GLOSARIO

Hacking Ético: Práctica de identificar vulnerabilidades en sistemas con autorización para mejorar su seguridad.

Penetration Testing (Pentesting): Simulación de ciberataques para evaluar la seguridad de un sistema.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada.

Exploit: Código o técnica que aprovecha una vulnerabilidad.

Zero-Day: Vulnerabilidad desconocida para el fabricante, sin parche disponible.

Payload: Parte del código malicioso que ejecuta una acción dañina.

Backdoor: Acceso secreto a un sistema, evitando autenticación.

Rootkit: Conjunto de herramientas para ocultar actividades maliciosas.

Malware: Software malicioso (ej. virus, troyanos, ransomware).

Ransomware: Malware que cifra archivos y exige rescate.

Phishing: Engaño para robar información mediante correos o sitios falsos.

Spear Phishing: Phishing dirigido a una persona/organización específica.

SQL Injection: Inyección de código SQL para manipular bases de datos.

XSS (Cross-Site Scripting): Inyectar scripts maliciosos en páginas web.

CSRF (Cross-Site Request Forgery): Forzar al usuario a ejecutar acciones no deseadas.

DDoS (Denial of Service): Sobrecargar un sistema para dejarlo inoperativo.

Man-in-the-Middle (MitM): Interceptar comunicación entre dos partes.

Brute Force: Intentar combinaciones para adivinar credenciales.

Dictionary Attack: Usar listas de palabras comunes en ataques de fuerza bruta.

Social Engineering: Manipulación psicológica para obtener información.

Kali Linux: Distribución Linux con herramientas de pentesting.

Metasploit: Framework para desarrollar y ejecutar exploits.

Nmap: Escáner de puertos y redes.

Wireshark: Analizador de tráfico de red.

Burp Suite: Suite para testing de seguridad web.

John the Ripper: Herramienta para cracking de contraseñas.

Aircrack-ng: Suite para auditoría de redes Wi-Fi.

Hydra: Herramienta para ataques de fuerza bruta.

OWASP ZAP: Proxy para testing de seguridad en aplicaciones web.

Ghidra: Herramienta de ingeniería inversa desarrollada por la NSA.

Firewall: Sistema que filtra tráfico de red.

IDS/IPS (Intrusion Detection/Prevention System): Detecta/bloquea intrusiones.

VPN (Red Privada Virtual): Conexión cifrada para privacidad.

SSL/TLS: Protocolos de cifrado para comunicaciones seguras.

Packet Sniffing: Captura de paquetes de red para análisis.

ARP Spoofing: Engañar a una red para redirigir tráfico.

Port Forwarding: Redirigir tráfico a un puerto específico.

Tor: Red para navegación anónima.

Cifrado (Encryption): Proceso de convertir datos en un formato ilegible.

AES (Advanced Encryption Standard): Algoritmo de cifrado simétrico.

RSA: Algoritmo de cifrado asimétrico.

Hash: Función que convierte datos en una cadena única (ej. SHA-256).

Salting: Añadir datos aleatorios a contraseñas antes de hashearlas.

PKI (Public Key Infrastructure): Infraestructura de claves públicas.

Certificado Digital: Credencial electrónica para autenticación.

SSL Stripping: Ataque para degradar conexiones HTTPS a HTTP.

Diffie-Hellman: Protocolo para intercambio seguro de claves.

Steganography: Ocultar información dentro de otros archivos (ej. imágenes).

Bash: Shell de Linux para scripting y automatización.

PowerShell: Herramienta de scripting en Windows.

Command Injection: Ejecutar comandos OS mediante vulnerabilidades.

Privilege Escalation: Ganar mayores permisos en un sistema.

Kernel: Núcleo del sistema operativo.

Registry (Windows): Base de datos de configuración del sistema.

OWASP : Lista de riesgos críticos en aplicaciones web.

JWT (JSON Web Token): Estándar para autenticación web.

CORS (Cross-Origin Resource Sharing): Política de acceso entre dominios.

API Security: Protección de interfaces de programación.

Web Shell: Script malicioso para controlar un servidor web.

Clickjacking: Engañar al usuario para que haga clic en elementos ocultos.

Session Hijacking: Robar la sesión de un usuario.

HTTP Headers: Cabeceras que afectan la seguridad web.

Content Security Policy (CSP): Política para mitigar XSS.

