunos criterios para clasificar ataques y amenazas pueden ser
  - El origen del ataque
  - La complejidad
  - El objetivo

Ataques según su origen

- Hay que aclarar que las las redes de datos son atacadas principalmente por personas.
- Su origen
  - Externos
  - Internos
    - Las amenazas internas básicamente son dos:
      - Ataques de falsificación
      - Ataques de DOS

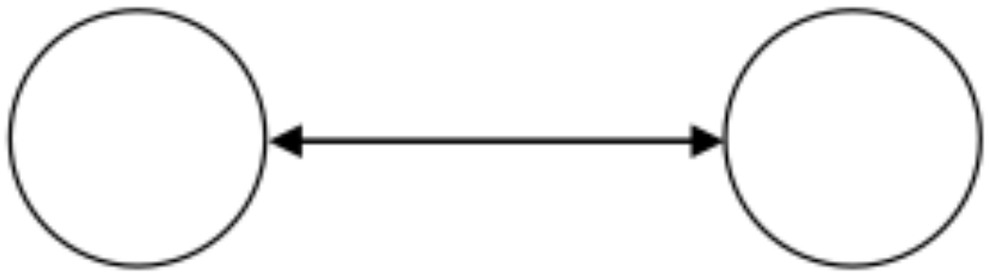
Ataques según la complejidad

- No estructurados: No se define un objetivo especifico.
- Estructurados: Son ataques que se enfocan como un proyecto

  – En estos tipos de ataque intervienen las personas
    - Atacantes pasivos: son aquellos que fisgonean por el sistema pero no lo modifican o destruyen
    - Atacantes activos: aquellos que dañan el objetivo atacado

Ataques según su objetivo

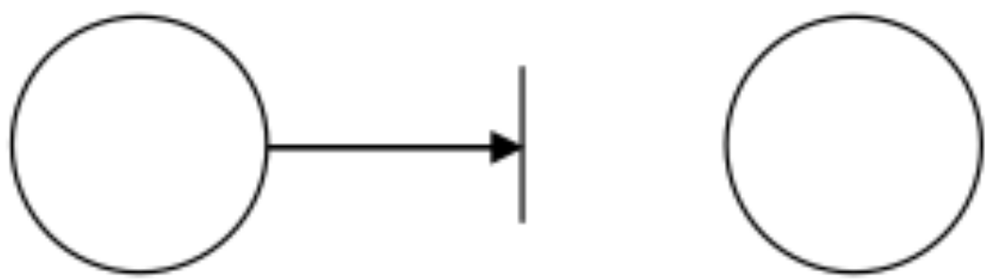
- En general en un sistema se genera un flujo de información desde su origen hacia un destino



Ataques según su objetivo

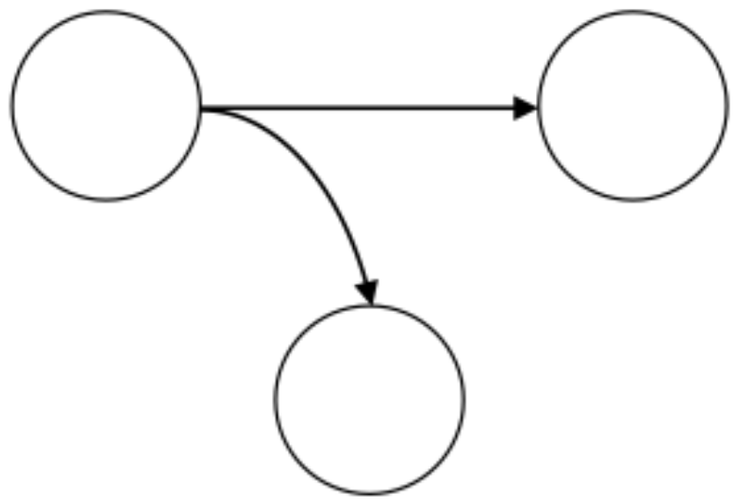
- Cuatro categoría muy generales de ataques son:

