

Πίνακας Περιεχομένων

Εισαγωγή	χίχ
----------------	-----

Κεφάλαιο 1 • Ανάλυση Συστημάτων, Τεχνολογία της Πληροφορίας και Ασφάλεια 1

Εισαγωγή στην Ανάλυση Συστημάτων	2
Ορισμός του Εύρους του Προβλήματος	9
Καθορισμός Στόχων, Περιορισμών, Κινδύνων και Κόστους	9
Εφαρμογή της Ανάλυσης Συστημάτων στην Τεχνολογία της Πληροφορίας	13
Η Φύση των Δεδομένων	14
Οι Τεχνολογίες	14
Πώς Χρησιμοποιεί ο Οργανισμός το Σύστημα;	14
Πώς Χρησιμοποιούν οι Άνθρωποι το Σύστημα;	14
Μοντέλα και Ορολογία	14
Η Ασφάλεια σαν μία Συνεχής Διαδικασία	22
Η Επιβίωση του Ικανότερου: Ο Μύθος της Απόλυτης Ασφάλειας	22
Μείωση των Κινδύνων: Μελέτες Επιτυχίας και Αποτυχίας	24
Ο Κύκλος Ζωής της Ανάπτυξης ενός Συστήματος: Η Ασφάλεια σαν μία Αέναη Διαδικασία	26
Θεμελιώδης Ορισμός	26
Προσδιορισμός των Λειτουργικών Απαιτήσεων	27
Ανάπτυξη Προδιαγραφών Ασφάλειας	27
Επανεξέταση του Πλάνου	27
Ανάπτυξη και Απόκτηση	28
Επανεξέταση Συστατικών και Κώδικα	28
Αναθεώρηση του Συστήματος σαν Σύνολο	28
Πιστοποίηση	29
Υλοποίηση	29
Επικύρωση	30
Λειτουργία και Συντήρηση	31
Συνεχής Εγρήγορση	31
Ανασκόπηση	32

Κεφάλαιο 2 • Η Αναγκαιότητα της Ασφάλειας 35

Το Σκεπτικό ενός Εισβολέα	37
Εισβολείς, Χάκερ και Cracker	37
Γιατί θα Ήθελε Κάποιος να Καταστρέψει την Ημέρα μου;	40
Επιθέσεις εκ των Εσω	40

Εξωτερικές Επιθέσεις	42
Μελέτη Εφαρμογής	47
Πόση Ασφάλεια Χρειάζεστε;	48
Ανάλυση Κινδύνων	48
Ποιους Πόρους Θέλω να Προστατέψω;	49
Από Ποιες Οντότητες Προσπαθώ να Προστατέψω τους Πόρους μου;	53
Ποιος θα Ήθελε να Παραβιάσει το Δίκτυό μας;	54
Πόσες Πιθανότητες Έχω να Δεχτώ Επίθεση;	54
Ποιο Είναι το Άμεσο Κόστος;	55
Ποιο Είναι το Μακροπρόθεσμο Κόστος;	56
Πώς Μπορώ να Προστατέψω Αποτελεσματικά σε Σχέση με το Κόστος τους Πόρους μου;	56
Κατάρτιση του Προϋπολογισμού για τα Μέτρα Ασφάλειας	58
Τεκμηριώστε τα Ευρήματά σας	59
Ανασκόπηση	60
 Κεφάλαιο 3 • Βασικές Αρχές Επικοινωνίας Δικτύων	63
Η Ανατομία ενός Πλαισίου Δεδομένων	64
Τα Πλαίσια στο Ethernet	64
Η Ενότητα Κεφαλίδας ενός Πλαισίου	66
Εύρεση Διευθύνσεων	68
Η Δουλειά ενός Πρωτοκόλλου	71
Το Μοντέλο OSI	72
Πώς Λειτουργεί το Μοντέλο OSI;	76
Περαιτέρω Πληροφορίες για το Επίπεδο Δικτύου	80
Routers	80
Πίνακες Δρομολόγησης	82
Στατική Δρομολόγηση	82
Δρομολόγηση Βασιζόμενη σε Διάνυσμα Απόστασης	84
Βασιζόμενη στην Κατάσταση Σύνδεσης Δρομολόγηση	92
Χρήση Ετικετών Δρομολόγησης και MPLS	96
Επικοινωνία Βασιζόμενη ή Μη στην Σύνδεση	99
Βασιζόμενες στην Σύνδεση Μορφές Επικοινωνίας	100
Επικοινωνία Χωρίς Σύνδεση	103
Οι Επιπτώσεις στην Ασφάλεια	105
Υπηρεσίες Δικτύου	106
Η Ειδική Περίπτωση: Το Πρωτόκολλο Μεταφοράς Αρχείων (FTP)	113
Άλλες Υπηρεσίες του IP	117
Επικοινωνίες σε Ανώτερα Επίπεδα	136
Ανασκόπηση	136

