מדריך אבטחת מידע והגנה מפני האקרים

דורון סיון

עריכה ועיצוב: **שרה עמיהוד, יצחק עמיהוד, מירי אלעני**

עיצוב עטיפה: **שרון רז**

שמות מסחריים
שמות המוצרים והשירותים המוזכרים בספר הינם שמות מסחריים רשומים של החברות שלהם. הוצאת הוד-עמי עשתה כמיטב יכולתה למסור מידע אודות השמות המסחריים המוזכרים בספר זה ולציין את שמות החברות, המוצרים והשירותים. שמות מסחריים רשומים (**registered trademarks**) המוזכרים בספר צוינו בהתאמה.

הודעה חשובה
בנוסף, קרא בעיון את המבוא לספר זה.
ספר זה מיועד לתת מידע אודות מוצרים שונים. נעשו מאמצים רבים לגרום לכך שהספר יהיה שלם ואמין ככל שניתן, אך אין משתמעת מכך אחריות כלשהי.
תוכן הספר וההפניות לספרים, לתוכנות, לאתרים ולמקורות מידע המוזכרים בו מסופקים "כמו שהם (**as is**)". השימוש בכל אלה הוא על אחריותו הבלעדית של המשתמש. הוצאת הוד-עמי והמחבר אינם אחראים כלפי יחיד או ארגון עבור כל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר, ובכלל זה (רשימה חלקית): הפרעה במתן שירות, אובדן מידע, אובדן זמן, אובדן רווח וכד'.
המשתמש רשאי להשתמש בתוכנות המוזכרות בספר ו/או לפנות לאתרים ו/או למקורות מידע אחרים על אחריותו. כל אלה הם בבעלות ובאחריות החברות המייצרות, משווקות ומציגות אותם. הוד-עמי והמחבר אינם גובים תשלום עבור השימוש בתוכנות ובמידע ממקורות אחרים המוזכרים בספר. הוד-עמי והמחבר אינם מספקים תמיכה בהתקנה ו/או ההפעלה של התוכנות ו/או בגישה לאתרים ומידע אחר. מחלקת התמיכה בהוצאת הוד-עמי תגיש עזרה רק עבור מקרים של אי בהירות של הסבר בספר או שיבוש דפוס. כל שאלה לגבי תוכנה ו/או אתר ו/או מקור מידע כלשהם יש להפנות אל מפתחי/יוצרי/משווקי התוכנה ו/או אל בעלי האתרים ו/או מקורות המידע.
הוצאת הוד-עמי והמחבר עשו כל מאמץ שתוכן הספר יהיה אמין ושלם. עם זאת, ההוצאה והמחבר אינם טוענים לאמינות ולשלמות של התכנים המוצגים בספר זה, ובמיוחד דוחים כל אחריות, ובכלל זה טענה להתאמה של הנאמר בספר למקרה ספציפי כלשהו. לא ניתן ליצור או להרחיב אחריות על ידי מידע שיווקי ו/או פרסומי כלשהו. ייתכן שההצעות ו/או ההמלצות הניתנות בספר לא יתאימו לכל מצב ומקרה. הספר משווק ונמכר תוך הבנה שההוצאה והמחבר אינם מספקים שירותים שונים הכרוכים בשימוש בספר, אלא לשם הבנת הכתוב ותיקון שיבושי לשון. לקבלת שירות מקצועי יש לפנות אל בעלי המקצוע בתחום. הן ההוצאה והן המחבר אינם אחראים לכל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר. אין בכוונת ההוצאה ו/או המחבר להמליץ או להעדיף תוכנה ו/או אתר ו/או מקור מידע כלשהם. רק המשתמש הוא שיחליט כיצד לנהוג על פי המוצג בספר. המשתמש צריך להיות ער לעובדה שאתרי האינטרנט הינם דינמיים ועלולים להיסגר, לשנות את התכנים שלהם וכד'. ההוצאה והמחבר אינם אחראים לשינויים אשר עלולים לחול באתרים המוזכרים בספר, ועל כן להיות שונים ממה שהוצג בספר.

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

© כל הזכויות שמורות הוצאת הוד-עמי לספרי מחשבים בע"מ

ת.ד. 6108 הרצליה 46160 טלפון: 09-9564716 פקס: 09-9571582 **info@hod-ami.co.il**

1-700-7000-44 www.**hod-ami**.co.il

אין להעתיק או לשדר בכל אמצעי שהוא ספר זה או קטעים ממנו בשום צורה ובשום אמצעי אלקטרוני או מכני, לרבות צילום והקלטה, אמצעי אחסון והפצת מידע, ללא אישור בכתב מאת ההוצאה, אלא לשם ציטוט קטעים קצרים בציון שם המקור.
All Rights Reserved

מס"ת ISBN 965-361-377-4

מדריך

אבטחת מידע
והגנה
מפני האקרים

דורון סיון

הספר מוקדש בחום ואהבה לאשתי
דליה
ולילדיי עופר, נעה ועמית

תוכן עניינים מקוצר

מבוא 19
פרק 1: תקשורת מחשבים 23
פרק 2: Hacking 79
פרק 3: NGX – Check Point Firewall 235
פרק 4: PIX – Cisco Firewall 285
פרק 5: ISA – Microsoft Firewall 323
פרק 6: גישות ומודלים בתחום אבטחת המידע 363

אינדקס 409

תוכן עניינים

מבוא 19
כיצד ניתן להתגונן בפני פריצה למחשב (Hacking)? 20

פרק 1: תקשורת מחשבים 23
מודל שבע השכבות 25
השכבה הפיסית 26
טופולוגיות פיסיות 26
Star 26
Mesh 26
ציוד תקשורת 27
ציוד לחיבור ברשת 27
ציוד לחיבור בין רשתות 27
חיווט 27
זוג שזור – TP (Twisted Pair) 28
סיב אופטי 28
תקשורת אלחוטית 29
רכזות – Access Point 29
עמדות 29
נתבים 30
שכבת עורק הנתונים – Data Link Layer 30
כתובת פיסית 31
שכבת הרשת 32
כתובות לוגיות – Logical Network Address 32
שיטות ניתוב 34
שכבת התעבורה – Transport Layer 37
שכבת השיח – Session Layer 41
שכבת התצוגה – Presentation Layer 41
שכבת היישום – Application Layer 42
סיכום מודל שבע השכבות 42
סקירת תשתיות Ethernet 44
מבנה המנה ב- Ethernet 44
רכזות 45
תקן 802.1X 46
רשתות מרחביות (WAN) 48
קו נל"ן (נקודה לנקודה) – Point to Point 48
ממסר מסגרת – Frame Relay 48
טכנולוגיות לחיבור משתמשים לאינטרנט 49
ADSL 49
טכנולוגיית כבלים 49
נתבים – Routers 49
נתבי ADSL 51
נתבי CISCO 52
User EXEC Mode 52
Privileged EXEC Mode 52
Global Configuration Mode 53
Interface Configuration Mode 53
Line Configuration Mode 53
Router Configuration Mode 54
כללי 54
עדכון נתבים 54
ניתוב דינמי 55
RIP 55
OSPF 55
ניתוב סטטי 55
שימוש ב-Sniffer 56

מודל Internet 58
פירוט היישומים במודל 59
שכבת היישום 59
הפרוטוקולים השייכים לשכבת היישום 59
השכבה Host to Host 60
השכבה Internet 61
שכבת הגישה לרשת 61
כתובות IP 62
Class A 62
Class B 62
Class C 63
מסכת תת-רשת (Subnet Mask) 64
Default Gateway 64
השימוש בכתובות פנימיות 64
IPSec 66
מהו Tunnel? 68
VPN 70
SSL 73
Simple Network Management Protocol – SNMP 74
הגדרת סוכן SNMP 74
מושגים ושרתים 75
IP Address 75
Subnet Mask 75
Default Gateway 75
DNS 76
HOSTS 76
WINS 77
DHCP 77
רשימת פקודות 77
PING 77
ARP 77
NETSTAT 78
NBTSTAT 78
IPCONFIG 78
TRACERT 78
ROUTE 78
NSLOOKUP 78

