

# Περιεχόμενα

Ευχαριστίες .....	xxi
Εισαγωγή .....	xxiii

## Μέρος I

### Πολυλειτουργικά Εργαλεία

<b>1 Netcat και Cryptcat .....</b>	<b>3</b>
Netcat .....	4
Οι 101 Χρήσεις του Netcat .....	9
Cryptcat .....	24
<b>2 Εργαλεία Ανοικτού Κώδικα και Εργαλεία του Συστήματος:</b>	
<b>Τα Βασικά .....</b>	<b>25</b>
Εργαλεία Server Message Block Protocol .....	26
Εργαλεία Δικτύου: Η Πλευρά των Windows .....	26
Samba: η Πλευρά του UNIX .....	31
NBTSTAT .....	34
Regdmp .....	38
Finger .....	39
whois/fwhois .....	42
Ping .....	45

Fping .....	47
Traceroute .....	50
Hping .....	53
Rpcinfo .....	56
showmount .....	58
R-Tools .....	59
Rlogin, Rsh και Rcp .....	60
Η Ανεσφάλεια των R-tools .....	60
Rwho .....	60
Rexec .....	61
Who, W και Last .....	61
who .....	61
w .....	62
last .....	62
<b>3 Το Σύστημα X Window .....</b>	<b>65</b>
Επιλέγοντας έναν Διαχειριστή Παραθύρων .....	66
Ένα Μοντέλο Πελάτη/Διακομιστή .....	66
Πώς Επικοινωνούν οι Απομακρυσμένοι X Διακομιστές και Πελάτες .....	67
Ασφαλιζοντας τα X, Μέρος 1: Χρησιμοποιώντας Xhost και Xauth .....	68
Xhost .....	68
Xauth .....	69
Ασφαλιζοντας το X, Μέρος 2: Περνώντας την Κίνηση X Μέσω SSH .....	71
Οι Άλλοι Σημαντικοί Παίκτες .....	73
Xdm .....	73
Xinit και Startx .....	73
Xserver .....	74
Τώρα Ξέρετε... .....	74
<b>4 VMware .....</b>	<b>75</b>
Μεταφορά και Εγκατάσταση .....	76
Διαμόρφωση .....	77
Χειρισμός .....	85
<b>5 Cygwin .....</b>	<b>89</b>
Μεταφορά και Εγκατάσταση .....	90
Χειρισμός .....	92
Δομή Καταλόγων και Δικαιώματα Αρχείων .....	94
Εκτέλεση Εφαρμογών .....	95
Το XFree86 για το Cygwin .....	97

**Μέρος II**  
**Εργαλεία για Εισβολή και Έλεγχο Συστημάτων στο Δίκτυο**

<b>6</b>	<b>Σαρωτές Θυρών .....</b>	<b>103</b>
	Nmap .....	104
	NetScanTools .....	122
	SuperScan .....	125
	IpEye .....	131
	FScan .....	132
	WUPS .....	134
	Udp_scan .....	135
	Εγκατάσταση .....	136
<b>7</b>	<b>Εργαλεία Απαρίθμησης των Windows .....</b>	<b>143</b>
	Winfingerprint .....	144
	GetUserInfo .....	146
	Enum .....	148
	PsTools .....	152
<b>8</b>	<b>Web Εργαλεία Εισβολής .....</b>	<b>171</b>
	Σαρωτές Τρωτών Σημείων .....	172
	Whisker .....	172
	Nikto .....	179
	Stealth .....	185
	Twwwscan/Arirang .....	192
	Γενικά Εργαλεία .....	195
	Curl .....	195
	OpenSSL .....	198
	Stunnel .....	202
	Εξέταση Εφαρμογής .....	205
	Achilles .....	205
	WebSleuth .....	207
	Wget .....	207
<b>9</b>	<b>Διάρρηξη Κωδικών Πρόσβασης/ Εργαλεία Άμεσης Επίθεσης .....</b>	<b>211</b>
	PassFilt.dll και Πολιτικές Κωδικών Πρόσβασης των Windows .....	212
	Πολιτικές κωδικών πρόσβασης του PAM και του Unix .....	215
	OpenBSD login.conf .....	218
	John the Ripper .....	221
	L0phtCrack .....	233

