



Ασφάλεια Δικτύων

Εισαγωγή στη
Σύγχρονη Τεχνολογία



Περιεχόμενα

<i>Εισαγωγή</i>	xv
Κεφάλαιο 1 Αρχές της Ασφάλειας	1
Γιατί οι Υπολογιστές Δεν Είναι Ασφαλείς	2
Η Ιστορία της Ασφάλειας Υπολογιστών	4
-1945	5
1945-1955	7
1955-1965	7
1965-1975	7
1975-1985	8
1985-1995	9
1995-2005	11
2005-	12
Βασικές Έννοιες Ασφάλειας	13
Εμπιστοσύνη	13
Επαλήθευση	13
Αλυσίδα Εξουσίας	14
Υπευθυνότητα	15
Έλεγχος Προσπέλασης	15
Όροι Κλειδιά	17
Ερωτήσεις	18
Κεφάλαιο 2 Κατανόηση της Εισβολής	19
Τι Είναι Εισβολή	20
Τύποι Εισβολών	20
Ειδικοί Ασφάλειας	21
Έφηβοι Εισβολείς	21
Υποαπασχολούμενοι Ενήλικες	21
Εισβολείς από Ιδεολογία	22
Εγκληματίες Εισβολείς	23
Εταιρικοί Κατάσκοποι	23
Δυσανεστημένοι Υπάλληλοι	24
Τρόποι Εργασίας των Εισβολών	24
Απευθείας Εισβολή	25
Μέσω Τηλεφωνικής Κλήσης	25
Internet	26
Ασύρματα	26
Τεχνικές Εισβολής	27
Επιλογή Στόχου	27
Συλλογή Πληροφοριών	29
Επιθέσεις	30

viii Ασφάλεια Δικτύων

Όροι Κλειδιά.....	37
Ερωτήσεις.....	38
Κεφάλαιο 3 Κρυπτογράφηση και Επαλήθευση	39
Κρυπτογράφηση	40
Κρυπτογράφηση Μυστικού Κλειδιού	41
Μονόδρομες Συναρτήσεις (Κατατεμαχισμοί)	41
Κρυπτογράφηση Δημόσιου Κλειδιού	43
Υβριδικά Κρυπτοσυστήματα.....	44
Επαλήθευση	44
Επαλήθευση Κωδικού Πρόσβασης	45
Επαλήθευση Συνόδου	47
Επαλήθευση Δημόσιου Κλειδιού	48
Επαλήθευση Βάσει Πιστοποιητικού	49
Βιομετρική Επαλήθευση.....	50
Όροι Κλειδιά.....	51
Ερωτήσεις.....	52
Κεφάλαιο 4 Διαχείριση Ασφάλειας	53
Ανάπτυξη μιας Πολιτικής Ασφάλειας.....	54
Δημιουργία ενός Περιγράμματος Απαιτήσεων	
Πολιτικής Ασφάλειας	54
Βέλτιστες Πρακτικές Πολιτικής Ασφάλειας	58
Υλοποίηση της Πολιτικής Ασφάλειας	63
Εφαρμογή Αυτοματοποιημένης Πολιτικής	64
Ασφάλεια που Υλοποιείται από Ανθρώπους.....	65
Ενημέρωση της Πολιτικής Ασφάλειας	67
Ο Κύκλος Ζωής της Ασφάλειας.....	67
Όροι Κλειδιά.....	69
Ερωτήσεις.....	70
Κεφάλαιο 5 Ασφάλεια Συνόρων	71
Αρχές της Ασφάλειας Συνόρων	72
Κατανόηση των Firewalls.....	74
Θεμελιώδεις Λειτουργίες των Firewalls	74
Υπηρεσίες Διασφάλισης Απορρήτου των Firewalls	82
Εικονικά Ιδιωτικά Δίκτυα	83
Άλλες Υπηρεσίες Συνόρων	83
Επιλογή ενός Firewall	84
Όροι Κλειδιά.....	85
Ερωτήσεις.....	86
Κεφάλαιο 6 Εικονικά Ιδιωτικά Δίκτυα	87
Επεξήγηση των Εικονικών Ιδιωτικών Δικτύων.....	88
Ενθυλάκωση IP	88
Κρυπτογραφική Επαλήθευση	89
Κρυπτογράφηση Ωφέλιμου Φορτίου Δεδομένων.....	90