Κεφάλαιο 4 • Τοπολογίες Δικτύων και Ασφάλεια	139
Μετάδοση μέσω Δικτύου - Εισαγωγή	140
Ψηφιακή Επικοινωνία	140
Ηλεκτρομαγνητική Ακτινοβολία	142
Καλώδια Οπτικών Ινών	144
Περιορισμένη (Bound) και Απεριόριστη (Unbound) Μετάδοση	146
Επιλογή ενός Μέσου Μετάδοσης	149
Ασφάλεια σε Επίπεδο Τοπολογίας Δικτύου	151
Τοπολογίες τοπικών Δικτύων	151
Τοπολογίες Δικτύων Ευρείας Περιοχής	158
Frame Relay	159
Asynchronous Transfer Mode (ATM)	161
Ασύρματα Δίκτυα WAN	162
Βασικός Εξοπλισμός Δικτύωσης	163
Hubs	163
Γέφυρες	163
Switches	167
Routers	170
Σύγκριση μεταξύ Γεφυρών/Switches και Routers	174
Μεταγωγή στο Επίπεδο 3	175
Ανασκόπηση	176
Κεφάλαιο 5 • Συστήματα Firewall	179
Ορισμός μιας Πολιτικής Ελέγχου Πρόσβασης	180
Ο Ορισμός ενός Firewall	182
Πότε Χρειάζεται ένα Firewall;	183
Εισερχόμενες Συνδέσεις μέσω Μόντεμ και VPN	183
Εξωτερικές Συνδέσεις με Επαγγελματικούς Συνεργάτες	184
Μεταξύ Τμημάτων του Ιδίου Οργανισμού	184
Συγκεκριμένα Συστήματα	184
Λειτουργίες των Συστημάτων Firewall	184
Στατικό Φιλτράρισμα Πακέτων	185
Δυναμικό Φιλτράρισμα Πακέτων	195
Φιλτράρισμα Βασιζόμενο σε Πληροφορίες Κατάστασης	203
Διακομιστές Μεσολάβησης	204
Τύποι Firewall	209
Τι Είδους Firewall Πρέπει να Χρησιμοποιώ;	210
Ποιον Τύπο Πρέπει να Επιλέξω;	211
Βασιζόμενα σε Server Firewalls	212
Βασιζόμενα σε Hardware Firewalls	220
Επιπλέον Θέματα για τα Firewalls	222
Μετάφραση Διευθύνσεων	222

Καταγραφή και Ανάλυση Δραστηριοτήτων από το Firewall	227
Εικονικά Ιδιωτικά Δίκτυα (VPN)	229
Ανίχνευση Εισβολών και Αμυνα	229
Ενοποίηση και Ελεγχος Πρόσβασης	230
Εργαλεία Τρίτων Κατασκευαστών	231
Εσείς Αποφασίζετε	232
Εγκατάσταση ενός Firewall	232
Ανασκόπηση	234
Κεφάλαιο 6 • Το PIX Firewall της Cisco	237
Συνοπτική Παρουσίαση του PIX	238
Εγκατάσταση του PIX	239
Εγκατάσταση του PDM	241
Διαμόρφωση του PDM	244
Διαμόρφωση του PIX Firewall	247
Διαμόρφωση της Ασφάλειας στο PIX	253
Η Καρτέλα Access Rules	254
Κανόνες AAA	262
Κανόνες Φίλτρων	265
Η Καρτέλα Translation Rules	271
Η Καρτέλα Monitoring	282
Ανασκόπηση	284
Κεφάλαιο 7 • Συστήματα Ανίχνευσης Εισβολών	287
Τύποι Συστημάτων Ανίχνευσης Εισβολών	288
Συστήματα Ανίχνευσης Εισβολών σε Δίκτυα	289
Εργαλεία Ελέγχου της Ακεραιότητας του Συστήματος	290
Εργαλεία Παρακολούθησης των Αρχείων Καταγραφής Συμβάντων (LFM)	291
Εικονικά Δολώματα (Honeypots)	292
Περιορισμοί των Συστημάτων NIDS	293
Κατακλυσμός Σταγονιδίων	294
Άλλοι Γνωστοί Περιορισμοί των Συστημάτων NIDS	296
Τα Αντίμετρα που Διαθέτουν τα Συστήματα IDS	301
Συστήματα Ανίχνευσης Εισβολών για Έναν Υπολογιστή	304
NIDS Fusion: Ενοποίηση Δεδομένων	307
Snort: Ένα Δημοφιλές Σύστημα Ανίχνευσης Εισβολών σε Δίκτυα	309
Οι Κανόνες του Snort	310
Πριν Ξεκινήσετε	315
Διαμόρφωση του Snort	318
Παράδειγμα Συναγερμού του Snort	319
Υποδείξεις για την Χρήση του Snort	320
Ανασκόπηση	321

