רשתות מחשבים

סיכום – חלק א

פרקים 1–3: אינטרנט | Sockets | מודל חמש השכבות

מבוסס על: רשתות מחשבים – עומר רוזנבוים, ברק גונן, שלומי הוד

המרכז לחינוך סייבר – גרסה 4.0, אפריל 2026

תוכן עניינים

מבוא מטרות הספר, ידע מקדים, כלים נדרשים

פרק 1 כיצד עובד האינטרנט – רשת, לקוח, כתובות, שליחה וקבלה

פרק 2 תכנות ב-Socket – שרת, לקוח, כתובות, שליחה וקבלה

פרק 3 Wireshark ומודל חמש השכבות – שכבות, פקטות, פרוטוקולים

מבוא

אודות הספר

ספר זה עוסק ברשתות מחשבים ומיועד לתלמידים הלומדים במסגרת חלופת הגנת סייבר, וכן לכל מי שמעוניין ללמוד את התחום באופן עצמאי. הספר הוא פרקטי מאוד וכולל תרגול רב – כבר מהפרק השני הלימוד מלווה בכתיבת קוד Python.

ידע מקדים

- היכרות בסיסית עם שפת Python)משתנים, תנאים, לולאות, פונקציות, מחלקות(
- לא נדרש ידע קודם ברשתות

כלים נדרשים

3.13.7 Python	שפת התכנות המרכזית בה משתמש הספר
PyCharm	סביבת פיתוח נוחה לעבודה עם Python
4.x Wireshark	כלי לסנפת חבילות רשת (packet sniffing)
1.8 Npcap	דרייבר הסנפה מכרטיס רשת ב-Windows
Scapy	ספריית Python ליצירה ושליחה של פקטות

פרק 1: כיצד עובד האינטרנט?

WWW – Web Wide World

WWW (World Wide (Web הוא אוסף אתרי אינטרנט המקושרים זה לזה כמו רשת של קורי עכביש ומפוזרים בכל רחבי העולם. כאשר גולשים לאתר כלשהו, מתרחש תהליך של בקשה ותגובה:

- הדפדפן)לקוח – (Client שולח הודעת בקשה (Request) אל האתר
- השרת (Server) מחזיר הודעת תגובה (Response) המכילה את תוכן הדף

האתר מספק שירות לדפדפן – הוא השרת, והדפדפן הוא הלקוח.

כתובות IP

כתובת IP (IP Address)

כתובת המשמשת לזיהוי ישויות ברשת האינטרנט, בדומה לכתובת דואר. מורכבת מ-4 בתים (bytes), כל בית בטווח 0–255, מופרדים בנקודות. דוגמה: 192.168.1.1 עד 255.255.255.255 ועד 0.0.0.0.

לכל הודעה באינטרנט יש כתובת מקור (Source IP) וכתובת יעד (Destination IP), בדומה לכתובת מוען ונמען על מעטפה.

טיפ

את כתובת ה-IP שלכם ניתן לגלות דרך האתר whatismyip.com או בפקודת ipconfig בשורת הפקודה (cmd). שתי השיטות עשויות לתת תוצאות שונות – IP פרטי מול IP ציבורי)נלמד בפרק NAT).

GeoIP – מיקום גיאוגרפי לפי כתובת IP

קיימים מאגרי נתונים המאפשרים לקשר בין כתובת IP למיקום גיאוגרפי)מדינה, עיר(. מאגרים אלו אינם רשמיים ואינם מדויקים תמיד. כלי לדוגמה: geoiptool.com.

אזהרה

אי-דיוק ב-GeoIP עלול לגרום לבעיות חמורות: אם כתובת IP של פושע ממופה בטעות לשכונה הסמוכה לאזרח תמים, רשויות החוק עלולות לפשוט על ביתו בטעות.

