# Diccionario Ciberseguridad

# A

- AAA (Authentication, Authorization, Accounting): Modelo de seguridad que gestiona la identificación, permisos y auditoría de usuarios en sistemas informáticos.
- ACL (Access Control List): Lista de control de acceso que define qué usuarios o sistemas pueden acceder a ciertos recursos.
- AES (Advanced Encryption Standard): Algoritmo de cifrado simétrico utilizado para proteger datos de forma segura.
- Adware: Software no deseado que muestra anuncios en el dispositivo del usuario, generalmente como parte de otro programa gratuito.
- Air Gap: Método de seguridad que aísla un sistema crítico de redes externas para prevenir accesos no autorizados.
- Análisis de Vulnerabilidades: Proceso de identificación y mitigación de debilidades en sistemas informáticos.
- APT (Advanced Persistent Threat): Ataques avanzados y continuos realizados por actores maliciosos para robar información o comprometer sistemas.
- API (Application Programming Interface): Conjunto de protocolos y herramientas para el desarrollo de software.
- Antivirus: Programa diseñado para detectar, prevenir y eliminar malware de un sistema.
- Autenticación Multifactor (MFA): Método de verificación de identidad que requiere dos o más factores de autenticación.

# B

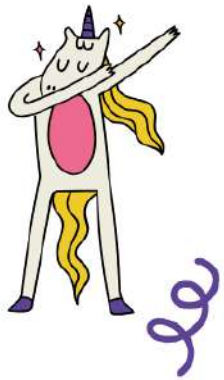
- Backdoor: Puerta trasera en un sistema que permite el acceso no autorizado sin pasar por los mecanismos de seguridad.
- BIOS (Basic Input/Output System): Firmware que inicializa el hardware de un dispositivo y carga el sistema operativo.
- Blockchain: Tecnología de registro distribuido utilizada para garantizar la seguridad y la integridad de los datos.
- Botnet: Red de dispositivos comprometidos controlados por un atacante para realizar actividades maliciosas.
- Brute Force Attack: Método de prueba y error utilizado para descifrar contraseñas o claves cifradas.
- Buffer Overflow: Vulnerabilidad que ocurre cuando un programa escribe más datos en un búfer de los que este puede manejar.
- Bug Bounty: Programa que recompensa a investigadores de seguridad por encontrar y reportar vulnerabilidades.
- BYOD (Bring Your Own Device): Política empresarial que permite a los empleados usar sus dispositivos personales para acceder a la red corporativa.

# C

- CISO (Chief Information Security Officer): Ejecutivo responsable de la seguridad de la información en una organización.
- CSIRT (Computer Security Incident Response Team): Equipo especializado en responder a incidentes de ciberseguridad.
- CVE (Common Vulnerabilities and Exposures): Base de datos de vulnerabilidades conocidas en sistemas informáticos.
- Cloud Security: Conjunto de medidas para proteger servicios y datos almacenados en la nube.
- Criptografía: Ciencia que estudia técnicas de cifrado para proteger la información.
- Cross-Site Scripting (XSS): Vulnerabilidad que permite inyectar scripts maliciosos en páginas web.
- Ciberespionaje: Actividad maliciosa que involucra el robo de información confidencial de gobiernos o empresas.
- Cifrado asimétrico: Método de cifrado que usa un par de claves (pública y privada) para proteger datos.
- Código malicioso (Malware): Software diseñado para dañar, interrumpir o infiltrarse en un sistema informático.
- Cookie: Pequeño archivo de datos almacenado en un navegador web que registra información sobre la actividad del usuario.

# D

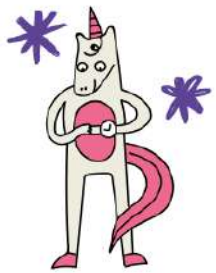
- **DDoS (Distributed Denial of Service):** Ataque que sobrecarga un servidor con tráfico falso para interrumpir su funcionamiento.
- **DMZ (Zona Desmilitarizada):** Red aislada entre una red interna y externa para agregar una capa de seguridad.
- **Data Breach:** Exposición no autorizada de datos confidenciales.
- **Deepfake:** Contenido manipulado mediante inteligencia artificial para parecer real, utilizado en ataques de desinformación o fraude.
- **DevSecOps:** Integración de la seguridad en el ciclo de desarrollo de software.
- **DNS Spoofing:** Ataque que manipula el sistema de nombres de dominio (DNS) para redirigir a usuarios a sitios falsos.
- **DLP (Data Loss Prevention):** Tecnología que protege contra la pérdida o el robo de datos sensibles.