- Interrupción: Es hacer inaccesible un elemento del sistema
  - Es un ataque a la disponibilidad (hardware o software)
  - Su detección puede ser inmediata



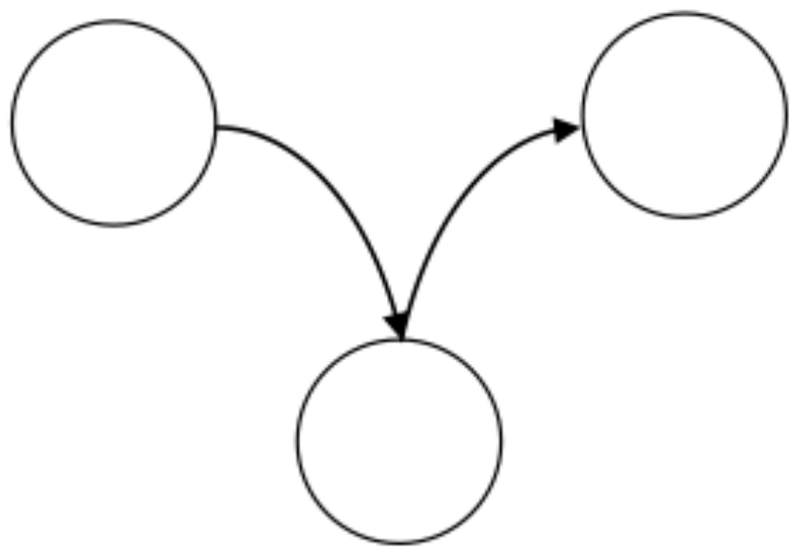
Ataques según su objetivo

- Interceptación: Tiene lugar cuando una parte no autorizada consigue acceder a un elemento durante la comunicación.
  - Este es un ataque a la confidencialidad.
  - Su detección es difícil. A veces no deja huella.



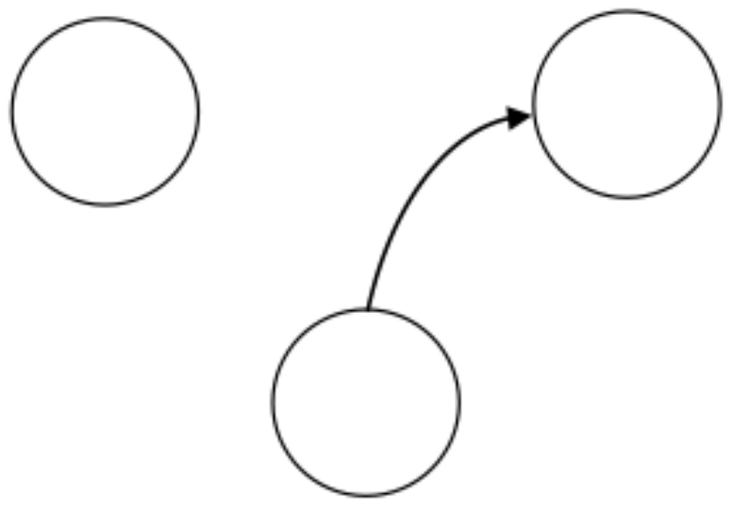
Ataques según su objetivo

- Modificación: Se produce cuando una parte no autorizada no sólo consigue acceder a la información no autorizada, sino que también la modifica en tránsito.
  - Es un ataque a la confidencialidad y a la integridad
  - Su detección puede ser fácil o difícil.