Κεφάλαιο 8 • Κρυπτογράφηση και Πιστοποίηση	323
Η Ανάγκη για Αυξημένη Ασφάλεια	324
Μετάδοση σε Μορφή Απλού Κειμένου	324
Παθητική Παρακολούθηση Απλού Κειμένου	326
Η Αναγκαιότητα ενός Καλού Μηχανισμού Πιστοποίησης	328
Πειρατεία Συνόδων	329
Επαλήθευση του Προορισμού	330
Εισαγωγή στην Κρυπτογράφηση	331
Μέθοδοι Κρυπτογράφησης	332
Τα Αδύνατα Σημεία της Κρυπτογράφησης	336
Η Παρέμβαση της Κυβέρνησης	340
Η Αναγκαιότητα ενός Καλού Μηχανισμού Κρυπτογράφησης	340
Λύσεις	341
Data Encryption Standard (DES)	342
Advanced Encryption Standard (AES)	342
Servers Ψηφιακών Πιστοποιητικών	343
To IPSEC (IP Security)	344
Kerberos	345
PPTP/L2TP	346
EAP (Extensible Authentication Protocol)	346
Remote Access Dial-In User Service (RADIUS)	347
Κρυπτογράφηση RSA	347
Secure Shell (SSH)	348
Secure Sockets Layer (SSL)	348
Συσκευές Ασφάλειας	349
SKIP (Simple Key Management for Internet Protocols)	350
Ανασκόπηση	351
Κεφάλαιο 9 • Εικονικά Ιδιωτικά Δίκτυα (VPN)	353
Εισαγωγή στην Τεχνολογία VPN	354
Χρήση Δικτύων VPN	356
Επιλογή ενός Προϊόντος VPN	361
Προϊόντα για VPN	363
Εναλλακτικές Λύσεις ως προς τα Δίκτυα VPN	365
Διαμόρφωση ενός Δικτύου VPN	366
Προετοιμασία του Συστήματος	366
Το Σχηματικό Διάγραμμα του VPN	366
Διαμόρφωση του VPN Server	367
Διαμόρφωση του VPN Client	373
Έλεγχος του VPN	377
Ανασκόπηση	380

Κεφάλαιο 10 • Ιοί, Δούρειοι Ιπποι και Worms 383

Χρήσιμα Στατιστικά Στοιχεία για τους Ιούς	384
Τι Είναι Ένας Ιός;	385
Αναπαραγωγή	386
Απόκρυψη	389
Βόμβες	393
Ιοί Κοινωνικής Μηχανικής	393
Worms	395
Δούρειοι Ιπποι	398
Αποτρεπτικά Μέτρα	399
Έλεγχος Πρόσβασης	400
Επαλήθευση του Ελεγκτικού Αθροίσματος	401
Παρακολούθηση Διεργασιών	401
Προγράμματα Ανίχνευσης Ιών	403
Ευριστικοί Σαρωτές	405
Εργαλεία Ανίχνευσης Ιών σε Επίπεδο Εφαρμογής	406
Μία Στρατηγική για την Προστασία από Ιούς	407
Προστασία των Σταθμών Εργασίας	408
Προστασία των Λειτουργικών Συστημάτων των Servers	410
Προστασία Συστημάτων UNIX	411
Ανασκόπηση	412

