

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO 1. ANTECEDENTES	7
1.1 Desarrollo del software libre.....	8
1.2 Sistemas operativos de libre distribución	12
1.3 Las redes de computadoras	14
1.4 Servicios de red	20
1.5 Modelos OSI y TCP/IP	21
1.6 Protocolos de red	26
1.7 Normas de seguridad	35
1.8 Tipos de amenazas en una red	37
CAPÍTULO 2. ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD DE LA RED	41
2.1 Normas de evaluación.....	42
2.2 Generalidades de la red y servicios a proteger.....	44
2.3 Modelado de amenazas y gestión de riesgos	46
2.4 Diseño del perímetro de la red	52
2.5 Características del sistema operativo	55
2.6 Requerimientos de seguridad del servidor	56
2.7 Herramientas de filtrado y monitoreo	58
CAPÍTULO 3. HERRAMIENTAS DE SOFTWARE LIBRE A IMPLEMENTAR EN LA RED	61
3.1 Herramientas para reforzar el sistema operativo	62
3.2 Protección de contraseñas y ataques de fuerza bruta	67
3.3 Seguridad del equipo	69
3.4 Herramientas para web	73
3.5 Rastreadores	76
3.6 Herramientas para auditar y defender la red	78

CAPÍTULO 4. CONFIGURACIÓN E IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE DEFENSA	85
4.1 Herramientas para reforzar el sistema operativo	86
4.2 Protección de contraseñas y ataques de fuerza bruta	91
4.3 Seguridad del equipo	93
4.4 Herramientas para web	99
4.5 Rastreadores	100
4.6 Herramientas para auditar y defender la red	102
CAPÍTULO 5. PRUEBAS DEL SISTEMA DE DEFENSA	117
5.1 Plan de pruebas	118
5.2 John the Ripper	119
5.3 Nessus	121
5.4 Nikto	124
5.5 Wireshark	126
5.6 Turtle Firewall	129
5.7 El Sistema de Detección de Intrusos	133
CAPÍTULO 6. PRÁCTICA REFORZAMIENTO DE LA SEGURIDAD CON BASTILLE (HARDENING).....	139
CONCLUSIONES	155
ANEXOS	161
Anexo 1. Práctica – Alumnos, reforzamiento de la seguridad con Bastille (hardening)	162
GLOSARIO	177
BIBLIOGRAFÍA	181