# GLOSARIO

1. **Hacking Ético**: Práctica legal y autorizada para evaluar la seguridad de sistemas informáticos.
2. **Pentesting (Pruebas de Penetración)**: Simulación controlada de ataques para encontrar vulnerabilidades.
3. **Vulnerabilidad**: Debilidad o falla en un sistema que puede ser explotada.
4. **Exploit**: Código o técnica que aprovecha una vulnerabilidad para comprometer un sistema.
5. **Ingeniería Social**: Técnica para manipular personas y obtener información confidencial.
6. **Phishing**: Fraude que simula ser una entidad confiable para robar datos.
7. **Footprinting**: Recolección inicial de información sobre un objetivo para planificar un ataque.
8. **Reconocimiento Pasivo**: Obtención de información sin interactuar directamente con el objetivo.
9. **Reconocimiento Activo**: Búsqueda de información interactuando directamente con el objetivo.
10. **Escaneo de Puertos**: Proceso para identificar puertos abiertos en un dispositivo.
11. **Escaneo de Vulnerabilidades**: Análisis para detectar fallas de seguridad conocidas.
12. **Fuerza Bruta**: Método que prueba todas las combinaciones posibles para romper contraseñas.
13. **Backdoor (Puerta Trasera)**: Acceso oculto que permite entrar sin autorización.
14. **Rootkit**: Software diseñado para ocultar la presencia de malware.
15. **Keylogger**: Programa que registra las teclas pulsadas en un teclado.
16. **Sniffing**: Captura y análisis de tráfico de red.
17. **Spoofing**: Falsificación de identidad para engañar a un sistema o usuario.
18. **SQL Injection**: Ataque que inserta código SQL malicioso en una base de datos.
19. **XSS (Cross-Site Scripting)**: Inserción de scripts maliciosos en páginas web.
20. **DoS (Denial of Service)**: Ataque que interrumpe el funcionamiento de un servicio.
21. **DDoS (Distributed Denial of Service)**: DoS ejecutado desde múltiples dispositivos.
22. **Firewall**: Dispositivo o software que controla el tráfico de red entrante y saliente.
23. **IDS (Intrusion Detection System)**: Sistema que detecta accesos o ataques no autorizados.
24. **IPS (Intrusion Prevention System)**: Sistema que bloquea ataques detectados en tiempo real.
25. **VPN (Virtual Private Network)**: Red privada que cifra y protege la conexión a internet.
26. **Hash**: Valor único generado a partir de datos para proteger su integridad.
27. **Criptografía**: Ciencia que protege la información mediante códigos y cifrados.
28. **Token**: Elemento para autenticar usuarios, como un código o dispositivo.
29. **Zero-Day**: Vulnerabilidad desconocida por los desarrolladores y sin parche.
30. **MitM (Man in the Middle)**: Ataque donde un atacante intercepta comunicaciones entre dos partes.
31. **PrivEsc (Privilege Escalation)**: Técnica para obtener permisos elevados en un sistema.
32. **Enumeración**: Identificación detallada de recursos, usuarios y servicios en un sistema.
33. **Payload**: Código malicioso enviado para ejecutar acciones tras una explotación.
34. **Shell**: Interfaz para controlar un sistema mediante comandos.
35. **Meterpreter**: Herramienta que permite controlar remotamente un sistema comprometido.
36. **Burp Suite**: Software para probar la seguridad de aplicaciones web.
37. **Nmap**: Herramienta para descubrir hosts y servicios en una red.
38. **Wireshark**: Programa para analizar paquetes de datos en la red.
39. **Metasploit**: Plataforma para desarrollar y ejecutar exploits.
40. **OSINT (Open Source Intelligence)**: Información recopilada de fuentes públicas.
41. **Dominio**: Nombre que identifica a un sitio web en internet.
42. **Subdominios**: Divisiones dentro de un dominio principal que organizan servicios.
43. **Mapeo DNS**: Proceso de identificación de registros DNS relacionados con un dominio.
44. **Name Servers (NS)**: Servidores que administran la información DNS de un dominio.
45. **Registros MX**: Configuraciones DNS que especifican servidores de correo.
46. **Registros TXT**: Registros DNS que almacenan información como SPF o claves.
47. **SPF (Sender Policy Framework)**: Política que define qué servidores pueden enviar correos en nombre de un dominio.
48. **DMARC**: Protocolo que ayuda a prevenir fraudes en correos electrónicos.
49. **WHOIS**: Servicio para consultar la información de registro de un dominio.
