

Contenido

C1. El valor de la estrategia

El mercado.....	1
Nuestro producto	2
Nuestro cliente	4
El rol de la seguridad	6
El proceso	6
Navegando juntos	9
En resumen	9

C2. Tipos de análisis de seguridad

Diferentes enfoques.....	11
Todo tiempo pasado fue mejor... ..	11
Una tendencia predecible.....	12
Un haz de luz	13
Análisis de seguridad	15
Posicionamiento	15
Visibilidad	16
<i>Blind/Blackbox</i>	17
<i>Double blind/ Blackbox</i>	17
<i>Graybox</i>	17
<i>Double Graybox</i>	17
<i>Whitebox</i>	18
<i>Reversal</i>	18
Perfil adoptado	18
Etapas de un análisis de seguridad	19
Etapa de reconocimiento pasivo.....	19
Etapa de reconocimiento activo superficial	20
Etapa de reconocimiento activo en profundidad.....	20
Etapa de análisis de vulnerabilidades .	20
Etapa de explotación o ataque puro... ..	20

Etapa de consolidación	20
Etapa de borrado de rastro	21
Etapa de reporte	21
Tipos de análisis de seguridad.....	21
<i>Vulnerability assessment</i>	22
<i>Penetration test</i>	22
<i>Ethical hacking</i>	23
Perfil de un <i>security tester</i>	24
Manejo de idiomas	25
Habilidades de comunicación	25
Ética	25
Amplia percepción.....	26
Creatividad	26
Capacidad para el trabajo en equipo .	26
Pasión	27
En resumen	27

C3. Reconocimiento pasivo

Todo tiene un motivo de ser... ..	29
Ambiciosa inteligencia	31
Recolectando a la antigua.....	32
Obteniendo datos del dominio	32
Descubriendo dominios, subdominios y un poquito más.....	35
La carrera de grado más admirada: "Ingeniería social"	41
Consideraciones fundamentales	42
Bases y principios básicos	43
Técnicas seductivas.....	49
Técnicas invasivas:	50
<i>Long life to Google Hacking</i>	51
Por lo menos pensado... ..	60
Recolectando en la Web 2.0.	62

C4. Reconocimiento activo

Contacto directo	67
Identificación de sistemas activos	68
<i>Knock knock!!</i>	68
Identificación de puertos abiertos	70
Estados de los puertos	70
<i>Open</i> /Abierto	70
<i>Close</i> /Cerrado	70
<i>Filtered</i> /Filtrado	71
Técnicas de escaneo de puertos	71
TCP <i>Connect scan</i>	71
TCP <i>Syn scan</i>	72
TCP <i>Ack scan</i>	72
TCP <i>X-Mas scan</i>	72
TCP <i>Null scan</i>	72
TCP <i>Fin scan</i>	72
TCP <i>Idle scan</i>	73
UDP <i>scan</i>	73
Identificación de sistemas operativos	73
Analizando huellas	74
Posicionamiento del <i>security tester</i>	75
Cantidad de puertos abiertos en el sistema objetivo	75
Detección de sistema operativo activo	76
Detección de sistema operativo pasivo	76
Identificación de servicios	76
Captura de <i>banners</i>	77
Análisis de protocolos	78

C5. Análisis de vulnerabilidades

El concepto	79
Entonces... el problema	81
¿Servicio o producto?	84
Dónde se clasifican las vulnerabilidades ...	86
¿Cómo seleccionamos una solución efectiva?	88

Gestión de análisis de vulnerabilidades.....	90
Herramientas y productos	92
Falsos positivos, falsos negativos	94
Claves para el análisis efectivo en la empresa	96

C6. Ataque puro y consolidación

Hacia nuevos escenarios.....	99
Ataque puro	101
A las armas.....	103
Consolidación	105
En resumen	109

C7. Informe de resultados

El valor de la información	111
Dirección	113
Gerencia	113
Técnico.....	113
El valor percibido de la Dirección.....	113
Detalle de resultados.....	117
Introducción.....	117
Resultados obtenidos	117
Principales fortalezas	119
Principales debilidades.....	119
El informe técnico	121
En resumen	125

C8. Una solución integral

Volviendo a las raíces	127
El nivel de riesgo adecuado	129
Y de nuevo el cliente... molestando	130
Entregable	132
El informe, ¿y después?.....	133
En resumen	133
Anexo.....	134
Metodología utilizada.....	134