

# Πίνακας Περιεχομένων

Πρόλογος .....	17
Ευχαριστίες .....	20
Εισαγωγή .....	21

## ΜΕΡΟΣ Ι

### Αναγνώριση Στόχου

Παρακολούθηση της Ασφάλειας του Δικτύου .....	2
<b>▼ 1</b> Αναγνώριση Συστημάτων .....	9
Γιατί Είναι Απαραίτητη η Αναγνώριση; .....	10
Αναγνώριση Μέσω Internet .....	11
Βήμα 1. Καθορίστε το Εύρος των Δραστηριοτήτων σας .....	12
Βήμα 2. Συλλογή Πληροφοριών για το Δίκτυο .....	16
Βήμα 3. Διερεύνηση στο DNS .....	25
Βήμα 4. Αναγνώριση του Δικτύου .....	29
Ανασκόπηση .....	33
<b>▼ 2</b> Σάρωση .....	35
Έλεγχος εάν Ένα Σύστημα Είναι σε Λειτουργία .....	36
Εξακρίβωση των Υπηρεσιών που Τρέχουν ή Ακροάζονται .....	44
Τύποι Σάρωσης .....	44
Προσδιορισμός των Ενεργών TCP και UDP Υπηρεσιών .....	46
Εργαλεία Σάρωσης Θυρών για τα Windows .....	52
Σύνοψη των Εργαλείων Σάρωσης Θυρών .....	57
Εξακρίβωση Λειτουργικού Συστήματος .....	60
Ενεργητική Αναγνώριση Σωρού .....	61

## X Χάκερ - Επίθεση και Αμυνα

Παθητική Αναγνώριση Σωρού .....	64
Εργαλεία Αυτοματοποιημένης Αναγνώρισης .....	66
Ανασκόπηση .....	68
▼ 3 Ενεργητική Συλλογή Πληροφοριών .....	69
Ενεργητική Συλλογή Πληροφοριών .....	71
Απαρίθμηση Κοινών Υπηρεσιών του Δικτύου .....	73
Ανασκόπηση .....	123

## ΜΕΡΟΣ II

### Διείδυση σε Επίπεδο Λειτουργικού Συστήματος

Οι Κίνδυνοι των Ελέγχων Διείδυσης .....	126
▼ 4 Επιθέσεις σε Συστήματα με Windows 95/98 και Me .....	126
Επιθέσεις σε Συστήματα με τα Win 9x από Απόσταση .....	131
Άμεση Σύνδεση σε Κοινόχρηστους Πόρους των Win 9x .....	131
Δούρειοι Ιππιοί και Πίσω Πόρτες στα Win 9x .....	137
Γνωστά Τρωτά Σημεία Εφαρμογών Server .....	142
Γνωστά Τρωτά Σημεία Εφαρμογών Server .....	142
Τοπικές Επιθέσεις στα Win 9x .....	143
Τα Windows Millennium Edition (Me) .....	150
Επιθέσεις Εξ Αποστάσεως σε Συστήματα με τα Windows Me .....	150
Τοπικές Επιθέσεις στα Windows Me .....	150
Ανασκόπηση .....	152
▼ 5 Επιθέσεις σε Συστήματα με Windows NT .....	153
Σύνοψη .....	155
Τι δεν θα Καλύψουμε .....	156
Επιθέσεις Χωρίς Πιστοποίηση .....	156
Επιθέσεις Μέσω του SMB .....	156
Επιθέσεις στο IIS .....	175
Επιθέσεις με Πιστοποίηση .....	185
Κλιμάκωση Δικαιωμάτων .....	185
Κλοπή Πληροφοριών .....	190
Έλεγχος από Απόσταση και Πίσω Πόρτες .....	200
Ανακατεύθυνση Θύρας .....	204
Γενικά Αντίμετρα Εναντι των Παραβιάσεων με Δικαιώματα Administrator .....	206
Κάλυψη των Ιχνών .....	210
Απενεργοποίηση της Καταγραφής Συμβάντων .....	210
Εκκαθάριση του Αρχείου Καταγραφής Συμβάντων .....	211
Απόκρυψη Αρχείων .....	211
Εργαλεία Ασφάλειας για την Οικογένεια NT .....	212
Εγκαταστήστε τις Διορθώσεις .....	212
Πολιτικές Ομάδων .....	213
Ipsec .....	215
Runas .....	216

