

Índice

I	Introducción y Objetivos	9
1.	Introducción	9
2.	Motivación	10
3.	Metodología	11
4.	Planificación	11
4.1.	Evaluación del Coste	12
II	Estudio previo	14
5.	Estado del Arte	14
5.1.	Arquitectura de red	14
5.2.	Ataques y defensas del sistema	15
5.3.	Definición del dispositivo	16
5.4.	Características del servidor de seguridad	17
5.5.	Productos existentes en el mercado	20
5.5.1.	Appliances	21
5.5.2.	Distribuciones de servidor de seguridad	22
6.	Estudio de viabilidad	25
6.1.	Módulos de los que se compone el sistema	25
III	Aportación del proyecto	27
7.	Requisitos	27
7.1.	Catálogo de requisitos	27
8.	Diseño	29
8.1.	Descripción general	29
8.2.	Selección de módulos	30
8.3.	Descripción del módulo Squid	31
8.3.1.	Descripción de Squid	31
8.3.2.	Reflexión sobre funcionalidades y parámetros	32
8.3.3.	Clasificación de parámetros	34

8.4.	Descripción del módulo DansGuardian	37
8.4.1.	Descripción de DansGuardian	37
8.4.2.	Reflexión sobre los parámetros y clasificación de estos.	38
8.5.	Descripción del Módulo Antivirus (ClamAV)	41
8.5.1.	Introducción	41
8.5.2.	ClamAV	41
8.5.3.	Base de datos de virus. FreshClam.	41
8.5.4.	Squid ClamAV Redirector. SCAVR	42
8.5.5.	Reflexión sobre los parámetros y clasificación de estos	44
8.6.	Descripción del Módulo Firewall (iptables + fireHOL)	46
8.6.1.	Introducción	46
8.6.2.	Descripción de iptables y fireHOL	46
8.6.3.	fireHOL	47
8.6.4.	Reflexión sobre los parámetros	48
8.7.	Descripción del Módulo Detector de Intrusiones IDS. (Snort)	51
8.7.1.	Introducción	51
8.7.2.	Descripción de Snort	51
8.7.3.	Reflexión sobre los parámetros y clasificación de estos	54
8.8.	Diseño de interfaces	56
9.	Implementación	60
9.1.	Introducción	60
9.2.	Modelo de Clases del sistema	60
9.3.	Consideraciones sobre la arquitectura del sistema	63
9.3.1.	Librerías estándares utilizadas	63
9.3.2.	Definición de formularios en XML	64
9.3.3.	Gestión de errores	65
9.4.	Detalles de la implementación	67
9.4.1.	Clase “Configurador” – Modos de operación	67
9.4.2.	Control de los Servicios del sistema	68
9.4.3.	Implementación de la definición de formularios en XML	69
9.4.4.	Clase estática ManejoErrores - Gestión de errores de la aplicación	69
9.4.5.	Procesamiento de ficheros. Clase Config y Extensiones	71
9.4.6.	Validación de campos de formulario. Extensión de patForms	72

10.Creación de distribución en CD auto-arrancable	74
10.1. Proyecto Metadistros	74
10.1.1. La distribución base	75
10.1.2. El calzador	77
10.2. Arranque del sistema	78
10.3. Creación de Metadistro Anubix	79
10.3.1. Preparación del Calzador	80
10.3.2. Preparación de la Distribución base. Sources	81
11.Validación	83
11.1. Pruebas de interfaces y contenidos	83
11.2. Pruebas funcionales y de operación	83
11.3. Pruebas de carga	83
11.4. Pruebas de rapidez de acceso	83
11.5. Pruebas de accesibilidad	84
11.6. Pruebas de usabilidad	84
12.Conclusiones y líneas futuras de trabajo	85
IV Anexos	88
A. Mapa conceptual del software libre	88
B. Estructura del directorio principal de la aplicación	89
C. Detalles del proxy Squid	91
C.1. Instalación y configuración de Squid	91
C.2. Parámetros de configuración de Squid	91
C.3. Parámetros de configuración principales	97
D. Detalles del filtro de contenidos DansGuardian	101
D.1. Instalación y configuración de DansGuardian	101
D.2. Parámetros de configuración de DansGuardian	101
E. Detalles del antivirus ClamAV	107
E.1. Instalación y configuración	107
E.2. Parámetros de configuración de ClamAV, freshclam y SCAVR	109
F. Detalles del cortafuegos fireHOL	112
F.1. Instalación y configuración de fireHOL	112
F.2. Parámetros de configuración de fireHOL	113