Χαρακτηριστικά των Εικονικών Ιδιωτικών Δικτύων	90
Συνηθισμένες Υλοποιήσεις Εικονικών Ιδιωτικών Δικτύων	91
IPSec.....	92
2.2TP	93
PPTP	94
PPP/SSL ή PPP/SSH	95
Βέλτιστες Πρακτικές Εικονικών Ιδιωτικών Δικτύων	96
Όροι Κλειδιά.....	99
Ερωτήσεις.....	100
Κεφάλαιο 7 Διασφάλιση Απομακρυσμένων και Οικιακών Χρηστών	101
Το Πρόβλημα της Ασφάλειας Απομακρυσμένων Χρηστών	102
Τρύπες Ασφάλειας Εικονικών Ιδιωτικών Δικτύων	102
Φορητοί Υπολογιστές.....	102
Προστασία των Απομακρυσμένων Υπολογιστών.....	103
Συνδέσεις Εικονικών Ιδιωτικών Δικτύων	104
Προστασία Δεδομένων και Αξιοπιστία	106
Δημιουργία Αντιγράφων Ασφαλείας και Αρχαιοθέτηση.....	106
Προστασία από Απομακρυσμένους Χρήστες	107
Όροι Κλειδιά.....	108
Ερωτήσεις.....	109
Κεφάλαιο 8 Κακόβουλο Λογισμικό και Προστασία από Ιούς	111
Κατανόηση του Κακόβουλου Λογισμικού.....	112
Κατανόηση των Ιών	112
Προστασία από Ιούς	117
Αποτροπή.....	117
Φυσική Ανοσοποίηση	118
Ενεργή Προστασία	118
Κατανόηση των Λογισμικών Σκουληκιών και των Δούρειων Ίππων	119
Προστασία από Σκουλήκια	121
Υλοποίηση Προστασίας από Ιούς	121
Προστασία από Ιούς στο Σύστημα Πελάτη	122
Προστασία από Ιούς στο Διακομιστή.....	123
Προστασία από Ιούς στην Πύλη E-mail	124
Προστασία από Ιούς με Firewalls.....	124
Προστασία από Ιούς σε Επίπεδο Εταιρείας	125
Όροι Κλειδιά.....	125
Ερωτήσεις.....	126
Κεφάλαιο 9 Δημιουργία Ανοχής σε Σφάλματα	127
Αιτίες που Συμβαίνουν Απώλειες.....	128
Ανθρώπινο Σφάλμα.....	128
Συνηθισμένα Συμβάντα Αποτυχιών	128
Εγκλήματα	130
Συμβάντα στο Περιβάλλον	132
Μέτρα για Ανοχή σε Σφάλματα	133

x Ασφάλεια Δικτύων

Δημιουργία Αντιγράφων Ασφαλείας	133
Τροφοδοτικά Αδιάλειπτης Λειτουργίας και Γεννήτριες.....	138
Πλεονάζουσα Συστοιχία Ανεξάρτητων Δίσκων (RAID)	139
Άδειες Χρήσης.....	141
Ασφάλεια Συνόρων	141
Παρακολούθηση.....	141
Αποθήκευση εκτός των Εγκαταστάσεων.....	141
Αρχειοθέτηση	142
Έλεγχος Πραγματικής Λειτουργίας	142
Πλεονασμός Κυκλωμάτων	143
Φυσική Ασφάλεια	143
Συμπλέγματα Διακομιστών	144
Όροι Κλειδιά.....	147
Ερωτήσεις.....	148

Κεφάλαιο 10 Ασφάλεια των Windows 149

Τοπική Ασφάλεια των Windows	150
Ταυτότητες Ασφάλειας.....	151
Σύνδεση	152
Προσπέλαση Πόρων.....	153
Αντικείμενα και Άδειες.....	154
Άδειες Συστήματος Αρχείων NTFS	157
Σύστημα Κρυπτογράφησης Αρχείων	158
Ασφάλεια Δικτύων Windows	159
Ενεργός Κατάλογος	159
Πιστοποίηση Kerberos και Ασφάλεια Τομέα	160
Πολιτική Ομάδας.....	163
Ασφάλεια Πόρων Κοινής Χρήσης.....	166
IPSec.....	169
Όροι Κλειδιά.....	171
Ερωτήσεις.....	172

