Glosario

1. **Hacking Ético:** La práctica autorizada de probar la seguridad de sistemas, redes y aplicaciones para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas por atacantes maliciosos.
2. **Pentesting (Prueba de Penetración):** Un ejercicio de seguridad simulado y autorizado para evaluar la fortaleza de las defensas de un sistema, red o aplicación.
3. **VAPT (Vulnerability Assessment and Penetration Testing):** Un enfoque combinado que incluye la identificación exhaustiva de vulnerabilidades (VA) y la explotación controlada de las mismas (PT).
4. **Metodología OSSTMM (Open Source Security Testing Methodology Manual):** Un estándar para probar la seguridad operacional, que abarca diversos aspectos de la seguridad.
5. **Metodología OWASP Testing Guide:** Un marco integral para probar la seguridad de aplicaciones web, desarrollado por la comunidad OWASP.
6. **Marco NIST Cybersecurity Framework:** Un conjunto de directrices y estándares para ayudar a las organizaciones a gestionar y reducir los riesgos de ciberseguridad.
7. **Ciclo de Vida de Desarrollo Seguro (SDLC - Secure Development Life Cycle):** La integración de prácticas de seguridad en cada fase del desarrollo de software.
8. **Modelado de Amenazas (Threat Modeling):** Un proceso estructurado para identificar posibles amenazas, vulnerabilidades y contramedidas en un sistema.
9. **Gestión de Riesgos (Risk Management):** El proceso de identificar, evaluar, tratar y monitorear los riesgos de seguridad.
10. **Matriz de Riesgos:** Herramienta para clasificar los riesgos en función de su probabilidad e impacto.
11. **Superficie de Ataque (Attack Surface):** El conjunto total de puntos de entrada potenciales que un atacante puede usar para acceder a un sistema o red.

12. **Cadena de Muerte Cibernética (Cyber Kill Chain):** Un modelo que describe las fases de un ataque cibernético, desde el reconocimiento hasta la acción sobre los objetivos.
13. **IoC (Indicator of Compromise):** Artefactos forenses en una red o sistema que indican una intrusión.
14. **APT (Advanced Persistent Threat):** Un ataque sigiloso y continuo, a menudo dirigido por estados o grupos bien organizados, que gana acceso no autorizado y permanece sin ser detectado durante un período prolongado.
15. **Red Teaming:** Un ejercicio de seguridad avanzado donde un equipo simula un adversario real para probar las capacidades de defensa de una organización.
16. **Blue Teaming:** El equipo de seguridad que defiende contra los ataques y trabaja para mejorar la postura de seguridad de la organización.
17. **Purple Teaming:** Colaboración entre Red Team y Blue Team para maximizar el aprendizaje y la mejora de la seguridad.
18. **Seguridad Ofensiva:** Disciplinas y prácticas enfocadas en la simulación de ataques para encontrar vulnerabilidades y probar las defensas.
19. **Seguridad Defensiva:** Disciplinas y prácticas enfocadas en la protección de sistemas, redes y datos contra ataques.
20. **Postura de Seguridad:** La posición general de una organización en términos de su capacidad para defenderse contra las amenazas cibernéticas.
21. **Reconocimiento Pasivo:** Recopilación de información de fuentes públicas sin interactuar directamente con el objetivo.
22. **Reconocimiento Activo:** Interacción directa con el objetivo para recopilar información, con mayor riesgo de detección.
23. **OSINT (Open Source Intelligence):** Recopilación y análisis de información de fuentes públicas.
24. **Dorking (Google Hacking):** Uso de operadores de búsqueda avanzados para encontrar información sensible o configuraciones erróneas expuestas públicamente.
25. **Metadatos:** Datos que describen otros datos (ej. autor, fecha de creación en documentos).