פרק 2: Hacking 79
בעיות הקשורות לשכבה הפיסית 80
בעיות הקשורות לשכבת עורק הנתונים 84
התקפות בנושא Switch 92
בעיות הקשורות לשכבת הרשת 97
Hacking מול נתבי Cisco ומנגנון SNMP 100
סניפרים (Sniffers) 102
בעיות הקשורות לשכבת התעבורה 107
SNMP 113
בעיות אבטחה הקשורות לשכבות 5-7 של מודל השכבות 118
סיסמאות 118
תוכנות לפריצת סיסמאות 119
פריצת סיסמאות של קבצים 126
הצפנות ברשת 127
סיכום מודל השכבות 130
איסוף מידע על הארגון 130
טיפים 140
איסוף מידע ופגיעה ברמת רשת 142
כלי איתור של עמדות ושירותים 143
כלים לפגיעה בשירותים 143
Hacking על מערכות הפעלה 145
Windows 145
סיכום ודרכי התגוננות 151
Linux 152
סיכום ודרכי התגוננות 156
Services 157
דרכי פגיעה בשרתי Windows ואופן התגוננות 157

דרכי פגיעה ודרכי הגנה על שרת DNS 158
הכרטיסייה Forwarders 163
הכרטיסייה Advanced 164
הכרטיסייה Root Hints 165
הכרטיסייה Security 166
היכן כדאי למקם שרת DNS? 167
שילוב בין שרת DNS לבין שרת DHCP 169
שרת IIS 171
הכרטיסייה Web Site 171
הכרטיסייה Directory Security 172
Authentication and access control 172
IP address and domain name restrictions 173
Secure communications 173
הכרטיסייה Home Directory 175
בקר domain 176
הקשחת שרתים 180
הקשחת שרת Windows 2000/2003 180
הקשחת שרת SQL 180
הקשחת שרת IIS 181
הקשחת עמדות Windows 95/98 182
הקשחה בעזרת האשף שמגיע ב- Service pack לשרתי Windows 2003 182
נקודות למחשבה בשרת דואר Exchange 184
ניצול פרצות בתוכנה 186
הקדשת תשומת לב ל-Process 191
וירוסים ותוכנות ריגול (Spy) 193
מהם וירוסים? 193
הנזק הנגרם למחשב 194
התמודדות עם וירוסים 194
התמודדות עם וירוסים חמקנים 195
התמודדות בפני פריצות למחשב ותוכנות Spy 196
תוכנות Spy 202
דוגמאות לשימוש בתוכנות סמויות 204
מציאת הקשר בין יישומים שרצים במחשב לבין פורטים פתוחים 208
הגדרות אבטחה ב- Internet Explorer 209
הכרטיסייה התקשרויות 209
הכרטיסייה מתקדם 211
הכרטיסייה תוכן 212
הכרטיסייה כללי 212
הכרטיסייה אבטחה 213
הצפנה 214
פרטיות 215
שלמות 216
פונקציית ערבול (hash) 216
נוהל עבודה של אלגוריתם RSA 217
אימות 219
ניהול מפתחות מרכזי במערכת אסימטרית 220
נוהל עבודה עם אלגוריתם סימטרי 220
שימוש משולב בשתי הטכנולוגיות 221
סוגי התקפות 222
סיסמאות 223
טיפים 224
אימות באתרי אינטרנט 226
מהו הסיכון שבשימוש בתוכנות שיתופיות ברשת? 230
SQL Injection 231
לימוד המערכת 231
שלב המטרות 232

פרק 3: NGX – Check Point Firewall 235

נוהל בדיקת מנה (Packet) 236
דור ראשון – Packet Filter 237
דור שני – Proxy Gateway 238
דור שלישי – Stateful Inspection 239
מבנה המערכת 241
Single Gateway Product 241
Enterprise Management Product 241

התקנה של המערכת בלינוקס 242
התקנה ב-Windows 244
הכרת תפריטי הניהול 245
Network Objects 245
Services 246
Resources 246
Servers and OPSEC Application 246
Users and Administrators 247
VPN Communities 247
יצירת Rules (חוקים) 247
זמני פעולה 251
מעקב 252
קביעת אובייקטים 252
יצירת אובייקט שייצג רשת 253
יצירת אובייקט שייצג שרת 254
הגדרת אובייקט שייצג Firewall 254
2 חוקי החובה ואופן התקנת ה-Rules 256
חוקי החובה 256
בדיקה והתקנה 258
ניהול מעקב ובקרה 259
LOG 260
Check point configuration 261
License 262
ניהול הגדרות המערכת 263
NAT – תרגום כתובת IP פנימית לכתובת חיצונית 264
כיצד להגדיר זאת? 265
שילוב עם Active Directory 267
הגנה על תוכן 270
SmartDefense 270
Web Intelligence 272
OPSEC 273
סינון על סמך קובץ שיוצרים מראש 276
חיבור VPN 277
Remote-access VPNs 277
נוהל ההגדרה 278
Intranet VPNs 280

פרק 4: PIX – Cisco Firewall 285
מאפיינים עיקריים של PIX 286
משפחת המוצרים של PIX 287
נוהל עבודה והגדרות 288
פקודות כלליות 288
ASA 289
מתאמים 290
פקודות לאפשור התעבורה 291
הגדרות שעה ועבודה מול Syslog Server 292
עבודה מול Syslog Server 293
פקודות Show 294
שימוש ב-NAT וב-PAT 295
שימוש ב-ACL (Access List) 296
VPN 298
חסימת ניסיונות לביצוע Ping 299
קבוצות 299
חסימת תוכן 301
Java Applet and ActiveX 301
סינון וחסימת URL 302
Stateful Inspection 302
פקודת fixup 303
הגנה על שרת FTP 303
הגנה על שרת הדואר 304
הגנה מפני תקיפות של פיצול Packet (מנה) 305
הגנה מפני תקיפות, Syn Attack 305
IDS (Intruder Detection) 306
יכולותיו הייחודיות של PIX 309
תמיכה ב-VLAN 309

תמיכה בניתוב 310
ניתוב סטטי 310
ניתוב דינמי 311
מחיקת סיסמת Enable 312
חיבור VPN 313
הגדרות VPN בצד של PIX 314
חיבור VPN בצד של לקוח 316
ניהול גרפי של המערכת 318

פרק 5: ISA – Microsoft Firewall 323

אופן השימוש ב-ISA 324
נקודת הקישור בין הארגון לבין האינטרנט 324
נקודת הקישור בין סניפים 326
התקנת המערכת 326
מהלך ההתקנה 326
ומה לאחר ההתקנה? 327
סוגי לקוחות 328
פתרון אבטחה כולל 329
גישה מרוחקת ל-ISA וגיבויים 331
אפשור גישה מרוחקת 331
גיבויים ותחזוקה 332
יצירת Rules והגדרות 332
הגדרת Access Rules 334
פירוט סדר הפעולות 335
אופן בקרה על זרימת המידע ב-Firewall 342
כיצד פועלת מערכת IDS ב-ISA? 344
מערכת המעקב אוספת מידע לפי פירוט זה 344
בקרה ברמת שכבה שלישית (IP) ורביעית (TCP, UDP) 344
בקרה ברמת היישום 345
System Policy 346
גישה מבחוץ לאתרים פנימיים 348
שרת הדואר Exchange 351
סינון ואבטחה לשירות HTTP 353
אישור או מניעת תנועה לפי החתימה Signature 355
VPN 357
סוגי החיבור ב-VPN 358
ניטור ובקרה 361