Σύλληψη Κατακερματισμένων Κωδικών Πρόσβασης των Windows .....	237
PwDump .....	237
LsAdump2 .....	240
Ενεργά Εργαλεία Άμεσης Επίθεσης .....	241
SMBGrind .....	241
Nbaudit (nat) .....	242
<b>10 Αφύλακτες Πόρτες και Εργαλεία Απομακρυσμένης Πρόσβασης .....</b>	<b>245</b>
VNC .....	247
Netbus .....	253
Back Orifice .....	258
SubSeven .....	267
Loki .....	272
stcpshell .....	275
Knark .....	277
<b>11 Απλά Εργαλεία Ελέγχου Προέλευσης .....</b>	<b>283</b>
Flawfinder .....	284
RATS .....	289
<b>12 Συνδυασμός Εργαλείων Ελέγχου Συστημάτων .....</b>	<b>295</b>
Nessus .....	296
Εγκατάσταση .....	298
STAT .....	310
Retina .....	319
Internet Scanner .....	324
Tripwire .....	333
Χειρισμός: Η Έκδοση Ανοικτού Κώδικα .....	335
Χειρισμός: Η Εμπορική Έκδοση .....	344
Ασφάλιση των Αρχείων σας με το Tripwire .....	347

### Μέρος III

#### Εργαλεία για Επίθεση και Έλεγχο του Δικτύου

<b>13 Ανακατεύθυνση Θυρών .....</b>	<b>353</b>
Datapipe .....	355
FPipe .....	357
<b>14 Sniffers .....</b>	<b>367</b>
Επισκόπηση των Sniffer .....	368
BUTTSniffer .....	370
Tcpdump και WinDump .....	379
Εγκατάσταση .....	379
Ethereal .....	389

Dsniff .....	397
Εγκατάσταση .....	398
Χειρισμός: Τα Εργαλεία .....	398
Επικίνδυνα Εργαλεία .....	403
Snort: Ένα Σύστημα Εντοπισμού Εισβολής .....	403
Εγκατάσταση και Χειρισμός .....	404
Τα Πρόσθετα του Snort .....	407
Και Πολλά Άλλα .....	410
<b>15 Ασύρματα Εργαλεία .....</b>	<b>415</b>
NetStumbler .....	417
AiroPeek .....	419
<b>16 War Dialers .....</b>	<b>423</b>
ToneLoc .....	424
Δημιουργία του Αρχείου tl.cfg .....	424
Εκτέλεση μιας Σάρωσης .....	427
Περιήγηση στο Περιβάλλον του ToneLoc .....	431
Τεχνικές Αρχείων .dat .....	431
THC-Scan .....	436
Διαμόρφωση του THC-Scan .....	436
Εκτέλεση του THC-Scan .....	438
Περιήγηση στο THC-Scan .....	439
Χειρισμός των Αρχείων .dat του THC-Scan .....	440
Πέρα από τη Συμβολοσειρά Σύνδεσης .....	442
<b>17 Εργαλεία Στοίβας TCP/IP .....</b>	<b>443</b>
ISIC: Ελεγκτής Ακεραιότητας IP Στοίβας .....	444
Συμβουλές και Τεχνάσματα .....	447
Iptest .....	449
Nemesis: Δημιουργία Πακέτων .....	452
Πέρα από τη Γραμμή Εντολών .....	457

