

Contents



01

CHAPTER

ความปลอดภัยและการรักษาความปลอดภัย ของระบบคอมพิวเตอร์และเครือข่าย

การรักษาความปลอดภัยของระบบคอมพิวเตอร์
และเครือข่าย

การรักษาความปลอดภัยด้านกายภาพ

การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย
และลูกข่าย

การรักษาความปลอดภัยของระบบเครือข่าย
และอุปกรณ์เครือข่าย

การรักษาความปลอดภัยของข้อมูล

องค์ประกอบพื้นฐานความปลอดภัยของข้อมูล

Confidentiality (ความลับของข้อมูล)

Integrity (ความคงสภาพของข้อมูล)

Availability (ความพร้อมใช้งานของข้อมูล)

องค์ประกอบเพิ่มเติม

สภาพแวดล้อมของความปลอดภัย

ภัยคุกคาม (Threat)

เหตุสุดวิสัย (Accidental)

มาตรฐานความปลอดภัย

ISO/IEC 27001

ISO/IEC TR 13335

ISO/IEC 15408:2005/Common Criteria/ITSEC

ITIL

FIPS PUB 200

NIST 800-14

IT BPM

COBIT

COSO

ตัวอย่างการโจมตี

การสอดแนมและการดักฟัง/ดักจับข้อมูล

การโจมตีแบบ MITM

การโจมตีแบบ DoS

การโจมตี Web Application

การข้ามผ่านการตรวจสอบสิทธิ์ LAN และ Wireless LAN

การโจมตีเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่าย

การบริหารและประเมินความเสี่ยงของระบบคอมพิวเตอร์
และเครือข่าย

ความหมายของความเสี่ยง

ขั้นตอนการประเมินความเสี่ยงของระบบคอมพิวเตอร์
และเครือข่าย

การบริหารความเสี่ยง

สรุป

02

CHAPTER

วิทยาการรหัสลับ

การเข้ารหัสในยุค Classic

Caesar cipher

Monoalphabetic ciphers

Polyalphabetic Encryption

One-Time Pad

Playfair cipher

การเข้ารหัสในยุค Modern

DES (Data Encryption Standard)

Tripple-DES (3DES)

AES (Advanced Encryption Standard)

Symmetric Key Cryptography

Asymmetric Key Cryptography

RSA

ECC

Hash

MD5

SHA

Digital Signatures

CA (Certificate Authority)

การพิสูจน์ทราบตัวตน (Authentication)

ประเภทของการพิสูจน์ตัวตน

การพิสูจน์ตัวตนโดยใช้รหัสผ่าน

การพิสูจน์ตัวตนโดยใช้ PIN

การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพ

การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว

การพิสูจน์ตัวตนโดยการเข้ารหัส

และถอดรหัสโดยใช้ Public-key cryptography

การพิสูจน์ตัวตนโดยใช้ลายมือชื่อดิจิทัล

การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ

โปรโตคอลในการพิสูจน์ตัวตน

03

CHAPTER

ความปลอดภัยของเว็บ

Session Hijacking

ตัวอย่างการทำ Session Hijacking

โดยการดักจับ Session ID และใช้เบราว์เซอร์พิเศษ

ตัวอย่างการทำ Session Hijacking

โดยใช้เครื่องมือ Side Jacking



Contents

ตัวอย่างการทำ Session Hijacking	66
โดยการขโมย Cookie ข้ามเครือข่ายอินเทอร์เน็ต	66
การป้องกัน Session Hijacking	67
SQL Injection	69
การข้ามผ่านการตรวจสอบสิทธิ์ด้วย SQL Injection	70
การป้องกัน SQL Injection	72
Remote File Inclusion	74
ความหมายของการโจมตีแบบ Remote File Inclusion	74
จะเกิดอะไรขึ้นหลังจากที่ไฟล์ของแฮกเกอร์ถูก Include	74
การป้องกันการแฮกด้วย File Inclusion	76
สรุปเกี่ยวกับ Remote File Inclusion	78
Cross Site Scripting (XSS)	78
ความหมายของ XSS	78
ตัวอย่างการโจมตีด้วย XSS	79
การป้องกัน XSS	82
Cross Site Request Forgery (CSRF)	83
ความหมายของ Cross Site Request Forgery	83
เหยื่อที่ผลกระทบจากการโจมตี Cross Site Request Forgery	84
วิธีป้องกัน Cross Site Request Forgery	84
Parameter Manipulation	85
Cookie Manipulation	85
HTTP Header Manipulations	85
HTML Form Field Manipulation	86
URL Manipulation	86
Login Cracking	87
ตัวอย่างการแคร็กรหัสผ่านแบบ Dictionary Attack	88
ตัวอย่างการแคร็กรหัสผ่านแบบ Brute Force	88