# E

- **E2EE (End-to-End Encryption):** Cifrado de extremo a extremo que asegura que solo el remitente y el destinatario puedan leer los mensajes.
- **EDR (Endpoint Detection and Response):** Tecnología que supervisa amenazas en dispositivos finales.
- **Ethical Hacking:** Práctica de hackers éticos para encontrar vulnerabilidades con el permiso de las organizaciones.
- **Exploit:** Código o técnica utilizada para aprovechar vulnerabilidades en un sistema.
- **eIDAS:** Regulación europea sobre la identificación electrónica y servicios de confianza.

# F



- Factor de autenticación: Elemento utilizado para verificar la identidad, como contraseñas, huellas dactilares o tokens.
- False Positive (Falso Positivo): Alerta de seguridad incorrecta que identifica un evento legítimo como una amenaza.
- False Negative (Falso Negativo): Cuando un sistema de seguridad no detecta una amenaza real.
- Firewall: Sistema de seguridad que controla el tráfico de red entrante y saliente según reglas predefinidas.
- Firmware: Software integrado en dispositivos de hardware para su funcionamiento.
- Forensics (Informática Forense): Ciencia de investigar incidentes de ciberseguridad y recolectar evidencia digital.
- Fuzzing: Técnica de prueba que introduce datos aleatorios en un sistema para detectar vulnerabilidades.
- Full Disk Encryption (FDE): Método de cifrado que protege todos los datos almacenados en un disco duro.
- Federated Identity: Modelo en el que una identidad de usuario se puede utilizar en múltiples sistemas.
- Footprinting: Técnica utilizada en la recopilación de información sobre un sistema antes de un ataque.

# G

- **GDPR (General Data Protection Regulation):** Reglamento de protección de datos de la Unión Europea.
- **Gateway:** Dispositivo que actúa como un punto de acceso entre redes diferentes.
- **Gestión de Identidades y Accesos (IAM):** Conjunto de procesos y tecnologías que garantizan que las personas adecuadas tengan acceso a los sistemas correctos.
- **Gray Hat Hacker:** Hacker que explora vulnerabilidades sin intención de dañar, pero a menudo actúa sin autorización.
- **Governance, Risk and Compliance (GRC):** Marco para alinear la gestión de seguridad con objetivos organizacionales y regulaciones.
- **Geofencing:** Técnica que restringe el acceso a servicios según la ubicación geográfica del usuario.
- **Gestión de parches:** Proceso de actualizar software y sistemas para corregir vulnerabilidades.
- **Gobernanza de datos:** Conjunto de políticas para la administración segura y responsable de los datos.
- **Group Policy (Política de Grupo):** Herramienta en Active Directory para gestionar configuraciones de usuarios y dispositivos.
- **Ghostware:** Malware avanzado que oculta sus rastros para evitar ser detectado.

# H

- **Hacker**: Persona que explora sistemas informáticos con el objetivo de entenderlos o explotarlos.
- **Honeypot**: Sistema de seguridad diseñado para atraer atacantes y analizar sus técnicas.
- **Hashing**: Proceso de conversión de datos en una cadena de caracteres de longitud fija para integridad y seguridad.
- **Hardening**: Proceso de reforzar la seguridad de un sistema o dispositivo.
- **HTTP (Hypertext Transfer Protocol)**: Protocolo que permite la comunicación entre navegadores y servidores web.
- **HTTPS (Hypertext Transfer Protocol Secure)**: Versión segura de HTTP que cifra los datos transmitidos.
- **HIDS (Host-based Intrusion Detection System)**: Sistema que detecta actividades sospechosas en dispositivos específicos.
- **Hypervisor**: Software que permite la virtualización de sistemas operativos en un solo hardware.
- **Hidden Threats (Amenazas Ocultas)**: Amenazas difíciles de detectar debido a su naturaleza camuflada.
- **Hardware Security Module (HSM)**: Dispositivo de hardware diseñado para gestionar claves criptográficas de manera segura.

