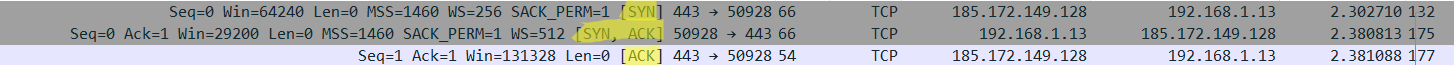


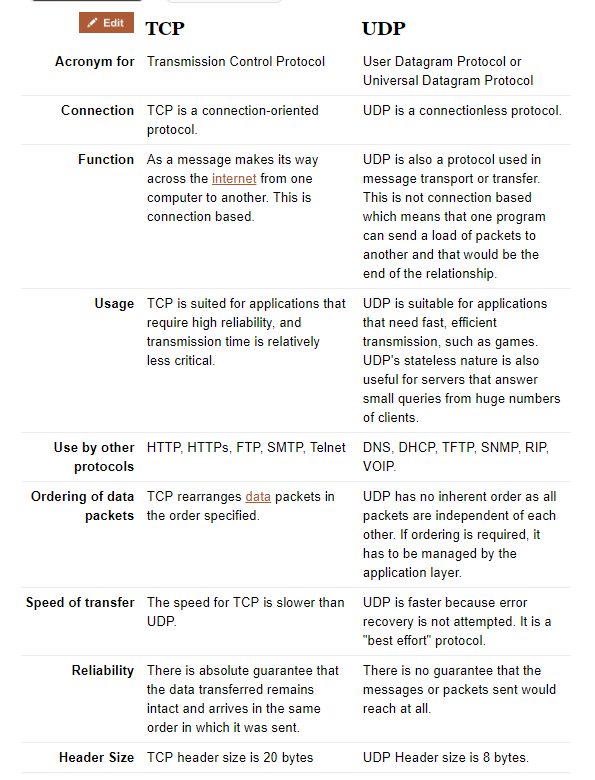
**מעבדה מספר 1**

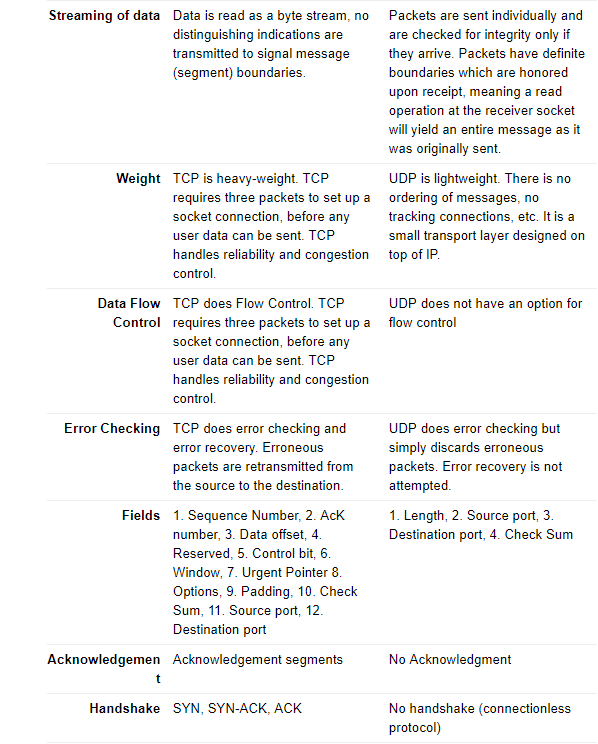
**תשובות**

**TCP**

**שאלות + תשובות:**

1. פתח wireshark ותתחיל להסניף את תעבורת הרשת שעוברת במחשב. כנס לדפדפן וגלוש באינטרנט. חפש הקמת תקשורת בTCP (Three-way handshake) צלם והסבר את התהליך. שים דגש איזה דגלים עולים.
2. הצג בטבלה את ההבדלים בין תקשורת TCP לתקשורת UDP





