1 AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Objetivo

- Describir los ataques más dañinos y predominantes en Internet, incluyendo los ataques de software malicioso, para identificar las propiedades deseables en una comunicación segura.

Manual de clases

Última modificación:
18 de junio de 2022

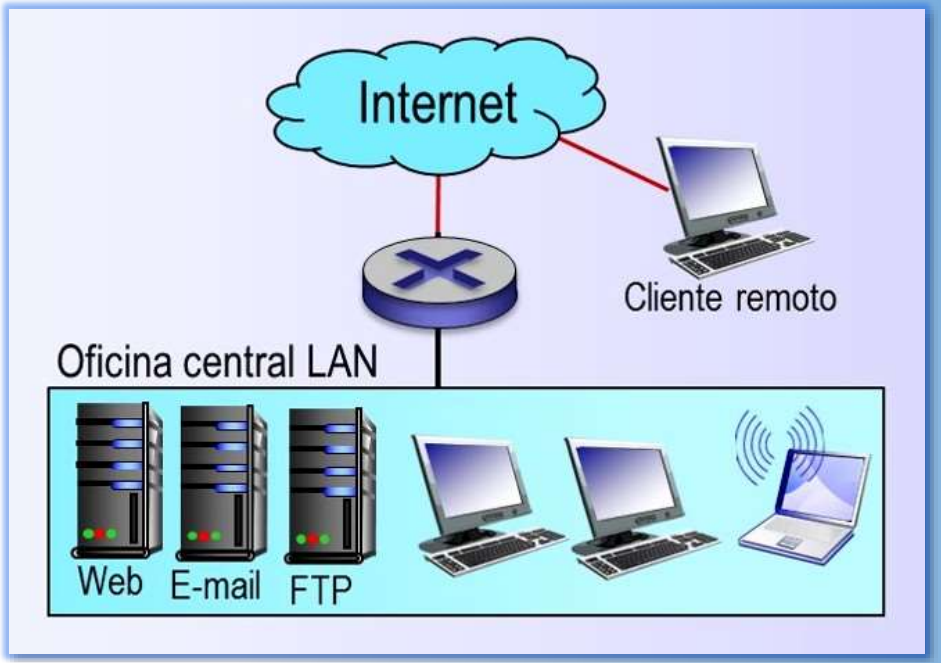
Tema 1 de:
SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.

0. ESTUDIO DE CASO – SEGURIDAD EN REDES

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Escenario de las redes

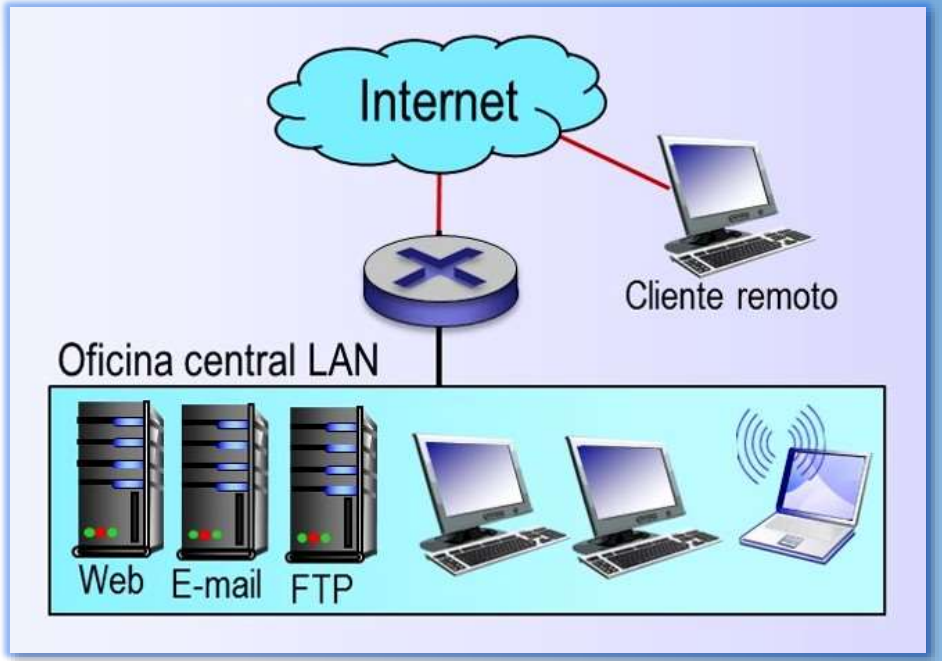


- **Una empresa** recién constituida contrata servicios especializados para evaluar las medidas de seguridad de su arquitectura de red informática.
  - ▶Según el diagrama previo elaborado (topología lógica y física), todos los hosts se conectan directamente a Internet a través de un router, lo cual podría acarrear problemas.
  - ▶¿Qué soluciones se propondrían para conseguir una red más segura?
- **Un análisis de seguridad** arroja el siguiente diagnóstico.
  - ▶Es una red plana.
  - ▶No hay elementos de monitorización.
  - ▶No se filtra tráfico de entrada ni de salda.
  - ▶Los servicios internos, como bases de datos, son públicos.
  - ▶No se verifica malware o spam en el correo electrónico.
  - ▶El cliente remoto accede directamente a servicios.
- **Surge la pregunta**: ¿cómo se aborda la seguridad en redes?

Estudio de caso – Seguridad en redes

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Cómo se aborda la seguridad en redes?