Subdomain Takeover: Apropiarse de subdominios no configurados.

GDPR (Reglamento General de Protección de Datos): Ley de privacidad en la UE.

PCI DSS: Estándar de seguridad para transacciones con tarjetas.

ISO 27001: Estándar de gestión de seguridad de la información.

Bug Bounty: Programas que recompensan por reportar vulnerabilidades.

Responsible Disclosure: Reportar vulnerabilidades de forma ética.

Cracker: Persona que realiza hacking con fines maliciosos (no ético).

White Hat: Hacker ético.

Black Hat: Hacker malicioso.

Grey Hat: Hacker que actúa sin autorización pero sin malicia.

Cybersecurity Framework: Marco de trabajo para gestión de riesgos (ej. NIST).

Red Team: Equipo que simula ataques.

Blue Team: Equipo que defiende y monitoriza.

Purple Team: Colaboración entre Red y Blue Team.

Threat Hunting: Búsqueda proactiva de amenazas.

SIEM (Security Information and Event Management): Sistema para monitoreo de seguridad.

EDR (Endpoint Detection and Response): Solución para detectar amenazas en endpoints.

SOC (Security Operations Center): Centro de operaciones de seguridad.

APT (Advanced Persistent Threat): Ataques prolongados y sofisticados.

Indicators of Compromise (IoC): Señales de una posible intrusión.

TTPs (Tactics, Techniques, and Procedures): Métodos usados por atacantes.

Dark Web: Parte de Internet no indexada por motores de búsqueda.

Deep Web: Contenido no accesible públicamente (no necesariamente ilegal).

Botnet: Red de dispositivos infectados controlados por un atacante.

Keylogger: Registra las pulsaciones del teclado.

Spyware: Software que espía actividades del usuario.

Adware: Software que muestra publicidad no deseada.

Logic Bomb: Código que se ejecuta al cumplirse una condición.

Fuzzing: Técnica para encontrar bugs mediante entrada aleatoria.

Hardening: Fortalecer la seguridad de un sistema.

Sandbox: Entorno aislado para ejecutar código sospechoso.

Watering Hole Attack: Infectar sitios web frecuentados por el objetivo.

Pivoting: Moverse a través de una red comprometida.

Living Off the Land (LotL): Usar herramientas legítimas del sistema para ataques.

Shodan: Motor de búsqueda de dispositivos conectados a Internet.

CVE (Common Vulnerabilities and Exposures): Listado público de vulnerabilidades.

CVSS (Common Vulnerability Scoring System): Sistema de puntuación de vulnerabilidades.

OSINT (Open Source Intelligence): Inteligencia basada en fuentes abiertas.

Doxing: Exponer información privada de una persona sin consentimiento.

Honeypot: Trampa para detectar ataques.

Canary Token: Alerta para detectar accesos no autorizados.

Active Directory (AD) Exploitation: Ataques a entornos Windows basados en AD (ej. Kerberos).

Pass the Hash: Robar hashes de contraseñas para autenticarse sin descifrarlas.

Golden Ticket: Ticket falsificado de Kerberos para acceso persistente.

BloodHound: Herramienta para mapear relaciones en Active Directory.

Lateral Movement: Moverse entre sistemas en una red comprometida.

PrivExchange: Explotar Microsoft Exchange para escalar privilegios.

DNS Tunneling: Usar DNS para filtrar datos o evadir firewalls.

NTLM Relay Attack: Redirigir autenticaciones NTLM para comprometer sistemas.

Token Impersonation: Suplantar tokens de sesión en Windows.

ROP (Return-Oriented Programming): Técnica de explotación para bypass de DEP.

AWS Pentesting: Pruebas de seguridad en entornos Amazon Web Services.

S3 Bucket Misconfigurations: Configuraciones inseguras en almacenamiento AWS S3.

IAM (Identity and Access Management): Gestión de permisos en la nube.

Container Escape: Escapar de un contenedor (ej. Docker) al host.

Kubernetes Hardening: Fortalecer clústeres de Kubernetes.

Serverless Security: Riesgos en arquitecturas sin servidor (ej. AWS Lambda).

CloudTrail: Servicio de AWS para registrar actividad.

Shadow IT: Uso de servicios en la nube no autorizados por la organización.

CASB (Cloud Access Security Broker): Control de seguridad para aplicaciones en la nube.