ענן האינטרנט

Hop)קפיצה(

העברת הודעה בין שני רכיבי רשת המחוברים ישירות זה לזה. הודעה היוצאת מישראל אל שרת ב-GeoogleE בארה"ב עוברת בדרך דרך עשרות רכיבים, כאשר כל מעבר בין שני רכיבים סמוכים נקרא Hop.

כל הרכיבים ברשת משתמשים בכתובת ה-IP של ההודעה כדי לדעת לאן להעביר אותה הלאה.

כלי traceroute

הכלי tracert (Windows) / traceroute (Linux) מאפשר לראות את המסלול שעוברת הודעה מהמחשב שלנו אל היעד: רשימת כתובות ה-IP של כל הרכיבים בדרך, וזמן ה-turn-dirp לכל אחד מהם.

שימוש: tracert -d www.google.com

System Name Domain – DNS

פרק 1 – כיצד עובד האינטרנט?

DNS)מערכת שמות דומיין(

מנגנון המתרגם שמות דומיין קריאים)כמו www.kan.org.il(לכתובות IP)כמו 172.66.43.92(. ההמרה מתרחשת בכל פעם שמשתמשים בשם דומיין – בגלישה בדפדפן, בשימוש ב-gnip, tracert ועוד.

תהליך הגלישה בפועל:

1. המחשב שולח שאילתת DNS לשרת ה-SND: "מה כתובת ה-PI של www.kan.org.il?"
2. שרת ה-SND מחזיר: "172.66.43.92"
3. המחשב שולח את בקשת ה-PTTH אל כתובת ה-PI שקיבל
4. השרת מחזיר את תוכן הדף

כלים שימושיים בפרק 1

ping	בדיקת קיום מחשב ברשת + מדידת זמן הלוך-ושוב
tracert	מעקב אחר המסלול שהודעה עוברת עד ליעד
nslookup	תרגום שמות דומיין לכתובות IP
ipconfig	הצגת הגדרות כרטיסי הרשת (IP, Gateway, DNS)

פרק 2: תכנות ב-stekcoS

מודל שרת-לקוח (Client-Server)

מודל שרת-לקוח הוא צורת התקשורת הנפוצה ביותר באינטרנט:

- שרת (Server) – רכיב המספק שירות
- לקוח (Client) – רכיב המשתמש בשירות

הלקוח שולח בקשה, והשרת מחזיר תגובה. גלישה לאתר, שימוש בדואר אלקטרוני, שיחות וידאו – כולם מבוססים על מודל זה.

מהו Socket?

Socket

נקודת קצה של חיבור בין שני רכיבים. ניתן לדמות אותו לצינור המעביר מידע בין שתי תוכנות – על אותו מחשב, או על שני מחשבים שונים. נקודת הכניסה ונקודת היציאה של המידע נקראות Socket.

כתובת של Socket

לכל Socket יש שני מזהים:

- כתובת IP – מזהה את הרכיב)מחשב, שרת וכו'(
- מספר פורט (Port) – מזהה את התוכנית הספציפית על הרכיב

פורט הוא מספר בטווח 0–65535. הדמיה: IP = מספר בניין, פורט = מספר דירה.

API של Socket ב-Python

צד לקוח

import socket	ייבוא מודול ה-tekcos
s = socket.socket()	יצירת אובייקט socket
s.connect(('IP', port))	התחברות לשרת לפי IP + פורט
s.send(data.encode())	שליחת מידע)כ-setyb(
data = s.recv(1024).decode()	קבלת מידע)עד 1024 בתים(
s.close()	סגירת החיבור ושחרור משאבים

צד שרת

s = socket.socket()	יצירת socket שרת
s.bind(('0.0.0.0', port))	קישור לכתובת ופורט (0.0.0.0 = כל כתובת)
s.listen()	האזנה לחיבורים נכנסים
(cs, addr) = s.accept()	המתנה לחיבור + קבלתו (blocking)
cs.recv() / cs.send()	תקשורת עם הלקוח דרך ה-tekcos החדש
cs.close() / s.close()	סגירת החיבור עם הלקוח / עצירת השרת

