

Índice

Prólogo	11
Capítulo I	
¿Qué son las Infraestructuras Críticas?	13
1. Definición.....	13
2. Ley PIC.....	14
3. Estado de las Infraestructuras críticas en otros países	16
Capítulo II	
Componentes en Sistemas Industriales.....	19
1. Sistemas Industriales.....	19
2. Principales componentes en Sistemas industriales.....	20
2.1 Nivel 1	20
2.1.1 PLC	20
2.1.2 RTU.....	25
2.1.3 IED.....	26
2.1.4 PAC	26
2.1.5 Actuadores	27
2.1.6 DCS.....	27
2.2 Nivel 2	28
2.2.1 MTU	28
2.2.2 HMI.....	28
2.2.3 SCADA.....	29
2.3 Nivel 3	30
2.3.1 Historian	30
2.3.2 MES	30
3. Protocolos de comunicación en Sistemas Industriales	31
3.1 DNP 3.0	32
3.2 ICCP.....	38
3.3 Modbus	39

3.4 Profibus	42
3.5 OPC	46

Capítulo III

Consideraciones especiales en sistemas industriales.....49

1. Integración OT/IT	49
1.1 OT: “Operational Technology”	49
1.2 Integración IT/OT	50
2. Safety o Security	54
2.1 Safety	56
2.2 Security	59
3. Historia ataques a sistemas industriales.....	63
3.1 El comienzo de todo “El dossier Farewell”	63
3.2 Ataque a Gazprom.....	63
3.3 Ataques no intencionados.....	64
3.4 Sector energético: Night Dragon.....	65
3.5 El gran cambio: Stuxnet.....	67
3.6 sKyWIper.....	70
3.7 DragonFly	72
3.8 Análisis del Ataque a Ucrania- Power Grid	74
3.8.1 Fase 1	76
3.8.2 Fase 2.....	77
3.9 Industroyer 2	78

Capítulo IV

Atacando sistemas industriales.....83

1. Pentesting en Sistemas Industriales.....	83
1.1 Obtención de información.....	83
1.1.1 Proyecto Shine.....	83
1.1.2 ZoomEye.....	90
1.1.3 Otros Buscadores.....	93
1.2 Escaneo de redes industriales.....	94
1.2.1 Nmap en redes industriales.....	94
1.2.2 Escaneando con Python	108
1.3 Conversión de Kali para pentesting industrial: Moki	117
1.4 Detección de vulnerabilidades en redes industriales.....	118
1.4.1 Nessus para redes industriales	118
1.4.2 Bandoiler.....	121
1.5 Explotación de Vulnerabilidades.....	124
1.5.1 Metasploit	125
1.5.2 Lectura/ Escritura en dispositivos industriales	132

1.5.3 Hacking ICS mediante el ERP.....	139
1.5.4 Ingeniería inversa de código.....	146
1.5.5 Vulnerabilidades comunes.....	159
1.5.6 Android.....	172
1.6 Bypass de Diodos de Datos.....	179
1.6.1 Emisiones Térmicas.....	180
1.6.2 Emisiones Electromagnéticas.....	182
1.6.3 Luz Visible o Infrarroja.....	186
1.6.4 Señales Acústicas.....	191
1.7 Anexo 1. Passwords por defecto.....	194

Capítulo V

¿Cómo securizar entornos críticos?203

1. Pentesting en entornos seguros203

2. Defensa en profundidad204

2.1 Capa 1..... 205

2.2 Capa 2..... 205

2.3 Capa 3..... 206

2.3.1 SNORT ICS..... 206

2.3.2 Tofino..... 207

2.3.3 Diodos de datos..... 208

2.4 Capa 4..... 213

2.5 Capa 5..... 214

3. Security Awareness.....214

3.1 Formación en Seguridad para personal general..... 215

3.2 Formación en Seguridad para profesionales..... 216

4. Conclusiones finales.....218

Índice alfabético221

Índice de imágenes225

Referencias.....233

Capítulo I..... 233

Capítulo II..... 233

Capítulo III..... 234

Capítulo IV..... 235

Capítulo V..... 237

Otros libros publicados.....239