1. הצג 4 פרוטוקולים מוכרים שמשתמשים בתקשורת TCP

* Web
* SSH, FTP, telnet
* SMTP, sending mail
* IMAP/POP , receive mail

1. השאלות הבאות תצטרך לכתוב קוד בפיתון. בתיקיה נמצאים 2 קבצים – server.py, client.py. במשימות הבאות עליך להוסיף קוד לקבצים הללו. יש לכתוב את הקוד רק במקום שמצוין בקבצים. להפעלת הקבצים הרץ תחילה את הserver ולאחריו את הclient הserver יחכה עד אשר הclient יקליד משהו.

בשאלות הבאות תצטרך להוסיף פעולות רק לserver.

1. בכל פעם שהserver מקבל משהו מהclient הוא צריך להדפיס למסך-

"The massage from the client is: [message]"

1. הserver לא מבדיל בין אותיות גדולות לאותיות קטנות, עזרו לו שבכל קריאה של ההודעה זה לא יהיה משנה אם האותיות גדולולת או קטנות.
2. הserver יודע לענות על דברים מסויימים כמו מה השעה, מה שמו, מה הת"ז זהות שלו, מה הIP שלו. (אם עובדים בזוגות יש לרשום את שני השמות והת"ז מופרדים בפסיק)

* כאשר הserver מקבל time הserver ישלח את התאריך והשעה (ניתן להשתמש בdatetime.now()
* כאשר הserver מקבל name הserver ישלח את השם שלך

"my name is [name]"

* כאשר הserver מקבל id ה server ישלח את הת"ז שלך

"my ID is [ID]"

* כאשר הserver מקבל ip הserver ישלח את הip שלו

"my ip is [IP]"

