

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

Capítulo IV

Atacando sistemas industriales.....79

1. Pentesting en Sistemas Industriales.....	79
1.1 Obtención de información.....	79
1.1.1 Proyecto Shine.....	79
1.1.2 ZoomEye.....	86
1.1.3 Otros Buscadores.....	89
1.2 Escaneo de redes industriales.....	90
1.2.1 Nmap en redes industriales.....	90
1.2.2 Escaneando con Python	104
1.3 Conversión de Kali para pentesting industrial: Moki	113
1.4 Detección de vulnerabilidades en redes industriales.....	114
1.4.1 Nessus para redes industriales	114
1.4.2 Bandoiler.....	117
1.5 Explotación de Vulnerabilidades.....	120
1.5.1 Metasploit	121



1.5.2 Lectura/ Escritura en dispositivos industriales	128
1.5.3 Hacking ICS mediante el ERP.....	135
1.5.4 Ingeniería inversa de código.....	142
1.5.5 Vulnerabilidades comunes	155
1.5.6 Android.....	168
1.5.7 Anexo 1. Passwords por defecto.....	175

Capítulo V

¿Cómo securizar entornos críticos?185

1. Pentesting en entornos seguros185

2. Defensa en profundidad.....186

2.1 Capa 1.....187

2.2 Capa 2.....187

2.3 Capa 3.....188

2.3.1 SNORT ICS.....188

2.3.2 Tofino.....189

2.3.3 Diodos de datos.....190

2.4 Capa 4.....195

2.5 Capa 5.....196

3. Security Awareness.....196

3.1 Formación en Seguridad para personal general.....197

3.2 Formación en Seguridad para profesionales.....198

4. Conclusiones finales.....200

Índice alfabético203

Índice de imágenes207

Referencias215