Κεφάλαιο 11 Διασφάλιση Διακομιστών Unix 173

Συνοπτική Ιστορία του Unix.....	174
Βασικά Στοιχεία Ασφάλειας στο Unix	177
Κατανόηση των Συστημάτων Αρχείων του Unix.....	177
Λογαριασμοί Χρηστών.....	180
Ασφάλεια Συστήματος Αρχείων	184
Λίστες Ελέγχου Προσπέλασης.....	186
Άδειες Εκτέλεσης	186
Όροι Κλειδιά.....	189
Ερωτήσεις.....	190

Κεφάλαιο 12 Ασφάλεια Δικτύων Unix 191

Βασικά Στοιχεία Ασφάλειας Δικτύων Unix	192
Ασφάλεια Απομακρυσμένης Σύνδεσης.....	193
Απομακρυσμένη Προσπέλαση.....	194

Περιεχόμενα xi

Εμβυσματούμενη Μονάδα Πιστοποίησης	195
Κατανεμημένη Σύνδεση	196
Κατανεμημένα passwd	196
NIS και NIS+	196
Kerberos	198
Ασφάλεια Κοινής Χρήσης Αρχείων	200
Πρωτόκολλο Μεταφοράς Αρχείων	201
Σύστημα Αρχείων Δικτύου	203
Πρωτόκολλο Μεταφοράς Υπερκειμένου	204
Samba	205
Firewalls σε Συστήματα Unix	206
IPTables και IPChains	207
TCP Wrappers	208
Firewall Toolkit (FWTK)	209
Όροι Κλειδιά	210
Ερωτήσεις	211
Κεφάλαιο 13 Ασφάλεια Διακομιστή Web	213
Προβλήματα Ασφάλειας στο Web	214
Υλοποίηση Ασφάλειας Διακομιστή Web	214
Συνηθισμένες Λύσεις Ασφάλειας	215
Ασφάλεια Apache	226
Ασφάλεια Internet Information Services	229
Όροι Κλειδιά	235
Ερωτήσεις	236
Κεφάλαιο 14 Ασφάλεια E-mail	237
Κρυπτογράφηση και Επαλήθευση E-mail	238
S/MIME	239
PGP	240
Πλαστογραφία Αλληλογραφίας	240
Ιοί E-mail	241
Ιοί του Outlook	242
Εμπορικά Συστήματα Σάρωσης για Ιούς σε Πύλες E-mail	242
AMaVis	243
Ασφάλεια Συνημμένων	244
Αφαίρεση Όλων των Συνημμένων	244
Επιτρέπεται Μόνο Συγκεκριμένα Συνημμένα	245
Αφαίρεση Μόνο των Επικίνδυνων Συνημμένων	245
Ξένοι Διακομιστές E-mail	248
Απρόσκλητα E-mail	249
Επαλήθευση SMTP	250
Συστημική Αποτροπή Απρόσκλητου E-mail	253
Όροι Κλειδιά	256
Ερωτήσεις	257

xii Ασφάλεια Δικτύων

Κεφάλαιο 15 Ανίχνευση Εισβολής	259
Συστήματα Ανίχνευσης Εισβολής	260
Συστήματα Επιθεώρησης	260
Συστήματα Παραπλάνησης	261
Συστήματα Παρακολούθησης	263
Διαθέσιμα Συστήματα Ανίχνευσης Εισβολής	263
Σύστημα Windows	264
Tripwire	265
Snort	265
Demarc PureSecure	266
NFR Network Intrusion Detector	267
Όροι Κλειδιά	267
Ερωτήσεις	268
 Παράρτημα Α Απαντήσεις στις Ερωτήσεις	 269
Κεφάλαιο 1	269
Κεφάλαιο 2	270
Κεφάλαιο 3	271
Κεφάλαιο 4	273
Κεφάλαιο 5	274
Κεφάλαιο 6	274
Κεφάλαιο 7	275
Κεφάλαιο 8	276
Κεφάλαιο 9	277
Κεφάλαιο 10	279
Κεφάλαιο 11	280
Κεφάλαιο 12	281
Κεφάλαιο 13	282
Κεφάλαιο 14	283
Κεφάλαιο 15	285
 Γλωσσάριο	 287
 <i>Ευρετήριο</i>	 303