Το .Net Framework . . . . .	217
Το Internet Connection Firewall. . . . .	217
Το Encrypting File System (Efs) . . . . .	217
Μία Σημείωση για το Raw Sockets και Άλλους Ανυπόστατους Ισχυρισμούς . . . . .	218
Ανασκόπηση . . . . .	219
<b>▼ 6</b> Επιθέσεις σε Συστήματα Novell . . . . .	<b>221</b>
Επαφή Χωρίς Σύνδεση. . . . .	223
Συλλογή Πληροφοριών για το Bindery και τα Δέντρα . . . . .	224
Ανοιγμα Ξεκλειδωτων Θυρών . . . . .	231
Συλλογή Πληροφοριών Μετά από Πιστοποίηση . . . . .	233
Απόκτηση Δικαιωμάτων Επύπτη . . . . .	238
Τρωτά Σημεία Εφαρμογών . . . . .	241
Επιθέσεις Εξαπάτησης (Pandora) . . . . .	248
Αφού Αποκτήσετε Δικαιώματα Επύπτη σ' Έναν Server . . . . .	251
Απόκτηση των NDS Αρχείων . . . . .	253
Παραποίηση των Αρχείων Καταγραφής . . . . .	259
Αρχεία Καταγραφής Συμβάντων της Κοσόλας . . . . .	260
Ανασκόπηση . . . . .	263
<b>▼ 7</b> Επιθέσεις σε Συστήματα Unix . . . . .	<b>265</b>
Η Αναζήτηση του Root . . . . .	266
Μία Σύντομη Επανάληψη. . . . .	266
Χαρτογράφηση Τρωτών Σημείων . . . . .	267
Απομακρυσμένη Εναντι Τοπικής Πρόσβασης . . . . .	267
Απομακρυσμένη Πρόσβαση . . . . .	268
Βασιζόμενες σε Δεδομένα Επιθέσεις . . . . .	271
Πρόσβαση στον Φλοιό . . . . .	279
Κοινοί Τύποι Απομακρυσμένων Επιθέσεων . . . . .	283
Τοπική Πρόσβαση . . . . .	307
Μετά από την Απόκτηση Δικαιωμάτων Root. . . . .	322
Rootkits . . . . .	323
Ανάκαμψη από Επιθέσεις Μέσω Rootkits . . . . .	334
Ανασκόπηση . . . . .	335

**ΜΕΡΟΣ III**

**Διείσδυση σε Επίπεδο Δικτύου**

Ανοίγοντας Σήραγγες στα Firewalls. . . . .	338
<b>▼ 8</b> Συνδέσεις Dial-Up & Vpn, Τηλεφωνικά Κέντρα και Συστήματα Φωνητικού Ταχυδρομείου . . . . .	<b>341</b>
Προετοιμασία. . . . .	342
War-Dialing. . . . .	344
Εξοπλισμός . . . . .	344
Νομικά Θέματα . . . . .	345
Άλλες Επιβαρύνσεις . . . . .	346
Λογισμικό . . . . .	346