# I

- IDS (Intrusion Detection System): Sistema que detecta actividad maliciosa en una red o sistema.
- IPS (Intrusion Prevention System): Sistema que previene ataques al bloquear tráfico malicioso.
- Identity Theft (Robo de Identidad): Uso fraudulento de la información personal de alguien sin su consentimiento.
- Incident Response (Respuesta a Incidentes): Conjunto de procesos para manejar y mitigar ataques de seguridad.
- IoT (Internet of Things): Dispositivos conectados a internet que pueden comunicarse entre sí.
- IP Spoofing: Técnica en la que un atacante falsifica su dirección IP para hacerse pasar por otra entidad.
- ISO 27001: Estándar internacional para la gestión de la seguridad de la información.
- IT Governance (Gobernanza de TI): Estrategias y políticas para gestionar los recursos de tecnología de la información.
- Integrity Check: Método para verificar que los datos no han sido alterados o modificados sin autorización.
- Insider Threat (Amenaza Interna): Riesgo de seguridad proveniente de empleados o personas con acceso legítimo a los sistemas.

# J

- **JavaScript Vulnerabilities:** Fallos en código JavaScript que pueden ser explotados por atacantes.
- **Jailbreaking:** Proceso de eliminación de restricciones en dispositivos móviles para obtener acceso completo al sistema.
- **JWT (JSON Web Token):** Estándar para el intercambio seguro de información entre partes mediante tokens cifrados.
- **Jitter:** Variabilidad en la latencia de transmisión de datos en una red.
- **Just-in-Time Access:** Modelo de seguridad en el que los usuarios reciben acceso temporal a recursos específicos.
- **Job Rotation (Rotación de Puestos):** Estrategia para mitigar riesgos internos en seguridad al cambiar las responsabilidades de los empleados regularmente.
- **Jump Server:** Servidor de acceso seguro utilizado para administrar otros sistemas en una red protegida.

# K

- **Kerberos:** Protocolo de autenticación que utiliza tickets para permitir la comunicación segura en redes.
- **Keylogger:** Software o hardware que registra las pulsaciones del teclado para capturar credenciales y otra información sensible.
- **Kill Chain:** Modelo que describe las fases de un ataque cibernético, desde el reconocimiento hasta la explotación y exfiltración de datos.
- **Kali Linux:** Distribución de Linux utilizada para pruebas de penetración y auditoría de seguridad.
- **Key Exchange (Intercambio de Claves):** Proceso mediante el cual dos partes acuerdan una clave de cifrado para una comunicación segura.
- **Kernel:** Núcleo del sistema operativo que gestiona los recursos del hardware y software.
- **KVM (Kernel-based Virtual Machine):** Tecnología de virtualización que convierte un sistema Linux en un hipervisor.
- **K-Anonymity:** Técnica de privacidad de datos que garantiza que la información de un individuo no pueda ser identificada dentro de un conjunto de datos.
- **Keystroke Dynamics:** Método de autenticación basado en el análisis del patrón de escritura de un usuario.
- **Kubernetes Security:** Conjunto de prácticas y herramientas para proteger clústeres y contenedores en Kubernetes.

# L

- LDAP (Lightweight Directory Access Protocol): Protocolo para acceder y gestionar información en directorios distribuidos.
- Log Analysis (Análisis de Registros): Proceso de revisión de registros del sistema para detectar actividades sospechosas.
- Least Privilege (Principio de Mínimos Privilegios): Concepto de seguridad que limita los permisos de los usuarios al mínimo necesario.
- LAN (Local Area Network): Red que conecta dispositivos en un área geográfica limitada, como una oficina o edificio.
- Lateral Movement (Movimiento Lateral): Técnica utilizada por atacantes para moverse dentro de una red comprometida.
- Load Balancer (Balanceador de Carga): Dispositivo o software que distribuye tráfico entre múltiples servidores para optimizar rendimiento y seguridad.
- Logic Bomb (Bomba Lógica): Código malicioso programado para activarse en un momento determinado.
- Logging: Registro de eventos en un sistema para monitoreo y auditoría.
- Lua Scripting: Lenguaje de scripting utilizado en herramientas de seguridad y análisis de redes.
- Low and Slow Attack: Técnica de ataque en la que el atacante realiza acciones lentamente para evitar ser detectado.