- ▶**1. Identificar amenazas**. Surgen las preguntas: ¿qué es lo que puede ir mal? ¿en qué sentido son vulnerables las redes de computadoras? ¿Cuáles son los tipos de ataques hoy día? Se recopila información sobre los problemas de seguridad que predominan en la actualidad.
- ▶**2. Definir escenario de seguridad**. Se identifican y definen las propiedades deseables en una comunicación segura.
- ▶**3. Analizar herramientas para seguridad**. Se analiza cómo pueden utilizarse los principios fundamentales de la criptografía para crear protocolos de red seguros.
- ▶**4. Seleccionar protocolos seguros.** Se analizan y seleccionan los protocolos seguros en cada una de las cuatro capas superiores, comenzando por la capa de aplicación.
- ▶**5. Seleccionar dispositivos de seguridad operacional**. Se considera la seguridad operacional, la cual se ocupa de la protección de las redes institucionales frente a los ataques. En particular, firewalls y los sistemas de detección de intrusos.

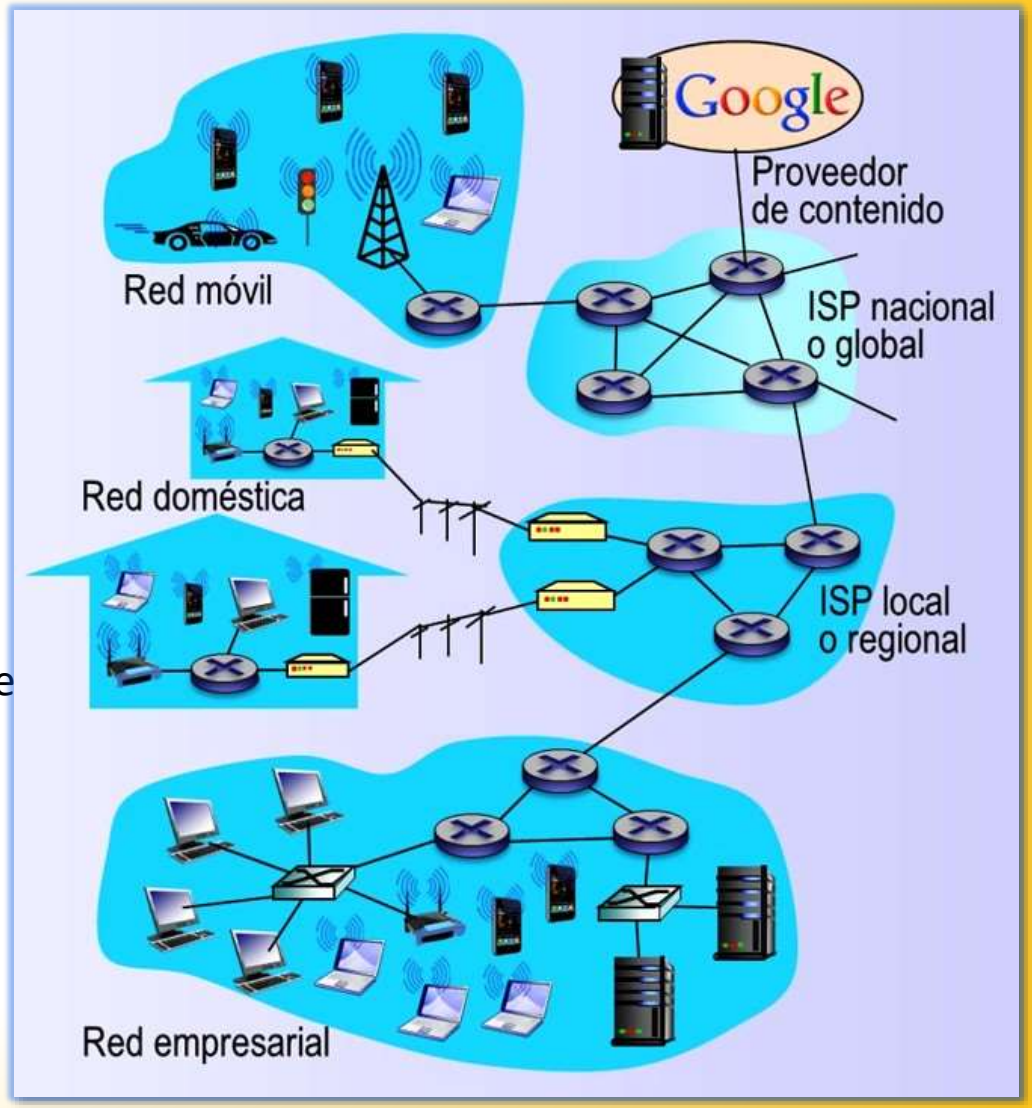
1. LA SEGURIDAD EN REDES

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

(Kurose, 2017)

¿A qué hace referencia la seguridad en las redes?

- **Internet** se ha convertido en una herramienta crítica para muchas instituciones, incluyendo empresas pequeñas y medianas, universidades y organismos gubernamentales.
- **Muchas personas** confían en Internet para llevar a cabo sus actividades profesionales, sociales y personales. Miles de millones de "cosas" (incluyendo dispositivos corporales y electrodomésticos) se conectan hoy en día a Internet.
- **Detrás** de todas estas utilidades y toda esta excitación, hay un lado oscuro: desde el punto de vista de un administrador de red, el mundo se divide de forma bastante nítida en dos bandos:
  - ▶Los buenos, aquellos que pertenecen a la red de la organización y que deben poder acceder a los recursos internos de la misma de una forma relativamente poco restringida y….
  - ▶Los malos, todos los demás, aquellos que deben ser cuidadosamente escrutados a la hora de acceder a los recursos de la red.
- **El campo de la seguridad de red** se ocupa de ver cómo "los malos "pueden atacar a las redes de computadoras y cómo se las puede defender de esos ataques, o mejor todavía, de cómo diseñar nuevas arquitecturas que sean inmunes a tales ataques.