## xii Χάκερ - Επίθεση και Αμυνα

---

Επιθέσεις Ωμής Βίας Μέσω Script - Ο Χειροκίνητος Τρόπος . . . . .	362
Μία Τελευταία Σημείωση . . . . .	372
Επιθέσεις σε Ηλεκτρονικά Τηλεφωνικά Κέντρα . . . . .	374
Επιθέσεις σε Συστήματα Φωνητικού Ταχυδρομείου . . . . .	378
Επιθέσεις σε Συνδέσεις VPN . . . . .	383
Ανασκόπηση . . . . .	388
<b>▼ 9 Συσκευές Δικτύωσης . . . . .</b>	<b>391</b>
Εντοπισμός . . . . .	392
Ανίχνευση . . . . .	392
IP Lookup . . . . .	395
Αναζήτηση Αυτόνομων Συστημάτων . . . . .	396
Κανονικό Traceroute . . . . .	396
Traceroute με Πληροφορίες ASN . . . . .	397
Show Ip Bgp . . . . .	397
Ομάδες Συζήτησης . . . . .	398
Ανίχνευση Υπηρεσιών . . . . .	399
Επιθέσεις στο Δίκτυο . . . . .	405
Το Επίπεδο 1 του OSI . . . . .	406
Το Επίπεδο 2 του OSI . . . . .	406
Ανίχνευση Μέσων στο Επίπεδο 2 . . . . .	406
Υποκλοπή Πληροφοριών σε Βασιζόμενα σε Switches Δίκτυα . . . . .	408
Το Επίπεδο 3 του Μοντέλου OSI . . . . .	416
Dsniff . . . . .	418
Προβλήματα που Οφείλονται σε Λανθασμένη Διαμόρφωση . . . . .	420
Επιθέσεις σε Πρωτόκολλα Δρομολόγησης . . . . .	427
Ανασκόπηση . . . . .	438
<b>▼ 10 Διείδυση σε Ασύρματα Συστήματα . . . . .</b>	<b>439</b>
Αναγνώριση Ασύρματων Συστημάτων . . . . .	440
Εξοπλισμός . . . . .	441
GPS . . . . .	444
Σάρωση και Απαρίθμηση Ασύρματων Δικτύων . . . . .	455
Εργαλεία Sniffer για Ασύρματα Δίκτυα . . . . .	456
Εργαλεία Παρακολούθησης Ασύρματων Δικτύων . . . . .	458
Έλεγχος Πρόσβασης Βασιζόμενος σε Διευθύνσεις Mac . . . . .	467
Απόκτηση Πρόσβασης (Επίθεση στο 802.11) . . . . .	468
Έλεγχος Πρόσβασης Βάσει Διευθύνσεων MAC . . . . .	470
Επιθέσεις Εναντίον του Αλγόριθμου του WEP . . . . .	471
Μέτρα για την Θωράκιση του WEP . . . . .	473
Εργαλεία τα Οποία Εκμεταλλεύονται τις Αδυναμίες του WEP . . . . .	473
Επιθέσεις Αρνησης Εξυπηρέτησης . . . . .	477
Επισκόπηση του 802.1x . . . . .	477
Ανασκόπηση . . . . .	479

▼ 11	Firewalls . . . . .	481
	Τύποι Firewalls . . . . .	482
	Αναγνώριση των Firewalls . . . . .	483
	Προχωρημένες Τεχνικές Εντοπισμού Firewalls . . . . .	487
	Σάρωση Μέσα από Firewalls . . . . .	490
	Φιλτράρισμα Πακέτων . . . . .	494
	Τρωτά Σημεία των Βασιζόμενων σε Διακομιστές Μεσολάβησης Επιπέδου Εφαρμογής Firewalls . . . . .	498
	Τρωτά Σημεία του Wingate . . . . .	500
	Ανασκόπηση . . . . .	502
▼ 12	Επιθέσεις Αρνησης Εξυπηρέτησης . . . . .	503
	Τα Κίνητρα των Ανθρώπων που Εξαπολύουν Επιθέσεις DOS . . . . .	504
	Τύποι Επιθέσεων DOS . . . . .	505
	Κατανάλωση Εύρους Ζώνης . . . . .	505
	Εξάντληση Πόρων . . . . .	506
	Λάθη Προγραμματισμού . . . . .	506
	Επιθέσεις σε Συστήματα Δρομολόγησης και DNS . . . . .	507
	Γενικευμένες Επιθέσεις DOS . . . . .	508
	Πολιορκία Τοποθεσιών . . . . .	510
	Επιθέσεις DOS σε Συστήματα με UNIX και Windows . . . . .	514
	Επιθέσεις DOS από Απόσταση . . . . .	514
	Καταμεμημένες Επιθέσεις Αρνησης Εξυπηρέτησης . . . . .	518
	Τοπικές Επιθέσεις Αρνησης Εξυπηρέτησης . . . . .	523
	Ανασκόπηση . . . . .	525

