

Índice

Página:

Introducción

Objetivo	2
Descripción del problema	2
Solución	3
Justificación	4
Método	5
Estructura del proyecto de tesis	5

1. Capítulo I Marco Teórico

1.1. Software Libre	7
1.1.1. Historia, definición y características	7
1.1.2. GNU/Linux	8
1.1.3. Libertades del software Libre	8
1.1.4. Software Propietario vs Software Libre	9
1.1.5. Tipos de licencia Open Source	10
1.1.5.1. General Public Licence (GNU GPL)	11
1.1.5.2. Berkeley Software Distribution (BSD)	11
1.2. Monitoreo de red	
1.2.1. Definición	12
1.3. Netflow	
1.3.1. Definición	13
1.3.2. Flujo	13
1.3.2.1. Calculo de flujo	13
1.3.3. Funcionamiento del protocolo Netflow	15
1.3.3.1. Conceptos Básicos	15
1.3.3.2. Componentes básicos del protocolo Netflow	17
1.3.3.3. Memoria volátil dedicada Netflow (cache)	17
1.3.4. Versiones de Netflow	19
1.3.4.1. Netflow V5 vs V9	19
1.3.5. Ventajas y consideraciones de utilizar Netflow	20
1.3.6. Aplicación de la tecnología Netflow en el área de seguridad informática	21
1.3.6.1. Netflow enfocado en la detección de ataques y anomalías	22
1.4. Conceptos de Seguridad Informática	23
1.4.1. Conceptos básicos de seguridad	23
1.4.2. Vulnerabilidades, amenazas y ataques	
1.4.2.1. Vulnerabilidad	24
1.4.2.2. Amenaza	24
1.4.2.3. Ataque	24
1.4.2.3.1. Clasificación de los ataques	24
1.5. Malware	
1.5.1. Definición	26
1.5.2. Clasificación del malware	26
1.5.2.1. Virus	26
1.5.2.2. Backdoor	26

1.5.2.3.	Bootnets (Redes zombies)	26
1.5.2.4.	Exploid	26
1.5.2.5.	“Zero day” Ataques de día cero	26
1.5.2.6.	Gusanos (Worm)	27
1.5.2.7.	Hoax	27
1.5.2.8.	Keylogger	27
1.5.2.9.	Phishing	27
1.5.2.10.	Spam	27
1.5.2.11.	Spyware	28
1.5.2.12.	Trojanos	28
1.5.3.	Comportamiento del malware	28
1.5.4.	Mecanismos de prevención	30
2.	<u>Capítulo II Investigación y elección del software libre a implementar</u>	
2.1.	Introducción	32
2.2.	Investigación sobre las alternativas de software libre	32
2.3.	Nfsen vs Stager	37
2.4.	Elección de la alternativa Open Source	40
2.5.	Comparación entre versión de Netflow comercial y Nfsen	41
3.	<u>Capítulo III Implementación del protocolo Netflow y del software “Listry-AIGC”.</u>	
3.1.	Introducción	45
3.2.	Implementación del protocolo Netflow	45
3.3.	Implementación del software “Listry-AIGC”	47
3.3.1.	¿Qué es el software Listry-AIGC?	
3.3.2.	Nfdump Definición	49
3.3.2.1.	Nfcapd Funcionamiento	50
3.3.2.2.	El intérprete nfdump	51
3.3.2.3.	Ejemplos de la herramienta nfdump	52
3.3.3.	Nfsen Definición y funcionamiento	55
3.3.3.1.	Funcionamiento de Nfsen	55
3.3.3.2.	Profiles	56
3.3.3.3.	Alertas	57
3.3.3.4.	Plugins	59
4.	<u>Capítulo IV Implementación del detector de malware</u>	
4.1.	Introducción	63
4.2.	Estrategia de protección	63
4.2.1.	Medidas de protección	63
4.3.	Comportamiento del malware	64
4.4.	Esquema de seguridad implementado en la institución	68
4.5.	Creación del plugin “escaneo” en Nfsen	69
4.5.1.	Estrategia de desarrollo del plugin escaneo	69
4.5.2.	Componentes del plugin escaneo	70
4.5.3.	Funcionamiento del plugin escaneo.	72
4.5.3.1.	Funcionamiento del módulo escaneo.pm	72

4.5.3.2.	Funcionamiento del módulo escaneo.php	95
5.	<u>Capítulo V Pruebas.</u>	
5.1.	Introducción	97
5.2.	Pruebas	97
5.2.1.	Pruebas enfocadas a monitoreo	97
5.2.2.	Pruebas enfocadas en la detección de malware	103
5.2.2.1.	Escenario A	104
5.2.2.2.	Escenario B	105
5.2.2.3.	Escenario C	106
5.2.2.4.	Escenario D	107
	<u>Conclusiones</u>	110
	Anexos.	
A.	<u>Glosario</u>	114
B.	<u>Guía de Instalación del software “Listry-AIGC”</u>	121
C.	<u>Manual de usuario del software “Listry-AIGC”</u>	136
D.	<u>Código del plugin escaneo</u>	159
	<u>Bibliografía y referencias.</u>	183