# M

- MAC Address (Media Access Control Address): Dirección física única asignada a cada dispositivo de red.
- Malware: Software malicioso diseñado para dañar o comprometer sistemas.
- MITM (Man-in-the-Middle Attack): Ataque en el que un atacante intercepta y altera la comunicación entre dos partes.
- Multi-Factor Authentication (MFA): Método de autenticación que requiere múltiples factores, como una contraseña y un código SMS.
- Memory Dump (Volcado de Memoria): Copia del contenido de la memoria RAM utilizada en análisis forense.
- Metadata: Información adicional sobre un archivo o comunicación, como la fecha de creación o el remitente.
- Mobile Device Management (MDM): Herramientas utilizadas para administrar y asegurar dispositivos móviles en una empresa.
- Malvertising: Uso de anuncios en línea para distribuir malware.
- Masquerading Attack: Técnica en la que un atacante se hace pasar por una entidad legítima para engañar a usuarios.
- Machine Learning Security: Aplicación de aprendizaje automático para detectar y prevenir amenazas de ciberseguridad.

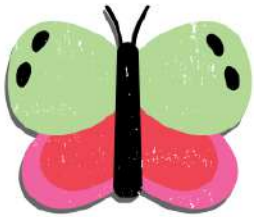
# N

- **NAT (Network Address Translation):** Técnica que permite que varios dispositivos en una red privada compartan una única dirección IP pública.
- **Network Security (Seguridad de Red):** Prácticas y tecnologías para proteger redes de accesos no autorizados, ataques y malware.
- **NIDS (Network Intrusion Detection System):** Sistema que monitorea tráfico de red en busca de actividad maliciosa o violaciones de seguridad.
- **NIPS (Network Intrusion Prevention System):** Similar a un NIDS, pero con la capacidad de bloquear tráfico malicioso automáticamente.
- **Nonce:** Número aleatorio utilizado una sola vez en protocolos de autenticación y cifrado para evitar ataques de repetición.
- **Null Session:** Conexión anónima a un recurso compartido de Windows que puede ser explotada por atacantes.
- **NSA (National Security Agency):** Agencia de seguridad de EE.UU. encargada de inteligencia y ciberseguridad.
- **Network Forensics:** Análisis de tráfico de red para identificar ataques y rastrear actividades maliciosas.
- **Nmap (Network Mapper):** Herramienta de código abierto utilizada para escaneo de redes y descubrimiento de dispositivos.
- **NTP (Network Time Protocol):** Protocolo que sincroniza la hora entre sistemas en una red.

# O

- **OSINT (Open-Source Intelligence):** Recopilación de información de fuentes públicas para ciberseguridad y análisis de amenazas.
- **OAuth (Open Authorization):** Protocolo de autenticación que permite el acceso seguro a recursos sin compartir credenciales.
- **OTP (One-Time Password):** Contraseña de un solo uso, común en autenticación de dos factores (2FA).
- **Obfuscation (Ofuscación):** Técnica que altera el código o datos para hacerlos más difíciles de entender y analizar.
- **On-Premises Security:** Medidas de seguridad aplicadas a infraestructura tecnológica dentro de una organización.
- **OWASP (Open Web Application Security Project):** Organización sin fines de lucro que promueve la seguridad en aplicaciones web.
- **Operational Security (OpSec):** Práctica de proteger información crítica contra el acceso de adversarios.
- **Offline Attack:** Ataque en el que un hacker obtiene datos cifrados y los analiza fuera de línea para descifrarlos.
- **Over-the-Air (OTA) Updates:** Actualizaciones enviadas remotamente a dispositivos, utilizadas en seguridad móvil e IoT.
- **OAuth Token:** Credencial digital generada para autenticar usuarios sin necesidad de ingresar contraseñas repetidamente.