Κεφάλαιο 11 • Πρόληψη και Ανάκαμψη από Καταστροφές 415

Κατηγορίες Καταστροφών	416
Καταστροφές στο Δίκτυο	417
Μέσα Επικοινωνίας	418
Τοπολογία	420
Τοπολογίες Τοπικών Δικτύων	420
Τοπολογίες για Δίκτυα Ευρείας Περιοχής (WAN)	425
Σημεία Αστοχίας	428
Αποθήκευση των Αρχείων Διαμόρφωσης	431
Καταστροφές που Απειλούν τους Servers	432
Τροφοδοτικά Αδιάλειπτης Παροχής (UPS)	433
RAID	434
Εφεδρικοί Servers	437
Ομαδοποίηση των Servers σε Συστοιχίες (Clustering)	439
Εφεδρικά Αντίγραφα Δεδομένων	440
Παροχές Υπηρεσιών Εφαρμογών	444
Ανάκαμψη του Server	444
Ακραίες Καταστροφές	446
Μη-Καταστροφικός Έλεγχος	448
Τεκμηρίωση των Διαδικασιών	448

Το VERITAS Storage Replicator	449
Προετοιμασία Πριν από την Εγκατάσταση του VSR	450
Εγκατάσταση του VSR	451
Διαμόρφωση του VSR	453
Διαμόρφωση των Παραμέτρων για την Λειτουργία Αντιγραφής	457
Ανασκόπηση	464
 Κεφάλαιο 12 • Θέματα Ασφάλειας για Περιβάλλοντα με τα Windows	467
Σύνοψη των Windows NT	468
Το Active Directory	470
Η Δομή των Domain	475
Αποθήκευση Πληροφοριών Domain	475
Σχέσεις Εμπιστοσύνης Μεταξύ των Domain	476
Λογαριασμοί Χρηστών	477
Αναγνωριστικά Ασφάλειας	477
Το Security Account Manager των Windows NT	479
Καθορισμός Πολιτικών Ομάδων στα Windows 2000	480
Ορισμός Πολιτικών στα Windows NT	492
Πολιτικές και Προφίλ	498
Το Σύστημα Αρχείων	503
Δικαιώματα για Κοινόχρηστους Πόρους	504
Ασφάλεια σε Επίπεδο Αρχείων	506
Καταγραφή Συμβάντων	511
Διαμόρφωση του Event Viewer	511
Εξέταση των Αρχείων Καταγραφής Συμβάντων	512
Παρακολούθηση Συμβάντων Συστήματος	514
Διορθώσεις για την Ασφάλεια	516
Διαθέσιμες Υπηρεσίες IP	517
Computer Browser	518
DHCP Relay Agent	518
Microsoft DHCP Server	518
Microsoft DNS Server	518
Microsoft Internet Information Server (IIS)	519
Microsoft TCP/IP Printing	520
Network Monitor Agent	521
RIP	522
RPC Configuration	522
Simple TCP/IP Services	522
SNMP Service	523
Windows Internet Naming Service (WINS)	523
Φιλτράρισμα Πακέτων με τα Windows NT	524
Ενεργοποίηση του Φιλτραρίσματος Πακέτων	524

Διαμόρφωση της Λειτουργίας Φιλτραρίσματος Πακέτων	526
Λίγες Τελευταίες Σκέψεις για τις Θύρες	528
Ασφάλεια DCOM	529
Επιλογή του Πρωτοκόλλου Μεταφοράς για το DCOM	530
Περιορισμός των Θυρών που Χρησιμοποιούνται από το DCOM	532
DCOM και NAT	533
Οι Θύρες που Χρησιμοποιούν οι Υπηρεσίες των Windows	533
Επιπλέον Αλλαγές σε Κλειδιά του Registry	535
Εμφάνιση Αρχικού Μηνύματος πριν από την Σύνδεση	535
Απόκρυψη του Αμέσως Προηγούμενου Ονόματος Σύνδεσης	536
Ασφάλιση του Registry στα Windows NT Workstation	537
Ασφαλής Πρόσβαση στο Event Viewer	537
Εκκαθάριση του Αρχείου Μεταγωγής	538
Τα Windows 2000	538
Δικαιώματα για την Προσπέλαση του Συστήματος Αρχείων	539
Κρυπτογράφηση με το EFS	539
Kerberos Έκδοση 5	542
Υπηρεσίες Πιστοποιητικών και Παραγωγής Δημόσιων Κλειδιών	547
Το Πρωτόκολλο IPsec	549
Εξυπνες Κάρτες	551
Windows .NET	553
Η Πολιτική Ασφάλειας του .NET	554
Εργαλεία για την Επιβολή Πολιτικών Ασφάλειας	555
Συστάσεις για την Υλοποίηση της Πολιτικής Ασφάλειας	556
Ανασκόπηση	557
 Κεφάλαιο 13 • Θέματα Ασφάλειας για το Unix	559
Το Ιστορικό του Unix	560
Το FreeBSD	561
Το Linux	562
Το Σύστημα Αρχείων του Unix	563
Οι Κωδικοί UID και GID	564
Δικαιώματα Αρχείων	565
Διαχείριση Λογαριασμών	569
Το Αρχείο Password	570
Το Αρχείο Group	573
PAM (Pluggable Authentication Module)	575
Περιορισμός της Σύνδεσης του Χρήστη Root μόνο στην Τοπική Κονσόλα	578
Βελτιστοποίηση του Πυρήνα του Unix	579
Εκτέλεση του make	580
Αλλαγή των Ρυθμίσεων του Προγράμματος Οδήγησης Δικτύου	590
Διαχείριση Υπηρεσιών IP	591