פרק 6: גישות ומודלים בתחום אבטחת המידע 363

כלל ראשון – נסה לחשוב כהאקר 367
דברים שניתן לעשות ברמת הרשת 367
דברים שניתן לעשות ברמת Host 367
פגיעה ברמת היישום 368
כלל שני – היערך בהתאם 368
הגנה על יישומים 368
הגנה על Host 369
הגנה ברמת הרשת 370
כיצד ליצור אבטחה ברמת יישום 372
Threat Model 372
מודל Stride 374
מהם הכלים שישמשו אותנו להערכת הסיכונים 374
כלים טכנולוגיים לאבטחת מידע מאוחסן ומידע שעובר ברשת 376
כלים טכנולוגיים לאבטחה בעת העברת מידע 376
דרכי התמודדות מול Hacking ברמת יישום 377
Cross-site scripting 377
Buffer Overflow 379
SQL injection 382
דרכים לטיפול בבעיות אבטחה ביישומים 383
אבטחה מומלצת עבור Intranet 386
Integrity 387
Authentication 387
Authorization 387
טיפים 387
אבטחה מומלצת עבור Extranet 387
אבטחה מומלצת עבור Internet 389
תכנון מבנה רשת שכוללת שרתי דואר, WEB ואנטי וירוס 390

ריכוז שיטות פריצה (Hacking) וכלי הגנה, בהתאם למודל 7 השכבות 392
אתרים חשובים 393
פעולות במקרה של פריצה או פגיעה במידע 396
בדיקות שיש לעשות כאשר יש חשש לחדירה לארגון 396
בדיקות בעזרת מוצרים קיימים 397
MBSA 397
GRC 401
פגיעה במידע עקב וירוסים או נזק ממקור חיצוני דוגמת שריפה 402
גניבת מידע פנים ארגוני על ידי עובד מתוסכל 402
קריסת שרתים, שירותים או קווי תקשורת
באופן שמונע את המשך הפעילות 404
מודלים ונהלים בתחום אבטחת מידע 405
תקן ISO17799 405

אינדקס 409

פרק 2

Hacking

פרק זה ממוקם לאחר פרק רשתות התקשורת ולפני לימוד Firewall ולא בכדי. יש להכיר היטב את נושא רשתות התקשורת כדי להבין פרק זה במלואו, שכן בפרק זה ניכנס לנעליו של האקר ונלמד על דרכי פעולתו תוך שימוש במושגים מפרק רשתות התקשורת.

כדי להבין לעומק את דרכי התקיפה של ההאקר, נכיר בפרק זה כלי Hacking שונים. ללא היכרות זו לא תוכל לטפל כראוי בתקיפות של האקרים. זו אינה קלישאה, אנשי IT המנסים להתמודד עם האקרים בעזרת כלים של אנשי IT בלבד, וללא הקצאת זמן הולם למטרה – מתקשים לעמוד במשימות ההגנה. מטרת פרק זה אינה להפוך אותך להאקר, אלא להציג בפניך שלל כלים המשמשים האקרים כדי שתהיה מודע לכך שבסבירות גבוהה מאוד אינך מוגן כנדרש. בהמשך יוצגו בפניך מגוון כלים של האקרים, כולל הדגמות והפניות ספציפיות, וזאת כדי לגרום לך לנסות ולחשוב אחרת בנושא אבטחת המידע.

בוודאי כבר למדת על מודל שבע השכבות. המודל מתחיל מהשכבה הפיסית ומגיע עד שכבת היישום. גם כאן נעסוק בנושא האקינג לפי מודל זה. תחילה נסקור בעיות אבטחה ברמה הפיסית דוגמת השראות. נמשיך לשכבה השנייה בה נכיר התקפות בנושא כתובות MAC והאקינג על Switch. בשכבה השלישית נכיר את הנתב וההתקפות עליו, כולל סריקת כתובות IP כמובן. בשכבה הרביעית נכיר התקפות מבוססות TCP, ולסיום נכיר התקפות ברמת סיסמאות, גניבת מפתחות הצפנה וניצול Buffer Overflow ביישומים (אפליקציות).

כלל ידוע הוא שכדי להתגונן היטב חובה להכיר את כלי התקיפה. בהמשך הפרק אציג את כלי התקיפה בפירוט רב. רק זכור שהמטרה היא ללמוד להתגונן. כמו כן עליך לשנן את הנקודה החשובה הבאה: רק כשליש מניסיונות התקיפה מגיעים מבחוץ. רוב ניסיונות התקיפה הם פנים ארגוניים, כלומר על ידי עובדים של הארגון או מי שמורשים להיכנס למחשבים של הארגון. התעלמות מנקודה חשובה זו גורמת לך לבנות חומות הגנה לא יעילות.

בפרק זה נתמקד בפעולות התקיפה של ההאקר. בפרקים שעוסקים ב- Firewalls נלמד כיצד הם מסייעים לך בהתמודדות עם תקיפות, ובפרק הסיכום נלמד כיצד להיערך ברמה הארגונית לתקיפות פנים וחוץ ארגוניות.

בעיות הקשורות לשכבה הפיסית

כיוון שהשכבה הפיסית עוסקת בתשתיות, נתמודד בפרק זה עם תשתית לא מאובטחת, כגון חוטי נחושת ותקשורת אלחוטית.

לגבי חוטי נחושת, מכיוון שזרם חשמלי העובר בקו נחושת יוצר שדה מגנטי סביבו, ניתן לחבר ציוד מתוחכם בקרבת הכבל שיפענח את האותות העוברים, בזכות ההשראה הנוצרת סביב הכבל.

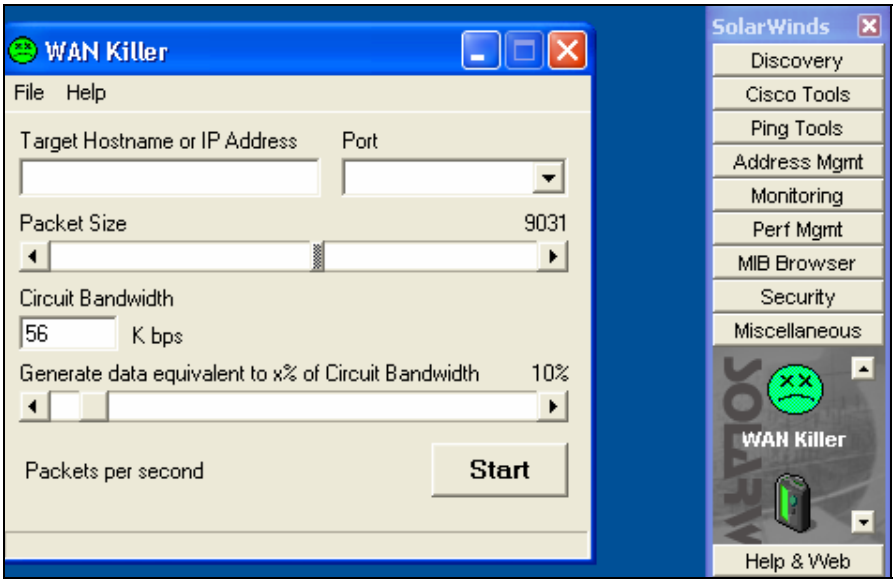
לספקנים מביניכם – חשבתם פעם מדוע מהירות המחשב אינה זהה בכל? מדוע המעבד כה מהיר אך מעבר המידע בלוח האם ובכרטיסים איטי בהרבה? לא ניתן לשדר בתדרים כה גבוהים דרך חוטי נחושת מכיוון שעקב ההשראה הגבוהה חוטי הנחושת

יפריעו אחד לשני. אותה השראה משמשת גם את אלה המעוניינים להאזין למידע, לכן במקומות מאובטחים משתמשים בסיבים אופטיים. לסיב זה אין השראה, כיוון שהמעבר הוא של קרני אור ולא של אותות חשמליים. בנוסף, לא ניתן לנתקו ולחבר אלמנט נוסף מבלי שזה יורגש מייד.

כמובן שאין טוב בלי רע, ומחיר התקנת סיב אופטי עשוי להרתיע אותך. שקול התקנה של הסיב בין מקומות אסטרטגיים.

