1. APT: Amenaza Persistente Avanzada, ataque sofisticado y prolongado.

2. Active Fingerprinting: Identificación activa del sistema operativo mediante paquetes personalizados.

3. ASN: Autonomous System Number, identifica redes conectadas a internet.

4. Banner Grabbing: Técnica para recolectar información de servicios.

5. Base64: Codificación de datos en texto ASCII.

6. BSSID: Identificador de red inalámbrica del punto de acceso.

7. Burp Collaborator: Servidor que detecta interacciones fuera de banda en pruebas de seguridad.

8. Byte Injection: Técnica que inyecta bytes maliciosos en paquetes.

9. CDN: Red de distribución de contenido.

10. CERT: Equipo de respuesta ante emergencias informáticas.

11. Certspotter: Herramienta para monitorear certificados TLS públicos.

12. Clickjacking: Engaño visual para hacer clic en contenido oculto.

13. CNAM: Registro que da información de un dominio o subdominio.

14. Cookie Poisoning: Alteración de cookies para modificar sesiones.

15. Credential Stuffing: Uso masivo de credenciales filtradas.

16. Cross-Site Tracing (XST): Técnica que explota el método TRACE HTTP.

17. CSP: Content Security Policy, política que evita inyecciones de código.

18. CSRF: Ataque que fuerza acciones no deseadas desde un navegador autenticado.

19. CVE: Vulnerabilidad comúnmente reconocida.

20. CVSS: Sistema de puntuación de severidad de vulnerabilidades.

21. DANE: Mecanismo para autenticar certificados usando DNSSEC.

22. DDoS: Denegación de servicio distribuida.

23. DKIM: Método de validación de correos con firmas criptográficas.

24. DNS Brute Force: Ataque que intenta descubrir subdominios mediante fuerza bruta.

25. DNS Cache Snooping: Técnica para identificar consultas DNS previas.

26. DNS Poisoning: Alteración maliciosa de respuestas DNS.

27. DNS Zone Transfer: Proceso que puede filtrar información si está mal configurado.

28. DoH: DNS sobre HTTPS, cifra consultas DNS.

29. Dumpster Diving: Búsqueda de información en basura física o digital.

30. EC2: Servicio de instancias virtuales de Amazon Web Services.

31. EDR: Endpoint Detection and Response.

32. Encabezados HTTP: Información adicional enviada en una solicitud/respuesta web.

33. Entropy: Medida del desorden o aleatoriedad, útil para analizar datos cifrados.

34. Enumeration: Técnica para listar recursos en una red.

35. ESP: Encapsulating Security Payload, parte de IPsec.

36. Exfiltration: Extracción de datos sin autorización.

37. Exploit: Código que aprovecha una vulnerabilidad.

38. Favicon Hash: Huella digital de un sitio web a partir de su ícono.

39. FIM: File Integrity Monitoring.

40. Fingerprint: Identificación de un sistema por características únicas.

41. FOCA: Herramienta para recolectar metadatos de documentos.

42. Form Hijacking: Intercepción de formularios para capturar datos.

43. FQDN: Nombre de dominio completamente calificado.

44. FTP Bounce: Técnica que abusa del protocolo FTP para escanear puertos.

45. fuzzing: Técnica que envía datos aleatorios para detectar fallos.

46. gTLD: Dominio de nivel superior genérico como .com o .org.

47. HAR File: Registro de actividad de red en navegadores.

48. Hash Collision: Dos entradas diferentes producen el mismo hash.

49. Headers Injection: Inyección maliciosa en encabezados HTTP.

50. Heartbleed: Famosa vulnerabilidad en OpenSSL.

51. HSTS: Mecanismo que fuerza HTTPS.

52. Hybrid Analysis: Análisis de malware combinando técnicas estáticas y dinámicas.

53. ICMP Tunneling: Uso de paquetes ICMP para evadir firewalls.

54. IDOR: Vulnerabilidad donde usuarios acceden a objetos ajenos modificando identificadores.

55. IDS: Sistema de detección de intrusos.

56. iframe Injection: Inyección de iframes maliciosos en páginas web.

