Glosario

ACL (Access Control List)
Lista que controla quién puede acceder a qué recursos en una red..

Adware
Software que muestra anuncios no deseados y a menudo recopila datos del usuario.

APT (Advanced Persistent Threat)
Ataque sofisticado que se mantiene activo por mucho tiempo en un sistema objetivo.

ARP (Address Resolution Protocol)
Protocolo que convierte direcciones IP en direcciones MAC.

ARP Spoofing
Técnica en la que un atacante envía mensajes ARP falsos para interceptar tráfico de red.

Ataque de diccionario
Tipo de ataque de fuerza bruta que usa una lista de palabras comunes para adivinar contraseñas.

Autenticación de dos factores (2FA)
Método de seguridad que requiere dos pruebas para verificar identidad.

Backdoor
Acceso oculto a un sistema, instalado por un atacante o un desarrollador.

Banner Grabbing
Técnica para recopilar información de un sistema a través de los mensajes de bienvenida de servicios como HTTP o FTP.

BGP (Border Gateway Protocol)
Protocolo de enrutamiento utilizado para intercambiar información entre sistemas autónomos en Internet.

Bitácora de red
Registro de eventos y actividades relacionadas con el tráfico en una red.

Botnet
Red de dispositivos infectados controlados remotamente por un atacante.

Burp Suite
Herramienta para pruebas de seguridad en aplicaciones web que permite interceptar, modificar y analizar tráfico.

Captura de paquetes
Técnica de análisis de tráfico que permite observar los datos que circulan en la red.

CIFS (Common Internet File System)
Protocolo para compartir archivos entre dispositivos a través de una red.

Cifrado simétrico
Algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar datos.

Cifrado asimétrico
Usa un par de claves (pública y privada) para cifrar y descifrar mensajes.

Cliente-Servidor
Modelo donde un cliente solicita servicios y un servidor los entrega.

Cloud Security
Prácticas para proteger sistemas, datos y servicios en plataformas en la nube.

Comando ping
Herramienta que comprueba la conectividad entre dos dispositivos mediante ICMP.

Cookie
Pequeño archivo que los sitios web guardan en el navegador para mantener sesiones o rastrear usuarios.

Cortafuegos (Firewall)
Sistema que filtra tráfico entrante y saliente según reglas de seguridad.

Criptografía
Ciencia de codificar y descodificar mensajes para proteger la información.

Cross-Site Scripting (XSS)
Vulnerabilidad que permite insertar scripts maliciosos en páginas web visitadas por otros usuarios.

CSRF (Cross-Site Request Forgery)
Ataque que hace que un usuario realice acciones no deseadas en una web donde está autenticado.

DDoS (Distributed Denial of Service)
Ataque que busca saturar un servicio web mediante múltiples solicitudes simultáneas.

DHCP (Dynamic Host Configuration Protocol)
Protocolo que asigna direcciones IP automáticamente a dispositivos en una red.

DMZ (Demilitarized Zone)
Zona intermedia entre la red interna y externa para exponer servicios públicos sin comprometer la red interna.

DNS (Domain Name System)
Sistema que traduce nombres de dominio a direcciones IP.

DNS Spoofing
Ataque en el que se falsifican respuestas DNS para redirigir a sitios maliciosos.

DoS (Denial of Service)
Ataque que impide el acceso a un recurso legítimo sobrecargándolo.

Eavesdropping
Escucha no autorizada de comunicaciones digitales.

EFS (Encrypting File System)
Funcionalidad de Windows que permite cifrar archivos en el disco.

Encabezado HTTP
Parte de una petición o respuesta HTTP que contiene metadatos sobre la comunicación.

Escaneo de puertos
Técnica usada para descubrir servicios disponibles en un sistema objetivo.

Escucha pasiva
Monitoreo de tráfico de red sin intervenir en la comunicación.

Exploit
Código que aprovecha una vulnerabilidad para ejecutar acciones no autorizadas.

Factor de autenticación
Elemento usado para verificar identidad, como contraseña, huella o token.