# P



- **Phishing:** Técnica de engaño para obtener credenciales o información personal mediante correos o sitios web falsos.
- **Penetration Testing (Pentesting):** Pruebas de seguridad realizadas por expertos para identificar vulnerabilidades explotables en sistemas.
- **Patch Management:** Proceso de aplicar actualizaciones de seguridad a software y sistemas operativos.
- **Privileged Access Management (PAM):** Control de acceso a cuentas y permisos administrativos en una organización.
- **Public Key Infrastructure (PKI):** Conjunto de políticas y tecnologías para la gestión de claves criptográficas y certificados digitales.
- **Packet Sniffing:** Captura y análisis de paquetes de datos en una red para propósitos de seguridad o ataque.
- **Payload:** Parte de un malware que ejecuta una acción maliciosa en el sistema afectado.
- **Port Scanning (Escaneo de Puertos):** Técnica utilizada para identificar servicios activos en un sistema mediante la exploración de puertos.
- **Pass-the-Hash Attack:** Ataque en el que un hacker usa un hash de contraseña robado para autenticarse sin necesidad de descifrarlo.
- **Password Manager:** Software que almacena y gestiona contraseñas de manera segura.

# Q

- **Quantum Cryptography (Criptografía Cuántica):** Técnica de cifrado que utiliza principios de la mecánica cuántica para garantizar la seguridad de la información.
- **Quarantine (Cuarentena):** Acción tomada por software de seguridad para aislar archivos sospechosos y evitar su ejecución.
- **QoS (Quality of Service):** Conjunto de tecnologías que garantizan el rendimiento óptimo de una red, priorizando ciertos tipos de tráfico.
- **Query (Consulta):** Solicitud de información realizada a una base de datos o sistema.
- **Queue (Cola de Procesos):** Mecanismo de almacenamiento temporal utilizado en sistemas operativos y redes para gestionar tareas pendientes.
- **Quick Response (QR) Code Attack:** Tipo de ataque en el que códigos QR maliciosos redirigen a los usuarios a sitios fraudulentos.
- **Qubit:** Unidad básica de información en computación cuántica, que puede representar múltiples estados simultáneamente.
- **Quishing:** Phishing realizado a través de códigos QR, donde los usuarios escanean un código y son dirigidos a sitios maliciosos.
- **Quantum Key Distribution (QKD):** Método de intercambio de claves de cifrado basado en mecánica cuántica.

# R

- **Ransomware:** Tipo de malware que cifra los archivos del usuario y exige un rescate para desbloquearlos.
- **Red Team:** Grupo de seguridad ofensiva encargado de simular ataques para evaluar la defensa de una organización.
- **Reverse Engineering (Ingeniería Inversa):** Técnica de análisis de software o hardware para entender su funcionamiento y detectar vulnerabilidades.
- **Rootkit:** Software malicioso diseñado para ocultar la presencia de malware en un sistema y otorgar acceso persistente a atacantes.
- **RBAC (Role-Based Access Control):** Modelo de control de acceso basado en roles dentro de una organización.
- **Remote Code Execution (RCE):** Vulnerabilidad que permite a un atacante ejecutar código de manera remota en un sistema.
- **RAID (Redundant Array of Independent Disks):** Tecnología que mejora la redundancia y el rendimiento del almacenamiento mediante la combinación de múltiples discos.
- **Resilience (Resiliencia):** Capacidad de un sistema o red para recuperarse rápidamente de ataques o fallos.
- **Risk Assessment (Evaluación de Riesgos):** Proceso de identificación y análisis de amenazas potenciales en ciberseguridad.
- **Router:** Dispositivo que dirige el tráfico de red entre dispositivos y redes diferentes.

# S

- **SOC (Security Operations Center):** Centro de operaciones de seguridad encargado de monitorear y responder a amenazas en tiempo real.
- **Spoofing:** Técnica en la que un atacante falsifica una identidad o dirección para engañar a un sistema o usuario.
- **SQL Injection:** Ataque en el que comandos SQL maliciosos se inyectan en formularios para manipular bases de datos.
- **Social Engineering (Ingeniería Social):** Manipulación psicológica de personas para obtener acceso a información o sistemas.
- **SIEM (Security Information and Event Management):** Herramienta que centraliza, correlaciona y analiza eventos de seguridad en una red.
- **Sandboxing:** Técnica que ejecuta programas en un entorno aislado para prevenir daños en el sistema principal.
- **Symmetric Encryption (Cifrado Simétrico):** Método de cifrado en el que la misma clave se usa para cifrar y descifrar datos.