## ΜΕΡΟΣ IV

### Επιθέσεις σε Επίπεδο Λογισμικού

	Εσύ Λες Αντίο, Εγώ Λέω Γεια . . . . .	528
▼ 13	Ελεγχος Εξ Αποστάσεως και Προβλήματα Ασφάλειας . . . . .	529
	Εύρεση Λογισμικού Απομακρυσμένου Ελέγχου . . . . .	530
	Σύνδεση . . . . .	531
	Αδυναμίες . . . . .	532
	Το Virtual Network Computing (VNC) . . . . .	539
	Microsoft Terminal Server και Citrix ICA . . . . .	543
	Ο Server . . . . .	544
	Οι Client Εφαρμογές . . . . .	544
	Μετάδοση Δεδομένων . . . . .	544
	Εύρεση Στόχων . . . . .	544
	Επιθέσεις στο Terminal Server . . . . .	547
	Επιπλέον Ζητήματα Ασφάλειας . . . . .	551
	Πηγές Πληροφοριών . . . . .	552
	Ανασκόπηση . . . . .	553

## **xiv** Χάκερ - Επίθεση και Αμυνα

---

▼ 14 Προχωρημένες Τεχνικές	555
Πειρατεία Συνόδων	556
Πίσω Πόρτες	558
Δούρειοι Ιππιοί	580
Κρυπτογραφία	583
Ορολογία	583
Κατηγορίες Επιθέσεων	583
Επιθέσεις εναντίον του Secure Shell (SSH)	584
Υπονόμευση του Περιβάλλοντος του Συστήματος: Rootkits και Εργαλεία Απεικόνισης	586
Κοινωνική Μηχανική	589
Ανασκόπηση	591
▼ 15 Επιθέσεις στο Web	593
Επιθέσεις σε Web Servers	594
Αποκάλυψη Πηγαίου Κώδικα	595
Επιθέσεις Κανονικοποίησης	597
Προβλήματα Ασφάλειας Σχετιζόμενα με το WebDAV	597
Καταστάσεις Υπερχείλισης Buffer	600
Τρωτά Σημεία του Cold Fusion	609
Εργαλεία Σάρωσης για την Εύρεση Προβλημάτων Ασφάλειας σε Web Servers	611
Επιθέσεις σε Εφαρμογές Web	612
Εύρεση Ευάλωτων Εφαρμογών Web με το Google	613
Σάρωση του Web	614
Αξιολόγηση Web Εφαρμογών	615
Κοινά Προβλήματα Ασφάλειας Εφαρμογών Web	623
Ανασκόπηση	629
▼ 16 Κίνδυνοι για τους Χρήστες του Internet	631
Καταστροφικός Μεταφερτός Κώδικας	633
Η Τεχνολογία Activex της Microsoft	633
Προβλήματα Ασφάλειας της Java	645
Το Τέρας των Cookies	649
Internet Explorer και Πλαίσια της HTML	654
Πλαστοπροσωπία στο SSL	656
Επιθέσεις Μέσω Ηλεκτρονικού Ταχυδρομείου	659
Επιθέσεις Μέσω Ηλεκτρονικού Ταχυδρομείου - Τα Βασικά	659
Εκτέλεση Κώδικα Μέσω Email	662
"Σκουλήκια" στο Outlook	676
Επιθέσεις Μέσω Συνημμένων Αρχείων	679
Εξερχόμενες Συνδέσεις από το Client Σύστημα	687
Επιθέσεις Μέσω IRC	690
Γενικά Αντίμετρα Εναντι Επιθέσεων σε Χρήστες του Internet	692
Ανασκόπηση	693

**ΜΕΡΟΣ V**

**Παραρτήματα**

▼ <b>A</b>	Θύρες. ....	697
▼ <b>B</b>	Τα 14 Σοβαρότερα Προβλήματα Ασφάλειας . . . . .	703
▼	Ευρετήριο . . . . .	705