Falsificación de IP
Suplantación de dirección IP para ocultar el origen real de una comunicación.

Firewall de próxima generación
Dispositivo de seguridad que combina funciones de firewall tradicional con inspección profunda de paquetes.

Forense digital
Disciplina que recopila, analiza y preserva evidencias digitales para investigaciones.

FOCA
Herramienta que analiza metadatos en documentos públicos para obtener información sensible.

Fuerza bruta
Método de ataque que prueba múltiples combinaciones posibles hasta encontrar la correcta.

Gateway
Dispositivo que conecta redes diferentes y actúa como traductor de protocolos.

Google Hacking
Uso de operadores avanzados de búsqueda de Google para encontrar información sensible.

GPO (Group Policy Object)
Conjunto de reglas usadas en Windows para gestionar la configuración de sistemas y usuarios.

GPS Spoofing
Manipulación de señales GPS para alterar ubicaciones reales.

GRE (Generic Routing Encapsulation)
Protocolo que encapsula paquetes para transportar tráfico entre redes.

Honeypot
Sistema diseñado para atraer atacantes y analizar sus métodos.

Host
Dispositivo conectado a una red que ofrece servicios o recursos.

HTTPS
Versión segura del protocolo HTTP con cifrado SSL/TLS.

Hash
Valor único generado mediante una función matemática para representar datos.

Hardening
Proceso de asegurar un sistema eliminando configuraciones innecesarias o débiles.

IDS (Intrusion Detection System)
Sistema que detecta accesos no autorizados en una red o sistema.

IPS (Intrusion Prevention System)
Sistema que detecta y bloquea ataques en tiempo real.

IPSec
Conjunto de protocolos que aseguran comunicaciones IP mediante cifrado.

IoC (Indicator of Compromise)
Prueba forense que indica que un sistema puede estar comprometido.

Ingeniería social
Técnica de manipulación psicológica usada para obtener información confidencial.

JavaScript Injection
Inyección de código malicioso JavaScript en una aplicación web vulnerable.

JWT (JSON Web Token)
Método seguro de transmitir información entre partes como objeto JSON firmado.

Kerberos
Protocolo de autenticación que usa tickets para permitir comunicaciones seguras.

Keylogger
Software o hardware que registra las teclas pulsadas en un teclado.

Kali Linux
Distribución de Linux especializada en pruebas de penetración y auditoría de seguridad.

LDAP (Lightweight Directory Access Protocol)
Protocolo para acceder y mantener servicios de directorio distribuidos.

LFI (Local File Inclusion)
Vulnerabilidad que permite a un atacante incluir archivos locales en un servidor.

Linux
Sistema operativo de código abierto ampliamente usado en servidores y redes.

MAC Address
Identificador único asignado a interfaces de red para comunicación en redes locales.

Malware
Software malicioso diseñado para dañar, explotar o comprometer un sistema.

Man-in-the-Middle (MitM)
Ataque donde el atacante intercepta y posiblemente altera la comunicación entre dos partes.

Metasploit
Framework que permite desarrollar y ejecutar exploits contra objetivos vulnerables.

Mutillidae
Aplicación web intencionalmente vulnerable usada para entrenar pruebas de penetración.

NAT (Network Address Translation)
Traduce direcciones IP privadas a una pública para acceso a internet.

Netcat
Herramienta de red usada para lectura y escritura de datos a través de conexiones TCP/IP.

Nmap
Herramienta de escaneo de red para descubrir hosts y servicios.

NFC (Near Field Communication)
Tecnología inalámbrica de corto alcance usada para pagos y transferencias.

OWASP
Proyecto abierto que promueve buenas prácticas en la seguridad de aplicaciones web.

OWASP ZAP
Herramienta gratuita para pruebas de seguridad automatizadas en aplicaciones web.

OSINT
Recopilación de inteligencia a partir de fuentes abiertas y públicas.

OTP (One-Time Password)
Contraseña válida por una sola sesión o transacción.