תקשורת אלחוטית והטיפול בה, אלה נושאים מורכבים יותר. הוזלת המחירים ביחד עם שיפור עוצמת השידור, העלתה את שכיחות השימוש בה. עם זאת, מנהלי הרשת עדיין חוששים בצדק מהרעיון שאנטנה מרכזית משדרת לסביבה, וכל מי שנמצא בתחום יכול עקרונית לנסות ולהתחבר אליה.

תופתע לגלות כמה פשוט וקל לגרום לנזק משמעותי ברמת התשתית. לדוגמה, התוכנה הבאה גורמת לעומס ברמת WAN על ידי יצירת תעבורה רבה. לאחר שמקלידים את כתובת היעד והפורט המבוקשים, ואת גודל המנה (Packet) אשר תופנה ליעד, ניתן לקבוע בחלק התחתון של המסך איזה יחס מרוחב הפס של הרשת אתה מעוניין שהתוכנה תתפוס.



קיימים התקנים שמחוברים בשקע של המחשב ונמצאים בין הכבל שמגיע לשרת לבין השקע במחשב. במצב זה כל התעבורה דרך ההתקנים האלה משודרת באופן אלחוטי לסביבה הקרובה וניתן להאזין לה.

בעיה נוספת שקשורה במיוחד לשימוש ברשת אלחוטית, היא יכולת האזנה קלה גם בדרך שונה מזו שהוזכרה למעלה, והדברים ידועים ומוכרים. היתרון של שימוש ברשת אלחוטית גורר עימו כמובן בעיות לא מעטות כשהחמורה שבהן נעוצה בעובדה שכל מי שנמצא בטווח של המשדר מסוגל לקרוא נתונים ואף לשלוח מידע דרכה. מספר תוכנות שמסייעות במיוחד לביצוע **Sniffer** ברשת אלחוטית, הן:

- Kismet (למערכת הפעלה לינוקס).
- Airsnort (למערכת הפעלה לינוקס).
- Netstumbler (למערכת הפעלה Windows). התוכנה תסייע באיתור רכזות באזורך, AP (Access Point).
- Wildpacket airopeek (למערכת הפעלה Windows). התוכנה תסייע באיתור עמדות ברשת שגילית.
- וכמובן LANguard scanner for WLAN (למערכת הפעלה Windows). התוכנה תעניק לך את יכולת הסריקה ברשת.

- לפני שנתקדם, נסקור מספר מושגים בסיסיים:
- MAC Address – הכתובת הפיסית של כרטיס הרשת שלך.
- SSID(Service Set IDentifier), מספר שמייצג את שם הרשת האלחוטית.

כצעד ראשון יש לנסות וללכוד את הרשתות שבסביבה. מומלץ להשתמש בכרטיס אלחוטי המצויד באנטנה חזקה שניתן לרכוש באינטרנט, כך תגדיל את שטח הכיסוי. כעת הפעל את תוכנת Netstumbler. התוכנה תוכל לבחור סריקה של SSID וכל מה שיימצא בטווח יופיע לפניך, כולל כתובת MAC של הרכזת. כל שנותר כעת הוא להשתמש ב-Sniffer אלחוטי דוגמת Kismet, ומכיוון שאתה יודע את כתובת ה-MAC של הרכזת, ניתן לבצע סינון לפי הנדרש מכל ה-Frames שנלכדו.

האקר יכול שלא להסתפק בכך ובעזרת תוכנה דוגמת ESSID-jack הוא יכול לגרום לעמדה שלך לחשוב שהוא הנתב. לאחר שההאקר יתקין שני כרטיסי רשת, כל התעבורה שלך תעבור למעשה דרכו. הוא גם יכול להשתמש ב-LANguard (השימוש בה יודגם בהמשך) ולראות את השירותים הפעילים והשיתופיים שלך. אם האקר מעוניין לפגוע בך ולגרום לקריסת המערכת שלך, הוא יתחיל להפציץ את הרשת בעזרת תוכנות שמייצרות מנות (Packets), דוגמת Gspoog או LANforge. כתוצאה, הרשת שלך תהפוך לאיטית יותר ויותר עד שתקרוס.

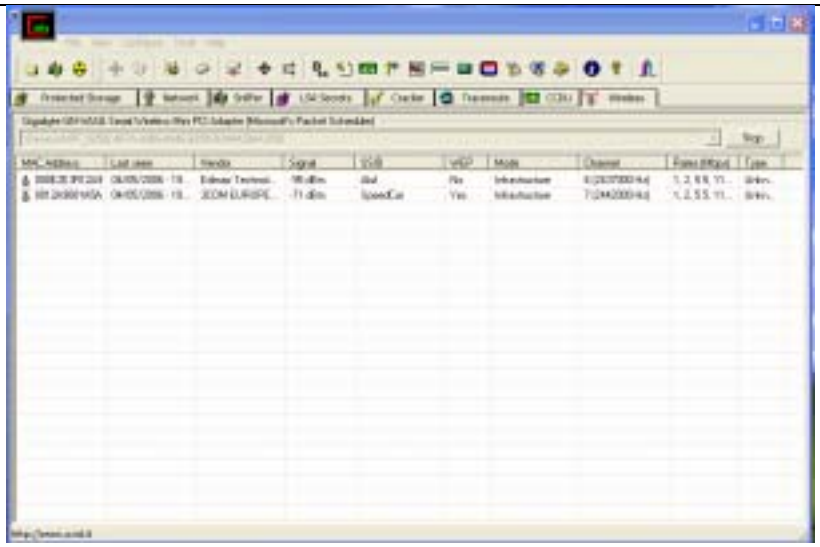
שימוש במערכת מוצפנת דוגמת WEP (Wired Equivalent Privacy), לא יעזור בהרבה, כי המערכת מעניקה הגנה למספר שעות בלבד. WEP עובדת אמנם בסיסמה סימטרית חזקה בשם RC4, אולם לתוכנות שמייצרות מנות יש מנגנון שחוזר על עצמו מדי 224=16M מנות. לכן ההאקר יתחבר לרשת שלך ויתחיל ליזום תעבורה, במקביל לשימוש בכלי פריצה דוגמת Airsnorts או WEBcrack. כדי להתגבר על הבעיה פותח תקן אבטחה בשם WPA (Wi-Fi Protected Access) שפותר את בעיות האבטחה של WEP ובין השאר דואג לייצור בתדירות גבוהה של מפתח ההצפנה. הדבר מקשה על ההאקר את הפריצה, מכיוון שהוא מתקשה לחלץ את הקוד בפרק זמן קצר מאוד. עם זאת, במערכת גדולה ייתכן חוסר תיאום בתקנים שיפורטו להלן, והדבר עלול להקל על ההאקר.

התקנים הנפוצים לעניין זה, לדוגמה: שילוב של 802.11 הישן שעובד עם WEP יחד עם כרטיסים בתמיכת 802.1x שתומכים ב-WPA, וגם בכרטיסים חדשים דוגמת 802.11i שתומכים ב-AES (Advanced Encryption Standard) ומהווים שיפור משמעותי באבטחה. יש שילובים שעלולים להוריד את רמת האבטחה ולהקל על ההאקר.

כללי עזר מקובלים:

1. הקפד על רמה אחידה של תקנים ברמה הגבוהה ביותר.
2. הקפד לבצע מדי זמן מה בעצמך Sniffer כדי לראות אם יש פעולה חריגה.
3. נסה להיכנס לנעליו של האקר: בעזרת מחשב נייד והתוכנות שצוינו, צא מהבניין, נסה לאתר את הרשת שלך ובדוק האם אתה יכול להזיק לעצמך. לפי התוצאות תדע מהי רמת המוכנות שלך.
4. שנה את הגדרות ברירת המחדל של סיסמת המפקח ברכזת, שם הרכזת וה-SSID.
5. אל תאפשר ביצוע SSID Broadcasting לרכזת (אל תאפשר זאת דרך הגדרות הנתב). זכור, הנתב משמש גם כרכזת והוא נקרא גם **AP** (Access Point). אם אינך יודע כיצד לבצע זאת, בצע את הפעולות הבאות: לאחר שהתחברת לרשת, גש לשורת הפקודה והרץ ipconfig. הכתובת של הנתב היא כתובת AP. כל שנותר הוא לגלוש לכתובת זו ולשנות הגדרות.