Zero Trust Architecture: Modelo de seguridad que verifica cada solicitud.

Firmware Analysis: Análisis de firmware embebido en dispositivos IoT.

JTAG/UART Exploitation: Interfaces para depurar/exploitar hardware.

RFID Cloning: Copiar tarjetas RFID (ej. sistemas de acceso).

BadUSB: Dispositivos USB modificados para inyectar comandos.

CAN Bus Injection: Ataques a redes de automóviles (ej. via OBD-II).

ESP8266/ESP32: Microcontroladores usados en proyectos de seguridad IoT.

Side-Channel Attacks: Extraer información mediante consumo de energía o tiempo.

Glitching: Alterar físicamente un dispositivo para bypass de seguridad.

SDR (Software Defined Radio): Usar radiofrecuencia para interceptar señales.

PoC (Proof of Concept): Demostración técnica de una vulnerabilidad.

IDA Pro: Herramienta profesional para ingeniería inversa.

Ghidra: Alternativa open-source a IDA Pro (desarrollada por la NSA).

Obfuscation: Ofuscar código para dificultar su análisis.

Packing: Comprimir/empaquetar malware para evadir detección.

YARA: Herramienta para identificar patrones en malware.

Sandbox Evasion: Técnicas para evitar detección en entornos sandbox.

Polymorphic Malware: Malware que cambia su código para evadir AV.

APT Groups: Grupos de amenazas persistentes avanzadas (ej. APT29).

Threat Intelligence: Recopilación y análisis de datos sobre amenazas.

MITRE ATT&CK: Marco de referencia de tácticas y técnicas de ataque.

APK Analysis: Auditoría de aplicaciones Android.

Frida: Framework para instrumentación dinámica en apps móviles.

Jailbreak/Rooting: Eliminar restricciones en iOS/Android.

Smishing: Phishing a través de SMS.

Mobile Device Management (MDM): Soluciones para gestionar dispositivos corporativos.

Biometric Bypass: Evadir autenticación por huella o rostro.

Man-in-the-Mobile (MitMo): Ataques específicos a dispositivos móviles.

Certificate Pinning: Fijar certificados para prevenir MitM en apps.

Flutter Security: Riesgos en apps desarrolladas con Flutter.

Post-Quantum Cryptography: Algoritmos resistentes a computación cuántica.

Homomorphic Encryption: Cifrado que permite operaciones sobre datos cifrados.

Elliptic Curve Cryptography (ECC): Criptografía basada en curvas elípticas.

Obfuscated Protocols: Protocolos diseñados para evadir censura (ej. Shadowsocks).

Cryptojacking: Uso no autorizado de recursos para minar criptomonedas.

ZK-SNARKs: Pruebas criptográficas de conocimiento cero.

OAuth 2.0 Exploits: Vulnerabilidades en flujos de autorización.

Blockchain Security: Auditoría de contratos inteligentes (ej. Solidity).

Secure Multi-Party Computation (MPC): Cálculos distribuidos sin revelar datos.

BGP Hijacking: Redirigir tráfico mediante manipulación de rutas BGP.

QUIC: Protocolo de transporte usado por HTTP/3.

VoIP Hacking: Ataques a sistemas de voz sobre IP.

SCADA Security: Seguridad en sistemas industriales.

SCAP (Security Content Automation Protocol): Estandarización de vulnerabilidades.

SNMP Exploitation: Ataques al protocolo de gestión de red.

IP Spoofing: Falsificar la dirección IP de origen.

802.1X: Autenticación en redes cableadas/Wi-Fi.

Rogue Access Point: Punto de acceso Wi-Fi falso.

WPA3: Último estándar de seguridad Wi-Fi.

Chain of Custody: Documentación forense para evidencias digitales.

eDiscovery: Proceso legal para obtener datos electrónicos.

PCI ASV (Approved Scanning Vendor): Entidades autorizadas para escaneos PCI DSS.

ISO 27002: Guía de controles de seguridad de la información.

NIST CSF (Cybersecurity Framework): Marco de ciberseguridad del NIST.

SOC 2: Informe de controles de seguridad en servicios en la nube.

CIS Benchmarks: Mejores prácticas de configuración segura.

Data Sovereignty: Leyes sobre ubicación física de datos.

Ethical Wall: Barrera para evitar conflictos de interés en auditorías.

Hacktivism: Hacking con motivos políticos o sociales (ej. Anonymous).

