GLOSARIO – HACKING ÉTICO

Omar Alejandro Perez Anota

UT CANCUN 22394061

ACK (Acknowledgment): Confirmación de recepción en una conexión TCP.

ACL (Access Control List): Lista que define permisos de acceso para usuarios.

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

API (Application Programming Interface): Interfaz que permite la comunicación entre software.

APT (Advanced Persistent Threat): Ataque persistente, sofisticado y dirigido.

ARP (Address Resolution Protocol): Traduce direcciones IP a MAC.

ARP Spoofing: Suplantación ARP para interceptar tráfico.

ASN (Autonomous System Number): Identificador único de red en sistemas autónomos.AWS, Azure, Google Cloud: Plataformas de computación en la nube.

Backdoor: Puerta trasera para mantener acceso a un sistema.

BeEF: Framework para ataques a navegadores web.

BGP, OSPF, RIP: Protocolos de enrutamiento entre routers.

Blue Team: Grupo que defiende la infraestructura (defensiva).

Broken Authentication: Fallas en los mecanismos de autenticación.

Brute Force: Múltiples intentos de contraseña.

Buffer Overflow: Error que permite sobrescribir la memoria.

Bug Bounty: Recompensa por descubrir vulnerabilidades.

Burp Intruder: Realiza ataques de forma automática.

Burp Proxy: Intercepción y modificación del tráfico HTTP/HTTPS.

Burp Repeater: Reenvía solicitudes modificadas.

Burp Scanner: Escaneo automatizado de vulnerabilidades.

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

Captura de Paquetes: Registro y análisis del tráfico de red (usualmente con Wireshark o tshark).

CIA Triad: Confidencialidad, Integridad y Disponibilidad: pilares de la seguridad informática.

Command Injection: Inyección de comandos del sistema en una aplicación vulnerable.

Cookie Poisoning: Manipulación de cookies para alterar sesiones.

CSP (Content Security Policy): Cabecera de seguridad que restringe la carga de contenido malicioso.

CSRF (Cross Site Request Forgery): Falsificación de solicitudes desde un usuario autenticado.

CVE (Common Vulnerabilities and Exposures): Identificadores únicos de vulnerabilidades públicas.

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

DNS Zone Transfer: Técnica para obtener todos los registros de una zona DNS.

DNS Query/Response: Solicitudes y respuestas DNS observables en Wireshark.

DoS/DDoS: Ataques de denegación de servicio.

DHCP: Protocolo que asigna direcciones IP dinámicas.

Eavesdropping: Escucha pasiva del tráfico de red.

Escaneo SYN: Escaneo que envía paquetes SYN sin completar la conexión.

Escaneo OS: Detección del sistema operativo remoto.

Exploit: Código que aprovecha vulnerabilidades.

Enumeración: Recolección activa de información sobre recursos, servicios y usuarios.

Filtro BPF: Expresiones para filtrar tráfico en Wireshark y Tshark.

Fuzzer: Herramienta que introduce entradas aleatorias para detectar fallas.

FIN (Finish): Flag TCP que indica intención de cerrar la conexión.

Firewall: Dispositivo/software que filtra tráfico según reglas.

FOCA: Herramienta de ElevenPaths para análisis de metadatos y DNS.

Forense Digital: Análisis técnico para recuperación de evidencia digital.

Fingerprinting: Detección de servicios, software o SO.

Fuerza Bruta: Método de prueba y error para romper contraseñas.

Geolocalización IP: Determina ubicación geográfica aproximada de una IP.

Hacking Ético: Pruebas de seguridad autorizadas con fines de mejora.

Hash: Valor criptográfico único que representa un dato.

HTML Injection: Inserción de código HTML en aplicaciones vulnerables.

HTTP: Protocolo de transferencia de hipertexto sin cifrado.

HTTP GET/POST: Métodos HTTP usados en solicitudes web.

HTTPS: Versión cifrada de HTTP usando TLS/SSL.

Hypervisor: Software que permite virtualizar sistemas operativos (ej. VirtualBox, VMware).

IAM (Identity and Access Management): Gestión de identidades y accesos.

ICMP: Protocolo para mensajes de diagnóstico de red.

ICMP Type/Código: Ej. Echo Request (tipo 8), Echo Reply (tipo 0).

IDS/IPS: Sistemas de detección y prevención de intrusiones.

Inyección SQL: Ataque que manipula consultas SQL.

IP Spoofing: Falsificación de dirección IP.

IPsec: Protocolo para asegurar comunicaciones IP.

Kali Linux: Distribución especializada en pruebas de penetración.

JWT (JSON Web Token): Token para autenticación basada en JSON.