G. Detalles del detector de intrusiones Snort	117
G.1. Opciones de ejecución de Snort	117
G.2. Instalación y configuración de Snort	117
G.3. Parámetros de configuración de Snort	119
H. Descripción detallada de diseño de interfaces	121
H.1. Formularios de configuración del módulo Proxy (Squid)	121
H.1.1. Formulario “Control del Módulo”	121
H.1.2. Formulario “Configuración básica”	122
H.1.3. Formulario “Proxy Padre”	123
H.1.4. Formulario “Control de acceso”	124
H.1.5. Formulario “Otros parámetros”	128
H.1.6. Reflexión acerca de los formularios de configuración del módulo Proxy . . .	128
H.1.7. Relación con los parámetros de configuración del software squid	130
H.1.8. Importación/Exportación de parámetros	132
H.2. Formularios de configuración del módulo Antivirus (ClamAV)	133
H.2.1. Formulario “Control del Módulo”	133
H.2.2. Formulario “Configuración”	134
H.2.3. Formulario “Actualizaciones”	135
H.2.4. Reflexión acerca de los formularios de configuración del módulo Antivirus .	135
H.2.5. Relación con los parámetros de configuración del software ClamAV	136
H.2.6. Importación/Exportación de parámetros	137
H.3. Formularios de configuración del módulo Filtro de Contenidos (DansGuardian) . .	138
H.3.1. Formulario “Control del Módulo”	138
H.3.2. Formulario “Configuración básica”	138
H.3.3. Formulario “Grupos especiales de usuarios”	139
H.3.4. Formulario “Filtro de URL’s”	140
H.3.5. Formulario “Filtro de contenidos”	141
H.3.6. Reflexión acerca de los formularios del módulo Filtro de Contenidos	142
H.3.7. Relación con los parámetros de configuración del software DansGuardian .	144
H.3.8. Importación/Exportación de parámetros	146
H.4. Formularios de configuración del módulo Firewall (FireHOL)	147
H.4.1. Formulario “Control del Módulo”	147
H.4.2. Formulario “Configuración general”	149
H.4.3. Formulario “Reglas automáticas”	151
H.4.4. Formulario “Reglas definidas por el usuario”	152
H.4.5. Reflexión acerca de los formularios de configuración del módulo Firewall . .	153

H.4.6. Relación con los parámetros de configuración del software <code>FireH0L</code>	155
H.4.7. Importación/Exportación de parámetros	155
H.5. Formularios de configuración del módulo IDS (<code>Snort</code>)	157
H.5.1. Formulario “Control del Módulo”	157
H.5.2. Formulario “Habilitar reglas”	157
H.5.3. Formulario “Gestión de reglas”	158
H.5.4. Reflexión acerca de los formularios de configuración del módulo IDS	159
H.5.5. Relación con los parámetros de configuración del software <code>Snort</code>	160
H.5.6. Importación/Exportación de parámetros	162
I. Re-implementación de <code>patForms_Definition</code>	163
J. Interfaz de la clase estática <code>ManejoErrores</code>	168
K. Arranque de un sistema GNU/LINUX	171
L. Arranque del sistema LiveCD-Metadistros	173
M. Script para la creación de Metadistro	182
N. Resultados de validaciones. Listas de comprobación.	183
N.1. Pruebas de interfaces y contenidos	183
N.2. Pruebas funcionales y de operación	183
N.3. Pruebas de rapidez de acceso	184
N.4. Pruebas de usabilidad	184

Índice de figuras

1.	Arquitectura de red típica.	14
2.	Módulos del sistema	26
3.	Funcionamiento Squid	31
4.	Integración de DansGuardian + Squid	37
5.	Integración de ClamAV en el flujo de datos.	42
6.	Iptables – Flujo de datos	47
7.	Componentes de Snort	53
8.	Formulario “principal”	56
9.	Formulario “auxiliar”	57
10.	Modelo de Clases del Sistema	60
11.	Definición de los formularios mediante HTML y XML	64
12.	Ejemplo de código de gestión de errores	70
13.	Infraestructura del Sistema Metadistros	76
14.	Esquema funcional del calzador Metadistros	78
15.	Mapa conceptual del software libre	88
16.	Módulo ‘Proxy (Squid)’ – Control del Módulo	121
17.	Módulo ‘Proxy (Squid)’ – Configuración básica	122
18.	Módulo ‘Proxy (Squid)’ – Proxy Padre	123
19.	Módulo ‘Proxy (Squid)’ – Control de acceso	124
20.	Módulo ‘Proxy (Squid)’ – Control de acceso - Mover Regla	126
21.	Módulo ‘Proxy (Squid)’ – Control de acceso - Nueva / Editar Regla	127
22.	Módulo ‘Proxy (Squid)’ – Otros parámetros	128
23.	Módulo ‘Antivirus (ClamAV)’ – Control del módulo	133
24.	Módulo ‘Antivirus (ClamAV)’ – Configuración	134
25.	Módulo ‘Antivirus (ClamAV)’ – Actualizaciones	135
26.	Módulo ‘Filtro de Contenidos (DansGuardian)’ – Control del módulo	138
27.	Módulo ‘Filtro de Contenidos (DansGuardian)’ – Configuración básica	138
28.	Módulo ‘Filtro de Contenidos (DansGuardian)’ – Grupos especiales de usuarios	139
29.	Módulo ‘Filtro de Contenidos (DansGuardian)’ – Filtro de URL’s	140
30.	Módulo ‘Filtro de Contenidos (DansGuardian)’ – Filtro de contenidos	141
31.	Módulo ‘Firewall (FireHOL)’ – Control del módulo	147
32.	Módulo ‘Firewall (FireHOL)’ – Estado de FireHOL	148
33.	Módulo ‘Firewall (FireHOL)’ – Configuración general	149
34.	Módulo ‘Firewall (FireHOL)’ – Reglas automáticas	151
35.	Módulo ‘Firewall (FireHOL)’ – Reglas definidas por el usuario	152

36.	Módulo 'IDS (Snort)' – Control del Módulo	157
37.	Módulo 'IDS (Snort)' – Habilitar reglas	157
38.	Módulo 'IDS (Snort)' – Gestión de reglas	158
39.	Módulo 'IDS (Snort)' – Gestión de reglas – Editar reglas	159