26. **Subdominios:** Dominios secundarios de un dominio principal, a menudo usados para segregar servicios.
27. **Enumeración DNS:** Proceso de descubrimiento de registros DNS relacionados con un dominio.
28. **Registros WHOIS:** Información pública sobre el propietario de un dominio o dirección IP.
29. **Robo de Zona DNS (DNS Zone Transfer):** Técnica para obtener una copia de la base de datos DNS de un servidor, revelando la estructura de la red.
30. **Shodan:** Motor de búsqueda para dispositivos conectados a internet (IoT, servidores, etc.), no solo páginas web.
31. **Censys:** Plataforma de búsqueda de Internet que proporciona visibilidad del panorama de IPv4 y puertos/servicios.
32. **FOCA (Fingerprinting Organizations with Collected Archives):** Herramienta para extraer metadatos de documentos y obtener información de la organización.
33. **theHarvester:** Herramienta para recolectar información de OSINT (correos, subdominios, nombres, etc.) de diversas fuentes públicas.
34. **Maltego:** Herramienta de código abierto para la minería de datos y el reconocimiento de información, mostrando relaciones entre entidades.
35. **SpiderFoot:** Herramienta de OSINT de automatización para recopilar, procesar y almacenar inteligencia sobre un objetivo.
36. **Reconocimiento con Nmap Scripting Engine (NSE):** Uso de scripts de Nmap para automatizar tareas de reconocimiento y enumeración avanzadas.
37. **Escaneo de Puertos:** Identificación de puertos abiertos en un host.
38. **Escaneo de Vulnerabilidades (Vulnerability Scanning):** Uso de herramientas automatizadas para identificar vulnerabilidades conocidas.
39. **Servicios y Banners:** Información que revelan los servicios que se ejecutan en puertos abiertos (ej. "Apache/2.4.29").
40. **Escaneo Credencializado:** Escaneo de vulnerabilidades que utiliza credenciales válidas para obtener una visión más profunda del sistema.

41. **Escaneo No Credencializado:** Escaneo de vulnerabilidades sin credenciales, simulando un atacante externo.
42. **Enumeración SMB/NetBIOS:** Descubrimiento de recursos compartidos de red, usuarios y grupos en sistemas Windows.
43. **Enumeración SNMP:** Descubrimiento de información sobre dispositivos de red gestionados.
44. **Enumeración LDAP:** Descubrimiento de información de directorios.
45. **Enumeración NTP:** Descubrimiento de información de servidores de tiempo.
46. **Vulnerabilidades de Configuración (Configuration Weaknesses):** Deficiencias en la configuración de un sistema o aplicación que pueden ser explotadas.
47. **CVE (Common Vulnerabilities and Exposures):** Base de datos pública de identificadores para vulnerabilidades de seguridad conocidas.
48. **CVSS (Common Vulnerability Scoring System):** Un estándar para calificar la gravedad de las vulnerabilidades de seguridad.
49. **SCAP (Security Content Automation Protocol):** Estándar del NIST para la automatización de la seguridad.
54. **Exploit:** Código o secuencia de comandos que aprovecha una vulnerabilidad específica.
55. **Payload:** El código malicioso que se ejecuta después de una explotación exitosa.
56. **Shellcode:** Un pequeño fragmento de código que se utiliza como payload en un exploit para obtener una shell.
57. **Reverse Shell:** Una conexión de shell iniciada por la máquina víctima hacia la máquina del atacante, a menudo para evadir firewalls.
58. **Bind Shell:** Una conexión de shell donde la máquina víctima abre un puerto y el atacante se conecta a él.
59. **Post-Explotación:** Acciones realizadas después de obtener acceso inicial a un sistema, como escalada de privilegios o pivoteo.
60. **Escalada de Privilegios (Privilege Escalation):** Obtener mayores niveles de acceso en un sistema (ej. de usuario normal a administrador/root).

61. **Pivoteo (Pivoting):** Usar un sistema comprometido como punto de partida para atacar otros sistemas dentro de la misma red.
62. **Movimiento Lateral (Lateral Movement):** Técnicas utilizadas para moverse a través de una red comprometida de un sistema a otro.
63. **Pass-the-Hash (PtH):** Técnica de ataque donde un atacante autentica contra un recurso de red usando el hash de una contraseña, sin conocer la contraseña en texto plano.
64. **Golden Ticket Attack:** Un ataque avanzado de Kerberos donde un atacante genera un TGT (Ticket Granting Ticket) falsificado para obtener acceso irrestricto a cualquier servicio en el dominio.
65. **Silver Ticket Attack:** Un ataque de Kerberos donde un atacante genera un TGS (Ticket Granting Service) falsificado para un servicio específico.
66. **Kerberoasting:** Técnica para extraer hashes de contraseñas de cuentas de servicio de Active Directory.
67. **BloodHound:** Herramienta para mapear y visualizar las relaciones de Active Directory para identificar rutas de ataque.
68. **Metasploit Framework:** Plataforma integral para el desarrollo, prueba y ejecución de exploits.
69. **MsfVenom:** Generador de payloads dentro de Metasploit.
70. **Meterpreter:** Payload avanzado de Metasploit que ofrece un control extensivo sobre el sistema objetivo.
71. **Zero-Day Exploit:** Un exploit para una vulnerabilidad que es desconocida para el proveedor del software y, por lo tanto, no hay parche disponible.
72. **Cero-Click Exploit:** Un exploit que no requiere interacción de la víctima para ejecutarse.
73. **Armas de Día Cero (Zero-Day Weapons):** Exploits de día cero que han sido empaquetados y utilizados en ataques.
74. **Fuzzing:** Técnica de prueba de software donde se alimentan entradas inválidas, inesperadas o aleatorias a un programa para encontrar fallos o vulnerabilidades.