50. **FOCA**: Herramienta para extraer metadatos de documentos públicos.
51. **Metadatos**: Datos que describen información oculta en archivos digitales.
52. **Shodan**: Motor de búsqueda que encuentra dispositivos conectados a internet.
53. **Servicios Expuestos**: Aplicaciones accesibles públicamente desde internet.
54. **CVE (Common Vulnerabilities and Exposures)**: Registro público de vulnerabilidades conocidas.
55. **Google Dorks**: Técnicas avanzadas para buscar información sensible en Google.
56. **TTL (Time To Live)**: Tiempo que un registro DNS permanece en caché.
57. **Geolocalización IP**: Estimación de la ubicación geográfica de una IP.
58. **Rutas Internas**: Directorios o ubicaciones internas descubiertas en sistemas o documentos.
59. **Software y Versiones**: Información sobre programas usados y su versión, útil para seguridad.
60. **Puertos Críticos**: Puertos comunes como 22 (SSH), 80 (HTTP) y 443 (HTTPS).
61. **Versión Vulnerable**: Versión de software con fallos conocidos de seguridad.
62. **Autor del Documento**: Persona identificada en los metadatos de un archivo.
63. **Amazon Registrar**: Empresa que registra nombres de dominio.
64. **Google Cloud Platform**: Plataforma de servicios en la nube de Google.
65. **IP Pública**: Dirección IP accesible desde internet.
66. **DNSDumpster**: Herramienta para obtener información DNS y subdominios.
67. **CentroLOPS.net**: Plataforma usada para análisis OSINT.
68. **Reconocimiento Web**: Análisis de sitios web para obtener información.
69. **Open Ports**: Puertos de red que están abiertos y aceptan conexiones.
70. **Banner Grabbing**: Técnica para obtener información del software de un servicio.
71. **Fingerprinting**: Identificación precisa de sistemas operativos o aplicaciones.
72. **WAF (Web Application Firewall)**: Firewall especializado en proteger aplicaciones web.
73. **Captcha Bypass**: Técnicas para evitar sistemas CAPTCHA.
74. **Directory Traversal**: Ataque que accede a archivos fuera del directorio permitido.
75. **Command Injection**: Ejecución de comandos arbitrarios en un servidor vulnerable.
76. **Brute Force Tool**: Software diseñado para realizar ataques de fuerza bruta.
77. **Social Engineering Toolkit (SET)**: Herramienta para simular ataques de ingeniería social.
78. **ARP Spoofing**: Ataque que falsifica direcciones MAC en una red local.
79. **MAC Address Spoofing**: Falsificación de la dirección física de un dispositivo.
80. **Credential Dumping**: Robo masivo de credenciales almacenadas en un sistema.
81. **Reverse Shell**: Conexión remota iniciada desde la máquina comprometida hacia el atacante.
82. **Persistence**: Técnicas para mantener acceso continuo a un sistema comprometido.
83. **Escalada Lateral**: Movimiento dentro de una red para comprometer otros sistemas.
84. **Pivoting**: Uso de una máquina comprometida para atacar otras dentro de la red.
85. **Payload Encoders**: Técnicas para modificar payloads y evadir detección.
86. **Obfuscation**: Técnicas para ocultar código malicioso o actividad sospechosa.
87. **Wordlist**: Lista de palabras usadas para ataques de fuerza bruta o diccionario.
88. **Rainbow Tables**: Tablas precomputadas para revertir funciones hash y crackear contraseñas.
89. **Dictionary Attack**: Ataque basado en probar contraseñas usando una lista común de palabras.
90. **Malware**: Software diseñado para dañar o comprometer sistemas.
91. **Spyware**: Software que espía actividades del usuario sin consentimiento.
92. **Adware**: Programa que muestra publicidad no deseada.
93. **Ransomware**: Malware que cifra datos y exige rescate para recuperarlos.
94. **Botnet**: Red de dispositivos infectados controlados remotamente por un atacante.
95. **C2 (Command and Control)**: Servidor usado para controlar dispositivos comprometidos.
96. **Bug Bounty**: Programa que recompensa la detección responsable de vulnerabilidades.
97. **Seguridad Ofensiva**: Estrategias para probar y mejorar la seguridad mediante ataques controlados.
98. **Seguridad Defensiva**: Medidas para proteger sistemas y detectar intrusos.
99. **Auditoría de Seguridad**: Evaluación formal de la seguridad de sistemas o redes.
100. **Hardening**: Proceso de fortalecer la seguridad de un sistema reduciendo vulnerabilidades.