Υπηρεσίες IP	591
inetd και xinetd	597
Άλλες Υπηρεσίες	600
TCP Wrapper	602
Λίστα Υποδείξεων για το Unix	603
Προ-Εγκατάσταση	603
Διαμόρφωση του Συστήματος	603
Ανασκόπηση	606
 Κεφάλαιο 14 • Θέματα Ασφάλειας για το NetWare	609
Ο Πυρήνας του Λειτουργικού Συστήματος NetWare	610
Πιστοποίηση C2	612
Υπηρεσίες Καταλόγου του NetWare	613
Η Σχεδίαση του NDS	613
Διαχείριση Λογαριασμών	615
Η Καρτέλα Επιλογών Identification	616
Η Καρτέλα Επιλογών Logon Restrictions	616
Η Καρτέλα Επιλογών Password Restrictions	617
Η Καρτέλα Επιλογών Network Address Restriction	618
Η Καρτέλα Επιλογών Intruder Lockout	619
Η Καρτέλα Επιλογών Rights to Files and Directories	620
Group Membership	622
Security Equal To	622
Το Σύστημα Αρχείων	623
Η Μάσκα Κληρονομούμενων Δικαιωμάτων	623
Καταγραφή Συμβάντων και Παρακολούθηση	625
Το Εργαλείο Auditcon	626
Ασφάλεια Δικτύου	628
Υπογραφή Πακέτων	628
Το Βοήθημα Filtcfg	630
Η Υπηρεσία PKIS (Public Key Infrastructure Service)	633
Η Υπηρεσία Πιστοποίησης NMAS της Novell	634
Προσαρμογή των Ρυθμίσεων Ασφάλειας του NetWare	636
Το Script SECURE.NCF	637
Η Εντολή Secure Console	637
Ασφάλεια και Απομακρυσμένη Πρόσβαση στην Κονσόλα	637
Ο Παράγοντας Πανδώρα	640
Ανασκόπηση	640
 Κεφάλαιο 15 • Η Ανατομία μιας Επίθεσης	643
Συλλογή Πληροφοριών	644
Η Εντολή whois	645

Η Εντολή nslookup	648
Μηχανές Αναζήτησης	650
Διερεύνηση του Δικτύου	651
Η Εντολή traceroute	652
Σάρωση Υπολογιστών και Υπηρεσιών	654
Παθητική Παρακολούθηση	658
Ελεγχος για Τρωτά Σημεία	659
Εξαπόλυση της Επίθεσης	662
Κρυφοί Λογαριασμοί	663
Επιθέσεις MITM (Man in the Middle)	664
Υπερχείλιση Buffer	666
Επιθέσεις που Βασίζονται στο Πεδίο SYN	667
Επιθέσεις Σταγονιδίων	668
Επιθέσεις Smurf	670
Επιθέσεις Ωμής Βίας	671
Επιθέσεις που Απαιτούν Φυσική Πρόσβαση	673
Ανασκόπηση	675
Παράρτημα Α • Οδηγίες και Πηγές Πληροφοριών για Θέματα Ασφάλειας	677
<i>Ευρετήριο</i>	<i>689</i>