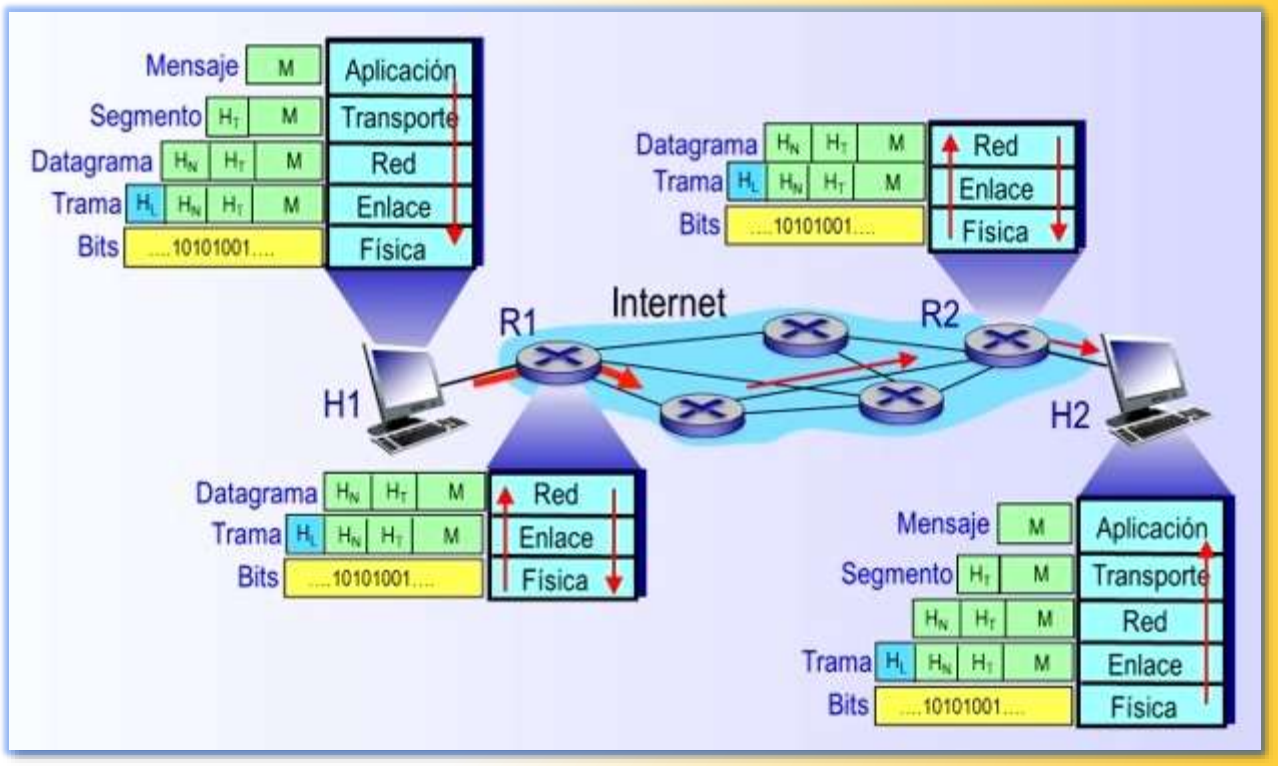


AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Por qué Internet se ha convertido en un lugar inseguro?

(Kurose, 2017)

- **Básicamente**, la respuesta es que Internet fue diseñada originalmente de esa manera, ya que se basaba en el modelo de un “grupo de usuarios que confiaban entre sí, conectados a una red transparente”, un modelo en el que, por definición, no había necesidad de pensar en la seguridad.
- **Muchos aspectos** de la arquitectura de Internet original reflejan profundamente esta idea de confianza mutua.
  - Por ejemplo, la posibilidad de que un usuario envíe un paquete a cualquier otro usuario es la opción predeterminada, al igual que lo normal es creer que la identidad del usuario es la que declara, en lugar de autenticarle por defecto.
- **Pero actualmente Internet** no implica realmente "usuarios de confianza mutua”.



- **Sin embargo**, los usuarios de hoy día necesitan comunicarse aunque no necesariamente confíen entre sí. Pueden desconfiar del hardware, del software e incluso del aire a través del que se comunican.
- **Se tiene que tener presente** que la comunicación entre usuarios de mutua confianza es la excepción, mas que la regla. Este es el mundo de las redes modernas de comunicaciones.

2.- ATAQUES A LAS REDES MODERNAS

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Qué son los ciberataques y qué tipos existen?

- **¿Qué es un ciberataque?** Es un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos o redes de computadoras. El objetivo es dañar, alterar o destruir organizaciones o personas. Además, pueden anular los servicios que prestan, robar datos o usarlos para espiar.

ATAQUE DDOS

Sucede cuando un grupo de personas o automatismos atacan a un servidor u ordenador desde muchos equipos a la vez. Esto provoca que los recursos del servidor acaben no siendo suficientes, se colapse y deje de funcionar. Si se trata de un equipo que mantiene una web, servicio o comunidad, esta cae con el servidor.

INGENIERÍA SOCIAL

Práctica para obtener información confidencial a través de la manipulación de usuarios. Una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos.

ROBO DE IDENTIDAD

Obtener información personal como contraseñas, números de identificación, números de tarjetas de crédito o datos personales con la intención de actuar de manera fraudulenta en nombre de la víctima. La información puede ser usada para varios propósitos ilegales.

BOTNETS

Red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques DDoS sin consentimiento de los propietarios de los equipos.

PUPS

Programas Potencialmente no Deseados. Son programas que se instalan en ocasiones sin el consentimiento expreso del usuario y que pueden menoscabar el control de privacidad y confidencialidad del usuario, utilizar recursos del equipo, etc.

CIBERACOSO

Acoso o intimidación por medio de las tecnologías digitales. Sucede en redes sociales, plataformas de mensajería, plataformas de juegos o teléfonos móviles.

Ataques a las redes modernas

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Qué son los ciberataques y qué tipos existen? (cont.)

PHISHING

Envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial.

CONTENIDO ILEGAL

El contenido digital ilegal puede ser descubierto en línea en una variedad de espacios incluyendo web, redes sociales y servicios para compartir archivos.