57. Info Disclosure: Filtración de información sensible.

58. Injection: Técnica para alterar consultas con datos externos.

59. INTELLIGENT SCAN: Escaneo inteligente en herramientas como Burp.

60. IoC: Indicador de Compromiso.

61. IP Spoofing: Suplantación de IP para ocultar origen real.

62. JARM: Huella digital TLS basada en patrones de respuesta del servidor.

63. JSON Hijacking: Robo de datos JSON mediante scripts.

64. Kerberoasting: Ataque contra servicios Kerberos.

65. LFI: Inclusión local de archivos en aplicaciones web.

66. LLMNR Poisoning: Suplantación de respuestas en redes locales.

67. Log Injection: Alteración de registros para ocultar actividad.

68. Mac Flooding: Ataque que satura tablas MAC en switches.

69. Maltego: Herramienta OSINT para relaciones entre entidades.

70. MITM: Interceptor entre dos partes que creen comunicarse entre sí.

71. Mutillidae: Aplicación web vulnerable usada para prácticas de hacking ético.

72. MX Record: Registro DNS que define el servidor de correo.

73. Nessus: Escáner de vulnerabilidades.

74. Netcat: Herramienta para conectividad de red, también usada en explotación.

75. NMAP Scripting Engine (NSE): Scripts que amplían funciones de Nmap.

76. NoSQL Injection: Inyección dirigida a bases de datos NoSQL.

77. NS Record: Registro DNS que define los servidores autoritativos.

78. NTLM Relay: Técnica que reutiliza autenticaciones NTLM.

79. OS Fingerprinting: Identificación del sistema operativo de un host.

80. OSINT: Inteligencia de fuentes abiertas.

81. OWASP ZAP: Herramienta para pruebas automatizadas de seguridad web.

82. Packet Sniffing: Intercepción de paquetes de red.

83. Passive Reconnaissance: Obtención de información sin interactuar con el objetivo.

84. PFS: Perfect Forward Secrecy, protege claves antiguas aunque se comprometa la actual.

85. PII: Información personal identificable.

86. Pivoting: Uso de una máquina comprometida para moverse lateralmente.

87. Port Knocking: Técnica para abrir puertos solo tras una secuencia específica.

88. p0f: Herramienta para reconocimiento pasivo de sistemas operativos.

