Módulo 6: Seguridad de sistemas y redes

Lección 1: Amenazas y Ataques en Redes

Objetivos de la Lección

Al finalizar, el estudiante podrá:

1. Identificar los principales tipos de malware, virus, gusanos y sus métodos de propagación en redes.

2. Analizar el impacto y las variantes modernas de ataques de denegación de servicio (DoS/DDoS).

3. Reconocer las tácticas psicológicas utilizadas en ingeniería social y SPAM.

4. Explicar cómo las vulnerabilidades web como XSS y CSRF afectan la seguridad de red y la información.

5. Relacionar los diferentes vectores de ataque con la tríada de seguridad: **Confidencialidad, Integridad y Disponibilidad (CIA)**.

Introducción a la Lección

Las redes modernas son el punto de convergencia entre usuarios, dispositivos y servicios críticos. Sin embargo, cada uno de estos puntos es también una posible puerta de entrada para ataques. Desde ataques de **worms autorreplicantes** que se propagan sin intervención humana, hasta campañas o ataques de **phishing masivo** que engañan a empleados, las amenazas en red son tanto **técnicas como humanas**.

En esta lección se estudian los principales ataques que comprometen la seguridad de los sistemas interconectados, analizando sus **métodos, ejemplos reales y contramedidas prácticas**.

Desarrollo del Tema

Malware, Virus y Gusanos

Definición general:

Malware (del inglés *malicious software*) es cualquier programa diseñado para dañar, espiar o tomar control de un sistema sin el consentimiento del usuario.

Tipos principales de Malware

Tipo	Descripción	Ejemplo real	Impacto
Virus	Se adhiere a archivos legítimos y se ejecuta al abrirlos.	*ILOVEYOU (2000):* se propagó por correo infectando archivos .vbs (**Visual Basic Scripting Edition**).	Pérdida de integridad y datos.
Gusano (Worm)	Se replica automáticamente por la red, sin intervención del usuario.	*WannaCry (2017):* explotó la vulnerabilidad SMBv1 en Windows. SMBv1 (**Server Message Block versión 1**), su función es compartir archivos, impresoras y recursos en red, esto en Windows.	Saturación de red y cifrado de archivos.

Tipo	Descripción	Ejemplo real	Impacto
Troyano (Trojan)	Se disfraza como software legítimo.	*Emotet (2020):* distribuido por correos falsos de facturas.	Robo de credenciales y propagación interna.
Spyware / Keylogger	Espía la actividad del usuario, captura contraseñas.	*RedLine Stealer (2024):* roba cookies y credenciales de navegadores.	Pérdida de confidencialidad.
Ransomware	Cifra datos y exige rescate.	*LockBit 3.0 (2023):* ataques a hospitales y universidades.	Interrupción total de servicios.

Ciclo de vida del malware (Modelo 5E)

1. **Entrada:** llega mediante phishing, descargas o dispositivos USB.
2. **Ejecución:** se activa al abrir un archivo o exploit.
3. **Expansión:** se replica dentro de la red (por SMB, RDP (Remote Desktop Protocol), etc.).
4. **Explotación:** cifra datos o roba información.
5. **Evasión:** desactiva antivirus, borra logs o cambia claves.

Controles de defensa

- Mantener antivirus y EDR (Endpoint Detection and Response).

- Aplicar parches de seguridad y deshabilitar SMBv1.
- Restringir macros en Office y ejecutar sandboxing de correos.
- Mantener copias de seguridad *offline* verificadas.

Ataques de Denegación de Servicio (DoS / DDoS)

Definición: ¿Qué es un ataque de Denegación de Servicio (DoS)?

Ataque que **agota recursos del sistema o red**, provocando que un servicio deje de estar disponible para usuarios legítimos.