   במסך הבא הרצתי Sniffer אלחוטי בעזרת Cain, ומצאתי רשתות שפועלות באזור. ייתכן שרשתות אלה מאובטחות כנדרש, אך מדוע לפרסם אותם בכלל אם מדובר בארגון קטן? מומלץ שכל משתמש יגדיר ידנית בהגדרות החיבור SSID.



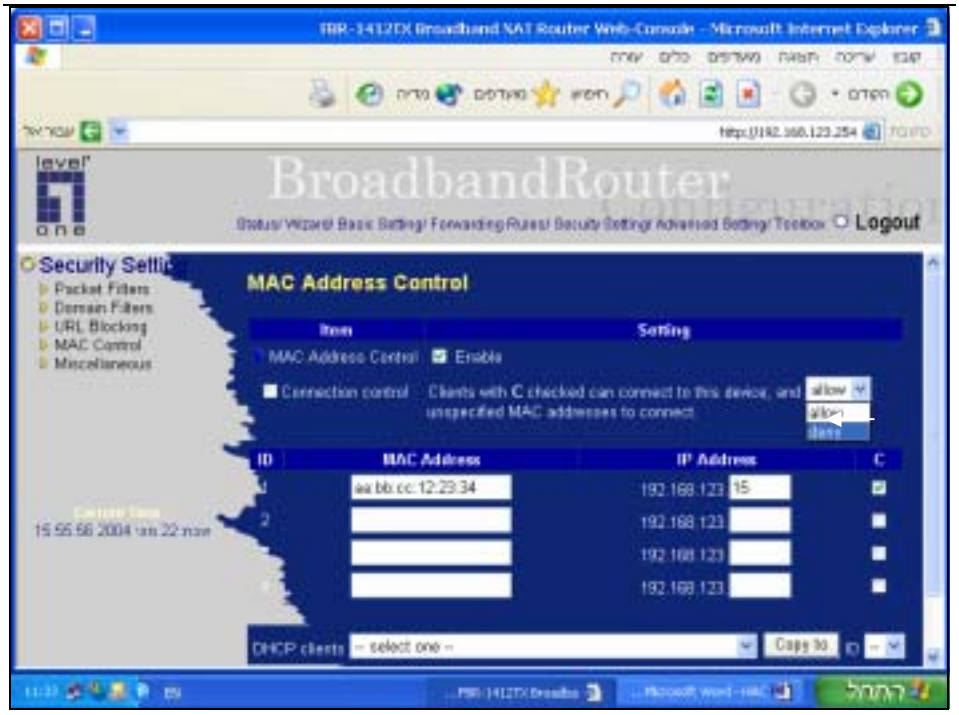
6. כדאי להתקין את עדכוני התוכנה והאבטחה של החברה, הדבר מומלץ באופן כללי ובמיוחד בהתמודדות עם האקרים. יש להקפיד על התקנת Patch (תיקוני תוכנה) בכל מערכות ההפעלה בארגון, ובדרך כלל ניתן להתקין מנגנון אוטומטי שיבצע זאת.
7. אם אינך משתמש ב-SNMP, בטל את פעולתו, מכיוון שניתן למשוך דרכו מידע רב ואף לשנות הגדרות. בדוגמה הבאה ניתן לראות כיצד אפילו תוכנות דוגמת LANguard יודעות לאסוף מידע על מערכת מרוחקת בעזרת SNMP.

SNMP info (system)
sysDescr - Microsoft Windows CE Version 5.0 (Build 1400)
sysUpTime - 7 hours, 40 minutes, 38 seconds
sysContact - Your System Contact Here
sysName - TC11
sysLocation - Your Location Here
Object_ID - 1.3.6.1.4.1.311.1.1.3.3 (Microsoft Windows CE Version 3.0 (Multiple Other Devices too))
Vendor - Microsoft

תוכנות אחרות דוגמת Getif יעשו שימוש באמור בסעיף 7 לעיל ביחס ל-SNMP וינסו לשנות הגדרות (נושא SNMP יוסבר בהמשך בפירוט).

בעיות הקשורות לשכבת עורק הנתונים

השכבה השנייה קשורה לנושא הכתובות הפיסיות (MAC Address). ההתקן המוכר שעושה שימוש בכתובות אלו הוא ה-Switch. מטבע הדברים **סעיף זה יעסוק בשינוי כתובת MAC תוך כדי התחזות לאחר, בפריצה לרכזת ובשינוי הגדרות**.



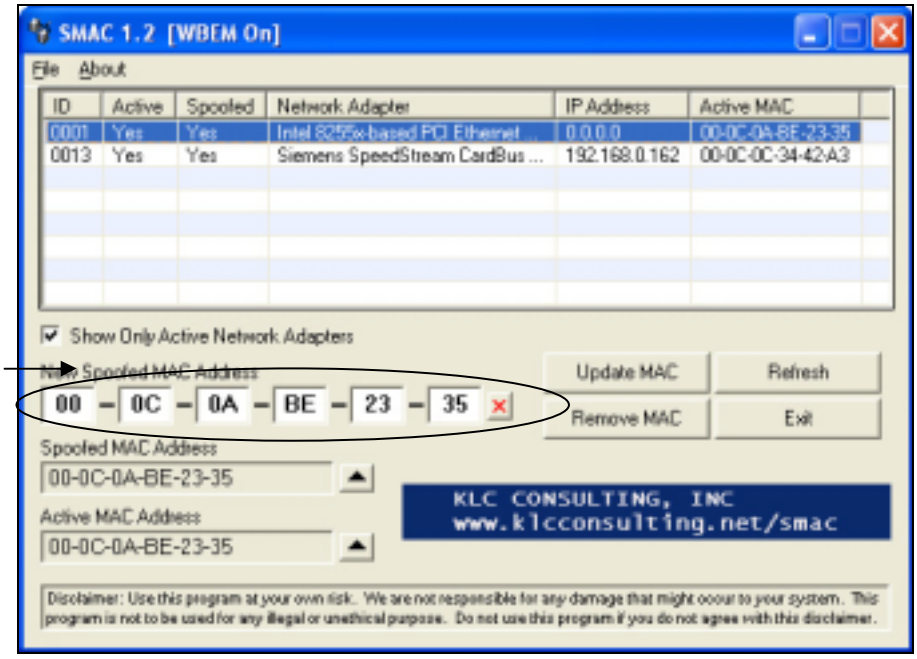
אפשור חיבור לנתב עבור כתובת MAC ספציפית

כאשר אתה רוכש רכזת אלחוטית, כברירת מחדל היא מאפשרת לכל העמדות להתחבר אליה. ניתן באופן די פשוט להיכנס לתפריט הרכזת (או הנתב האלחוטי) ולציין את הכתובות הפיסיות שיכולות להתחבר לרכזת. כדאי לציין בנתב האלחוטי את כתובות ה-MAC המורשות להשתמש ברשת, כדי למנוע מלא מורשים להשתמש ברשת.

בדוגמה זו אני גולש לנתב, בוחר מהתפריט את MAC Control ומכאן מגיע למספר אפשרויות בהתאם לנתב. לדוגמה בחרתי כאן לאשר התחברות לכתובת שצוינה בלבד.

אולם כפי שתראה בדוגמה הבאה, הבעיה היא שניתן לשנות את כתובת ה-MAC בקלות דרך שורת הפקודה. לכן האקר שלכד מנה יודע מהי כתובת ה-MAC ויכול לשנות את כתובתו בזו שלך.

שינוי כתובת ה-MAC ב-Windows: בעזרת תוכנת SMAC מהאתר www.klcconsulting.net, ניתן לקבוע כתובת MAC של כרטיס (מערכת ההפעלה ושאר העמדות ברשת יחשבו שהכתובת השתנתה אך למעשה השינוי אינו אמיתי).