Packet Sniffing
Captura de paquetes de datos que circulan en una red.

Phishing
Técnica para obtener datos sensibles engañando al usuario con mensajes falsos.

p0f
Herramienta pasiva de fingerprinting de sistemas operativos.

Proxy
Servidor que actúa como intermediario entre el cliente y otro servidor.

Pentesting
Prueba de penetración diseñada para evaluar la seguridad de un sistema.

QoS (Quality of Service)
Mecanismo que prioriza el tráfico de red según importancia o necesidad.

Quantum Cryptography
Uso de principios de física cuántica para desarrollar sistemas de comunicación segura.

Ransomware
Tipo de malware que cifra archivos y exige un rescate para liberarlos.

Red Team
Equipo ofensivo que simula ataques reales para evaluar la seguridad.

Reconocimiento Activo
Obtención de información mediante interacción directa con el objetivo.

Reconocimiento Pasivo
Recolección de información sin interactuar directamente con el sistema objetivo.

Rootkit
Software malicioso que oculta su presencia o la de otros programas maliciosos.

Sandbox
Entorno controlado donde se ejecutan archivos sospechosos sin riesgo para el sistema real.

Scanning
Proceso de descubrimiento de dispositivos, puertos o servicios en una red.

Shodan
Buscador que indexa dispositivos conectados a Internet con información técnica detallada.

SMB (Server Message Block)
Protocolo para compartir archivos, impresoras y otros recursos en red.

Snort
Sistema de detección de intrusos basado en reglas.

Spoofing
Suplantación de identidad digital mediante la falsificación de información de origen.

Spyware
Software que recopila información del usuario sin su conocimiento.

SQL Injection
Vulnerabilidad que permite ejecutar comandos SQL arbitrarios en una base de datos.

SSL/TLS
Protocolos criptográficos que proporcionan seguridad en comunicaciones por internet.

TCP/IP
Conjunto de protocolos de red usados en Internet para comunicaciones.

Tshark
Versión de línea de comandos de Wireshark para captura y análisis de tráfico de red.

Tor
Red que permite navegación anónima mediante el enrutamiento cifrado de tráfico.

Traceroute
Herramienta que muestra la ruta que siguen los paquetes en una red hasta su destino.

UDP (User Datagram Protocol)
Protocolo de transporte rápido y sin conexión usado en streaming y DNS.

UAC (User Account Control)
Sistema de Windows que limita privilegios para evitar cambios no autorizados.

Update
Proceso de actualización de software para corregir errores o vulnerabilidades.

URL Filtering
Bloqueo o permiso de sitios web según sus URL.

VLAN (Virtual LAN)
Segmentación lógica de redes dentro de una red física.

VPN (Virtual Private Network)
Red segura que permite comunicación cifrada a través de Internet.

Virus
Malware que se replica y propaga alterando el funcionamiento del sistema infectado.

Vishing
Phishing mediante llamadas telefónicas para engañar a usuarios y obtener información.

Vulnerability
Debilidad en un sistema que puede ser explotada por atacantes.

WAF (Web Application Firewall)
Filtro que protege aplicaciones web analizando y controlando el tráfico HTTP.

Wardriving
Búsqueda de redes Wi-Fi desde un vehículo en movimiento.

WiFi
Tecnología de comunicación inalámbrica para conectar dispositivos a redes locales e Internet.

Wireshark
Analizador de protocolos de red que permite inspeccionar el tráfico en detalle.

Worm
Malware autorreplicante que se propaga a través de redes.

XSS (Cross-Site Scripting)
Vulnerabilidad web que permite ejecutar scripts maliciosos en navegadores de otros usuarios.

XML Injection
Ataque que modifica datos XML para alterar el comportamiento de una aplicación.

YARA
Herramienta que permite identificar malware mediante reglas basadas en patrones.

Zero-Day
Vulnerabilidad desconocida por el fabricante y sin parche disponible.

ZAP (Zed Attack Proxy)
Herramienta de código abierto para encontrar vulnerabilidades en aplicaciones web.