Ataques según su objetivo

- Invención o generación: Una parte no autorizada inserta objetos falsos en el sistema, suplantando a un emisor legitimo
  - Ataque a la autenticidad
  - Su detección es difícil . Engloba delitos de falsificación y suplantación de identidad



Amenazas y ataques

- Amenazas lógicas: se encuentra todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema.
  - Software incorrecto
  - Herramientas de seguridad
  - Puertas traseras
  - Canales abiertos
  - Virus
  - Gusanos
  - Caballos de Troya

Amenazas y ataques

- Ataques: En los primeros años los atacantes involucraban poca sofisticación técnica.
- Actualmente los ataques son cada vez más sofisticados, y a la vez se requieren menos conocimientos técnicos para llevarlos a cabo

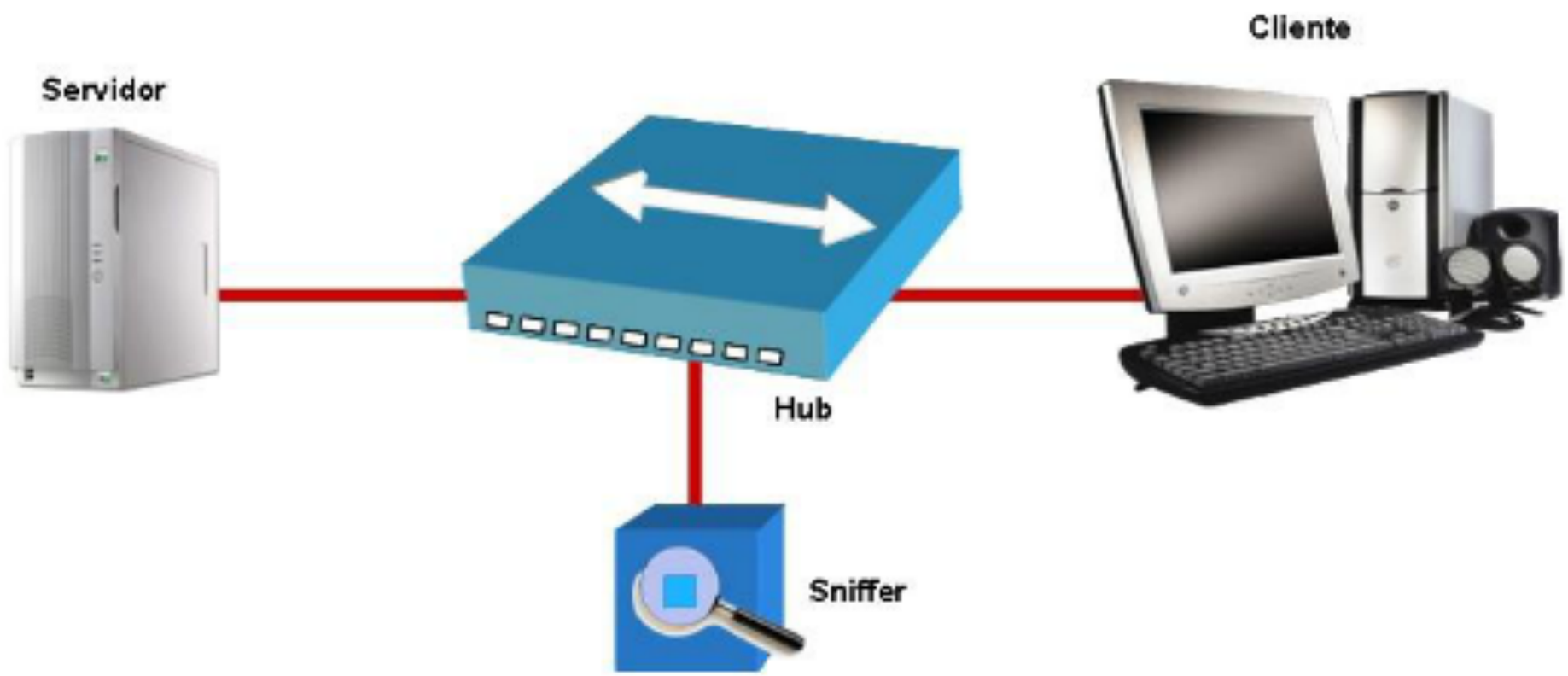
- Métodos de Reconocimiento
- Ataques de Acceso
- Ataque de DoS (Negación de Servicio)
- Software Malicioso

Métodos de Reconocimiento

- Reconocimiento: es el descubrimiento no autorizado y el mapeo de redes, sistemas, dispositivos, servicios y vulnerabilidades.
- Algunos de los métodos más comunes:
  - Packet Sniffing (Eavesdropping)
  - Descubrimiento de hosts
  - Escaneo de puertos
  - OS/fingerprinting
  - Application fingerprinting
  - Ingeniería social
  - Keylogging
  - Phishing

Eavesdropping

- El espiar (snooping) y el observar los paquetes en la red (sniffing) son términos comunes para el eavesdropping.