04

CHAPTER

ความปลอดภัยของระบบ LAN	89
ARP Attack	90
ARP Spoof	90
ARP DoS Attack และ Netcut	100
DHCP Attack	104
DHCP Spoof เพื่อทำให้แฮกเกอร์เป็น Main In The Middle	104
DHCP Spoofing เพื่อโจมตีแบบ DoS	106
การป้องกัน DHCP Attack	107
MAC Spoofing	110
ทำไมแฮกเกอร์ต้องปลอมแปลงค่า MAC Address	110
วิธีการเปลี่ยนค่า MAC Address	111
การโจมตีด้วยวิธีการปลอมแปลงค่า MAC Address	113
การป้องกันการปลอมแปลงค่า MAC Address	114

ความปลอดภัยของ SNMP	117
ช่องโหว่ของ SNMP	117
การป้องกันการเข้าถึงข้อมูลสำคัญผ่าน SNMP	118
การลักลอบเข้าถึงทรัพยากรในระบบ LAN	118
ลักลอบเข้าถึง Share Folder ที่แชร์เครือข่าย	118
ลักลอบใช้อินเทอร์เน็ตผ่าน Wireless LAN	120
ลักลอบใช้อินเทอร์เน็ตผ่าน Wire LAN	120
การ Hack เน็ตเวิร์กภายในผ่าน Firewall	121
การป้องกันอุปกรณ์เครือข่าย	122
ป้องกันการเข้าถึงทางกายภาพ	122
การเปลี่ยนไอพีแอดเดรสและรหัสผ่านดีฟอลต์	122
ทำการอัปเดต OS หรือ Firmware	122

05

CHAPTER

ความปลอดภัยของเครือข่าย LAN ไร้สาย	123
Introduction	123
พื้นฐานเกี่ยวกับ Wireless LAN	124
มาตรฐานของ Wireless LAN	124
โครงสร้างและรูปแบบการเชื่อมต่อ	125
การเพิ่มความปลอดภัยให้กับ Wireless LAN	126
เปลี่ยนค่า Default Configuration	126
ไมโครดคาสต์ SSID	128
กรอง MAC Address	129
เข้ารหัสด้วย WEP	130
ตัวอย่างการแคร็ก WEP	132
เข้ารหัสด้วย WPA-PSK	137
ตัวอย่างการแคร็ก WPA	140
เข้ารหัสด้วย WPA และตรวจสอบสิทธิ์โดยใช้ RADIUS	143
เข้ารหัสด้วย WPA และตรวจสอบสิทธิ์ผู้ใช้ Certificate	151
ป้องกันการเข้าถึงทางกายภาพ	151
สรุป	151

06

CHAPTER

ความปลอดภัยของเครื่องแม่ข่ายลินุกซ์	153
ความปลอดภัยทางกายภาพ	154
การตั้งรหัสผ่าน BIOS	154
การตั้งรหัสผ่าน Lilo และ Grub	154