75. **Desbordamiento de Búfer (Buffer Overflow):** Una vulnerabilidad donde un programa escribe datos más allá de los límites de un búfer, sobrescribiendo la memoria adyacente.
76. **ASLR (Address Space Layout Randomization):** Técnica de seguridad para dificultar la explotación de desbordamientos de búfer aleatorizando las posiciones de memoria.
77. **DEP (Data Execution Prevention):** Característica de seguridad que marca áreas de memoria como no ejecutables.
78. **ROP (Return-Oriented Programming):** Técnica de explotación avanzada que encadena pequeños fragmentos de código existentes (gadgets) para ejecutar lógica maliciosa.
79. **Shellshock:** Famosa vulnerabilidad en la shell Bash que permitía la ejecución remota de código.
80. **EternalBlue:** Exploit de SMB utilizado por WannaCry y NotPetya.
81. **Privilege Escalation Kernel:** Explotación de vulnerabilidades en el núcleo del sistema operativo para escalar privilegios.

Hacking de Aplicaciones Web

82. **OWASP Top 10:** Los 10 riesgos de seguridad más críticos para las aplicaciones web.
83. **Inyección SQL (SQL Injection):** Inserción de código SQL malicioso en un campo de entrada para manipular la base de datos.
84. **Inyección de Comandos (Command Injection):** Inyección de comandos del sistema operativo en una aplicación vulnerable.
85. **XSS (Cross-Site Scripting):** Inserción de scripts maliciosos en páginas web vistas por otros usuarios (Reflejado, Almacenado, Basado en DOM).
86. **CSRF (Cross-Site Request Forgery):** Ataque que engaña a un usuario autenticado para que envíe una solicitud HTTP no deseada a una aplicación web.
87. **Insecure Deserialization:** Vulnerabilidad donde la deserialización de datos controlados por el atacante puede resultar en ejecución remota de código.

88. **Broken Authentication and Session Management:** Fallas en los mecanismos de autenticación o gestión de sesiones que permiten a los atacantes suplantar la identidad de los usuarios.
89. **XXE (XML External Entities):** Vulnerabilidad en procesadores XML que permite a los atacantes leer archivos locales o realizar ataques SSRF.
90. **SSRF (Server-Side Request Forgery):** Vulnerabilidad que permite a un atacante hacer que el servidor realice solicitudes HTTP a un destino arbitrario.
91. **LFI (Local File Inclusion):** Vulnerabilidad que permite incluir archivos locales del servidor.
92. **RFI (Remote File Inclusion):** Vulnerabilidad que permite incluir archivos de un servidor remoto.
93. **Upload de Archivos Peligrosos:** Permitir a los usuarios subir archivos con extensiones peligrosas o sin validación adecuada.
94. **Directory Traversal (Path Traversal):** Ataque para acceder a archivos y directorios fuera del directorio web raíz.
95. **Clickjacking:** Engañar a un usuario para que haga clic en un elemento invisible en una página web.
96. **CORS (Cross-Origin Resource Sharing):** Un mecanismo que permite a los recursos de una página web ser solicitados desde otro dominio fuera del dominio desde el cual se sirvió el primer recurso.
97. **Subdomain Takeover:** Ataque donde un atacante toma control de un subdominio que apunta a un servicio que ya no está en uso.
98. **Burp Suite:** Herramienta integrada para pruebas de seguridad de aplicaciones web (proxy, scanner, intruder, repeater).
99. **OWASP ZAP (Zed Attack Proxy):** Herramienta de código abierto para encontrar vulnerabilidades en aplicaciones web.
100. **WAF (Web Application Firewall):** Un firewall que protege las aplicaciones web de ataques específicos.
101. **API Hacking:** Pruebas de seguridad y explotación de interfaces de programación de aplicaciones (APIs).

102. **GraphQL Injection:** Explotación de vulnerabilidades en endpoints de GraphQL.

Redes y Criptografía

102. **Sniffing:** Captura y análisis de paquetes de datos que fluyen a través de una red.

103. **Man-in-the-Middle (MitM):** Ataque donde el atacante intercepta y/o altera la comunicación entre dos partes.

104. **ARP Spoofing:** Técnica MitM donde el atacante falsifica la tabla ARP para redirigir el tráfico.

105. **DNS Spoofing:** Falsificación de registros DNS para redirigir el tráfico a sitios maliciosos.