#### Μέρος IV

#### Εργαλεία που Χρησιμοποιούνται σε Εγκληματολογικές Έρευνες και σε Απόκριση Περιστατικών

<b>18 Δημιουργία (και Χρήση) μιας Εργαλειοθήκης Άμεσων Αποκρίσεων στα Windows .....</b>	<b>461</b>
cmd.exe .....	463
Fport .....	463
Netstat .....	465
NBTSTAT .....	467

ARP .....	468
Pslist .....	469
kill .....	470
dir .....	471
Auditpol .....	473
Loggedon .....	474
NtLast .....	474
Dump Event Log (dumpel) .....	475
Regdmp .....	476
SFind .....	478
Md5sum .....	479
<b>19 Δημιουργία και Χρήση μιας Εργαλειοθήκης Άμεσων Αποκρίσεων για το Unix .....</b>	<b>485</b>
bash .....	487
Netstat .....	488
ARP .....	489
ls .....	490
w .....	492
last και lastb .....	492
Lsof .....	493
ps .....	495
kill .....	499
Md5sum .....	499
Carbonite .....	500
Execve_Sniffer .....	501
<b>20 Εμπορικές Εργαλειοθήκες για Αντιγραφή για Εγκληματολογική Έρευνα .....</b>	<b>505</b>
EnCase v3 .....	506
Format: Δημιουργία μιας Αξιόπιστης Δισκέτας Εκκίνησης .....	516
PDBLOCK: Μπλοκάρισμα Εγγραφής των Σκληρών Δίσκων .....	517
Safeback .....	518
SnapBack .....	529
Ghost .....	535
<b>21 Μια Μη Εμπορική Εργαλειοθήκη για Αντιγραφή για Εγκληματολογική Έρευνα .....</b>	<b>549</b>
dd: Ένα Εργαλείο Αντιγραφής για Εγκληματολογική Έρευνα .....	550
dd: Ένα Εργαλείο Καθαρισμού Σκληρών Δίσκων .....	556
losetup: Μετασχηματισμός ενός Κανονικού Αρχείου σε μια Συσκευή στο Linux .....	557
Η Βελτιωμένη Συσκευή Loopback του Linux .....	559

vnode: Μετασχηματισμός ενός Κανονικού Αρχείου σε μια Συσκευή στο FreeBSD. ....	561
md5sum και MD5: Επικύρωση των Συλλεχθέντων Αποδεικτικών Στοιχείων .....	563
<b>22 Εργαλειοθήκες που Βοηθούν στην Ανάλυση για Εγκληματολογική Έρευνα .....</b>	<b>569</b>
Forensic Toolkit .....	570
EnCase .....	582
To Coroner's Toolkit .....	603
<b>23 Εργαλεία που Βοηθούν στην Ανακατασκευή της Δραστηριότητας στο Internet .....</b>	<b>617</b>
Outlook Express .....	618
Outlook .....	620
Netscape Navigator/Communicator .....	621
Πελάτης της America Online .....	626
Ταχυδρομικά Κουτιά Unix .....	630
IE History .....	631
<b>24 Γενικοί Επεξεργαστές και Προγράμματα Προβολής .....</b>	<b>643</b>
Η Εντολή File .....	644
Hexdump .....	645
Hexedit .....	649
Vi .....	653
Frhed .....	657
Xvi32 .....	660
Quickview Plus .....	662
Midnight Commander .....	666
<b>Παράρτημα Χρήσιμα Γραφήματα και Διαγράμματα .....</b>	<b>675</b>
Κεφαλίδες Πρωτοκόλλου .....	676
Κεφαλίδες Ethernet .....	676
Κεφαλίδες ARP (Address Resolution Protocol) .....	677
Κεφαλίδες IP (Internet Protocol) .....	677
Κεφαλίδες TCP (Transmission Control Protocol) .....	678
Κεφαλίδες UDP (User Datagram Protocol) .....	678
Κεφαλίδες ICMP (Internet Control Message Protocol) .....	678
Πίνακας ASCII .....	681
Ευρετήριο .....	687