ความปลอดภัยขั้นพื้นฐาน	156
การตั้ง password	156
กลไกการเก็บรหัสผ่านของ Linux	157
John the Ripper	158
การกำหนดสิทธิ์ให้กับ User อย่างเหมาะสม	159
ลบผู้ใช้ที่ไม่ active ออกจากระบบ	159
ตั้งจำนวน connection ที่ authen พร้อมกับการป้องกันการแคร็ก	159
การกำหนด permission ของไฟล์	160
การจำกัดไม่ให้ root ล็อกอินและการใช้ sudo	161
การนำรหัสผ่าน root ไปใช้กับ service อื่นหรือระบบอื่น	162
ควร update และดูช่องโหว่ของซอฟต์แวร์ที่มีปัญหา	163
ความปลอดภัยของ Service	163
Sendmail	163
POP3/IMAP	165
Apache	166
Squid	170
FTP	171
DNS และ BIND	172
การปิด service ที่ไม่จำเป็น	173
การใช้ Linux บนเน็ตเวิร์กที่ไม่ปลอดภัย	175
การตรวจสอบว่าเน็ตเวิร์กของเราปลอดภัย	
ต่อการดักจับข้อมูลหรือไม่	176
SSH	176
HTTPS	177
SCP และ SFTP	178
POP3/IMAP Mail Server บน SSL	179
VPN, IPsec และ CIPE	180
ใช้ IPTABLES ทำ Personal Firewall	180
การป้องกันอื่นๆ	180
ตัวอย่างการโจมตี	181
Local hack และ Remote hack	181
เครื่องมือ BackTrack 4	181
การมอดลิตผ่านไฟร์วอลล์ด้วย SSL Tunnel	183
Root Kit	184
การวิเคราะห์เมื่อ Linux ถูกโจมตี	186
ตรวจสอบผู้ใช้ที่น่าสงสัย lastlog, last, lastb	186
ตรวจสอบ service ที่น่าสงสัย	186
ตรวจสอบ log ของ Application ต่างๆ	187
Tripwire	187
SE Linux	189
ตรวจสอบ Root Kit ด้วย chrootkit	189
การวางแผนป้องกันและการกู้คืนระบบ	190
การบู๊ตเมื่อเกิดเหตุฉุกเฉิน	190
การกู้คืนรหัสผ่าน	190
การสำรองไฟล์ด้วย tar	191

07

CHAPTER

ความปลอดภัยของวินโดวส์

193

Scan หาเป้าหมายและการแกะรอย	194
การแกะรอยจากอินเทอร์เน็ตโดยใช้ Whois และ Sam Spade	194
การแกะรอยจากอินเทอร์เน็ตโดยใช้ Search Engine	195
การสแกนพอร์ต	195
การตรวจหาเป้าหมายโดยใช้ข้อมูลจากแบนเนอร์	196
การรวบรวมข้อมูลจาก Netbios Name Service	197
การรวบรวมข้อมูลผ่านทาง RPC	198
การรวบรวมข้อมูลผ่านทาง SMB	199
การรวบรวมข้อมูลผ่านทาง DNS	200
การรวบรวมข้อมูลผ่านทาง SNMP	200
การดักจับและแคร็กรหัสผ่าน	201
ดักจับรหัสผ่าน FTP, Telnet และ POP3	201
ดักจับ LM Hash และ NTLM Hash แล้วนำมาแคร็กแฮชรหัสผ่าน	203
Remote Crack รหัสผ่าน	204
การโจมตีโดยใช้ Remote Registry และ Computer Management (Remote)	205
Command Shell แบบโต้ตอบ	208
การยกระดับสิทธิ์	211
เครื่องมือที่แยกเกอร์ใช้ยกระดับสิทธิ์บน Windows Server 2003 และ XP	211
เครื่องมือที่แยกเกอร์ใช้ยกระดับสิทธิ์บน Windows 2000 Server	213
การป้องกันการยกระดับสิทธิ์	213
การโจมตีทางกายภาพ	214
IIS Security	214
ช่องโหว่ IIS ที่เป็นที่รู้จักมากที่สุด	214
การโจมตี IIS ที่พบบ่อย	215
การเพิ่มความปลอดภัยให้ IIS ด้วย IISLockdown และ UriScan	218
SQL Server Security	219
คอนเซ็ปต์ด้านความปลอดภัยของ SQL Server	219
การสแกนหาเป้าหมาย SQL Server	220
การโจมตีแคร็กรหัสผ่านของ SQL Server	221
การดักจับรหัสผ่านของ SQL Server	223
การโจมตีแบบ Local	223
การโจมตีด้วย osql	224
การโจมตีโดยใช้ Extended Stored Procedure	224
การป้องกันการโจมตี SQL Server	225
การโจมตีทาง Terminal Service	225
การป้องกันการโจมตีทาง Terminal Service	226
Windows Client	227
สรุป	228