נקודות מפתח

- הפונקציה recv היא blocking – הקוד "קופא" עד שמגיע מידע
- recv מחזיר מחרוזת ריקה ("") כאשר החיבור התנתק
- חייבים לבצע encode() לפני שליחה ו-decode() אחרי קבלה (Python 3 דורש bytes)
- כתובת 127.0.0.1 (loopback) מאפשרת שרת ולקוח על אותו מחשב
- שני סוגי sockets שונים בשרת: אחד להאזנה (server_socket), אחד לכל לקוח (client_socket)

שים לב: חשוב לקרוא תמיד ל-close() בסיום. אחרת, הפורט נשאר "תפוס" ולא ניתן יהיה להפעיל שרת חדש על אותו פורט. אם השרת קרס לפני close(), ניתן להחליף לפורט אחר.

פרק 3: Wireshark ומודל חמש השכבות

מדוע צריך מודל שכבות?

רשת האינטרנט מכילה אינספור ישויות מיצרנים שונים המשתמשות בתקנים שונים. כדי שכולם יוכלו לדבר ביניהם, ארגון התקינה הבינלאומי (ISO) הגדיר את מודל OSI)שבע שכבות(, ובפועל נעשה שימוש במודל חמש השכבות.
יתרונות המודל:

- כל שכבה מסתירה את מימושה מהשכבה שמעליה)קופסה שחורה(
- שינוי מימוש של שכבה אינו משפיע על שאר המערכת
- כל שכבה מדברת עם שכבה מקבילה בצד השני דרך פרוטוקול

פרוטוקול

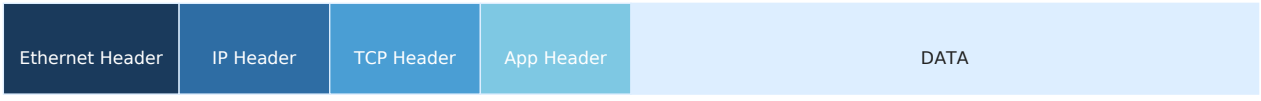
פרוטוקול (Protocol)
סט מוגדר של חוקים הקובע כיצד תתבצע התקשורת בין שני צדדים. בלי פרוטוקולים, כל ישות הייתה "מדברת" בשפה שלה, ולא היה ניתן לתקשר. דוגמאות: HTTP)גלישה(, SMTP)דואר(, DNS)שמות(.

מודל חמש השכבות

#	שם השכבה	תפקיד	פרוטוקו
1	**השכבה הפיזית**	העברת ביטים 0/1 על תווך פיזי–	
2	**שכבת הקו**	תקשורת בין ישויות סמוכות	Ethernet
3	**שכבת הרשת**	ניתוב מסלול מקור→יעד	IP
4	**שכבת התעבורה**	ריבוב אפליקציות + אמינות)אופציונלי(	TCP/IP UDP
5	**שכבת האפליקציה**	שימושים ספציפיים לאפליקציה	HTTP, DNS SMTP

מבנה פקטה – Encapsulation)כימוס(

כאשר נשלחת הודעה, כל שכבה מוסיפה Header משלה)תחילת המכילה מידע בקרה(לתחילת הפקטה שקיבלה מהשכבה שמעליה. תהליך זה נקרא כימוס .(Encapsulation)
בצד המקבל מתבצע תהליך הפוך – קילוף :(Decapsulation) כל שכבה מסירה את ה-redaeH שלה ומעבירה את שאר הנתונים לשכבה שמעליה.



שכבה 2 שכבה 3 שכבה 4 שכבה 5 מידע

הבחנה חשובה: ה-ataD של כל שכבה הוא הפקטה השלמה של השכבה שמעליה, כולל ה-redaeH שלה.

מדוע המידע מחולק לפקטות?