Keylogger: Software que registra pulsaciones del teclado.

LFI (Local File Inclusion): Inclusión de archivos locales en aplicaciones web vulnerables.

LDAP: Protocolo para acceso a directorios como Active Directory.

Maltego: Herramienta para inteligencia visual y OSINT.

Man-in-the-Middle (MITM): Ataque que intercepta comunicación entre dos partes.

Metadatos: Información interna de documentos como autor, fecha, etc.

Metasploit: Framework para desarrollar y ejecutar exploits.

Mimikatz: Herramienta para extraer contraseñas de memoria en Windows.

MSS (Maximum Segment Size): Tamaño máximo del segmento TCP permitido.

Mutillidae: Aplicación web deliberadamente vulnerable para prácticas.

nmap: Escáner de redes que detecta hosts, puertos y servicios.

nmap -sS: Escaneo SYN (stealth scan).

nmap -A: Escaneo agresivo que detecta versión, sistema operativo y ejecuta scripts NSE.

nmap --script: Permite ejecutar scripts NSE personalizados para análisis avanzado.

NSE (Nmap Scripting Engine): Motor de scripting para Nmap.

Netcat: Herramienta de red versátil para conexiones TCP/UDP.

OSINT (Open Source Intelligence): Inteligencia obtenida de fuentes públicas.

OWASP Top 10: Lista de las 10 vulnerabilidades más críticas en apps web.

pcap: Archivo que contiene capturas de paquetes, utilizado en Wireshark y tshark.

Penetration Testing: Simulación controlada de ataques para identificar vulnerabilidades.

PSH (Push): Flag TCP que indica al receptor que procese los datos inmediatamente.

PowerShell: Consola avanzada de administración y automatización en Windows.

RST (**Reset):** Flag TCP que indica reinicio o terminación forzada de una conexión.

Recon-ng: Framework modular para recopilación de inteligencia OSINT.

RFI (Remote File Inclusion): Inclusión de archivos remotos.

Reconocimiento Activo: Recolección de información interactuando con el objetivo.

Reconocimiento Pasivo: Recolección de información sin interactuar directamente.

Rootkit: Software malicioso que oculta procesos y acceso.

SEQ (Sequence Number): Número de secuencia usado para controlar el orden de los paquetes TCP.

Shodan: Motor de búsqueda de dispositivos conectados a Internet.

SMTP (Simple Mail Transfer Protocol): Envío de correos.

Snapshots: Puntos de restauración en máquinas virtuales.

SNMP (Simple Network Management Protocol): Gestión de dispositivos en red.

SPF (Sender Policy Framework): Previene suplantación en correos electrónicos.

SSL/TLS Handshake: Proceso de negociación de claves y autenticación en conexiones HTTPS.

SYN (Synchronize): Primer paquete del "three-way handshake" TCP.

SQLMap: Herramienta automatizada para detectar y explotar inyecciones SQL.

TCP Flags: Campo de control que define el tipo de segmento TCP (SYN, ACK, FIN, etc.).

TCP Three-way Handshake: Proceso de conexión TCP: SYN → SYN-ACK → ACK.

theHarvester: Herramienta OSINT para recolectar correos, dominios y subdominios.

Traceroute: Rastrea la ruta que siguen los paquetes hasta su destino.

TTL (Time To Live): Número máximo de saltos antes de descartar un paquete IP.

Tshark: Versión CLI de Wireshark, útil para automatización o entornos sin GUI.

URG (Urgent): Flag TCP para datos urgentes. Poco usado actualmente.

User-Agent: Cadena que identifica navegador o cliente web en solicitudes HTTP.

UDP (User Datagram Protocol): Protocolo sin conexión, rápido, pero no confiable.

VirtualBox: Software de virtualización.

VMware: Plataforma profesional para entornos virtualizados.

Vulnerability Scanning: Detección de debilidades en una app.

WAF (Web Application Firewall): Filtro de tráfico web malicioso.

Wayback Machine: Archivo de versiones antiguas de sitios web.

Whois: Protocolo para consultar registros de dominio.

Wireshark/tcpdump: Herramientas para captura y análisis de tráfico.

Wireshark: Analizador de protocolos de red gráfico.

XAMPP: Paquete de servidor local (Apache, MySQL, PHP, Perl) para pruebas y desarrollo web.

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

X.509: Estándar para certificados digitales en TLS/SSL.

ZAP Active Scan: Prueba activamente posibles vulnerabilidades.

ZAP Passive Scan: Escaneo sin interacción directa.

ZAP Spider: Rastrea todas las URLs del sitio web.

Zone Transfer: Técnica para obtener información completa de una zona DNS.