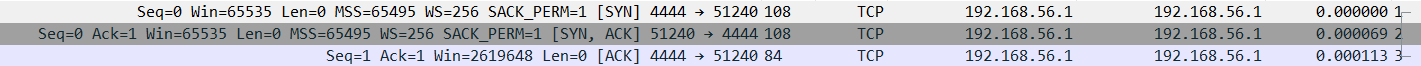
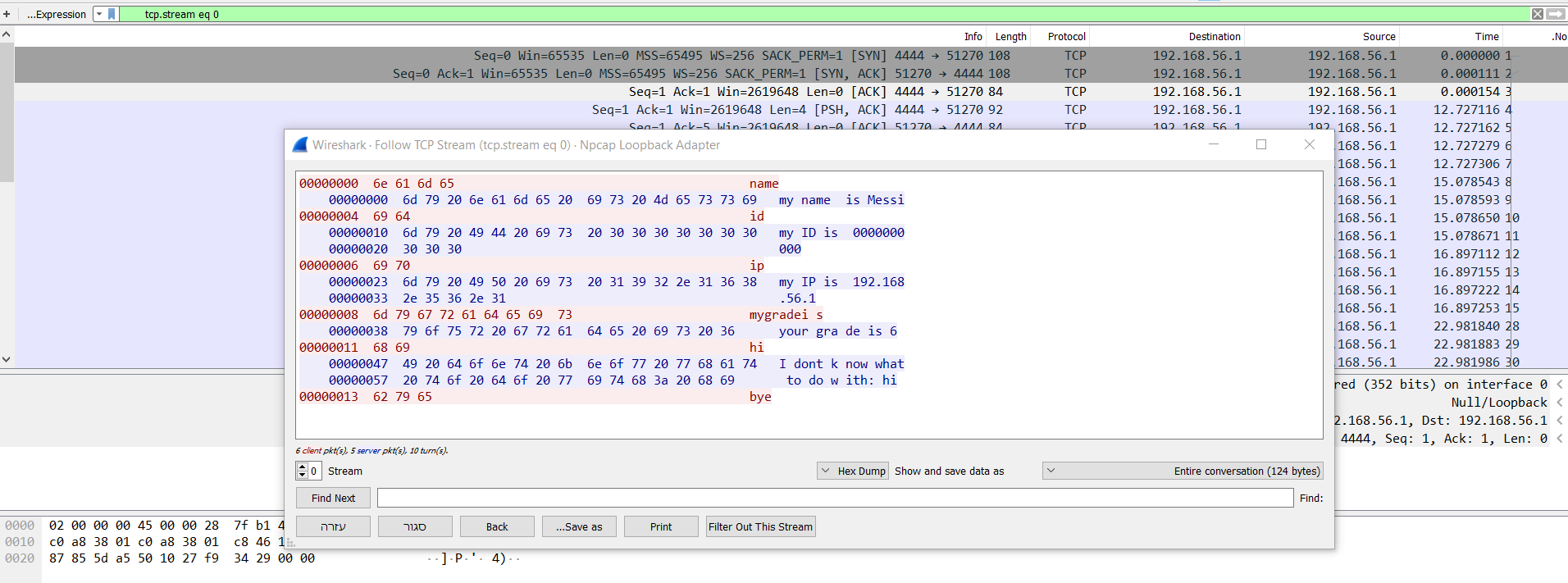
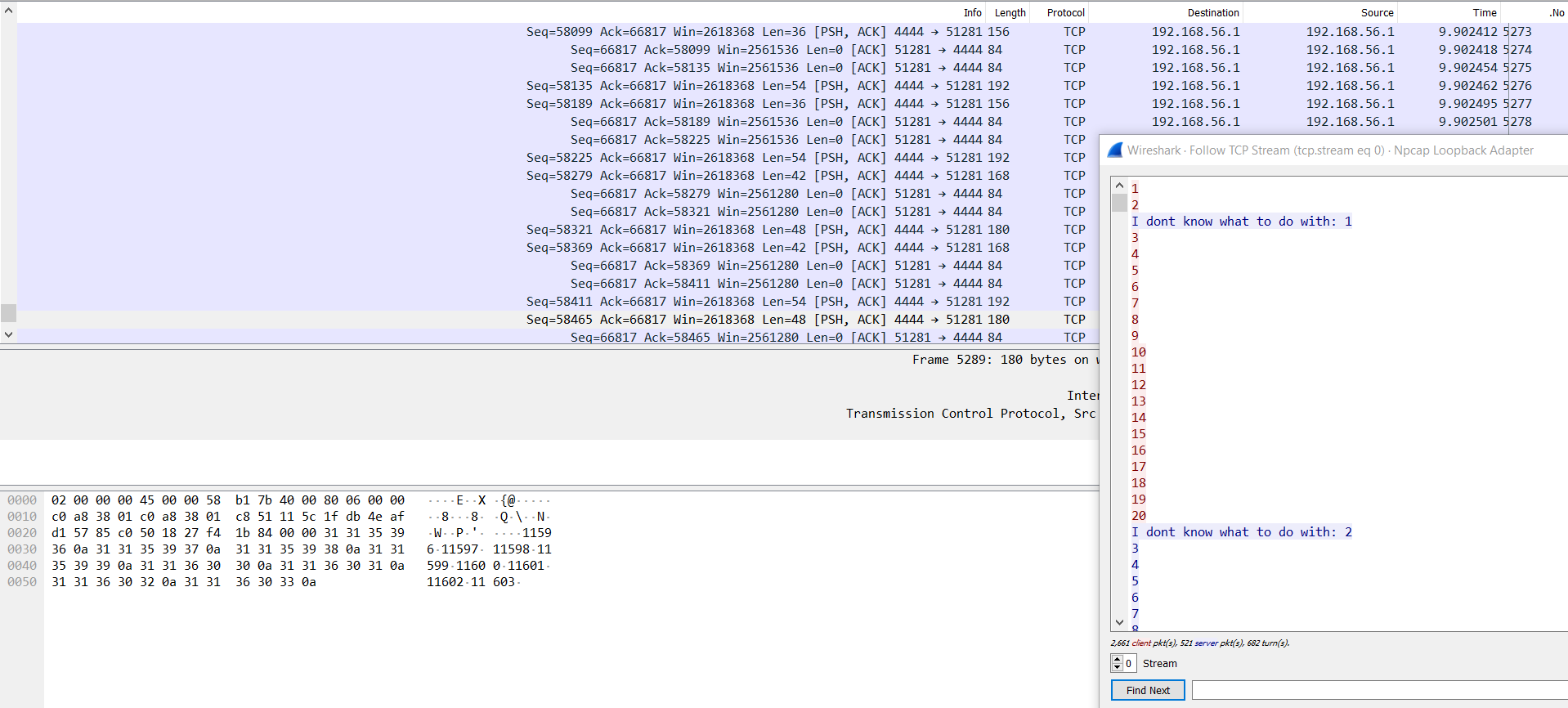
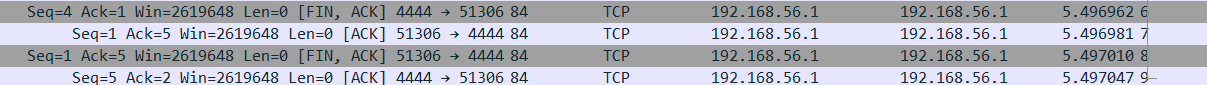
* בנוסף הserver מבצע בדיקה מעמיקה של התרגיל שלכם ונותן לכם ציון מ0 עד 100.