106. **SSL/TLS Stripping:** Ataque MitM que degrada una conexión HTTPS a HTTP, eliminando el cifrado.

107. **WPA/WPA2/WPA3:** Protocolos de seguridad para redes inalámbricas, de menor a mayor seguridad.

108. **PMKID Attack:** Una forma de ataque a redes WPA/WPA2 sin requerir un handshake completo.

109. **Evil Twin Attack:** Un punto de acceso Wi-Fi falso que imita uno legítimo para interceptar el tráfico.

110. **Jamming:** Interferir con la señal de radio para denegar el servicio inalámbrico.

111. **EAP (Extensible Authentication Protocol):** Marco de autenticación para redes cableadas e inalámbricas.

112. **Criptografía:** El estudio y la práctica de técnicas para comunicaciones seguras en presencia de adversarios.

113. **Cifrado Simétrico:** Uso de la misma clave para cifrar y descifrar.

114. **Cifrado Asimétrico (Clave Pública):** Uso de un par de claves (pública y privada) para cifrar y descifrar.

115. **Funciones Hash Criptográficas:** Funciones unidireccionales que producen un resumen de datos único (ej. MD5, SHA-256).

116. **Salting (Contraseñas):** Adición de un valor aleatorio (sal) a una contraseña antes de hashearla para evitar ataques de tabla arcoíris.

117. **Key Derivation Function (KDF):** Funciones que derivan una o más claves criptográficas a partir de una clave maestra o contraseña.

118. **TLS 1.3:** La última versión del protocolo TLS, con mejoras de seguridad y rendimiento.

119. **IPSec (Internet Protocol Security):** Suite de protocolos para proteger las comunicaciones IP.

120. **VPN (Virtual Private Network):** Conexión segura y cifrada a través de una red pública.

121. **Zero Trust Network:** Modelo de seguridad que asume que ninguna entidad (usuario, dispositivo, red) debe ser confiable por defecto.

122. **Ingeniería Social:** Manipulación psicológica para engañar a individuos y que divulguen información o realicen acciones.

123. **Phishing:** Ataque de ingeniería social para obtener credenciales o información sensible.

124. **Spear Phishing:** Phishing dirigido a individuos específicos.

125. **Whaling:** Phishing dirigido a ejecutivos de alto nivel (el "pez gordo").

126. **Vishing:** Phishing por teléfono.

127. **Smishing:** Phishing por SMS.

128. **Baiting:** Dejar un dispositivo infectado (ej. USB) en un lugar donde es probable que alguien lo encuentre y lo use.

129. **Pretexting:** Creación de un escenario o pretexto falso para engañar a la víctima.

130. **Tailgating (Piggybacking):** Seguir a alguien autorizado para obtener acceso no autorizado a un área restringida.

131. **Insider Threat:** Amenazas que provienen de dentro de la organización (empleados, ex-empleados, contratistas).

132. **Robo de Identidad:** Apropiación de datos personales para suplantar a alguien.

133. **Robo de Credenciales:** Obtención no autorizada de nombres de usuario y contraseñas.

134. **Keylogger:** Software o hardware para registrar pulsaciones de teclas.

135. **Rubber Ducky (USB Rubber Ducky):** Dispositivo USB que emula un teclado e inyecta payloads a alta velocidad.

136. **Malware:** Software malicioso.

137. **Gusano (Worm):** Malware auto-replicante que se propaga por la red.

138. **Troyano (Trojan Horse):** Malware disfrazado de software legítimo.

139. **Virus:** Malware que se adjunta a programas legítimos y requiere ejecución.

140. **Rootkit:** Software diseñado para ocultar la presencia de malware y mantener el acceso.

141. **Botnet:** Red de computadoras comprometidas controladas por un atacante.

142. **Ransomware:** Malware que cifra archivos y exige un rescate.

143. **Spyware:** Malware que espía la actividad del usuario.

144. **Adware:** Software que muestra publicidad no deseada.

145. **Polymorphic Malware:** Malware que cambia su código para evadir la detección de antivirus.

146. **Fileless Malware:** Malware que opera en la memoria RAM del sistema sin escribir en el disco.

147. **Honeypot:** Sistema trampa para atraer y estudiar a los atacantes.

148. **EDR (Endpoint Detection and Response):** Soluciones que monitorean y responden a amenazas en los puntos finales.

149. **SIEM (Security Information and Event Management):** Sistema que agrega y analiza eventos de seguridad de diversas fuentes.

150. **SOAR (Security Orchestration, Automation and Response):** Plataformas que automatizan y orquestan flujos de trabajo de respuesta a incidentes.