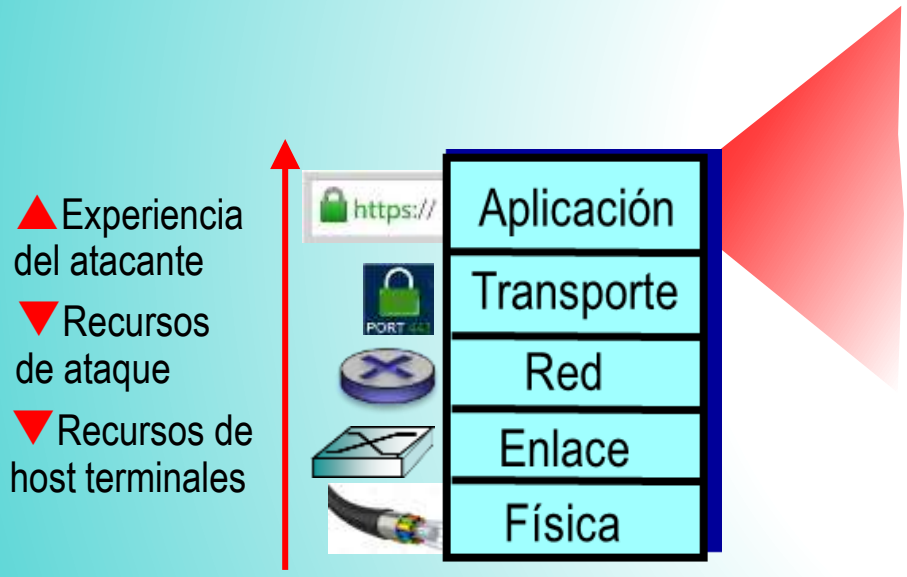
ESTAFAS EN LÍNEA

Delito que implica que una persona pretenda engañar a otra para que cometa un error que le lleve a cometer un acto de disposición en perjuicio ajeno o propio.
Siempre se hace con ánimo de lucro.
Las estafas telemáticas e informáticas tienen la misma regulación que un delito de estafa del Código Penal.

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Ataques enfocados en los protocolos de aplicación

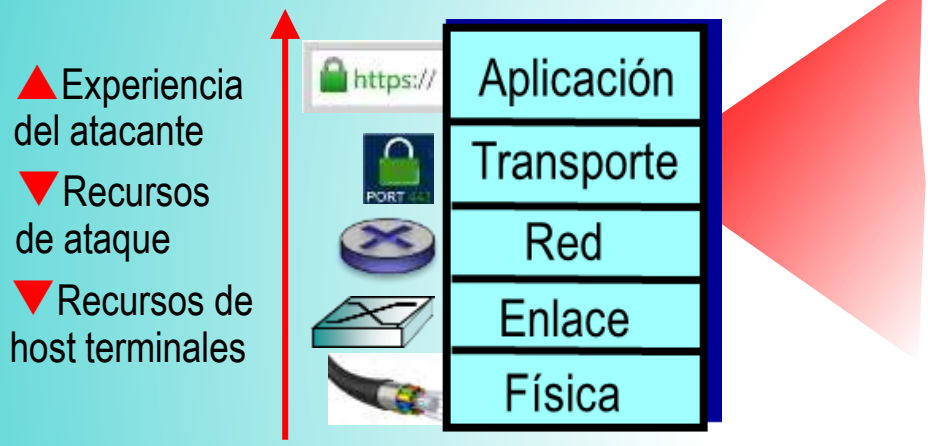
- **Ahora se analizarán** los ataques a las redes considerando la tendencia a enfocarse en aprovechar las vulnerabilidades o huecos que dejan los protocolos según las capas de modelo TCP/IP. Observe que para capas mas superiores, se necesita mayor experiencia y conocimientos informáticos por parte del atacante.



- ▶**Inundación HTTP GET**. Inundan los servidores afectando el tráfico de la red.
- ▶**Peticiones POST**. Se envían peticiones con la cabecera HTTP y luego disminuida, haciendo al servidor esperar sin rechazar la conexión.
- ▶**Slowloris**. Se sobrecarga un servidor al abrir y mantener muchas conexiones HTTP simultáneas, con el objetivo de denegación de servicio.
- ▶**Inyección SQL**. Es un método que se aprovecha de errores que existen en aplicaciones web, quebrantan las medidas de seguridad y pueden controlar la base de datos del sitio web y secuestrar la información de los usuarios.
- ▶**Inundación INVITE**. Es uno de los ataques más típicos de inundación, tanto para servidores como para terminales, modifica campos en el mensaje INVITE.
- ▶**Slow read.** Se envían peticiones HTTP legítimas pero se ralentiza el proceso de lectura de la respuesta retrasando el envío de ACK (HTTP es TCP).

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

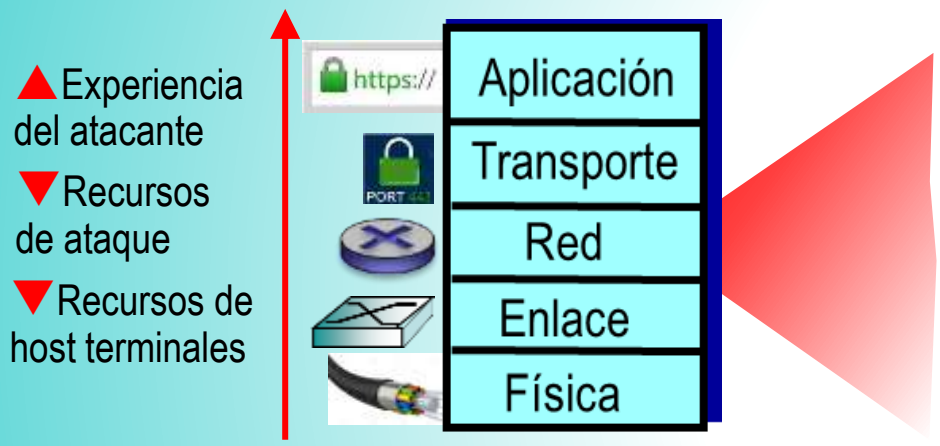
Ataques enfocados en los protocolos de transporte



