

TABLA DE CONTENIDOS

	página
Dedicatoria	I
Agradecimientos	II
Tabla de Contenidos	III
Índice de Figuras	VIII
Índice de Tablas	XI
Resumen	XII
Abstract	XIII
1. Introducción	2
1.1. Objetivos	2
1.1.1. Objetivo general	2
1.1.2. Objetivos específicos	2
1.2. Alcances	3
1.3. Descripción del problema	3
2. Marco de referencia	5
2.1. Seguridad de la información	5
2.1.1. Confidencialidad	7
2.1.2. Integridad	7
2.1.3. Disponibilidad	8
2.2. Defensa en profundidad	8
2.3. Conceptos generales	9
2.3.1. Activos	9
2.3.2. Amenazas	10
2.3.3. Controles	12
2.3.4. Riesgo	13
2.3.5. Vulnerabilidades	13

2.4.	Análisis y gestión de riesgos	13
2.4.1.	Análisis de riesgos	14
2.4.2.	Metodologías, guías y normas existentes	14
2.4.3.	NIST SP 800-30	15
2.4.4.	ISO/IEC 27005:2008	16
2.4.5.	OSSTMM	16
2.4.6.	Diferentes aproximaciones al análisis de riesgos	17
2.4.7.	Análisis cuantitativo	18
2.4.8.	Análisis cualitativo	20
2.4.9.	Gestión del riesgo	21
2.5.	Análisis de seguridad	22
2.5.1.	Posicionamiento	23
2.5.2.	Visibilidad	24
2.5.3.	Perfil adoptado	26
2.6.	Etapas de un análisis de seguridad	28
2.6.1.	Etapas de reconocimiento	28
2.6.2.	Etapas de reconocimiento activo superficial	28
2.6.3.	Etapas de reconocimiento activo en profundidad	29
2.6.4.	Etapas de análisis de vulnerabilidades	29
2.6.5.	Etapas de explotación o ataque puro	29
2.6.6.	Etapas de consolidación	30
2.6.7.	Etapas de borrado de rastro	30
2.6.8.	Etapas de reporte	30
2.7.	Tipos de análisis de seguridad	30
2.7.1.	Vulnerability assessment	31
2.7.2.	Penetration test	32
2.7.3.	Ethical Hacking	33
2.8.	Legislación Chilena	34
2.9.	Antecedentes metodológicos	36
2.9.1.	Penetration test	36
2.9.2.	Diferencia entre Pentesting y Vulnerability Assessment	37
2.9.3.	Cómo las vulnerabilidades son identificadas	38
2.9.4.	Motivos por los cuáles realizar un penetration test	38

3. Metodología	42
3.1. Etapa de reconocimiento pasivo	43
3.1.1. Resumen	44
3.2. Etapa de reconocimiento activo	45
3.2.1. Resumen	46
3.3. Etapa de análisis de vulnerabilidades	46
3.3.1. Gestión de análisis de vulnerabilidades	48
3.3.2. Resumen	49
3.4. Etapa de explotación o ataque puro	50
3.4.1. Ataque puro	50
3.4.2. Herramientas	51
3.5. Etapa de consolidación	52
3.5.1. Resumen	54
3.6. Etapa de reporte	54
3.6.1. Resumen	56
4. Evaluación de seguridad	57
4.1. Footprinting a una red objetivo	57
4.1.1. Contexto	57
4.1.2. Objetivos	57
4.1.3. Revisión de footprinting	58
4.1.4. Actividades a desarrollar para llevar acabo el footpring	59
4.1.5. Footprinting una red objetivo usando la herramienta ping	59
4.1.6. Footprinting una red objetivo usando la herramienta nslookup	63
4.1.7. Análisis de consultas de dominio y dirección IP usando SmartWhois	68
4.1.8. Traza de red usando Path Analyzer Pro	73
4.1.9. Cumplimiento de objetivos	78
4.2. Escaneo a una red objetivo	79
4.2.1. Contexto	79
4.2.2. Objetivos	80
4.2.3. Revisión de escaneo de redes	80
4.2.4. Actividades a desarrollar	81