בדוגמה רואים כיצד ניתן לבחור בכתובת MAC רצויה.

שינוי כתובת MAC בלינוקס: הראיתי כיצד ניתן בקלות לשנות את כתובת ה-MAC שלך עבור Windows. בעמדות לינוקס הדבר פשוט יותר וניתן לביצוע בפקודה אחת. המבנה הוא ifconfig eth0 hw ether 11:22:33:44:55:66, כאשר eth0 הוא מספר מתאם Ethernet הראשון, והמספר שרשום שם נתון כמובן לשיקולך (המילים hw ether מייצגות כתובת חומרה של Ethernet ועליך לרשום אותן כי זה מבנה הפקודה). לפני ביצוע הפעולה יש לבצע הורדה של הכרטיס (שקול ל-Disable ב-Windows) בעזרת הפקודה ifconfig eth0 down. לאחר ביצוע הפקודה של שינוי כתובת MAC, העלה את הכרטיס חזרה בעזרת ifconfig eth0 up.

במסך הבא הרצתי את הפקודה ifconfig כדי לראות את כתובת ה-IP ואת כתובת ה-MAC.

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:BD:C4:3C
          inet addr:192.168.2.190  Bcast:192.168.3.255  Mask:255.255.252.0
          inet6 addr: fe80::2d0:b7ff:febd:c43c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:347358 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3748 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:78825242 (75.1 MiB)  TX bytes:395860 (386.5 KiB)
```

כעת אני מריץ את הפקודה כדי לשנות את כתובת ה-MAC ל- AA:BB:CC:DD:EE:FF

```
[root@localhost ~]# ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF
```

כעת כל שנותר הוא לבדוק את הכתובת החדשה:

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr AA:BB:CC:DD:EE:FF
          inet addr:192.168.2.190  Bcast:192.168.3.255  Mask:255.255.252.0
          inet6 addr: fe80::2d0:b7ff:febd:c43c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:440795 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3774 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:115032999 (109.7 MiB)  TX bytes:400060 (390.6 KiB)
```

ואכן כתובת ה-MAC שונתה.

הערה!

ראוי לציין שההאקר לא צריך להתאמץ כל כך. רוב הנתבים מגיעים עם סיסמת admin (באתר החברה בדרך כלל רשום מהי סיסמת המפקח כברירת מחדל), ומכיוון שסביר שלא שינית את הסיסמה, הוא פשוט יגלוש לנתב שלך, ייכנס להגדרות ויוסיף את עצמו.

אם כן, כיצד משנים את כתובת ה-MAC ומהן הפעולות שניתן לבצע בעקבות שינוי זה?

כפי שוודאי אתה זוכר, השכבה השנייה עוסקת במעבר נתונים בתוך הרשת. כאן כבר לא עוסקים ברמת אותות חשמליים אלא ברמת **Frame** (מסגרת שבה נמצאים המידע, הכותרת והבקרה). Hacking ברמת שכבה שנייה מתמקד במידע הנמצא בכותרת. הוא לא עוסק בגניבת המידע עצמו אלא בפענוח המידע שבכותרת, זאת מכיוון ששם רשומה הכתובת שלך והוא מעוניין להתחזות אליך. כדי להבין את הנושא, להלן תזכורת קלה מהפרק "תקשורת מחשבים".

כאשר עמדה פונה אל עמדה אחרת, מתבצעות שתי פעולות:

- חילוץ כתובת IP משם המחשב (באינטרנט וברשתות מבוססות LDAP, דוגמת Active Directory של Windows, משתמשים בשרת DNS) וברשת קטנה בשרת WINS.
- חילוץ כתובת MAC מכתובת IP.

העברת המידע בתוך הרשת מבוצעת על סמך כתובת MAC. כלומר אם אני רוצה לפנות למחשב של עופר לדוגמה, מערכת ההפעלה שלי תנסה לחלץ את כתובת ה-IP שלו (בעזרת שרת שמשמש לחילוץ שמות, או דרך Broadcast) ואז את כתובת ה-IP שלו היא תמיר לכתובת MAC.

כיצד המערכת ממירה כתובת IP לכתובת MAC? ובכן, הרעיון פשוט. המחשב שלי שולח הודעה ברשת, בכותרת תהיינה רשומות כתובות ה-IP של עופר ושלי וכתובת ה-MAC שלי בלבד. מכיוון שאיני יודע את כתובת ה-MAC של עופר, בשדה של כתובת ה-MAC של עופר יהיה רשום FF:FF:FF:FF:FF:FF שמשמעותו Broadcast. **כל** העמדות ברשת יאזינו ל-Frame (מסגרת הנתונים) ויבדקו אם היא עצמה היעד. אחת העמדות תבין שהיא היעד והיא תענה לעמדה הפונה. כעת מערכת ההפעלה שלי יודעת מהי כתובת ה-MAC שלה. למנגנון זה קוראים **ARP**. כדי שבפעם הבאה אני אפנה ישירות למחשב של עופר ללא Broadcast, מערכת ההפעלה שלי שומרת בזיכרון את כתובת ה-IP של עופר ואת כתובת ה-MAC שלו.

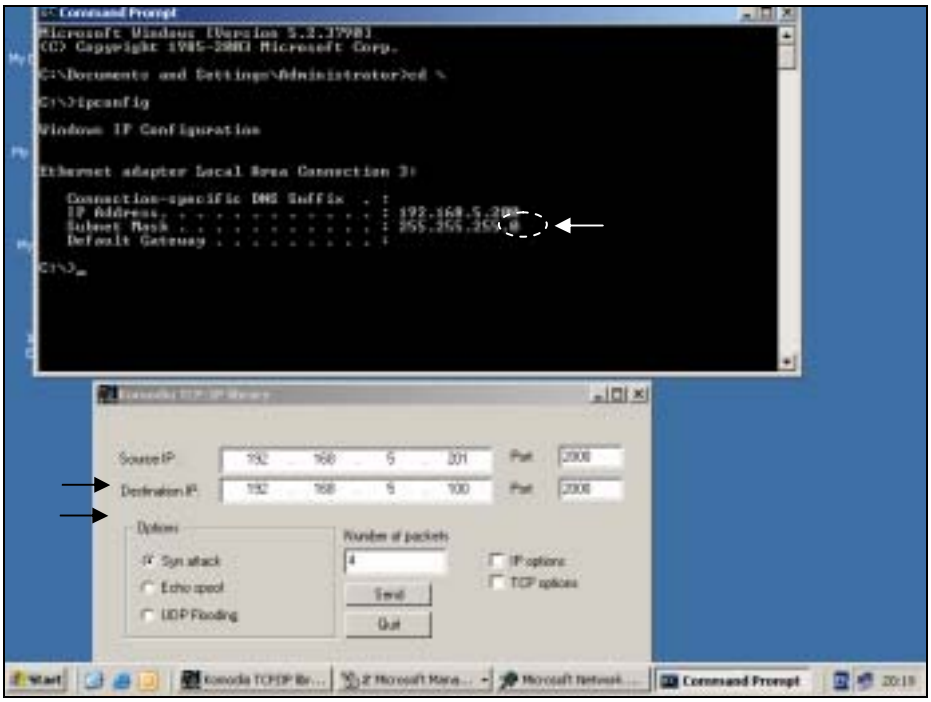
תוכל להיווכח בכך בעצמך על ידי הקלדת הפקודה (דרך שורת הפקודה) arp –g (הפקודה מציגה את הטבלה). עם זאת מדי מספר דקות (תלוי במערכת ההפעלה) המידע נמחק.

לכאורה הכל תקין. אולם הבעיה היא שנושא ARP שקוף למשתמש. זהו מנגנון שנועד לאפשר את העבודה מבלי שיהיה צורך לעדכן את המשתמש, והדבר עלול לגרור בעיות אבטחה קשות.