AI Security: Riesgos en modelos de IA (ej. adversarial attacks).

Quantum Hacking: Ataques a sistemas cuánticos.

Biohacking: Interacción entre biología y seguridad (ej. implantes RFID).

Smart Contract Auditing: Revisión de contratos en blockchain (ej. Ethereum).

Cyber-Physical Systems: Seguridad en sistemas que interactúan con el mundo físico.

Threat Modeling: Metodología para identificar riesgos en diseño.

Zero Knowledge Proofs: Demostrar conocimiento sin revelar información.

Script Kiddie: Persona que usa herramientas de hacking sin conocimiento técnico.

1337 (Leet): Lenguaje de símbolos usado en la cultura hacker.

Pwned: Término que indica que un sistema fue comprometido.

Adversary Emulation: Simular TTPs de grupos APT específicos.

C2 Frameworks (Command & Control): Herramientas como Cobalt Strike o Mythic.

Domain Fronting: Ocultar tráfico C2 detrás de servicios legítimos (ej. CDNs).

TA505: Grupo conocido por distribuir Locky y Dridex.

Living Off Trusted Sites (LOTS): Usar sitios legítimos (GitHub, Dropbox) para C2.

Malleable C2 Profiles: Configuraciones dinámicas en Cobalt Strike para evadir AV.

EDR Bypass: Técnicas para evadir Endpoint Detection and Response.

Process Hollowing: Inyectar código malicioso en procesos legítimos.

Sysmon: Herramienta de Microsoft para monitorizar actividad sospechosa.

AtomBombing: Técnica de inyección de código usando tablas atómicas.

Rowhammer: Explotar fallos en memoria DRAM para escalar privilegios.

Spectre/Meltdown: Vulnerabilidades en CPUs que permiten leer memoria.

Fault Injection: Inducir errores físicos en chips para bypass de seguridad.

eMMC Dumping: Extraer datos directamente de chips de almacenamiento.

Chip-Off Analysis: Desoldar chips para extraer datos forenses.

TEMPEST: Ataques mediante emisiones electromagnéticas.

USB Rubber Ducky: Dispositivo que emula teclado para inyectar comandos.

HID Attacks: Ataques usando dispositivos Human Interface Device.

NAND Mirroring: Clonar memoria NAND para bypass de autenticación.

JTAGulator: Herramienta para identificar puertos JTAG en PCBs.

Plausible Deniability: Negación creíble (ej.: cifrado con VeraCrypt).

Shamir’s Secret Sharing: Dividir secretos en partes distribuidas.

Oblivious RAM (ORAM): Acceder a memoria sin revelar patrones de acceso.

Mix Networks: Redes para anonimización (ej.: Tor).

Secure Enclaves: Zonas de ejecución segura (ej.: Intel SGX).

Zcash: Criptomoneda con privacidad mejorada.

Onion Routing: Enrutamiento en capas usado por Tor.

Differential Privacy: Técnicas para compartir datos sin revelar individuos.

Secure Multiparty Computation (SMPC): Cálculos conjuntos sin exponer datos.

Homomorphic Encryption: Operaciones sobre datos cifrados (ej.: Microsoft SEAL).

SolarWinds Attack: Ataque masivo a través de actualizaciones comprometidas.

Dependency Confusion: Explotar paquetes públicos con nombres similares a privados.

Typosquatting: Subir librerías maliciosas con nombres similares (ej.: "requets" vs "requests").

Code Signing Abuse: Robar certificados para firmar malware.

CI/CD Compromise: Inyectar código en pipelines de desarrollo (ej.: GitHub Actions).

Stolen Certificates: Uso de certificados digitales robados.

Watering Hole Attacks: Infectar sitios frecuentados por desarrolladores.

Malicious npm/PyPI Packages: Paquetes con código malicioso en repositorios públicos.

Compiler Exploits: Comprometer compiladores para insertar backdoors.

Hardware Backdoors: Chips o dispositivos comprometidos de fábrica.

Reentrancy Attacks: Explotar contratos inteligentes que permiten llamadas recursivas (ej.: DAO Hack).

Flash Loans: Préstamos sin colateral usados para manipular mercados.

MEV (Miner Extractable Value): Beneficios explotados por mineros/validadores.

Rug Pull: Estafa donde desarrolladores abandonan un proyecto y roban fondos.

