

Índice General

Introducción	1
1. Antecedentes teóricos.....	7
1.1 El concepto de código malicioso	7
1.2 Comportamiento general de un código malicioso	9
1.3 Clasificación de códigos maliciosos	9
1.4 El concepto de caja de arena	10
1.5 El concepto de red de arena	12
1.6 Infraestructura mínima de la red de arena.....	13
1.7 Introducción a las herramientas de análisis de códigos maliciosos.....	14
1.8 Introducción a la herramienta TRUMAN	17
2. Análisis y metodología.....	19
2.1 Introducción.....	19
2.2 Procesos del sistema.....	20
2.3 Ejecución de un binario en Microsoft Windows.....	21
2.4 Protocolos de red.....	23
2.5 Sistema de archivos	24
2.6 Registro de Microsoft Windows	26
2.7 Sistemas de detección de intrusos	26
2.7.1 Sistemas detectores de intrusos de host, HIDS	27
2.7.2 Sistemas detectores de intrusos de red, NIDS	27
2.8 Análisis de tráfico de red.....	28
2.9 Análisis dinámico de códigos maliciosos	28
3. Diseño y desarrollo	31
3.1 Introducción.....	31
3.2 Herramientas para la ejecución de binarios en Windows.....	31
3.3 Herramienta de análisis del sistema de archivos	32
3.4 Herramienta de análisis del registro de Windws	34

3.5 Herramienta de recopilación de información.....	35
3.6 Herramienta para el análisis de tráfico de red.....	37
3.7 Herramientas para la automatización de procesos.....	38
3.8 Herramientas para la administración de reportes	39
3.8.1 Difusión por correo electrónico.....	39
3.8.2 Difusión en ubicaciones de red	39
Conclusiones.....	41
Glosario.....	43
Referencias	51
Apéndices.....	55
Preparación de la infraestructura.....	55
Instalación de la herramienta TRUMAN ampliada.....	56
Instalación del Servidor	57
Instalación del Cliente.....	63
Ajustes generales.....	69
Anexos	71