GLOSARIO

RAUL HERNANDEZ PECH
IRIYC91

- Anonymous login: Entrar sin usuario ni contraseña por mala configuración.
- Análisis WHOIS: Muestra datos del dueño de un dominio.
- ARP Spoofing: Engaña a los dispositivos de red para robar o ver datos.
- Ataque de diccionario: Prueba contraseñas de una lista común.
- Ataque de sesión: Toma el control de la sesión de otro usuario.
- Banner grabbing: Lee mensajes de bienvenida para saber qué sistema se usa.
- Brute force distribuido: Ataque desde muchas IPs para evitar bloqueos.
- Buffer overflow: Usa más memoria de la permitida y puede ejecutar código.
- Cache poisoning: Cambia la caché para mostrar contenido falso.
- Captura de credenciales: Robo de usuarios y contraseñas en la red.
- Captura de tráfico: Ver y guardar datos que pasan por una red.
- Clickjacking: Hacer que alguien haga clic en algo sin saber.
- Command injection: Mandar comandos al sistema desde una app vulnerable.

- Content spoofing: Cambiar lo que se ve en una web para engañar.
- Cookie theft: Robo de cookies para usar otra cuenta.
- Credential stuffing: Probar contraseñas robadas en otros sitios.
- Cracking de contraseñas: Romper contraseñas cifradas.
- Cross-Site Scripting (XSS): Insertar código malicioso en sitios web.
- CSRF: Hacer que un usuario haga algo sin querer en su cuenta.
- Deserialización insegura: Cargar objetos manipulados que pueden hacer daño.
- DHCP Spoofing: Entregar direcciones IP falsas en una red.
- DNS enumeration: Buscar subdominios y registros de un sitio.
- DNS lookup: Recolectar información DNS de un dominio.
- DNS Spoofing: Redirigir a sitios falsos al resolver nombres.
- Encapsulation: Esconder datos maliciosos dentro de otros protocolos.
- Enumeración: Obtener información de un sistema o red.

- Escaneo sigiloso: Escanear sin que te detecten.
- Exploit: Código que usa una falla para atacar.
- Esteganografía: Esconder información dentro de archivos normales.
- Fuerza bruta: Probar muchas contraseñas hasta acertar.
- Footprinting: Reunir información básica sobre un objetivo.
- Fragmentación de paquetes: Dividir datos para evadir controles.
- Geolocalización de IP: Saber la ubicación aproximada de una IP.
- Google Dorking: Buscar con Google usando trucos para encontrar datos sensibles.
- Header injection: Insertar datos maliciosos en cabeceras HTTP.
- Host header injection: Cambiar la cabecera Host para engañar.
- HTTP response splitting: Dividir respuestas para mostrar contenido falso.
- ICMP scan: Usar ping para ver qué dispositivos están activos.

- IDOR: Acceder a datos sin permiso por IDs mal protegidos.
- Inyección: Insertar datos maliciosos en formularios o entradas.
- Inyección de comandos: Ejecutar comandos del sistema sin permiso.
- Inyección de código SQL: Insertar SQL malicioso en campos de entrada.
- Inyección de datos: Cambiar cómo funciona una app con datos falsos.
- Injection flaws: Fallos que permiten ejecutar código malicioso.
- Intervalos de paquetes: Cambiar tiempos entre paquetes para evitar ser detectado.
- Login bypass: Saltarse el inicio de sesión sin contraseña.
- Login sin autenticación: Entrar sin que el sistema lo pida.
- MAC flooding: Llenar la red para ver tráfico que no deberías.
- Man-in-the-middle (MITM): Interceptar datos entre dos partes.
- Metadatos: Información escondida en archivos (autor, fechas, etc).
- Null session: Entrar a recursos compartidos sin credenciales.

- Open redirect: Redirige a un sitio malicioso sin verificar la URL.
- OS fingerprinting: Saber qué sistema operativo usa un dispositivo.
- Parameter pollution: Mandar parámetros repetidos para confundir la app.
- Path traversal: Acceder a archivos prohibidos usando rutas modificadas.
- Ping scan: Usar ping para saber si un dispositivo está en línea.
- Port source no estándar: Usar puertos raros para evadir filtros.
- Privilege escalation: Obtener más permisos de los que deberías.
- RCE (Remote Code Execution): Ejecutar comandos en otro sistema desde lejos.
- Race condition: Fallo por ejecutar procesos al mismo tiempo sin control.
- Reconocimiento (OSINT): Buscar información pública del objetivo.
- Reconocimiento activo: Buscar información interactuando directamente.
- Reconocimiento pasivo: Buscar información sin que el objetivo sepa.

- Redirección maliciosa: Llevar al usuario a un sitio falso.
- Reflected XSS: Código malicioso que se ejecuta al momento.
- Scraping: Sacar datos de una página automáticamente.
- Service enumeration: Detectar servicios funcionando en un sistema.
- Session fixation: Hacer que un usuario use una sesión controlada por el atacante.
- SMB enumeration: Buscar recursos compartidos en red usando SMB.
- Sniffing: Escuchar el tráfico que pasa por una red.
- Sniffing activo: Modificar la red para poder ver el tráfico.
- SQL Injection: Inyectar código SQL en una app vulnerable.
- Stored XSS: Código malicioso guardado que se ejecuta al entrar a la página.
- Subdomain enumeration: Buscar subdominios de un sitio web.
- SYN scan: Ver qué puertos están abiertos enviando paquetes SYN.
- TCP handshake: Proceso para establecer una conexión entre dos dispositivos.

- TheHarvester: Herramienta para encontrar correos y subdominios.
- Token reuse: Volver a usar un token robado para acceder a una cuenta.
- Tunneling: Esconder tráfico dentro de otro protocolo como HTTP o DNS.
- Two-factor bypass: Saltarse la verificación en dos pasos.
- User-agent spoofing: Cambiar el tipo de navegador para engañar al sistema.
- Verbose error: Mensaje de error que da demasiada información.
- Vulnerabilidad: Fallo que puede ser usado por un atacante.
- Web Crawling: Navegar páginas de forma automática para recolectar datos.
- XSS (Cross-Site Scripting): Inyección de código en una web para dañar o robar.
- XML External Entity (XXE): Ataque que usa archivos XML para leer datos o conectarse fuera.
- Zero-day: Falla que nadie ha descubierto aún y no tiene solución.