Eavesdropping

- Esto se realiza con unos programas denominados “sniffers”
- Normalmente los buenos sniffers no se pueden detectar
  - Wireshark
  - Tcpdump
  - Dsniff
  - Darkstat
  - Ettercap
  - Cain & Abel
  - WinDump
  - Airodump-ng
- Contramedidas: Cifrado de conexiones

Escaneo

- Es un método para descubrir canales de comunicación susceptibles de ser explotados.
  - Ping-sweepers (herramientas de barrido de ping)
    - Herramientas TCP-ping (hping)
  - Escáneres de puertos.

Estados de puertos

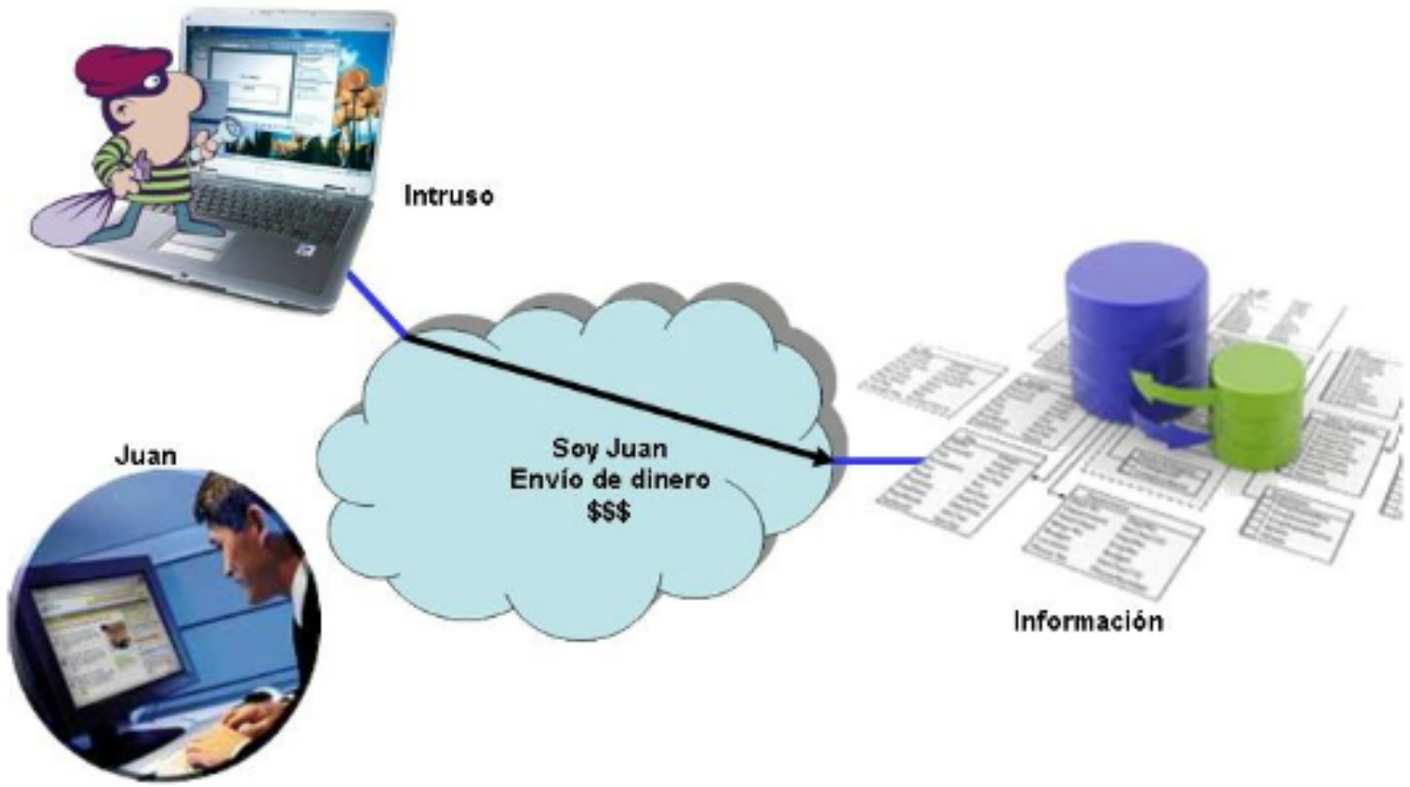
- Abierto: un puerto en este estado está disponible y escuchando por conexión
- Cerrado: no tiene una aplicación o servicio asociado que responda a las solicitudes de conexión.
- Filtrado: no es posible de ser accesado porque existe un dispositivo que filtra los paquetes (router o firewall)
- No-filtrado
- Abierto / filtrado
- Cerrado / filtrado

