ING. REDES INTELIGENTES Y CIBERSEGURIDAD

Universidad Tecnológica de Cancún.

Alumno:

Moo Canul Jesús Enrique

Grupo: IRIYC91

1. **AES, RSA, ECC:** Algoritmos de cifrado simétrico y asimétrico.
2. **Análisis de Tráfico**: Interpretación de datos capturados.
3. **ARP Spoofing**: Suplantación de direcciones ARP para interceptar tráfico.
4. **ASN (Autonomous System Number)**: Identificador único de redes.
5. **Authentication Testing**: Verificación de control de acceso.
6. **AWS, Azure, Google Cloud:** Plataformas de computación en la nube.
7. **Backdoor:** Puerta trasera para mantener acceso a un sistema.
8. **BeEF:** Framework para ataques a navegadores web.
9. **BGP, OSPF, RIP:** Protocolos de enrutamiento entre routers.
10. **Blue Team:** Grupo que defiende la infraestructura (defensiva).
11. **Broken Authentication**: Fallas en los mecanismos de autenticación.
12. **Brute Force**: Intentos repetidos de contraseña.
13. **Buffer Overflow:** Error que permite sobrescribir la memoria.
14. **Bug Bounty**: Recompensa por descubrir vulnerabilidades.
15. **Burp Intruder**: Realiza ataques automatizados.
16. **Burp Proxy**: Intercepta y modifica tráfico HTTP/HTTPS.
17. **Burp Repeater**: Reenvía solicitudes modificadas.
18. **Burp Scanner**: Escaneo automatizado de vulnerabilidades.
19. **Burp Suite**: Plataforma para pruebas de seguridad de aplicaciones web.
20. **Captcha Bypass**: Técnicas para saltar sistemas CAPTCHA.
21. **Captura de Paquetes**: Registro del tráfico que pasa por una red.
22. **CentroLOPS.net**: Portal que provee análisis e información OSINT.
23. **CIA (Confidencialidad, Integridad y Disponibilidad):** Principios clave de la seguridad informática.
24. **Clickjacking**: Engaña al usuario para hacer clic en contenido oculto.
25. **Command Injection**: Inyección de comandos del sistema.
26. **Common Crawl**: Repositorio masivo de datos de sitios web.
27. **Cookie Poisoning**: Alteración de cookies para obtener acceso.
28. **Credential Stuffing**: Uso de credenciales filtradas en múltiples sitios.
29. **CSP (Content Security Policy)**: Mitiga ataques como XSS.
30. **CSRF (Cross-Site Request Forgery)**: Forzar a usuarios a ejecutar acciones no deseadas.
31. **CSRF:** Ataque que fuerza a un usuario autenticado a ejecutar acciones no deseadas.
32. **CVE:** Identificadores públicos de vulnerabilidades conocidas.

33. **CWE (Common Weakness Enumeration)**: Clasificación de debilidades comunes.
34. **DHCP:** Protocolo que asigna direcciones IP dinámicas.
35. **Dirección IP**: Identificador numérico de un dispositivo en red.
36. **Directory Traversal**: Acceso a archivos fuera del directorio raíz.
37. **DNS:** Sistema que traduce nombres de dominio a direcciones IP.
38. **DNSDumpster**: Herramienta para recolección de información DNS.
39. **Docker:** Plataforma para crear, desplegar y ejecutar contenedores.
40. **Dockerfile:** Script para construir una imagen de Docker.
41. **Escaneo OS**: Detección del sistema operativo del host remoto.
42. **Filtro BPF**: Expresiones para filtrar tráfico en Wireshark y Tshark.
43. **Fingerprinting**: Identificación del sistema operativo, software o estructura de red.
44. **FingerprintJS**: Biblioteca para identificar navegadores de usuarios.
45. **FOCA**: Herramienta para extraer metadatos de documentos.
46. **FTP (File Transfer Protocol)**: Transferencia de archivos.
47. **Fuzzing**: Envío de entradas aleatorias para encontrar fallos.
48. **Geolocalización IP**: Determina ubicación geográfica aproximada de una IP.
49. **Google Dorking**: Búsqueda avanzada usando comandos especiales en Google.
50. **Hacking Ético:** Práctica autorizada de probar sistemas informáticos para identificar vulnerabilidades con el fin de mejorar su seguridad.
51. **Hash:** Función que transforma datos en una huella digital fija.
52. **HTML Injection**: Inserción de código HTML malicioso.
53. **HTTP (Hypertext Transfer Protocol)**: Comunicación web.
54. **HTTPS (HTTP Secure)**: HTTP con cifrado TLS.
55. **IAM:** Gestión de identidad y acceso en la nube.
56. **ICMP (Internet Control Message Protocol)**: Para mensajes de control.
57. **IP/Subneteo:** Método para dividir redes IP en subredes más pequeñas.
58. **Kali Linux:** Distribución Linux para pruebas de penetración.
59. **LFI (Local File Inclusion)**: Inclusión de archivos locales en la aplicación.
60. **Metadatos**: Información oculta en archivos que describe propiedades del documento.
61. **Metasploit:** Framework para explotación de vulnerabilidades.
62. **Mimikatz:** Herramienta para extraer contraseñas y hashes de memoria.
63. **MITM (Man In The Middle)**: Ataque en el que el tráfico es interceptado.
64. **Modelo OSI:** Marco de 7 capas para entender cómo se comunican los sistemas de red.