4.2.5.	Escaneo de sistemas y recursos de red utilizando Advanced IP Scanner	81
4.2.6.	Banner grabbing para determinar un objetivo remoto utilizando ID Serve	84
4.2.7.	Monitoreo de conexiones TCP/IP utilizando CurrPorts Tool .	87
4.2.8.	Escaneo de vulnerabilidades de red utilizando GFI LanGuard	89
4.2.9.	Exploración y auditoría una red usando Nmap	96
4.2.10.	Escaneo de una red utilizando la herramienta Nessus	101
4.2.11.	Escaneo de dispositivos en una red utilizando The Dude . . .	104
4.2.12.	Cumplimiento de objetivos	108
4.3.	Enumeración	108
4.3.1.	Contexto	108
4.3.2.	Objetivos	109
4.3.3.	Revisión de enumeración	109
4.3.4.	Actividades a desarrollar	109
4.3.5.	Enumeración de una red utilizando Nmap	109
4.3.6.	Enumeración de una red utilizando SoftPerfect Network Scanner	113
4.3.7.	Enumeración de una red utilizando SolarWinds Toolset	116
4.3.8.	Enumeración de una red utilizando Miranda	120
4.3.9.	Cumplimiento de objetivos	123
4.4.	Denegación de Servicio	124
4.4.1.	Revisión de Denegación de Servicio	125
4.4.2.	Actividades a desarrollar	125
4.4.3.	Inundación SYN a un host objetivo usando hping3	125
4.4.4.	Inundación HTTP usando Slowloris	128
4.4.5.	Cumplimiento de objetivos	131
5.	Mitigación	135
5.1.	Informe de Análisis de vulnerabilidades	135
5.1.1.	Objetivo del documento	135
5.1.2.	Alcances particulares	135
5.1.3.	Inventario y configuraciones	136
5.1.4.	Metodología general	137
5.1.5.	Resumen de resultados	138

5.1.6. Conclusiones y recomendaciones	144
5.2. Otras recomendaciones	144
6. Conclusiones	145
Bibliografía	148
Anexos	
A: Documentos adjuntos	153

ÍNDICE DE FIGURAS

	página
2.1. Seguridad de la información.	6
2.2. Tríada CIA.	7
2.3. Pasos de una metodología propuesta según la guía NIST SP-800.	15
3.1. Modelo de proceso de gestión de vulnerabilidades.	50
4.1. Ejecución de un ping simple contra el dominio.	60
4.2. Ejecución de un ping con un paquete de 1500 bytes.	61
4.3. Ejecución de un ping con un paquete de 1300 bytes.	62
4.4. Ejecución de un ping con TTL 3.	62
4.5. Ejecución de un ping con TTL 3 y 1 salto.	63
4.6. <code>nslookup</code> en modo interactivo.	65
4.7. <code>nslookup</code> determinando nombre canónico en un registro DNS.	66
4.8. <code>nslookup</code> enviando consultas DNS.	67
4.9. <code>nslookup</code> consultando sobre registros de correo electrónicos.	67
4.10. Consulta SmartWhois detección automática al primer dominio.	69
4.11. Consulta SmartWhois detección automática al segundo dominio.	70
4.12. Consulta SmartWhois detección automática al tercer dominio.	71
4.13. Consulta SmartWhois sólo dirección IP/ <i>hostname</i> del primer dominio.	72
4.14. Consulta SmartWhois sólo a la dirección IP/ <i>hostname</i> del tercer dominio.	73
4.15. Consulta de Path Analyzer Pro al primer dominio.	74
4.16. Consulta de Path Analyzer Pro al segundo dominio.	75
4.17. Consulta de Path Analyzer Pro al tercer dominio.	75
4.18. Resumen de ejecución de Path Analyzer Pro sobre los objetivos.	76
4.19. Archivo de registro de ejecución de Path Analyzer Pro.	77
4.20. Estadística de ejecución de Path Analyzer Pro sobre los objetivos.	78
4.21. Escaneo de Advanced IP Scanner al segmento de red interno del objetivo.	82
4.22. Escaneo de Angry IP Scanner al segmento de red interno del objetivo.	83
4.23. Escaneo de ID Serve al servidor web del objetivo.	85
4.24. Portal web de la National Vulnerability Database.	86