Medidas defensiva

- Evitar ataques de reconocimiento es virtualmente imposible
  - Algunas medida
    - Minimizar la exposición, haciendo público sólo aquello que por necesidad debe serlo.
    - Confinar servidores en zonas desmilitarizadas (DMZ)
    - Instalar medidas de seguridad perimetral (firewalls, sistemas IDS/IPS, etc.)
    - Implementar medidas para protección de datos

Amenazas y ataques

- Acceso: Es la capacidad para que un intruso desautorizado acceda a un dispositivo para el cual no tiene una cuenta o una contraseña



Amenazas y ataques

- Algunos ejemplos de ataque por acceso

Método	Ejemplos
Aprovechando el uso de contraseñas fáciles de adivinar	Fuerza Bruta Ataque con diccionarios
Aprovechando los errores o agujeros de las aplicaciones	Ataques a través de código específicos
A través de los Caballos de troya	Backdoors, Back Orifice, N
Ingeniería social	Pishing, caracterizado por información confidencial d

Método
Ataque Hombre en medio (Man in the middle attack)
Aprovechando relaciones de confianza entre servidores
Ataque por manipulación de datos
IP spoofing (IP falsificada)
Programas auto ejecutables (Autorooters o BOTS)

Spoofing (Suplantación de identidad)

- El objetivo de esta técnica es actuar en nombre de otro usuario.
- Una forma común de spoofing es conseguir el nombre y password de un usuario.
  - IP Spoofing
  - DNS Spoofing
  - Mail Spofing
  - ARP Spoofing
  - WebSpoofing

Negación de servicio

- DoS (Negación de servicio): La negación del servicio implica que un atacante inhabilite o corrompa las redes, los sistemas o los servicios con la intención de negar la disponibilidad de los servicios a los usuarios previstos
- A través de este ataque se intenta quebrantar los sistemas o hacerlos tan lentos al punto de que sean inutilizados

Negación de servicio

- DoS
  - E-mail bombs
  - E-mail spamming
  - CPU hogging (la mayoría programas Java, JavaScript)
  - Inundación con paquetes SYN (SYN Flood). Este ataque suele combinarse con IP spoofing