- **SSL/TLS (Secure Sockets Layer / Transport Layer Security):** Protocolos de cifrado que protegen la comunicación en internet.
- **Spear Phishing:** Variante de phishing que se dirige a individuos específicos con mensajes personalizados.

# T

- **Trojan Horse (Troyano):** Malware que se disfraza como software legítimo para engañar a los usuarios y permitir el acceso no autorizado a un sistema.
- **Two-Factor Authentication (2FA) (Autenticación de Doble Factor):** Método de autenticación que requiere dos formas de verificación para acceder a un sistema.
- **Threat Intelligence (Inteligencia de Amenazas):** Información sobre amenazas de ciberseguridad utilizada para anticipar y mitigar ataques.
- **Tampering (Manipulación de Datos):** Alteración no autorizada de información dentro de un sistema o red.
- **Token:** Dispositivo o software utilizado para generar credenciales de autenticación seguras.
- **Traffic Analysis (Análisis de Tráfico):** Monitoreo del tráfico de red para detectar patrones sospechosos o actividad maliciosa.
- **Tailgating (Ataque de Seguimiento):** Técnica en la que un atacante sigue físicamente a una persona autorizada para ingresar a un área restringida.
- **Threat Actor (Actor de Amenaza):** Individuo o grupo que lleva a cabo ataques cibernéticos con distintos fines.
- **TLS (Transport Layer Security):** Protocolo criptográfico que proporciona comunicación segura en redes.
- **Tokenization (Tokenización):** Proceso de reemplazar datos sensibles con un token único para proteger la información.

# U

- **Unauthorized Access (Acceso No Autorizado):** Entrada sin permiso a sistemas, redes o datos protegidos.
- **USB Drop Attack:** Ataque basado en ingeniería social donde un USB malicioso es dejado en un lugar público para que un usuario lo conecte a su dispositivo.
- **User Privileges (Privilegios de Usuario):** Nivel de acceso y permisos otorgados a un usuario dentro de un sistema.
- **UDP (User Datagram Protocol):** Protocolo de comunicación en red que permite la transmisión rápida de datos sin verificación de entrega.
- **UAC (User Account Control):** Función de seguridad en sistemas Windows que evita cambios no autorizados al requerir confirmación del usuario.
- **Unpatched Vulnerability (Vulnerabilidad sin Parchear):** Debilidad en un sistema que no ha sido corregida mediante una actualización de seguridad.
- **URL Spoofing:** Técnica de ataque en la que se falsifica la dirección de un sitio web para engañar a los usuarios.
- **Uptime:** Tiempo durante el cual un sistema está operativo y disponible sin interrupciones.
- **USB Forensics:** Análisis de dispositivos USB para extraer evidencia en investigaciones digitales.
- **Untrusted Network (Red No Confiable):** Red considerada insegura y que puede ser utilizada para ataques cibernéticos

# V

- **VPN (Virtual Private Network):** Tecnología que crea una conexión segura y cifrada entre un dispositivo y una red remota.
- **Virus:** Tipo de malware que se replica dentro de un sistema informático y puede dañar archivos o afectar el rendimiento del sistema.
- **Vulnerability Assessment (Evaluación de Vulnerabilidades):** Proceso de identificación y análisis de debilidades en sistemas de TI.
- **Virtualization (Virtualización):** Tecnología que permite la creación de entornos virtuales dentro de un único sistema físico.
- **VoIP (Voice over Internet Protocol):** Tecnología que permite realizar llamadas telefónicas a través de Internet.
- **Vishing:** Variante de phishing que utiliza llamadas telefónicas para engañar a las víctimas y obtener información personal.
- **Vendor Risk Management (Gestión de Riesgos de Proveedores):** Proceso de evaluación y control de los riesgos de seguridad asociados con terceros.
- **Vulnerability Exploit (Explotación de Vulnerabilidad):** Uso de software o técnicas para aprovechar una debilidad en un sistema y comprometerlo.
- **Virus Hoax (Bulo de Virus):** Mensaje falso que advierte sobre una amenaza inexistente con la intención de causar pánico o afectar sistemas.
- **Volumetric Attack:** Tipo de ataque DDoS que satura el ancho de banda de una red con tráfico masivo