89. PTR Record: Registro DNS inverso.

90. RAT: Herramienta de acceso remoto, muchas veces maliciosa.

91. Reflected XSS: Inyección de scripts en peticiones que se devuelven al usuario.

92. Replay Attack: Reutilización de datos capturados para obtener acceso.

93. RFI: Inclusión remota de archivos.

94. RST Scan: Técnica de escaneo que espera respuestas RST.

95. SaaS Misconfig: Configuración incorrecta de servicios en la nube.

96. SCTP: Protocolo de comunicación alternativo a TCP/UDP.

97. SDLC: Ciclo de vida del desarrollo seguro.

98. SEH Overwrite: Técnica de explotación basada en excepciones de Windows.

99. Session Fixation: Ataque donde se fuerza una sesión al usuario.

100. Shodan: Buscador de dispositivos conectados a internet.

101. SIEM: Sistema de gestión de eventos e información de seguridad.

102. SLAAC: Asignación automática de direcciones IPv6.

103. SMB Relay: Reenvío malicioso de autenticaciones SMB.

104. Smurf Attack: Ataque DDoS con paquetes ICMP.

105. Snort: IDS de código abierto basado en reglas.

106. SPF: Política para prevenir falsificación de remitentes en emails.

107. SQLMap: Herramienta para detectar y explotar inyecciones SQL.

108. SSH Tunneling: Encapsulamiento seguro de tráfico a través de SSH.

109. SSRF: Ataque que fuerza a un servidor a hacer peticiones internas.

110. Stack Smashing: Sobrescritura del stack para ejecución de código.

111. SSLStrip: Ataque que elimina cifrado SSL en conexiones.

112. STUN: Protocolo para descubrir IP pública detrás de NAT.

113. Subdomain Takeover: Toma de control de subdominios mal configurados.

114. SYN Flood: Ataque que agota recursos de conexión TCP.

115. TShark: Versión en consola de Wireshark.

116. TCP RST Injection: Corte forzado de conexiones TCP.

117. TLS Fingerprinting: Identificación por características de cifrado TLS.

118. TOCTOU: Condición de carrera entre verificación y uso.

119. UDP Scan: Escaneo de puertos UDP.

120. Unicode Obfuscation: Uso de caracteres Unicode para evadir filtros.

121. User-Agent Spoofing: Suplantación de agente de usuario en peticiones HTTP.

122. UTM: Unified Threat Management.

123. UXSS: Cross-site scripting desde la misma aplicación local.

124. VLAN Hopping: Movimiento entre VLANs mediante técnicas maliciosas.

125. VPN Leak: Filtración de IP real al usar VPN.

126. VTP Attack: Ataque al protocolo VLAN Trunking Protocol.

127. WAF Bypass: Evasión de firewalls de aplicaciones web.

128. WebSocket Hijacking: Control malicioso de conexiones WebSocket.

129. WHOIS: Información pública sobre dominios y propietarios.

130. WiFi Pineapple: Dispositivo para ataques MITM en redes WiFi.

131. Wireshark: Analizador de tráfico de red.

132. Wordlist: Lista de palabras usada para ataques de fuerza bruta.

133. X-Content-Type-Options: Encabezado que impide interpretación incorrecta de archivos.

134. X-Frame-Options: Encabezado que previene ataques de clickjacking.

135. X-XSS-Protection: Protección básica contra XSS en navegadores.

136. XML External Entity (XXE): Vulnerabilidad en procesadores XML.

137. YAML Deserialization: Riesgo al interpretar YAML no controlado.

138. Zero-Day: Vulnerabilidad desconocida por el fabricante.

139. ZAP Spider: Herramienta de rastreo en OWASP ZAP.

140. Zombie: Dispositivo comprometido que participa en botnets.

141. Zone Walking: Exploración de zonas DNSSEC.

142. .htaccess Bypass: Evasión de reglas impuestas en archivos .htaccess.

143. /etc/passwd Disclosure: Exposición del archivo de contraseñas en Linux.

144. .git Folder Disclosure: Acceso indebido a repositorios Git expuestos.

145. Burp Intruder: Herramienta para pruebas automatizadas en Burp Suite.

146. Burp Repeater: Envío repetido de peticiones para pruebas manuales.

147. Zap Active Scan: Análisis de seguridad activo automatizado.

148. Zap Passive Scan: Detección no intrusiva de vulnerabilidades.

149. Zap Contexts: Configuración de alcance en pruebas con ZAP.

150. FOCA Metadata: Extracción de datos ocultos en documentos.

151. DNSDumpster: Herramienta OSINT para recolección DNS.

152. CentralOps: Herramienta online para pruebas básicas de red.

153. theHarvester: Recolector de correos, dominios y hosts expuestos.

154. Shodan Filters: Parámetros de búsqueda avanzados en Shodan.

155. Nmap Stealth Scan: Escaneo sigiloso con paquetes SYN.

156. Wireshark Filters: Filtros para análisis preciso de tráfico.

157. Tshark Capture: Captura de paquetes por línea de comandos.

158. Burp Proxy: Interceptación de tráfico HTTP/S en Burp Suite.

159. ZAP HUD: Interfaz gráfica incrustada en el navegador de ZAP.

160. HTTP Smuggling: Manipulación de encabezados para evadir controles.

161. Reverse DNS Lookup: Resolución de IP hacia nombre de dominio.