- ▶**Inundación TCP SYN.** Es un ataque de denegación de servicio (DoS) que envía un número masivo de solicitudes SYN a un servidor para sobrepasar su capacidad con conexiones abiertas.
- ▶**Inundación UDP**. Es un ataque de denegación de servicio en el que se envía un gran número de paquetes UDP a un servidor para sobrecargar la capacidad de ese dispositivo para procesar y responder.
- ▶**Inundación de consultas DNS**. Es un ataque de denegación de servicio distribuido (DDos) en el que se inunda los servidores DNS de un dominio en particular en un intento de interrumpir la resolución de DNS para ese dominio.
- ▶**Ataque al protocolo SSL MiM**. Es una técnica que consiste en un ataque de hombre en el medio (Man-in-the-Middle) en el que se intercepta y redirige una conexión HTTPS de la víctima hacia otro servicio protegido con SSL o TLS. Aprovechando La confusión de protocolos se filtra información sensible.
- ▶**Ataque Land**. Es un ataque que consiste en enviar un paquete TCP SYN falso, donde la dirección IP del objetivo se utiliza tanto como de origen y de destino para confundir al objetivo cuando reciba el paquete y no sepa donde enviarlo, produciendo un bloqueo.

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

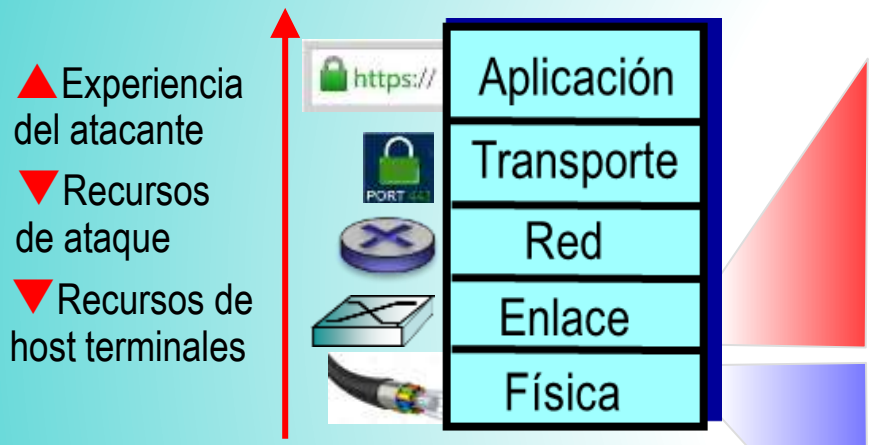
Ataques enfocados en los protocolos de red



- ▶**Ataque Smurt.** Es un ataque de denegación de servicio que intenta evitar que los usuarios legítimos tengan acceso a correo electrónico, páginas web y otros servicios que se basan en el objetivo infectado. Utiliza mensajes de ping al broadcast con suplantación de identidad para inundar el host objetivo.
- ▶**Fragmentación Teardrop**. Es un ataque de denegación de servicio. Consiste en enviar paquetes IP o fragmentos de paquetes IP que están indebidamente construidos.
- ▶**Inundación ICMP**. Es un ataque de denegación de servicio en el que se intenta sobrecargar un dispositivo objetivo con paquetes de solicitud ICMP, lo que provoca que el objetivo se vuelva inaccesible al tráfico normal.
- ▶**Inundación Ping.** Es un ataque de denegación de servicio en el que el atacante abruma a la víctima con "solicitudes de eco" (de *ping*).

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Ataques enfocados en los protocolos de enlace y en la infraestructura física de la red



- ▶**Generación de tramas falsas**. Es un ataque de inundación de direcciones MAC, se bombardea el switch con tramas falsas que contienen direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch esté llena.
- ▶**Inundación con el encabezado** de tramas repetidos. Es un ataque de inundación de datos.
- ▶**Interrupción o cortes** intencionales de los medios de transmisión.
- ▶**Fallas en los circuitos** causadas por trabajos de obras civiles.

Ataques a las redes modernas

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Clasificación de los principales ataques a las redes modernas

(Kurose, 2017)

- **Dada la frecuencia** y variedad de ataques existentes, así como la amenaza de nuevos y mas destructivos ataques futuros, la seguridad de red se ha convertido en un tema crucial en el campo de las redes de computadoras.
- **Para defender** a las redes de computadoras de esos ataques, o mejor todavía, para diseñar nuevas arquitecturas que sean inmunes a tales ataques, es preciso hacer una clasificación de los ataques más habituales actualmente en Internet. Se identifican cuatro clases de ataques.

Principales ataques a las redes modernas			
1. Introducción de software malicioso	**2. Ataque a los servidores y a la infraestructura de red**	**3. Examen y análisis de paquetes**	**4. Suplantación IP**
Virus	Ataque de vulnerabilidad	Programas sniffers	Inyección de paquetes
Gusano	Inundación del ancho de banda		
Troyano	Inundación de conexiones		

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Cómo se introduce el software malicioso?