כדי להבין את אופן העבודה חובה להכיר מספר מושגים:

Sniffer – תוכנה שמשמשת ללכידת Frames העוברים ברשת. קיימות תוכנות רבות לכך, דוגמת netmon של Microsoft, Tcpdump, וגם תוכנות מתוחכמות דוגמת dsniff שמסוגלת להוציא משלל המסגרות את שמות המשתמשים והסיסמאות (נסה עם המתג dsniff –n).

Spoofing – שינוי כתובת המקור. זו נקודה חשובה, זכור שרוב תוכנות ההגנה מתייחסות לכתובת היעד ולא לכתובת המקור. דהיינו רוב תוכנות ההגנה בודקות האם הבקשה לגיטימית; האם הפורט אליו רוצים לפנות לגיטימי; האם מותר לקבל את המנה; האם המשתמש מוכר ומורשה. הן פחות מתייחסות לשאלה האם זהו באמת המשתמש האמיתי. לכן, על ידי שינוי כתובת המקור, ניתן להתחזות למשתמש אחר ולקבל שירותים שהיו מורשים לאותו משתמש. בדוגמה הבאה אני משתמש בתוכנת Komodia כדי להתחזות לכתובת IP אחרת.



שים לב, כתובת ה-IP שלי היא 192.168.5.200, אבל בעזרת תוכנת Spoofing אני מציג עצמי ככתובת 192.168.5.201 (בתמונה מסומן Syn Attack, בהקשר לדיון בפרק PIX, אך כאן יש לבחור Echo spoof). היעד לתקיפה הוא כמובן 192.168.5.100. לאחר שאלחץ Send תופיע בטבלת ARP של היעד כתובת ה-MAC שלי ולא של 192.168.5.201. הנקודה מוסברת מייד במושג הבא.

ARP cache poisoning – שיבוש טבלת ARP של משתמשים ושרתים, כך שכשיפנו למחשב מסוים, הם יגיעו למחשב אחר. נקודה זו חשובה ולכן אפרט יותר.

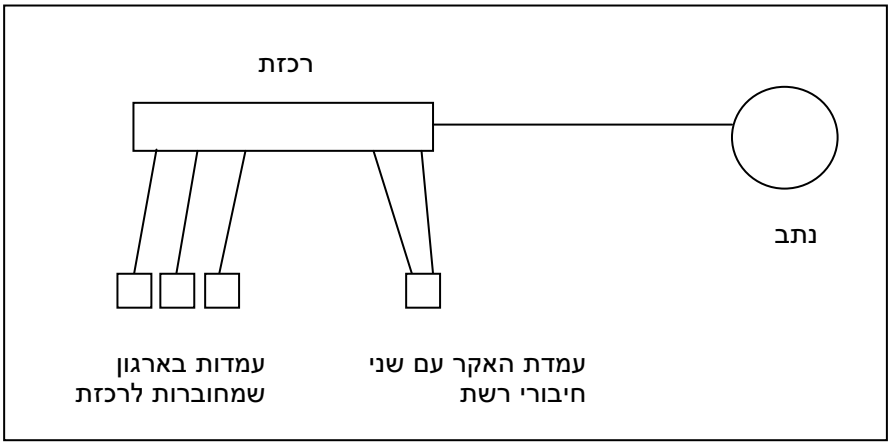
חשוב על כך, עופר פונה למחשב של נועה, כתוצאה מכך טבלת ARP של נועה תכיל את כתובת ה-IP ואת כתובת ה-MAC של עופר. כעת בעזרת תוכנת Spoofing פשוטה שניתן להוריד מהאינטרנט דוגמת Komodia שכבר הוצגה, אני מציין את כתובת ה-IP של עופר ומבצע Ping למחשב של נועה. המחשב שלה יראה שזו כתובת IP מוכרת וכתובת MAC שונה, יבין שזה כנראה רענון ויעדכן את הטבלה שלו. כעת כאשר נועה רוצה לשלוח מידע לעופר, המידע יגיע אלי, מכיוון שאצלה רשומה כתובת ה-IP של עופר וכתובת ה-MAC שלי ומה שקובע בתוך הרשת היא כתובת MAC.

זו רק ההתחלה, אני יכול לשלוח Broadcast ברשת. מכיוון שאני אפנה לכתובת חדשה ולא מוכרת לי, בשדה של כתובת IP (מקור) תהיה רשומה כתובת ה-IP של עופר ובשדה של כתובת MAC תהיה רשומה כתובת ה-MAC (מקור) שלי. כל העמדות יאזינו למידע ויעדכנו את כתובת ה-MAC שלהם, וכאשר ירצו לפנות לעופר – המידע יגיע אלי (אין כל קושי בבירור כתובת ה-IP של עופר: אני אפנה אליו דרך שכנים ברשת, ואז בפקודה arp –g אני אראה כתובת IP חדשה שהצטרפה לרשימה).

יהיו שיגידו "אצלי זה לא יקרה כי יש לי Switch". נכון אמנם ש-Switch יותר חכם מרכזת פשוטה (Hub) מכיוון שהוא מחבר ישירות בין מקור לבין יעד ולא תופס את כל הפורטים. אך זה לא המקרה במצב של Broadcast, כיוון שהרכזת אינה יודעת מיהו היעד ולכן המידע עובר בכל הפורטים. ההאקר יוכל בקלות לכתוב סקריפט שיבצע Ping, כדי לוודא שבכל המחשבים הטבלה תציג את כתובת ה-IP של עופר ואת כתובת ה-MAC שלי. חשוב שהסקריפט ירוץ כל דקה לערך, מכיוון שאם עופר יפנה למחשב של נועה הוא ידרוס מחדש את טבלת ה-ARP שלה ויכניס את הערכים הנכונים.

כעת מגיע תסריט יותר פשוט וחמור. אני מרכיב מחשב עם שתי כתובות IP (מומלץ עם שני כרטיסי רשת) ודרך מערכת ההפעלה מגדיר את המחשב כ-Router. לאחר הפעלת המחשב אני מקבל כמובן משרת DHCP כתובת IP, Subnet Mask וכתובת של הנתב. אם אבצע Ping לנתב אקבל מייד את כתובת ה-MAC שלו (בדוק בעזרת פקודת ARP). כעת אני שולח מנה (Packet) מסוג Broadcast, שמכילה את כתובת ה-IP של הנתב (Spoofing, לא לשכוח) ואת כתובת ה-MAC **שלי**, לכולם. המשמעות היא שכעת כל התעבורה מהארגון החוצה עוברת דרכי וממני לנתב. זכור, יש לי שני כרטיסים, אחד יזוהה כנתב על ידי העמדות והשני מחובר באופן רגיל לנתב. כך התעבורה מגיעה לכרטיס אחד, מתועדת וממשיכה החוצה דרך השני. פעולה זו נקראת **התקפת man in the middle** (המחשב שלי אמור לתפקד כנתב).

אל תהיה מופתע, נתב נחשב כעמדה רגילה. כאשר פונים לנתב כדי שיחבר אותנו ל-IP מרוחק אנו פונים אליו עם כתובת IP של היעד ועם כתובת MAC של הנתב הקרוב לעמדה. כתובת IP נשארת זהה לאורך כל הדרך ואילו כתובת MAC משתנה במעבר בין רשת לרשת. לכן ברגע שאצל כולם מופיעה כתובת ה-MAC שלי ככתובת הפיסית של הנתב, בכל פנייה לנתב, המסגרות למעשה מגיעות אלי.



לסיכום, ברשת TCP/IP תמיד מתמקדים בכתובת היעד, ושואלים האם היא מותרת ומה רצונה לבצע. לא בודקים את כתובת המקור ב-Frame. זהו מצב מסוכן, כי אם האקר דורס את טבלת ה-MAC שלך אתה עלול לשלוח מידע למחשב הלא נכון.