Buffer Overflow

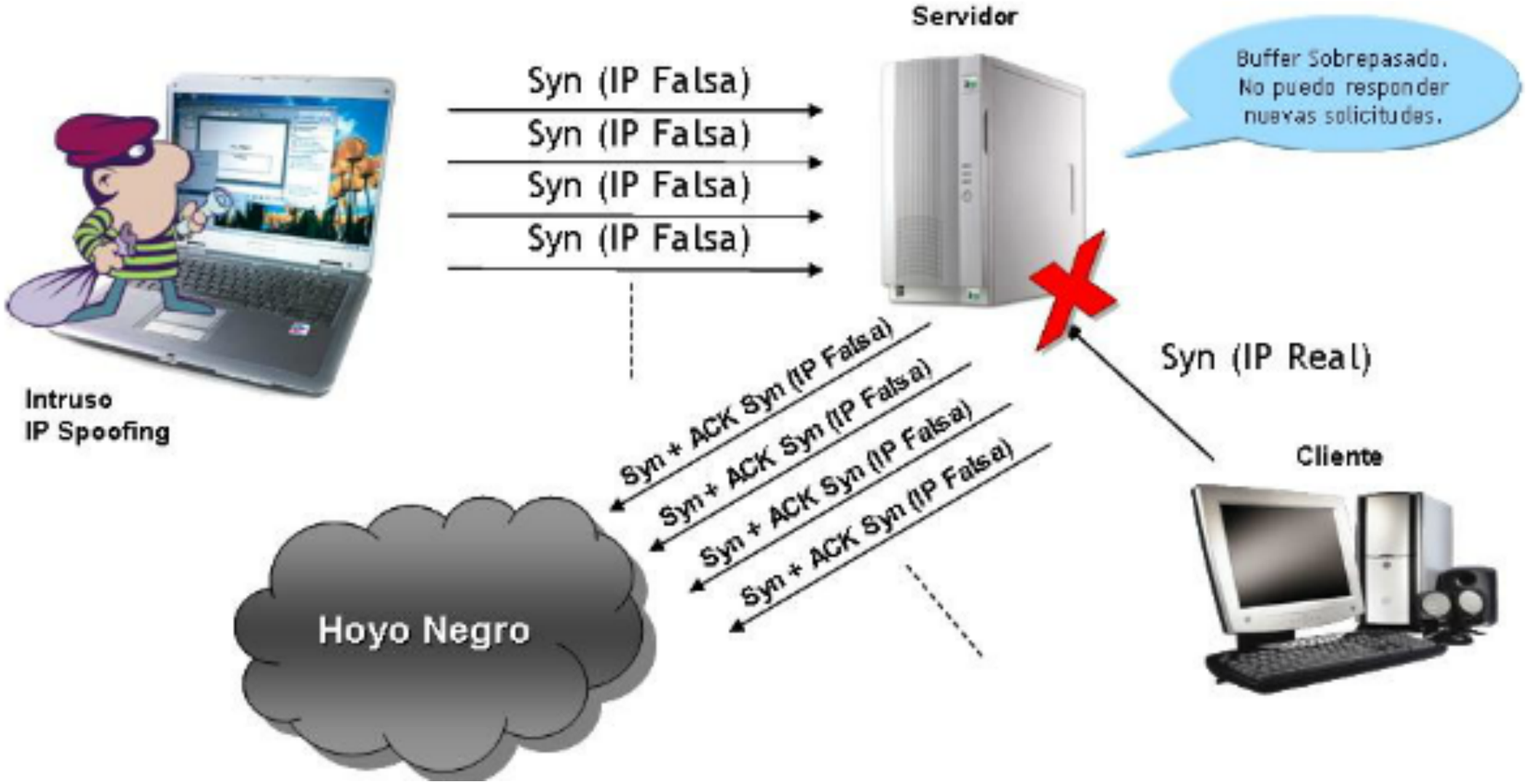
- Ataque de denegación de servicio clásico
- Un servicio o aplicación responde ante la recepción masiva de datos con un error de ejecución

Ping de la muerte

- IP ping > 65535 byte (ICMP echo request)
  - Enviar paquetes > 65535 bytes viola el protocolo IP
- Transmitidos en fragmentos
- Puede tirar a algún host al ensamblarse
- Los sistemas operativos moderno. (posteriores a 1997/1998) no son vulnerables a este ataque.