Contents

08

CHAPTER

ไฟร์วอลล์	229
Firewall Introduction	229
หน้าที่และการทำงานของไฟร์วอลล์	230
การออกแบบเครือข่ายและตำแหน่งที่ตั้งของไฟร์วอลล์	232
DMZ (Demilitarized Zone)	233
การออกแบบลักษณะเป็นชั้น	233
การใช้ไฟร์วอลล์ที่มีหลายอินเทอร์เฟซ	234
โปรโตคอลและพอร์ตต่างๆกับการตั้งกฎไฟร์วอลล์	235
HTTP	235
HTTPS	236
SMTP, POP3 และ IMAP	237
DNS	238
FTP	238
Proxy	240
SNMP	242
Terminal Service, Database port และ Windows port	242
NAT	248
Static NAT	248
Dynamic NAT หรือ Internet Share	244
ไฟร์วอลล์ชนิดต่าง ๆ	246
Packet Filtering Firewall	246
Stateful Firewall	247
Application Firewall	247
Personal Firewall	248
ตัวอย่างผลิตภัณฑ์ไฟร์วอลล์	249
IPTABLES	249
ISA Server	257
Access Control List (ACL) บน Cisco Router	261
ACL บน Squid	264
Commercial Firewall ระดับ Enterprise	267

09

CHAPTER

ไอดีเอสและไอพีเอส	271
ความสำคัญของ IDS/IPS	272
ประเภทของ IDS/IPS	272
Host based IDS	272
Network based IDS	273
IPS	274
การเชื่อมต่อ IDS/IPS	274
กลไกการทำงานและการเลือกใช้ IDS	277
การติดตั้งใช้งาน Snort	278
การติดตั้ง Snort	278
ทดสอบการใช้งานโปรแกรม Snort	280
โปรแกรมช่วยวิเคราะห์ Log ของ Snort	286

10

CHAPTER

ไวรัส เวิร์ม โทรจัน และมัลแวร์	289
ความหมายของมัลแวร์ชนิดต่างๆ	290
ไวรัส	290
เวิร์ม	290
โทรจัน	291
สปายแวร์	291
แอดแวร์	292
คีย์ล็อกเกอร์	292
มัลแวร์	293
Hybrid malware	293
Zombie Computer	293
ฟิชชิง	293
ประวัติความเป็นมาของไวรัส	293
วงจรชีวิตของไวรัส เวิร์ม และมัลแวร์อื่น	295
กำเนิด	295
แพร่เชื้อ	295
โจมตีระบบ	295
ถูกกำจัด	296
Top 10 Virus (Malware)	297
การป้องกันและกำจัดไวรัสรวมถึงมัลแวร์อื่นๆ	298
ใช้โปรแกรม Anti-Virus	298
เปลี่ยนมาใช้วินโดวส์เวอร์ชันที่ใหม่กว่า	298
ติดตั้ง Service Pack ล่าสุด	298
กำหนดให้วินโดวส์อัปเดตแพตช์อัตโนมัติ (Auto update)	299
ใช้งาน Personal Firewall	299
Top 10 Anti-Virus	299

11

CHAPTER

ระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์	301
ความหมายของ Log	301
เก็บ Log อย่างไรให้ตรงตาม พรบ.	303
โครงสร้างและประเภทของระบบ Log	304
โครงสร้างของระบบ Log	304
ประเภทของระบบ Log	306
Log Server ในปัจจุบัน	306
SRAN Security Center	306
SGC Sniff-LOG	307
Plawan Central Log	307
ข้อมูลการเปรียบเทียบคุณสมบัติพื้นฐานของ Log Server	307
บทสรุป	308