בתוכנה CainAbel שלפניך, ניתן לראות כיצד אני מבצע בקלות את הדריסה של טבלת MAC. יש לבחור כמובן את האפשרות השנייה Use Spoofed IP and MAC Addresses, ואז לבחור בכתובת IP רצויה ובכתובת MAC רצויה. רשום את כתובת ה-IP של הנתב ואת כתובת ה-MAC שלך. ודא שמסומנת למטה אפשרות Poison remote ARP cache every לפי הזמן הנוח לך. לאמיתו של דבר, מערכת Windows שומרת את המידע בטבלת ARP למשך חמש דקות, כך שאין טעם להפריז וליצור תעבורה מופרזת.

טיפ!

ביצוע ARP Spoofing יכול לגרום לקריסה של ה-Switch. במקרה כזה, ה-Switch עשוי לתפקד כ-Hub. משמעות הדבר שהתעבורה בין שתי עמדות עוברת למעשה בין כל העמדות, דבר שללא ספק נוח להאקר שכעת יכול בקלות ללכוד את כל המנות המועברות ברשת, בעזרת Sniffer.

הנחיות: כדאי למקם נתבים בין מחלקות במקום Switch; יש לוודא שאין נקודות רשת פנויות כדי שאף אחד לא יתחבר בשתי נקודות; ברר את כתובת ה-MAC של הנתבים ועקוב דרך Network Monitor אחר התעבורה; אם אתה חושד בשיבוש מערך הנתבים, כדאי שתבדוק זאת על ידי ביצוע הפקודה **Tracert** (שמציגה את רשימת הנתבים עד ליעד) לאתר הנמצא מחוץ לארגון.

בדוגמה הבאה ביצעתי Tracert לאתר באינטרנט. ניתן לראות את רשימת הנתבים מהרשת שלי ועד ליעד, ואת מספרם – במקרה זה עשרה (המספר האחרון מייצג את עמדת היעד ולא נתב, ולכן אין לספור אותו). המספר הראשון מייצג את כתובת ה-IP

של הנתב בארגון שלי. אם הייתי רואה שהמספר 10.10.10.80 מופיע במקום שני ברשימה, הייתי חושד שהותקפתי בדרך של שיבוש מערך הנתבים. במסך רואים גם שבפקודת Ping ערך TTL הוא 245. זאת מכיוון שערך ברירת המחדל הוא 255 וכל נתב בדרך מוריד מספר. מכיוון שהיו עשרה נתבים (עד רשת היעד), הערך ירד ל-245.

```
C:\>tracert www.walla.co.il

Tracing route to www.walla.co.il [192.118.82.140]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.10.10.80
  2    66 ms    58 ms    61 ms  212.29.206.54
  3    64 ms    61 ms    58 ms  212.29.206.62
  4    66 ms   208 ms    61 ms  212.150.73.50
  5    89 ms   254 ms   220 ms  212.25.109.253
  6    66 ms   257 ms   288 ms  hzq-219-188-2.dsl.bezeqint.net [62.219.188.2]
  7   132 ms   341 ms   195 ms  ras01.bezeqint.net [192.115.106.195]
  8    65 ms    67 ms    67 ms  hzq-25-85-18.cust.bezeqint.net [212.25.85.18]
  9    66 ms    65 ms    68 ms  192.118.68.13
 10    67 ms    67 ms    64 ms  192.168.11.2
 11    69 ms    69 ms    74 ms  192.118.82.140

Trace complete.

C:\>ping www.walla.co.il

Pinging www.walla.co.il [192.118.82.140] with 32 bytes of data:

Reply from 192.118.82.140: bytes=32 time=72ms TTL=245
Reply from 192.118.82.140: bytes=32 time=64ms TTL=245
Reply from 192.118.82.140: bytes=32 time=70ms TTL=245
Reply from 192.118.82.140: bytes=32 time=60ms TTL=245

Ping statistics for 192.118.82.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 72ms, Average = 66ms
```

התקפות בנושא Switch

כל העמדות והשרתים בארגון מחוברים ביניהם והחוצה דרך רכזת. מסיבה זו רכזת היא יעד לגיטימי לניסיונות פריצה, וחובה על מנהל הרשת לדעת לבצע מספר פעולות שיחסמו ניסיונות חדירה פשוטים. סעיף זה מיועד לבעלי ידע ברכזות הניתנות לניהול. הפקודות שמצוינות כאן מתייחסות לרכזות של Cisco.

קצת רענון – ברכזות מתוחכמות ניתן לשלוט על כל פורט ופורט (יציאות הרכזת) ולציין מי יכול להתחבר אליהם. כמו כן ניתן לאגד מספר פורטים לקבוצה שנקראת VLAN. מנהל התשתיות יכול להחליט האם חברים ב-VLAN2 יוכלו להגיע למחשבים ב-VLAN3 למשל. לרכזות אלו מוקצית כתובת IP וכך מנהלים אותן. ברכזות הפופולריות דוגמת Cisco Catalyst 2950 מגדירים את כתובת ה-IP לרכזת על ידי שיוכה למתאם לוגי שנקרא VLAN1.

כאשר פונים לרכזת דרך חיבור "היפר מסוף" מגיעים למסך שממנו לא ניתן לבצע הגדרות. לשם כך יש להקליד את הפקודה enable ואז להזדהות בסיסמה. לאחר מכן יש להקליד configure terminal ואז מגיעים למסך של הגדרות כלליות לכל הרכזת. הסמן ישתנה ל- Switch(config) כאשר המילה Switch תוחלף בשם הרכזת שלך. אם אתה רוצה להגדיר פורט ספציפי ברכזת, היכנס אליו בעזרת הפקודה Interface ומספר הפורט. לדוגמה:

Switch(config)interface fastethernet 0/2

הספרה 2 מייצגת את מספר הפורט. אם יש רק שורת פורטים אחת אזי כולה מתייחסת לספרה 0. בפועל רושמים בקיצור:

Int fa0/2

כעת ישתנה הסמן ל-

Switch(config-if)

כעת לאחר הרענון הקל, נכיר **מספר סוגי תקיפות ברמת רכזת**:

<u>א. שינוי מצב העבודה של Switch לעבודה של רכזת פשוטה – Hub</u>. כאשר עמדה פונה לעמדה אחרת והיא עוברת דרך המתג, המתג רואה האם כתובת המקור רשומה אצלו, ואם לא, הוא מוסיף אותה לרשימה. כך כאשר עמדה אחרת תפנה לאותה עמדה, הפנייה

תהיה unicast ולא Broadcast. לכן תהיה להאקר בעיה לבצע Sniffer ברשת וללכוד את המנות, מכיוון שהמנות מועברות ישירות לפורט של היעד.

לכל מתג יש כמות של כתובות שהוא יכול לשמור בזיכרון. בדרך כלל מספר הכתובות הוא 1000-2000. לכן אם בעמדה מסוימת משנים במהירות (בעזרת סקריפט) את כתובת ה-MAC ובכל פעם פונים למתג, הוא ירשום את כל הכתובות עד שה-Buffer יתמלא. כעת הוא יעבור למצב של הצפה (flooding) ולמעשה יתפקד כ-Hub. Hub כידוע אינו יודע להתמקד לפי כתובת MAC, כל פנייה מועברת לכל היציאות, וכך ניתן להאזין למידע.

דרכי התגוננות מול תקיפה זו:

1. ניתן לשריין כתובת MAC לפורט מסוים ברכזת, כך עמדה עם כתובת MAC אחרת לא תוכל להתחבר לפורט זה ברכזת. הפקודה פשוטה מאוד:

```
switch(config)mac-address-table static 0000.1111.2222 vlan 1 int fa0/1
```

בדוגמה זו המספר 0000.1111.2222 הוחלף במספר MAC והיציאה fa0/1 הוחלפה ביציאה הרלוונטית. המילה fa מייצגת Fast Ethernet, הספרה 0 מייצגת את שורת הפורטים, והספרה 1 את מספר הפורט. כך תעבור ותסמן את fa0/2, fa0/3 בהתאמה עד שתכסה את כל הפורטים.

2. אפשרות טובה יותר היא בעזרת הפקודה Switchport...

עד כה מתוך הספר

מדריך אבטחת מידע והגנה מפני האקרים

להזמנות צלצל עכשיו:

1-700-7000-44