

# ÍNDICE

ÍNDICE .....	1
Índice de figuras.....	4
Índice de tablas.....	5
INTRODUCCIÓN .....	7
A. Planteamiento del problema .....	7
B. Objetivo .....	9
C. Estructura de la tesis .....	9
1 ANTECEDENTES.....	11
1.1 Mecanismos para detección de tráfico de red malicioso .....	12
1.1.1 Firewalls .....	14
1.1.2 Sistemas de detección de intrusos (IDS) .....	16
1.1.3 Sistemas de prevención de intrusos .....	19
1.1.4 Analizadores de protocolos.....	21
1.1.5 Análisis de flujos .....	23
1.1.6 Análisis de bitácoras .....	25
1.2 Mecanismos alternativos para la detección de tráfico malicioso .....	28
1.2.1 Tecnologías Honeypot.....	28
1.2.2 Darknets .....	32
1.2.3 Telescopios de red .....	33
2 DARKNETS Y TELESCOPIOS DE RED .....	35
2.1 Introducción a las Darknets .....	36
2.2 Tráfico de red “no asignado” .....	36
2.3 Características de una Darknet .....	38
2.4 Esquema de funcionamiento y herramientas relacionadas .....	38
2.5 Análisis del modelo de detección en segmentos Darknet.....	41
2.5.1 Tiempos de detección .....	42
2.5.2 Detección en equipos únicos.....	43
2.5.3 Detección de múltiples paquetes .....	46
2.6 Darknets en ambientes académicos.....	48
2.7 Darknets a gran escala.....	49

2.7.1	Internet Motion Sensor (IMS).....	50
2.7.2	CAIDA .....	51
2.7.3	Team Cymru, The Darknet Project.....	53
2.7.4	iSINK (Internet Sink).....	54
2.7.5	The IUCC/IDC Internet Telescope .....	56
2.7.6	Internet Background Noise (IBN).....	57
2.7.7	Shadowserver .....	57
3	DISEÑO DE UN MECANISMO DE DETECCIÓN DE TRÁFICO MALICIOSO PARA REDUNAM .....	59
3.1	Análisis del problema .....	60
3.2	Darknet como mecanismo de detección de tráfico malicioso para RedUNAM.....	61
3.3	Análisis de la infraestructura.....	62
3.4	Diseño de una Darknet para RedUNAM .....	62
3.4.1	Alcance de la Darknet .....	63
3.4.2	Redirección del tráfico “no asignado” .....	64
3.4.3	Configuración de los servidores.....	65
3.4.4	Procesamiento de la información.....	67
3.4.5	Obtención de resultados .....	69
3.4.6	Utilidad de la información.....	71
4	IMPLANTACIÓN DE UNA DARKNET A GRAN ESCALA EN REDUNAM.....	73
4.1	Alcance de la implementación .....	74
4.2	Esquema de funcionamiento y herramientas utilizadas.....	76
4.2.1	Herramientas honeypot .....	77
4.2.1.1	Honeytrap .....	77
4.2.1.2	Dionaea.....	79
4.2.1.3	Kippo .....	79
4.2.2	Herramientas STA (Structured Traffic Analysis) .....	80
4.2.2.1	Herramientas IDS.....	80
4.2.2.2	Herramientas de análisis de flujos.....	82
4.2.3	Herramientas generales.....	83
4.3	Integración y funcionamiento de módulos .....	84
4.3.1	Captura y recopilación de datos .....	86
4.3.2	Funcionamiento módulo honeypot .....	86