Tipos de ataques DoS

Tipo	Descripción	Ejemplo	Defensa
Volumétrico	Inunda el ancho de banda con tráfico falso.	*1. UDP (User Datagram Protocol) Flood. Trabaja en la capa 4 del modelo OSI (Capa de Transporte)* *2. ICMP (Internet Control Message Protocol) Flood*. Trabaja en la capa 3 del modelo OSI (Capa de Red)	Filtros en routers, scrubbing centers, rate limiting.
Agotamiento de estado (Capa 4 modelo OSI)	Saturación de conexiones TCP (**Transmission Control Protocol**) (SYN flood).	*SYN (Synchronized) flood con paquetes falsos.* SYN Flood es un tipo de ataque **DoS / DDoS** que busca **agotarle la tabla de**	SYN cookies, firewalls stateful.

		conexiones (estado) al servidor.	
Aplicación (Capa 7 del modelo OSI, Aplicación)	Ataca directamente la **lógica** o los **recursos de la aplicación web**, no el ancho de banda ni las conexiones TCP. Su objetivo es **agotar CPU, RAM o procesos del servidor web** enviando solicitudes que son baratas para el atacante, pero **costosas para el servidor**. Solicitudes costosas (HTTP POST (Consultas de Bases de Datos, validaciones, carga de archivos), XML-RPC (WrodPress permite ejecutar muchas acciones con una sola solicitud)).	*Ataques a WordPress y API REST.*	WAF, limitación por IP, captchas.

Caso emblemático:

Botnet Mirai (2016) — infectó miles de dispositivos IoT (cámaras, routers) y lanzó un ataque de **1 Tbps** contra DynDNS, afectando sitios como Twitter, Netflix y GitHub.

Estrategias de mitigación

- Implementar balanceo de carga y CDNs.

- Contratar servicios anti-DDoS (Cloudflare, AWS Shield).
- Configurar umbrales de alertas con NetFlow.
- Mantener planes de contingencia (*runbooks*).

Ingeniería Social y SPAM

Definición general ¿Que es un ataque de Ingeniería Social?

Ataques que manipulan la **psicología del usuario** para obtener información o provocar acciones inseguras (clics, descargas, pagos, revelación de contraseñas).

Modalidades principales

Modalidad	Descripción	Ejemplo 2025	Contramedidas
Phishing	Correo o sitio falso imita una empresa real.	“Tu cuenta de Microsoft 365 será suspendida.”	Activar MFA, validar remitente y dominio.
Vishing	Llamada de voz fingiendo ser soporte técnico o banco.	“Su cuenta fue bloqueada, confirme su PIN.”	Contraseñas de seguridad y devolución de llamada.
Smishing	Mensaje SMS con enlace malicioso.	“Paquete retenido, pulse aquí.”	Filtrado de SMS, concienciación.

BEC (Business Email Compromise)	Ataque de ingeniería social donde el atacante **toma control o suplanta** una cuenta de correo empresarial para **engañar a empleados** y lograr transferencias bancarias falsas, cambios de cuentas de pago (fraude), robo de datos sensibles y hasta fraude de facturación (invoice fraud)	“Aprobado el pago urgente de $5,000.”	Políticas de doble aprobación de pagos.

SPAM

Mensajes masivos no solicitados, usados para:

- **Propagar malware o ransomware.**
- **Ejecutar ataques de phishing o fraude financiero.**
- **Saturar buzones (DoS lógico).**

Controles comunes:

- Filtros antispam (SpamAssassin, Proofpoint).
- Autenticación de correos: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting and Conformance).

- Modelos ML (Machine Learning) que detectan patrones anómalos.

- **Entrenamiento trimestral de concienciación.**

Vulnerabilidades Web: XSS y CSRF

Las aplicaciones web interconectadas amplían la superficie de ataque. Dos de las vulnerabilidades más comunes según OWASP son **Cross-Site Scripting (XSS)** y **Cross-Site Request Forgery (CSRF)**.

XSS (Cross-Site Scripting)

Permite al atacante insertar código JavaScript en una página confiable, ejecutándose en el navegador de la víctima.