(Kurose, 2017)

- **Los "malos"** puede introducir software malicioso en un host a través de Internet.
- **Cuando usted conecta** un dispositivo a Internet, lo hace porque desea enviar y recibir datos, lo que incluye todo tipo de cosas legítimas, como publicaciones Instagram, resultados de búsquedas, flujos de música, videoconferencias, películas de cine, etc.
- **Pero**, lamentablemente, junto con todos estos elementos legítimos también existen elementos maliciosos, lo que se conoce de forma colectiva como software malicioso o malware, que puede también acceder a otros dispositivos e infectarlos.
- **Una vez que el malware** ha infectado a un dispositivo, puede hacer todo tipo de maldades, como por ejemplo borrar archivos o instalar software espía que recopile información personal, como el número de cuentas, contraseñas y pulsaciones de teclas, y luego enviar esos datos a los "malos".
- **El dispositivo comprometido** también puede ser reclutado como parte de una red de miles de dispositivos comprometidos de forma similar, lo que se conoce de forma colectiva como botnet (red robot), que los atacantes controlan y aprovechan para la distribución de correo electrónica basura (*spam*) o para llevar a cabo ataques distribuidos de denegación de servicio contra los hosts objetivo.

Introducción de software malicioso (malware)

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

El malware se extiende en forma de virus, gusano o troyano

(Kurose, 2017)

1. Introducción de software malicioso
Virus
Gusano
Troyano

- **Gran parte del malware** que existe actualmente es auto replicante: una vez que infecta un host, busca cómo acceder desde dicho host a otros a través de Internet, y desde esos hosts que acaba de infectar, busca cómo acceder a otros. De esta forma, el malware auto replicante puede extenderse rápidamente en forma exponencial. El malware puede extenderse en forma de virus, de gusano o de troyano.
  - ▶Un virus es un malware que requiere cierta interacción del usuario para infectar el dispositivo. El ejemplo clásico es un adjunto de correo electrónico que contiene código ejecutable malicioso. Si un usuario recibe y abre un adjunto de este tipo, ejecutará el malware en el dispositivo. Una vez que se ha ejecutado, el virus, que es autoreplicante, puede enviar un mensaje idéntico con el mismo adjunto malicioso a todos los contactos de la libreta de direcciones.
  - ▶Un gusano es un malware que puede entrar en un dispositivo sin ninguna interacción explícita por parte del usuario. Por ejemplo, un usuario puede estar ejecutando una aplicación de red a la que un atacante puede enviar software malicioso. Sin que el usuario intervenga, la aplicación puede aceptar el malware y ejecutarlo, creando un gusano. El gusano instalado en el dispositivo recién infectado explora entonces Internet, buscando otros hosts que ejecuten la misma aplicación de red. Cuando encuentra hosts vulnerables, envía una copia de sí mismo a esos hosts.
  - ▶Un caballo de Troya es un malware que está oculto dentro de otro software que es útil.
- **Hoy día, el malware** está generalizado y es costoso defenderse de él. ¿qué pueden hacer los diseñadores de redes para defender a los dispositivos conectados a internet de los ataques de malware?

4. ATAQUE A SERVIDORES Y A LA INFRAESTRUCTURA DE REDES

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿En qué consisten los ataque a la infraestructura de redes?

(Kurose, 2017)

2. Ataque a los servidores y a la infraestructura de red
Ataque de vulnerabilidad
Inundación del ancho de banda
Inundación de conexiones

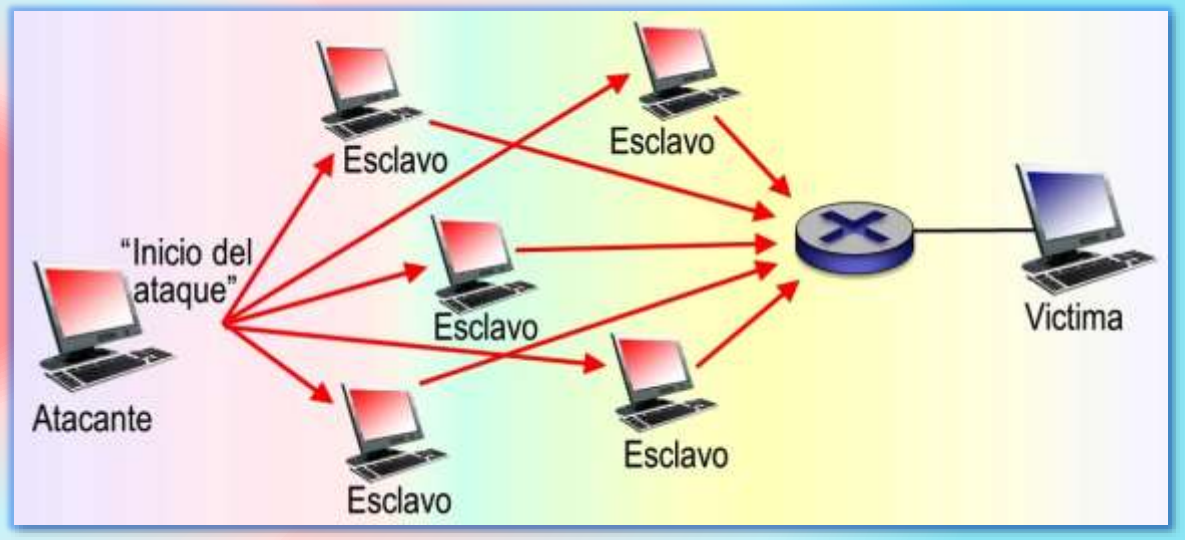
- **Los "malos"** pueden atacar a los servidores y a la infraestructura de red.
- **Otra amplia clase** de amenazas de seguridad son las que se conocen como ataques de negación de servicios (DoS). Un ataque DoS vuelve inutilizable una red, un host o cualquier otro elemento de la infraestructura para los usuarios legítimos. Los servidores web, los servidores de correo electrónico, los servidores DNS y las redes institucionales pueden ser, todos ellos, objeto de ataques DoS.
- **Los ataques DoS** son muy comunes en Internet, produciéndose miles de ataques de este tipo cada año. El sitio web Digital Attack Map permite visualizar los principales ataques DoS de ese día, a nivel mundial. La mayoría de los ataques DoS en Internet pueden clasificarse dentro de una de las tres categorías siguientes:
  - ▶Ataque de vulnerabilidad. Este ataque implica el envío de unos pocos mensajes especialmente diseñados a una aplicación o sistema operativo vulnerable que esté ejecutándose en un host objetivo. Si se envía la secuencia de paquetes correcta a una aplicación o un sistema operativo vulnerable, el servicio puede detenerse o, lo que es peor, el host puede sufrir una falla catastrófica.
  - ▶Inundación del ancho de banda. El ataque envía una gran cantidad de paquetes al host objetivo, de modo que se inunda el enlace de acceso del objetivo, impidiendo que los paquetes legítimos puedan alcanzar al servidor.
  - ▶Inundación de conexiones. El ataque establece un gran número de conexiones TCP completamente abiertas con el host objetivo. El host puede llegar a atascarse con estas conexiones fraudulentas, impidiendo así que acepte las conexiones legítimas.