4.3.2.1	Desarrollo y adaptación de herramientas.....	87
4.3.2.2	Clasificación de la información .....	89
4.3.2.2.1	Detección por reglas.....	89
4.3.2.2.2	Detección por patrones.....	90
4.3.2.3	Análisis de payloads .....	93
4.3.2.4	Almacenamiento de la información.....	93
4.3.2.4.1	Formato unificado TSU .....	94
4.3.2.4.2	Almacenamiento directo en base de datos (postgresql) .....	95
4.3.3	Funcionamiento módulo STA .....	96
4.3.3.1	Análisis de flujos.....	97
4.3.3.2	Detección por IDS.....	98
4.4	Rendimiento general del sistema.....	99
5	ANÁLISIS DE RESULTADOS .....	101
5.1	Carga del sistema .....	102
5.2	Efectividad de detección y clasificación.....	103
5.3	Utilidad de la información .....	105
5.4	Tareas pendientes y mejoras posibles.....	106
	CONCLUSIONES.....	107
	REFERENCIAS.....	111
	GLOSARIO .....	117
	ANEXOS .....	119
	Anexo A – Comparativa de tiempos de detección para Darknets de diferentes tamaños .....	120
	Anexo B – Esquema de la base de datos para almacenamiento de la información de los incidentes de la darknet.....	122
	Anexo C – Ejemplo del formato unificado para almacenamiento de información de incidentes .....	123
	Anexo D – Ejemplo del análisis de flujos (STA) .....	124
	Anexo E – Ejemplo de análisis de tráfico de red con IDS (STA) .....	126
	Anexo F – Ejemplo de información almacenada en el TSU .....	128
	Anexo G – Ejemplos de bitácoras del módulo.....	129

## ÍNDICE DE FIGURAS

Figura 1. SANS ISC-Survival time (enero 2005 - agosto de 2010)	13
Figura 2. Tipos de firewalls	15
Figura 3. Esquema de un IDS de host	18
Figura 4. Esquema de un IDS de red	18
Figura 5. Esquema de un IDS distribuido	19
Figura 6. Información proporcionada por el cliente de argus (ratop).	25
Figura 7. Esquema de conectividad de una honeynet	30
Figura 8. Esquema de una Darknet en una red en producción	37
Figura 9. Esquema de funcionamiento de una Darknet.	39
Figura 10. Relación tiempo-porcentaje para detección de un evento según el tamaño de una Darknet	45
Figura 11. Infraestructura del Internet Motion Sensor	50
Figura 12. Esquema de funcionamiento del IMS	51
Figura 13. Monitores del Archipelago de CAIDA	52
Figura 14. Actividad de las Darknet de The Darknet Project de Team-Cymru	54
Figura 15. Esquema de conectividad de iSink	55
Figura 16. Estadísticas generadas por IBN	57
Figura 17. Proceso de manejo de información de Shadowserver Foundation	58
Figura 18. Esquema general del telescopio de seguridad de la UNAM	61
Figura 19. Esquema general de la Darknet UNAM	65
Figura 20. Procesamiento de información de la Darknet	69
Figura 21. Esquema general del sistema de la Darknet UNAM	76
Figura 22. Modos de funcionamiento de honeytrap	78
Figura 23. Diagrama de funcionamiento del IDS Snort	81
Figura 24. Funcionamiento de Argus	83
Figura 25. Organización de herramientas en módulos de la Darknet	85
Figura 26. Proceso de manejo de información de la Darknet UNAM	85
Figura 27. Diagrama del módulo honeypot	87
Figura 28. Adaptación de honeytrap para implementación en Darknet UNAM	88
Figura 29. Patrones identificados por el módulo DKN	91
Figura 30. Algoritmo expiración y manejo de cola de eventos	92
Figura 31. Esquema de funcionamiento módulo STA	97
Figura 32. Etapas de la fase de prueba de la Darknet	102

## ÍNDICE DE TABLAS

Tabla 1. Ejemplo de firmas del IDS Snort	16
Tabla 2. Ejemplos de flujos de red	24
Tabla 3. Formatos de flujos de tráfico de red	25
Tabla 4. Subsistemas del honeywall	31
Tabla 5. Tipos de análisis y herramientas utilizadas en una Darknet	40
Tabla 6. Duración de eventos y porcentaje de detección según el tamaño de una Darknet para un caso específico.	46
Tabla 7. Infraestructura de “Archipelago” de CAIDA	52
Tabla 8. Darknets de “The DArknet Project”	53
Tabla 9. Estadísticas del telescopio de IUCC/IDC	56
Tabla 10. Esquema de roles de los servidores del proyecto	66
Tabla 11. Factores del análisis de tráfico estructurado	96
Tabla 12. Carga del sistema de la Darknet	103
Tabla 13. Estadísticas de detección de incidentes y captura de malware de la Darknet UNAM	104