Tipos:

Ejemplo: `https://sitio.com/search?q=<script>alert('XSS')</script>`

1. **Reflejado:** el código malicioso viaja en la URL.
2. **Almacenado:** el script se guarda en la base de datos (comentarios, perfiles).
3. **DOM-based:** el código se inyecta a través del DOM (JavaScript del lado cliente). Entiendase que DOM (**Document Object Model)** en el cual es la **estructura interna del documento HTML** que el navegador interpreta como objetos (nodos).

Impactos:

- Robo de cookies o tokens de sesión.

- Redirección a sitios falsos.

- Keylogging o manipulación del DOM.

Mitigaciones:

- Escapar correctamente las salidas (`output encoding`).
- Aplicar **CSP (Content-Security-Policy)**:
    - `Content-Security-Policy: default-src 'self'; script-src 'self'`
- Validar y sanitizar la entrada del usuario.

CSRF (Cross-Site Request Forgery)

Consiste en engañar al usuario autenticado para ejecutar una acción sin su consentimiento.

Ejemplo:

```
<img src="https://banco.com/transfer?to=attacker&amount=1000">
```

El navegador envía la cookie de sesión válida, ejecutando la transferencia sin notificación.

Defensas:

- Token CSRF único por sesión.
- Cookies con atributo `SameSite=Lax` o `Strict`.
- Verificación del encabezado `Origin` o `Referer`.

Conexión entre Ataques y CIA

Tipo de Ataque	C (Confidencialidad)	I (Integridad)	A (Disponibilidad)
Malware / Ransomware	🔴	🔴	🔴
DoS / DDoS	⚪	⚪	🔴
Ingeniería social	🔴	⚪	⚪
SPAM	🔴	⚪	⚪
XSS / CSRF	🔴	🔴	⚪

Leyenda de colores:

- **Rojo fuerte:** Alto impacto
- **Blanco / rosado claro:** Bajo impacto o impacto secundario

Cada ataque puede tener impacto múltiple, y su mitigación requiere **capas combinadas**: software actualizado, políticas, educación y segmentación de red.

Relación con Otros Conceptos

Esta lección conecta directamente con:

- **Fundamentos de seguridad:** aplica los conceptos CIA a ataques reales.
- **Seguridad de software:** vulnerabilidades XSS y CSRF nacen del código inseguro.
- **Control de acceso:** la ingeniería social evade controles de autenticación.

- **Criptografía:** se relaciona al cifrado de datos robados o manipulados.

Resumen de la Lección

- El malware, gusanos y virus explotan vulnerabilidades técnicas para propagarse.
- Los ataques DoS/DDoS afectan la disponibilidad mediante saturación de recursos.
- La ingeniería social y el SPAM explotan la confianza humana como vector de infección.
- XSS y CSRF manipulan la interacción web para robar credenciales y ejecutar acciones ilegítimas.
- Comprender cada tipo de ataque permite aplicar el principio de **defensa en profundidad**.

Actividad de la Lección — “Mapa de Amenazas en Red”

Objetivo: comprender la cadena “ataque → impacto → defensa”.

Instrucciones:

1. En grupos de 2 o 3 estudiantes, elijan un entorno (p. ej., universidad, hospital, tienda en línea).
2. Identifiquen:
    - Un **ataque de malware**.

    - Un **ataque DoS o DDoS**.
    - Una **táctica de ingeniería social o SPAM**.
    - Una **vulnerabilidad web (XSS o CSRF)**.
3. Creen un **mapa de amenazas** (diagrama de flujo) que muestre:
    - Cómo inicia el ataque.
    - Qué impacto tiene en la CIA.
    - Qué control o contramedida lo mitiga.
4. Presenten en clase una breve explicación del flujo.

Entregable:

- Diagrama digital (Draw.io o PowerPoint) y breve documento de una página con su análisis.

Referencias Recomendadas:

- Pfleeger, C. P., Pfleeger, S. L., & Coles-Kemp, L. (2023). *Security in Computing* (6th ed.).
- ENISA (2024). *Threat Landscape Report.*

- OWASP (2025). *Top 10 Web Application Security Risks.*

- US-CERT (2023). *Technical Alerts on WannaCry, Mirai, and Phishing Campaigns.*