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Ataque por inundación de ancho de banda

(Kurose, 2017)

- **Es evidente** que el atacante tendrá que enviar el tráfico a una velocidad similar a la velocidad de acceso del servidor para causar daño. Si la velocidad de acceso del servidor es muy grande, es posible que un único origen de ataque no sea capaz de generar el tráfico suficiente como para dañar al servidor.
- **Además**, si todo el tráfico procede de un mismo origen, un router situado en un punto anterior de la ruta podría detectar el ataque y bloquear todo el tráfico procedente de ese origen, antes de que llegue a aproximarse al servidor.
- **En un ataque DoS distribuido** (**DDoS**), como el de la figura, el atacante controla varios orígenes y hace que cada uno de ellos bombardee el objetivo con tráfico. Con este método, la tasa acumulada de tráfico para todos los orígenes controlados tiene que ser aproximadamente igual a la velocidad de acceso del servidor para inutilizarlo.



- **Actualmente**, se producen de forma continua ataques DDoS que utilizan botnets con miles de host comprometidos. Los ataques DDoS son mucho más difíciles de detectar y contrarrestar que los ataques DoS procedentes de un único host.
- **Surge la pregunta**: ¿qué pueden hacer los diseñadores de redes para defenderlas de los ataques DoS? Son necesarias diferentes defensas para cada uno de los tres tipos de ataques DoS.

5. EXAMEN Y ANÁLISIS DE PAQUETES

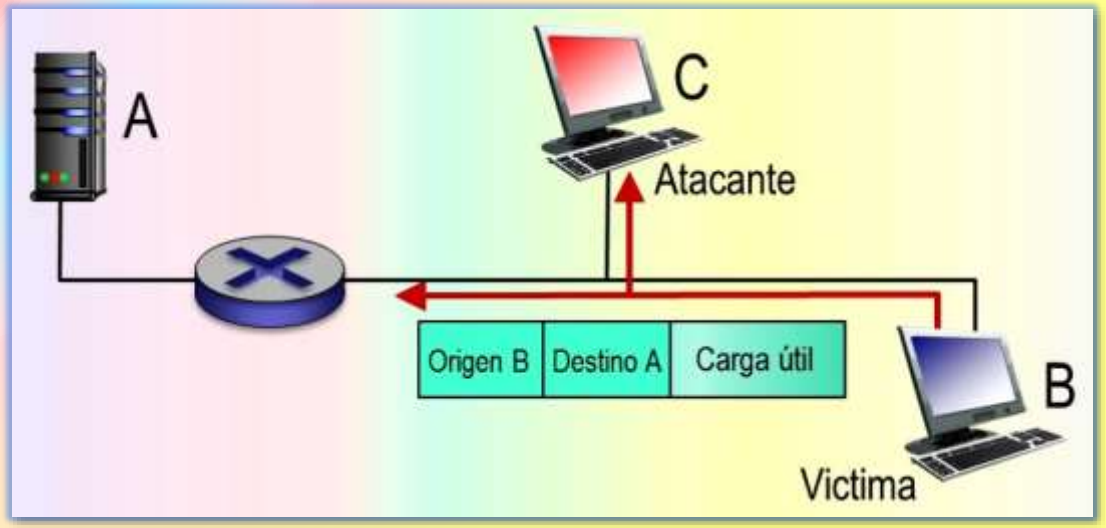
AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

3. Examen y análisis de paquetes
Programas sniffers

¿Cómo se husmean los paquetes?

(Kurose, 2017)

- **Los "malos"** pueden examinar y analizar paquetes.
- **Actualmente**, muchos usuarios acceden a Internet a través de dispositivos inalámbricos, tales como PC portátiles con conexión WiFi o smartphones con conexiones Internet móviles.
- **Aunque el acceso a Internet** es extremadamente útil y hace posibles maravillosas aplicaciones nuevas para los usuario móviles, también provoca una importante vulnerabilidad: colocando un receptor pasivo en las vecindades del transmisor inalámbrico, se puede recibir una copia de todos los paquetes que se están transmitiendo.
- **Estos paquetes** pueden contener todo tipo de información confidencial, incluyendo contraseñas, secretos comerciales y mensajes personales privados. Un receptor pasivo que registra una copia de todos los paquetes que pasan por él se denomina *sniffer* (husmeador de paquetes)
- **Los *sniffer*** también pueden implantarse en entornos cableados de multidifusión, como en muchas redes LAN Ethernet. Un sniffer puede obtener copias de todos los paquetes enviados a través de la LAN.
- **Además**, un atacante que consiga acceder al router de acceso (gateway) o al enlace de acceso a internet de una organización, puede colocar un sniffer que haga una copia de todos los paquetes entrantes y salientes de la organización.
- **Los paquetes** así monitorizados pueden ser analizados después en busca de información confidencial.



AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

Los software sniffer se comercializan

(Kurose, 2017)

- **Hay software *sniffer*** disponible de forma gratuita en varios sitios web y en forma de productos comerciales. Hay cursos sobre redes en los que se realizan practicas de laboratorio que implican escribir programas sniffer y un programa de reconstrucción de datos de la capa de aplicación.