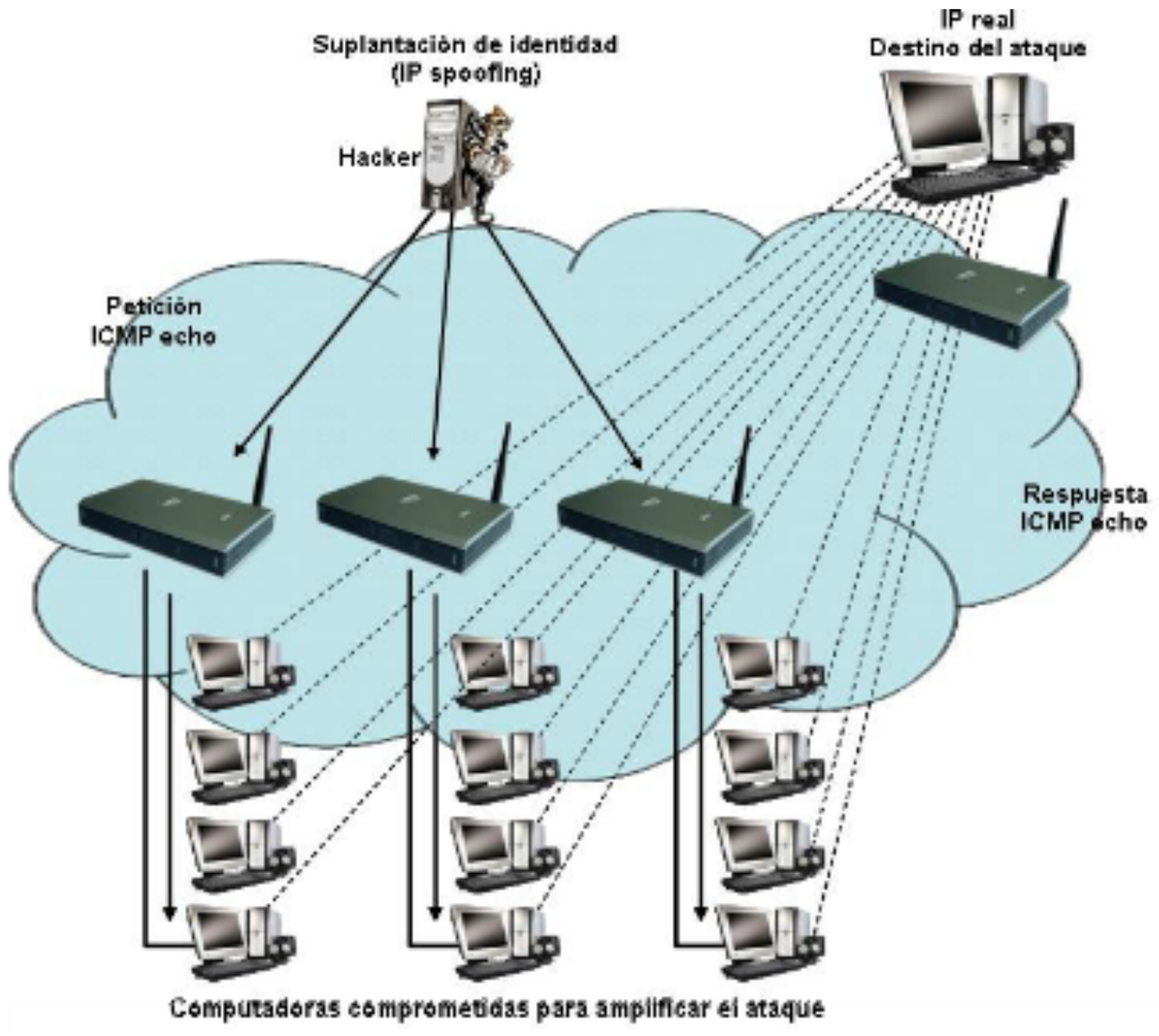
Amenazas y ataques

- Inundación con paquetes SYN (SYN Flood). Este ataque suele combinarse con IP



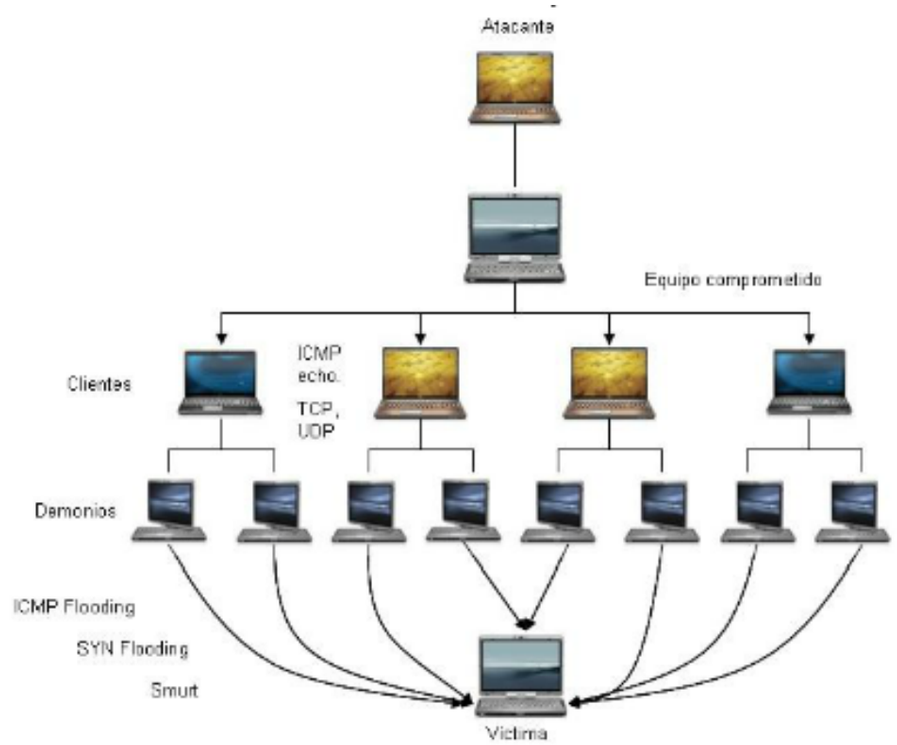
Amenazas y ataques

- DDoS: Se diseñaron para saturar los enlaces de la red con datos no deseados, provocando que el tráfico legítimo no puede ser transmitido. Ejemplo Smurff



Denegación de servicio

- TFN (Tribe Flood Network): son aplicaciones usadas para lanzar ataques DoS coordinados desde muchas fuentes contra uno o más blancos



Software malicioso (Malware)

- Es un software con intenciones maliciosas y que normalmente realiza acciones que el usuario no pretendía.
- La seguridad en redes esta relacionado con el Malware cuando éste se mueve a través de la red, a veces replicando y propagándose de un sistema a otro.
- Tipos básicos de Malware
  - Virus
  - Gusanos
  - Troyanos
  - Malware combinado o híbrido
  - Código web malicioso

Virus

- Código parasitario que se adjunta/inserta en los archivos de programa
- Eso sistema es infectado típicamente cuando el usuario ejecuta el código
- Tipos de daños
  - Destruir datos, degradar el rendimiento del sistema.
- Tipos
  - Virus de programa
  - Boot sector/ Registry Malware
  - Virus en una Macro

Gusanos

- La RFC 1135: Un gusano es un programa que puede ejecutarse de forma independiente, consumirá los recursos de su host y puede propagar una versión de trabajo completa de sí mismo en otra maquina.
- Normalmente se usa una vulnerabilidad conocida para infectar el sistema.
- Normalmente puede propagarse sin la interacción del usuario.
- Rapida propagación
- Normalmente, los gusanos no dañan el sistema en sí, pero pueden reducir rápidamente la disponibilidad en las redes y atar los recursos de las maquinas infectadas

Troyanos

- Diseñado para ocupar el lugar de un archivo o aplicación válido
- Los gusanos y virus se pueden usar para soltar Malware troyano.
- Se incluyen a los rootkits y troyanos de acceso remoto.

Rasonware

- Dos tipos
  - Denegación de acceso al sistema.
  - Encriptar archivos de la maquina víctima.