Glosario de Hacking Ético

0-day: Vulnerabilidad desconocida para el proveedor y sin parche disponible.

Access Control: Mecanismos que regulan el acceso a recursos o sistemas.

Active Fingerprinting: Técnica de reconocimiento activo para identificar el SO enviando paquetes personalizados.

Active Reconnaissance: Técnica que implica interactuar directamente con el objetivo para recolectar información.

Adware: Software que muestra anuncios, puede ser intrusivo o malicioso.

Antivirus: Software para detectar, prevenir y eliminar malware.

ARP Poisoning: Técnica que manipula la tabla ARP para interceptar tráfico de red.

Attack Surface: Total de puntos por donde un atacante puede explotar un sistema.

Backdoor: Acceso oculto a un sistema sin pasar por mecanismos de seguridad.

Banner Grabbing: Técnica para identificar versiones de software en puertos abiertos.

Black Hat: Hacker que realiza acciones ilegales o maliciosas.

Blue Team: Grupo encargado de defender la infraestructura frente a ataques.

Botnet: Red de dispositivos comprometidos controlados por un atacante.

Brute Force Attack: Método de prueba sistemática de contraseñas.

Buffer Overflow: Explotación de errores de memoria para ejecutar código arbitrario.

Bug Bounty: Programa que premia la identificación de fallos de seguridad.

Burp Suite: Plataforma para pruebas de seguridad en aplicaciones web.

CERT: Equipo de Respuesta ante Emergencias Informáticas.

Clickjacking: Técnica de engaño visual que induce a hacer clic en algo oculto.

Command Injection: Técnica para ejecutar comandos arbitrarios en el servidor.

Cookie Hijacking: Robo de cookies para suplantar sesiones.

Credential Dumping: Extracción de contraseñas o hashes desde memoria.

Credential Stuffing: Uso de credenciales filtradas en múltiples servicios.

CSRF: Ataque que hace que el usuario ejecute acciones sin saberlo.

Cyber Kill Chain: Modelo que describe las etapas de un ataque cibernético.

Cybersecurity: Práctica de proteger sistemas, redes y programas.

DDoS: Ataque que satura un recurso desde múltiples fuentes.

DHCP Snooping: Mecanismo de red que previene servidores DHCP no autorizados.

DNS Amplification: Tipo de DDoS usando respuestas DNS más grandes que las consultas.

DNS Enumeration: Técnica para descubrir información de dominio: subdominios, registros MX, etc.

DNS Poisoning: Técnica para alterar respuestas DNS legítimas.

Dnsdumpster: Herramienta de recolección pasiva de registros DNS.

DoS: Ataque que busca dejar un servicio fuera de línea.

Dumping: Extracción masiva de información de un sistema.

Enumeration: Proceso de listar usuarios, servicios, carpetas compartidas, etc.

Ethical Hacking: Evaluación legal y autorizada de la seguridad informática.

Evil Twin: Punto de acceso Wi-Fi falso para interceptar tráfico.

Exploit: Código que aprovecha una vulnerabilidad.

Finger: Protocolo antiguo usado para obtener información de usuarios remotos.

Firewall: Dispositivo o software que filtra el tráfico entrante y saliente.

FOCA: Herramienta para recolectar metadatos de documentos publicados.

Footprinting: Recolección de datos del objetivo en la fase de reconocimiento.

Fuzzer: Herramienta que envía entradas aleatorias para encontrar fallos.

Hash: Función unidireccional que representa datos en forma condensada.

HIDS: Sistema de detección de intrusos a nivel de host.

Honeypot: Sistema trampa para detectar o estudiar ataques.

ICMP Echo Scan: Escaneo mediante paquetes ICMP para detectar hosts activos.

IDS: Sistema que detecta accesos o actividades sospechosas.

Information Disclosure: Pérdida de confidencialidad por mal diseño o configuración.

Injection Attack: Inserción de código malicioso (SQL, LDAP, etc.).

Intrusion Prevention System (IPS): Sistema que bloquea tráfico malicioso automáticamente.

IP Spoofing: Falsificación de dirección IP para ocultar el origen.

IPID Scanning: Técnica de escaneo usando el campo de identificación IP.

Keylogger: Programa que graba las pulsaciones de teclado.

LFI: Vulnerabilidad que permite incluir archivos locales en un servidor.

MAC Spoofing: Falsificación de dirección MAC para ocultar identidad.

Man-in-the-Middle (MITM): Intercepción y manipulación de la comunicación.

Metasploit: Framework para el desarrollo y ejecución de exploits.

Mutillidae: Aplicación vulnerable para prácticas de pruebas web.

Network Mapping: Dibujo lógico de hosts, puertos y servicios en una red.

Nmap: Herramienta de escaneo de red, detección de servicios y SO.

OS Fingerprinting: Identificación del sistema operativo del objetivo.

OSINT: Inteligencia obtenida de fuentes públicas o abiertas.

OWASP ZAP: Herramienta automatizada para pruebas de seguridad web.

p0f: Herramienta de fingerprinting pasivo de sistemas.

Packet Sniffing: Captura y análisis del tráfico de red.

Passive Fingerprinting: Identificación del SO a partir de tráfico observado.

Passive Reconnaissance: Recolección de datos sin interactuar directamente con el objetivo.

Patch: Corrección de seguridad para una vulnerabilidad.

Payload. Parte de un exploit que realiza la acción maliciosa.

Penetration Testing: Simulación autorizada de un ataque para detectar fallos.

Phishing. Engaño para obtener datos confidenciales.

Ping Sweep: Técnica de reconocimiento de red que consiste en enviar paquetes ICMP Echo Request a múltiples direcciones IP para identificar cuáles están activas.

Pivoting: Técnica para moverse lateralmente en una red comprometida.

Port Knocking: Método para abrir puertos ocultos tras una secuencia de intentos.

Port Scanning: Identificación de puertos abiertos en un sistema.

Proxy: Intermediario entre el usuario y la red o servidor.

Ransomware: Malware que cifra datos y exige un rescate.

Reconnaissance: Primera etapa de un ataque, consiste en recolectar información.

Reverse Engineering: Proceso de descomponer software para entender su funcionamiento.

Rootkit: Conjunto de herramientas para mantener acceso oculto.

Scanning: Fase activa para encontrar vulnerabilidades.

Script Kiddie: Persona sin conocimientos que usa herramientas ajenas.

Session Hijacking: Ataque que roba una sesión activa.

Shodan: Motor de búsqueda de dispositivos conectados a Internet.

SIEM: Herramienta para análisis centralizado de eventos de seguridad.

Sniffing: Escucha pasiva de tráfico de red.

Social Engineering: Manipulación psicológica para obtener información confidencial.

Spoofing: Falsificación de identidad en cualquier capa (IP, DNS, ARP).

SQL Injection: Ataque que ejecuta comandos SQL maliciosos.

Subdomain Enumeration: Identificación de subdominios válidos de un sitio.

Threat Actor: Persona o grupo que lleva a cabo un ataque.

Trojan: Programa malicioso oculto como algo legítimo.

Web Application Firewall (WAF): Protección específica para aplicaciones web.

White Hat: Hacker ético que actúa con consentimiento.

Wireshark: Herramienta para capturar y analizar tráfico de red.

Worm: Malware autorreplicante que se propaga por red.

XSS: Inyección de scripts en páginas web.

Zero Trust: Modelo de seguridad que no confía ni en el usuario interno.

Zombie: Sistema comprometido que forma parte de una botnet.