Sybil Attacks: Crear múltiples identidades falsas en redes descentralizadas.

51% Attack: Controlar la mayoría del poder de hash en una blockchain.

Smart Contract Auditing Tools: Slither, MythX, Oyente.

Tornado Cash: Mezclador de criptomonedas para privacidad (y lavado).

ZK-Rollups: Soluciones de escalabilidad con pruebas de conocimiento cero.

Oracle Manipulation: Alterar datos que alimentan contratos inteligentes.

API Unhooking: Eliminar hooks de APIs monitoreadas por EDRs.

Direct Syscalls: Llamadas directas al kernel para evadir user-mode hooks.

Process Doppelgänging: Técnica de evasión usando transacciones NTFS.

Thread Stack Spoofing: Ocultar llamadas maliciosas en pilas de hilos.

Ghostwriting: Escribir en memoria de procesos sin inyección clásica.

Heaven’s Gate: Técnica para ejecutar código de 64 bits desde procesos 32 bits.

Module Stomping: Sobrescribir secciones de módulos legítimos en memoria.

Vectored Exception Handling (VEH): Manipular manejadores de excepciones.

Callback Hell: Abusar de callbacks del sistema para ejecución de código.

ETW Patching: Parchear Event Tracing for Windows para evadir logging.

Forensia Digital Avanzada

Memory Forensics: Analizar volcados de memoria con Volatility o Rekall.

Plaso (Log2Timeline): Herramienta para línea de tiempo forense.

The Sleuth Kit (TSK): Suite para análisis de discos.

Autopsy: Interfaz gráfica para TSK.

Windows Registry Analysis: Extraer claves como SAM, SYSTEM o USBSTOR.

Browser Artifacts: Recuperar historial, cookies y descargas.

File Carving: Recuperar archivos eliminados sin metadatos.

Stuxnet Analysis: Estudio del malware que atacó centrifugadoras nucleares.

JTAG Forensics: Extraer datos de dispositivos móviles mediante JTAG.

DFIR (Digital Forensics and Incident Response): Procesos para responder a incidentes.

VLAN Hopping: Saltar entre VLANs mal configuradas.

BGP Route Leaking: Filtrado no intencional de rutas BGP.

SDN Security: Riesgos en redes definidas por software.

ICMP Tunneling: Ocultar tráfico en pings (ej.: icmpsh).

QUIC Protocol Analysis: Desafíos en el cifrado de HTTP/3.

OT Security: Seguridad en redes industriales (Modbus, DNP3).

SCADA Honeypots: Trampas para atraer atacantes a entornos industriales.

SMB Exploits: Ataques a protocolo SMB (ej.: EternalBlue).

RDP Hardening: Proteger escritorio remoto de ataques.

Zero Trust Networking: Modelo "nunca confíes, siempre verifica".

Objection: Framework para pentesting móvil basado en Frida.

iOS Jailbreak Detection Bypass: Evadir detección de jailbreak.

Android Binder Exploits: Ataques al núcleo de IPC de Android.

ProGuard Analysis: Reversear código ofuscado en Android.

Swift/Objective-C Reversing: Ingeniería inversa en apps iOS.

WebView Exploits: Ataques a componentes WebView en apps móviles.

Firebase Misconfigurations: Bases de datos NoSQL expuestas en apps.

APK Tampering: Modificar APKs para bypass de licencias o inyección.

iOS Secure Enclave Exploits: Ataques al coprocesador seguro de Apple.

Emotet: Botnet avanzada de distribución de malware.

TrickBot: Malware bancario evolucionado a ransomware.

Conti/Ryuk: Familias de ransomware dirigido.

Lazarus Group: Grupo APT vinculado a Corea del Norte.

FIN7: Grupo cibercriminal especializado en POS.

DarkSide: Ransomware-as-a-Service (RaaS).

Pegasus: Spyware de NSO Group para iOS/Android.

Clop Ransomware: Variante que roba datos antes de cifrar.

REvil (Sodinokibi): RaaS con ataques de alto perfil.

Chaos RAT: Malware de acceso remoto de bajo perfil.

Hack The Box (HTB): Plataforma de entrenamiento en hacking.

CTF (Capture The Flag): Competencias de seguridad.

DEF CON: Conferencia de hacking más famosa del mundo.

Lockpicking: Cerrajería física como habilidad complementaria.