

◆ Contenido

Introducción	XI
---------------------------	----

Capítulo 1

Arquitectura de red y seguridad	1
1.1 Introducción	2
1.2 Arquitectura de red	2
1.2.1 Modelos de red	3
1.2.2 Enrutadores e interruptores	3
1.3 Protocolos de red	4
1.3.1 Protocolo de control de transmisión (TCP)	5
1.3.2 Protocolo de transferencia de archivos (FTP)	10

Capítulo 2

Arquitectura de Internet	11
2.1 Introducción	12
2.2 Protocolo de Internet (IP)	12
2.2.1 Direcciones IP	14
2.2.2 IPv4	14
2.2.3 Máscara de subred	16
2.2.4 Subredes	18
2.2.5 Compuerta estándar	20
2.2.6 IPv6	21
2.2.7 ID de la red y del host	26
2.3 Componentes del enrutador	27
2.3.1 Protocolo de control del host dinámico (DHCP)	27
2.3.2 Firewalls	27
2.3.3 Traducción de direcciones de red (NAT)	28
2.3.4 Direcciones IP públicas reservadas	29
2.4 Sistema de nombre de dominio (DNS)	29
2.5 HTTP	30
2.5.1 Localizador uniforme de recursos (URL)	31
2.5.2 Métodos HTTP	33
2.6 Protocolo SMTP	35
2.7 Modelos OSI y TCP/IP	36

Capítulo 3

Criptografía	39
3.1 Introducción	40

3.2 HTTP y SSL	40
3.2.1 SSL	41
3.2.2 Protocolo de enlace (handshake) SSL	42
3.2.3 SSL abierto (OpenSSL)	44
3.2.4 HSTS	52
3.3 Algoritmos o cifrados	53
3.3.1 Cifrados en flujo	53
3.3.2 Cifrados por bloque	57
3.3.3 Cifrado autenticado Authenticated Encryption (AE)	59
3.3.4 Estándar de cifrado avanzado (AES)	60
3.3.5 Otras herramientas de cifrado	63

Capítulo 4

Arquitectura de software	65
4.1 Introducción	66
4.2 Diagramas UML	66
4.2.1 Diagrama de componentes UML	67
4.2.2 Diagrama de despliegue de UML	72
4.2.3 Diagrama de flujo de datos UML (DFD)	73
4.3 Patrones de arquitectura de software	74
4.3.1 Arquitectura orientada a objetos (OOA)	75
4.3.2 Arquitectura orientada a recursos (ROA)	78
4.3.3 Arquitectura orientada a servicios (SOA)	79
4.4 Arquitectura de servidor Proxy	82
4.4.1 Cortafuegos y cifrado	83
4.4.2 Escalabilidad de la arquitectura	86
4.4.3 Almacenamiento en caché de datos	88
4.4.4 Servidores proxy web	88

Capítulo 5

Organización de un ambiente Pentest	91
5.1 Introducción	92
5.2 Configuración de Pentest	92
5.3 Cómo instalar una VirtualBox	93
5.4 Cómo instalar la máquina virtual Kali Linux	95
5.4.1 Configuración del disco duro	102
5.5 Sistema de archivos Linux	108
5.6 Advanced Packaging Tool (Herramienta de gestión de Paquetes, APT)	118
5.6.1 Más comandos APT	120
5.6.2 Comandos apt-cache	121
5.6.3 Gestor de paquetes Synaptic	122
5.7 Cómo instalar LAMP	123

5.8 Instalación de Visual Studio Code	127
5.9 Cómo clonar configuraciones Kali	128
5.10 Cómo instalar la máquina virtual de OWASP-BWA	132
5.11 Hackeo ético	140

Capítulo 6

Pruebas de penetración	141
6.1 Introducción	142
6.2 Fundación OWASP	142
6.3 Reconocimiento	143
6.3.1 Servicios de escaneo con nmap	143
6.3.2 Identificación de cortafuegos (firewalls) de la aplicación	143
6.3.3 Burp suite	146
6.3.4 Spiders y crawlers (arañas y rastreadores)	153
6.4 Inyección (SQL, OS, XXE y LDAP)	158
6.4.1 Escáneres automáticos	160
6.5 Irrupción en la autenticación y la sesión	168
6.6 Cross Site Scripting (XSS) Scripting de sitio cruzado	170
6.6.1 Escáner automático	171
6.7 Irrupción en el control de acceso	173
6.8 Configuración insegura	178
6.9 Exposición de datos sensibles	179
6.10 Insuficiente protección de un ataque	184
6.11 Cross-Site Request Forgery (CSRF) Falsificación de peticiones en sitios cruzados	186
6.12 Uso de componentes con vulnerabilidades conocidas	190
6.13 API desprotegidas	190

Capítulo 7

SECURE Software Lifecycle (SSLC)	191
7.1 Introducción	192
7.2 ¿Qué es información segura?	192
7.2.1 Activos	192
7.2.2 El triángulo de la CIA (Confidencialidad, Integridad y Acceso)	192
7.3 Secure Software Lifecycle (SSLC o ciclo de vida del software seguro)	193
7.3.1 El proyecto VideoBox	194
7.3.2 Propósito de la aplicación	194
7.4 SSLC: Analizar	195
7.5 SSLC: Diseño	196
7.5.1 Modelado de amenazas	198
7.6 SSLC: Plan de pruebas de penetración	204
7.6.1 Pruebas manuales de penetración	204
7.6.2 Pruebas de penetración automatizadas	204
7.7 SSLC: Programación defensiva	205
7.7.1 Principios del diseño del código	205

7.7.2 Mejores prácticas y listas de verificación	207
7.7.3 Access Control (Gestión de acceso)	208
7.7.4 Manejo de errores	221
7.7.5 RESTful API	223
7.7.6 La herramienta Curl	228
7.7.7 Jason Web Token (JWT)	232
7.7.8 Proyecto Bazar de ciudades	234
7.7.9 Mitigaciones	243
7.7.10 Proyecto VideoBox [continuación]	246
7.7.11 Revisión de código	247
7.8 SSLC: Pruebas pentest	250
7.9 SSLC: Cómo implementar	252
7.9.1 El modelo DevOps	252
Índice analítico	255