4.25. Listado con distintos tipos ataques posibles para el servidor web objetivo.	86
4.26. Listado de puertos TCP y UDP abiertos según CurrPorts Tool.	88
4.27. Exportación de resultados de CurrPorts Tool a un archivo HTML.	88
4.28. Escaneo de vulnerabilidades en la red objetivo con GFI LanGuard.	90
4.29. Resultado del escaneo de vulnerabilidades en la red objetivo.	91
4.30. Listado de equipos ordenados por severidad de sus vulnerabilidades.	91
4.31. Distribución de vulnerabilidades encontradas según su riesgo.	92
4.32. Vulnerabilidades bajas detectadas en un equipo específico	93
4.33. Vulnerabilidades potenciales detectadas en un equipo específico.	93
4.34. Vulnerabilidades bajas y potenciales detectadas en un equipo específico.	94
4.35. Vulnerabilidades mixtas detectadas en el equipo peor evaluado.	95
4.36. Revisión de interfaz de red desde BackTrack5 R3.	97
4.37. Escaneo de equipos “vivos” en la red objetivo.	98
4.38. Identificación de puertos abiertos y servicios de los <i>hosts</i> en la red.	100
4.39. Ejecución de Nessus sobre la red objetivo.	102
4.40. Presentación de <i>hosts</i> vulnerables tras escaneo con la herramienta Nessus.	102
4.41. Presentación de los distintos tipos de vulnerabilidades detectadas.	103
4.42. Recomendación de mitigación de una vulnerabilidad según Nessus.	104
4.43. Configuración de la herramienta de mapeo de red The Dude.	105
4.44. Mapa de red del objetivo a nivel de la capa de enlace 1/4.	106
4.45. Mapa de red del objetivo a nivel de la capa de enlace 2/4.	106
4.46. Mapa de red del objetivo a nivel de la capa de enlace 3/4.	107
4.47. Mapa de red del objetivo a nivel de la capa de enlace 4/4.	107
4.48. Revisión de interfaz de red y posterior levantamiento.	111
4.49. Escaneo de OS, versión, <i>scripts</i> y ejecución de traceroute.	112
4.50. Enumeración SNMP de dispositivos presentes en la red.	113
4.51. Enumeración de los <i>hosts</i> en la red objetivo.	115
4.52. Configuración de servicios SNMP en Microsoft Windows.	117
4.53. Definición de rango de IP en IP Network Browser.	117
4.54. Enumeración de <i>hosts</i> a través de IP Network Browser.	118
4.55. Información de sistema presente en un dispositivo enumerado.	119
4.56. Información de VLANs y tráfico en un dispositivo enumerado.	120

4.57. Enumeración de dispositivos de red mediante UPnP.	122
4.58. Listado de dispositivos enumerados en la red mediante UPnP.	123
4.59. hping3 previo a un ataque de DoS.	127
4.60. Ejecución del ataque DoS.	128
4.61. Definición del objetivo previo al ataque de DoS.	130
4.62. Ejecución del ataque de DoS mediante Slowloris.	131
4.63. Estado del servidor web a momento del ataque de denegación de servicio.	132
4.64. Estado del <i>firewall</i> al momento del ataque de denegación de servicio.	133
4.65. Notificación del CSIRT del Ministerio del Interior informando sobre el ataque.	134
5.1. Tabla de equipos y direcciones IP.	136
5.2. Configuración Ethernet del equipo donde se realizaron las pruebas. . .	137
5.3. Resumen de vulnerabilidades detectadas organizadas según dispositivo.	138
5.4. Resumen de vulnerabilidades detectadas organizadas según criticidad.	139
5.5. Resumen de vulnerabilidades detectadas organizadas según criticidad.	140
5.6. Vulnerabilidades criticas detectadas.	141
5.7. Vulnerabilidades medias detectadas.	142
5.8. Vulnerabilidades bajas detectadas.	143

ÍNDICE DE TABLAS

	página
2.1. Análisis cuantitativo (en dólares).	19
2.2. Análisis cualitativo.	21
2.3. Tabla análoga al valor SLE.	21