- **Puesto que los programas *sniffer*** son pasivos, es decir no inyectan paquetes en el canal, son difíciles de detectar. Por tanto, cuando se envían paquetes a un canal inalámbrico, se tiene que aceptar que existe la posibilidad de que algún atacante pueda registrar copias de dichos paquetes.

- **Una de las mejores** formas de defensa frente a los programas sniffer son las técnicas criptográficas.

6. SUPLANTACIÓN IP

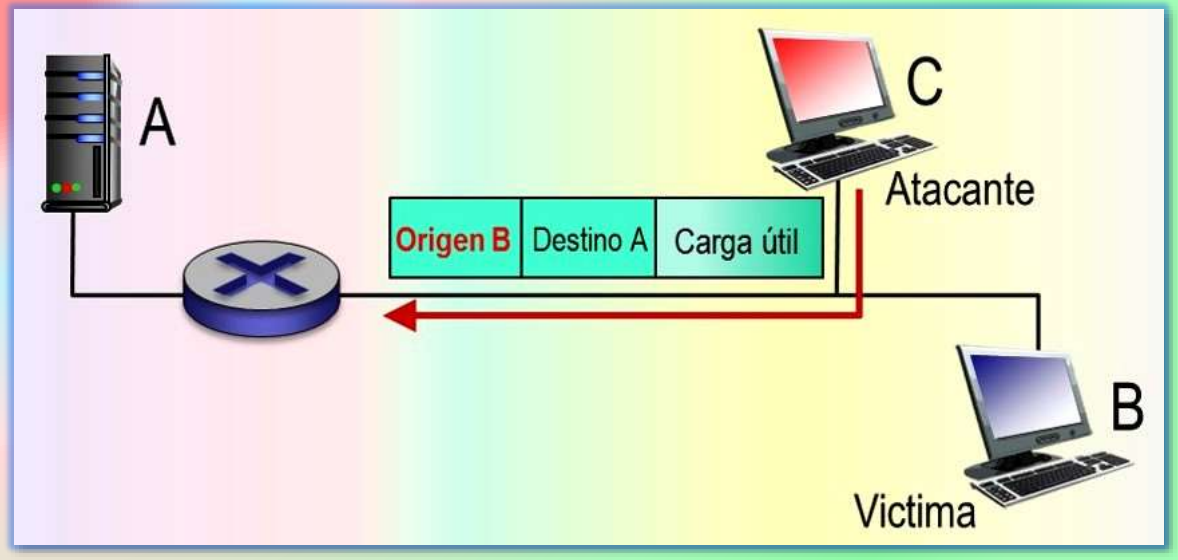
AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Cómo se suplanta el IP?

(Kurose, 2017)

4. Suplantación IP
Inyección de paquetes

- **Los "malos"** pueden suplantar la identidad de conocidos.
- **Es muy fáci**l crear un paquete con una dirección de origen, un contenido de paquete y una dirección de destino arbitrarios y luego transmitir dicho paquete a Internet, que reenviará el paquete a su destino.
- **Imagine que el receptor** confiado (por ejemplo, un router) que recibe tal paquete, toma la dirección de origen (falsa) como buena y luego reenvía el paquete hacia su destino.
- **La capacidad** de inyectar paquetes en Internet con una dirección de origen falsa se conoce como suplantación IP y es una de las muchas formas en las que un usuario puede hacerse pasar por otro.
- **Para resolver** este problema, se necesita aplicar un medio de autenticación en el punto terminal, es decir, un mecanismo que permita determinar con seguridad si un mensaje tiene su origen donde se cree que lo tiene.
- **Piense** ¿cómo pueden hacer esto las aplicaciones y protocolos de red?



Resumen y preguntas de repaso

(Kurose, 2017)

- **Resumen**. En esta presentación, se han descrito los ataques de seguridad a las redes modernas más habituales actualmente en Internet.
- ▶**P1.** ¿Cuál es la diferencia entre un virus y un gusano?
- ▶**P2**. Describa cómo se puede crear una red robot (botnet) y cómo se puede utilizar en un ataque DDoS
- ▶**P3**. Suponga que Ximena y Bill se están enviando paquetes entre sí a través de una red. Imagine que Renata se introduce en la red de modo que puede capturar todos los paquetes enviados por Ximena y que luego envía lo que ella quiere a Bill. Además, también puede capturar todos los paquetes enviados por Bill y luego enviar a Ximena lo que le parezca. Enumere algunos de los daños que Renata puede ocasionar desde su posición.

MAPA DE LOS SIGUIENTES TEMAS DE SEGURIDAD EN REDES

AMENAZAS DE SEGURIDAD EN LAS REDES MODERNAS

¿Cómo se abordará la seguridad en redes?

- **Hasta aquí**, ya se han identificado las amenazas de seguridad en las redes modernas.
- **En el siguiente tema**, se identificaran y definirán las **propiedades deseables** en una comunicación segura.

Principales ataques a las redes modernas			
1. Introducción de software malicioso	**2. Ataque a los servidores y a la infraestructura de red**	**3. Examen y análisis de paquetes**	**4. Suplantación IP**
Virus	Ataque de vulnerabilidad	Programas sniffers	Inyección de paquetes
Gusano	Inundación del ancho de banda		
Troyano	Inundación de conexiones		

- **Para una comunicación segura** es absolutamente necesario que los mensajes sean cifrados de alguna manera, por lo tanto, luego, se analizará cómo pueden utilizarse los principios fundamentales de la criptografía para crear protocolos de red seguros.
- **Luego**, se analizarán y seleccionarán los protocolos seguros en cada una de las cuatro capas superiores, comenzando por la capa de aplicación.
- **Por último**, se considerará la seguridad operacional, la cual se ocupa de la protección de las redes institucionales frente a los ataques. En particular, firewalls y los sistemas de detección de intrusos.

Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

FIN

Tema 1 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.