# W

- **Worm (Gusano Informático):** Malware que se propaga automáticamente entre dispositivos sin intervención del usuario.
- **White Hat Hacker:** Hacker ético que trabaja en la identificación y corrección de vulnerabilidades de seguridad.
- **Web Application Firewall (WAF):** Sistema de seguridad que protege aplicaciones web de ataques como inyecciones SQL o XSS.
- **Watering Hole Attack:** Técnica en la que un atacante infecta un sitio web popular entre las víctimas objetivo para comprometerlas.
- **Whaling Attack:** Variante de phishing dirigido a altos ejecutivos o personas con acceso a información crítica.
- **Wireless Security (Seguridad Inalámbrica):** Prácticas y protocolos para proteger redes Wi-Fi contra accesos no autorizados.
- **Wardriving:** Actividad de búsqueda de redes Wi-Fi abiertas o mal configuradas para explotarlas.
- **Weak Password (Contraseña Débil):** Clave de acceso fácil de adivinar que representa un riesgo de seguridad.
- **Windows Defender:** Software antivirus y de seguridad integrado en los sistemas operativos Windows.

- **+XSS (Cross-Site Scripting):** Vulnerabilidad en aplicaciones web que permite a atacantes inyectar scripts maliciosos en páginas vistas por otros usuarios.
- **XOR Encryption (Cifrado XOR):** Método de cifrado simple basado en la operación lógica XOR.
- **XML External Entity (XXE) Attack:** Ataque que explota debilidades en el procesamiento de XML para acceder a información sensible.
- **X.509 Certificate:** Estándar para la gestión de certificados digitales y la autenticación de identidad en redes.
- **X.25 Protocol:** Antiguo protocolo de redes de telecomunicaciones utilizado en conexiones de datos.
- **Xen Hypervisor:** Plataforma de virtualización de código abierto utilizada en servidores y entornos en la nube.
- **XFS (X File System):** Sistema de archivos de alto rendimiento utilizado en servidores y sistemas avanzados.
- **XaaS (Anything as a Service):** Concepto que agrupa diversos servicios basados en la nube, como SaaS, PaaS e IaaS.
- **XDR (Extended Detection and Response):** Solución de seguridad que combina monitoreo y respuesta ante amenazas en múltiples plataformas.
- **Xbox Live Security:** Medidas de seguridad aplicadas a la plataforma de juegos en línea de Microsoft.

# Y

- **YARA (Yet Another Recursive Acronym):** Herramienta utilizada para la detección de malware mediante reglas personalizadas.
- **Yubikey:** Dispositivo de autenticación en hardware utilizado para 2FA y seguridad avanzada.
- **YAML (YAML Ain't Markup Language):** Lenguaje de serialización de datos utilizado en configuraciones de infraestructura.
- **Yahoo Data Breach:** Una de las mayores filtraciones de datos en la historia, que afectó a miles de millones de usuarios.
- **Yield Farming Attack**: Explotación de vulnerabilidades en plataformas DeFi para obtener beneficios fraudulentos.
- **Yosemite Server**: Sistema de gestión de copias de seguridad utilizado en entornos empresariales.
- **YubiOTP:** Protocolo de autenticación basado en claves generadas por dispositivos Yubikey.
- **Yo-Yo Attack**: Estrategia en ciberseguridad donde un atacante interrumpe repetidamente un sistema para confundir a los defensores.
- **YAML Security:** Buenas prácticas para evitar la manipulación de archivos YAML en entornos DevOps.
- **Yellow Team:** Concepto en ciberseguridad que representa la colaboración entre Blue Team y Red Team en la gestión de amenazas.

# Z

- **Zero-Day Vulnerability (Vulnerabilidad de Día Cero):** Fallo de seguridad no conocido por los desarrolladores y que puede ser explotado antes de ser corregido.
- **Zero Trust Security:** Modelo de seguridad que asume que ningún usuario o dispositivo debe ser confiado por defecto.
- **Zombie Computer:** Dispositivo comprometido en una botnet y controlado por un atacante.
- **ZFS (Zettabyte File System):** Sistema de archivos diseñado para manejar grandes volúmenes de datos con alta seguridad.
- **ZIP Bomb:** Archivo comprimido diseñado para colapsar un sistema al descomprimirse.


Diccionario
Por Alesec