65. **Mutillidae**: Aplicación web vulnerable para prácticas de seguridad.
66. **Nmap**: Herramienta para escaneo de redes y detección de servicios.
67. **OSINT (Open Source Intelligence)**: Información recopilada de fuentes públicas.
68. **OWASP Top 10:** Lista de las 10 vulnerabilidades más críticas en aplicaciones web.
69. **OWASP ZAP**: Herramienta open-source de análisis de seguridad.
70. **PCI-DSS:** Normativa para proteger datos de tarjetas de pago.
71. **Pen Tester**: Profesional que realiza pruebas de penetración.
72. **Ping Sweep**: Envío de pings a múltiples hosts para descubrir cuáles están activos.
73. **PowerShell:** Consola de comandos avanzada para Windows.
74. **Protocolos de Red**: Conjunto de reglas para comunicación digital.
75. **Pruebas de Penetración Web**: Simulación de ataques para detectar vulnerabilidades.
76. **Purple Team:** Colaboración entre red y blue team.
77. **Recon-ng, Maltego:** Herramientas OSINT para recolectar información.
78. **Reconocimiento Activo**: Recolección de datos interactuando directamente con el objetivo.
79. **Reconocimiento Pasivo**: Técnica para obtener información sin interactuar directamente con el objetivo.
80. **Red Team:** Grupo que simula ataques (ofensiva).
81. **Registro CNAME**: Alias de otro nombre de dominio.
82. **Registro DNS A**: Asocia un dominio con una dirección IPv4.
83. **Registro MX**: Registro DNS para servidores de correo.
84. **Registro TXT**: Registro DNS con información adicional como SPF.
85. **RFI (Remote File Inclusion)**: Inclusión de archivos remotos.
86. **robots.txt**: Archivo que indica a los bots qué contenido evitar.
87. **Rootkit:** Software que oculta procesos o archivos para evitar detección.
88. **ROP (Return Oriented Programming):** Técnica avanzada de explotación.
89. **Scan de Puertos**: Detecta servicios abiertos en un host.
90. **Scan de Versiones**: Determina versión de servicios y sistemas.
91. **Scan SYN**: Escaneo de puertos con paquetes SYN.
92. **Scan UDP**: Escaneo para descubrir servicios usando UDP.
93. **Script NSE (Nmap Scripting Engine)**: Scripts de Nmap para tareas avanzadas.
94. **Scrum/Kanban:** Metodologías ágiles para gestión de proyectos.
95. **Security Headers**: Cabeceras HTTP que protegen contra ataques.
96. **Session Hijacking**: Secuestro de sesiones activas.

97. **Shodan**: Motor de búsqueda de dispositivos conectados a Internet.
98. **SIEM:** Sistema para gestionar y correlacionar eventos de seguridad.
99. **SMB, LDAP, RDP, SNMP:** Servicios de red comúnmente atacados.
100. **SMTP (Simple Mail Transfer Protocol)**: Envío de correos.
101. **Snapshots:** Puntos de restauración en máquinas virtuales.
102. **SNMP (Simple Network Management Protocol)**: Gestión de dispositivos en red.
103. **SPF (Sender Policy Framework)**: Previene suplantación en correos electrónicos.
104. **SQL Injection**: Inyección de código SQL para acceder a bases de datos.
105. **sqlmap:** Automatiza la detección de inyecciones SQL.
106. **SSL/TLS Scan**: Verifica certificados digitales de sitios web.
107. **STP:** Protocolo para evitar bucles en redes Ethernet.
108. **Subdominios**: Dominios secundarios bajo un dominio principal.
109. **TCP (Transmission Control Protocol)**: Protocolo orientado a conexión.
110. **TCP Three-way Handshake**: Proceso de inicio de conexión TCP.
111. **TCP/IP:** Conjunto de protocolos de comunicación para Internet.
112. **theHarvester**: Herramienta para recolectar correos, nombres de dominio y usuarios.
113. **TLS/SSL:** Protocolos para comunicaciones cifradas en red.
114. **Traceroute**: Muestra el camino que sigue un paquete hacia su destino.
115. **Tshark**: Versión de línea de comandos de Wireshark.
116. **UDP (User Datagram Protocol)**: Protocolo sin conexión.
117. **VLAN:** Red de área local virtual para segmentar tráfico en switches.
118. **VMware, VirtualBox:** Plataformas para virtualizar sistemas operativos.
119. **Volatility:** Herramienta para análisis forense de memoria RAM.
120. **Vulnerability Scanning**: Detección de debilidades en una app.
121. **WAF (Web Application Firewall)**: Filtro de tráfico web malicioso.
122. **Wayback Machine**: Archivo de versiones antiguas de sitios web.
123. **Whois**: Protocolo para consultar registros de dominio.
124. **Wireshark/tcpdump:** Herramientas para captura y análisis de tráfico.
125. **Wireshark**: Analizador de protocolos de red gráfico.
126. **Wordlist**: Lista de palabras usadas en ataques de diccionario.
127. **X.509:** Estándar de certificados digitales.
128. **XSS (Cross-site Scripting)**: Inyección de scripts maliciosos en sitios web.
129. **XSS:** Inyección de scripts en páginas web.
130. **ZAP Active Scan**: Prueba activamente posibles vulnerabilidades.

131. **ZAP Passive Scan**: Escaneo sin interacción directa.
132. **ZAP Spider**: Rastrea todas las URLs del sitio web.
133. **Zone Transfer**: Técnica para obtener información completa de una zona DNS.