- בקרת שגיאות טובה יותר – ניתן לשלוח מחדש רק את הפקטה הפגומה

- שילוב זרמי מידע במקביל – מספר אפליקציות יכולות לשלוח בו-זמנית
- מניעת הצפת הקו על ידי ישות יחידה (Starvation)
- סנכרון חומרה קל יותר

שכבה 1 – השכבה הפיזית

מעבירה ביטים 0 ו-1 מנקודה לנקודה עם כמה שפחות שגיאות. אינה מודעת לפקטות, מסגרות או כל מבנה של מידע – רק ביט אחד בכל פעם. תווכים: כבלי נחושת, סיב אופטי, גלים אלקטרומגנטיים ,WiFi) לווין).

שכבה 2 – שכבת הקו Data) (Link

מסתמכת על השכבה הפיזית ומוסיפה:

- ארגון המידע ב-semarF)מסגרות(
- תקשורת בין ישויות סמוכות ישירות
- מניעת התנגשויות)כשמספר ישויות שולחות על אותו קו(
- זיהוי שגיאות בסיסי

פרוטוקול עיקרי: .Ethernet גוש מידע: Frame)מסגרת(.

שכבה 3 – שכבת הרשת Layer) (Network

אחראית על מציאת המסלול הטוב ביותר בין שתי נקודות קצה ברשת .(routing) אינה עוסקת בתקשורת בין ישויות סמוכות, אלא במסלול הכולל.

- ניתוב מבוצע על ידי Routers)נתבים(
- פקטה יכולה לעבור דרך מספר קווים ורשתות שונות

פרוטוקול עיקרי: .IP גוש מידע: Packet)פקטה(.

שכבה 4 – שכבת התעבורה Layer) (Transport

מסתמכת על שכבת הרשת ומוסיפה שני שירותים:

- ריבוב אפליקציות (Multiplexing) – שימוש בפורטים כדי להפנות מידע לתוכנה הנכונה על אותה ישות
- אמינות)אופציונלי(– הבטחת הגעת כל הפקטות בסדר הנכון (TCP)

פרוטוקולים: TCP)אמין, מבוסס קישור(, UDP)מהיר, לא אמין(.
גוש מידע: Segment)סגמנט(ב-PCT.

שכבה 5 – שכבת האפליקציה Layer) (Application

מסתמכת על השכבות שמתחתיה ומאפשרת שימושים ספציפיים לאפליקציות. ה-stekcoS שלמדנו שייכים לשכבה זו – הם API שמערכת ההפעלה מספקת.

פרוטוקולים נפוצים:

- HTTP – גלישה באינטרנט
- SMTP – דואר אלקטרוני
- DNS – תרגום שמות דומיין
- FTP – העברת קבצים

Wireshark – כלי הסנפה

הסנפה Sniffing) (Packet

הפעולה בה אנו מסתכלים על חבילות המידע בדיוק כפי שנשלחו או התקבלו בכרטיס הרשת. Wireshark היא תוכנת הסנפה חינמית ועוצמתית המאפשרת לנתח את התעבורה ברשת.

סוגי מסננים ב-krahseriW

ל-krahseriW שני סוגי מסננים:

Capture Filter	רץ ב-revirD | לפני ההסנפה | מהיר, תחביר מצומצם
Display Filter	רץ בתוכנה | במהלך ההסנפה | איטי יותר, תחביר עשיר

דוגמאות Filters Display

- dns – הצגת כל פקטות ה-SND בלבד
- ip.src == 192.168.1.1 – פקטות ממקור ספציפי
- ip.addr == 192.168.1.1 – פקטות מ/אל כתובת ספציפית
- ip.dst =! 192.168.1.1 – פקטות שאינן מיועדות לכתובת זו
- tcp.port == 80 – פקטות TCP בפורט 80
- ip.addr == 1.2.3.4 or tcp.port == 22 – שילוב תנאים

מצב Promiscuous

הכנסת כרטיס הרשת ל"מצב פרוץ" – מאפשרת לראות בהסנפה גם מסגרות שאינן מיועדות למחשב שלנו)לדוגמה, מסגרות של מכשירים אחרים על אותה רשת(.