כאשר הserver מקבל getmygrade הserver יגריל מספר בין 0 ל 100 וישלח אותו

"your grade is [rand\_num]"

* כאשר הserver מקבל bye הוא סוגר את ההתקשרות עם הclient
* בכל קבלה אחרת הserver יחזיר

"I don’t know what to do with: [message]"

1. כעת הclient שולח – floodattack הסבירו מה הclient מבצע ומה קורה בserver.
2. הציעו 3 פתרונות לבעיה של הserver, כלומר כיצד הserver יוכל למנוע את ההתקפה. (פתרונות תיאורטיים, לא צריך לממש אותם).
3. כעת עליכם לממש בserver את אחת הדרכים שחשבתם עליהם. בסיום התהליך הserver ינתק את ההתקשרות עם הclient. (רמז- אתם יכולים להשתמש בפונקציה time.time() ובcounter שמוגדרים לכם בתחילת הקוד)
4. פתח wireshark הצג והסבר את הדברים הבאים
5. Three-way-handshake בין הserver לclient.
6. כל אחת מהפקודות שהserver מבצע
7. floodattack
8. סיום התקשרות עם הclient

פתרונות למעבדה 2 חלק מתקפת SYN Flooding Attack:

1. תאר את אופן ביצוע מתקפת SYN Flooding.

פתרון:

טרם סיום לחיצת היד המשולשת, השרת מאחסן את הקשר החצי פתוח בתור ייעודי, בעל תכולה סופית. במתקפה זו, גורמים להתמלאות מהירה של התור ועל ידי כך מניעת השרת מלקבל הודעות פתיחת קשרים חדשים. בצורה זו, על אף שצד השרת פעיל, הוא מנוע ממתן שירות עבור לקוחות.

כל שיש לעשות על מנת לבצע את המתקפה הינו כדלקמן:

1. שליחה עקבית של הודעות בקשה לפתיחת קשר, מכתובות שונות (אחרת המתקפה תחסם בקלות על ידי ה – firewall).
2. אין לבצע את השלב השלישי בלחיצת היד המשולשת.
3. תאר את נקודת התורפה המנוצלת עבור מתקפת ה- SYN Flooding.

פתרון:

טרם סיום לחיצת היד המשולשת, השרת מאחסן את הקשר החצי פתוח בתור ייעודי, בעל תכולה סופית. במתקפה זו, גורמים להתמלאות מהירה של התור ועל ידי כך מניעת השרת מלקבל הודעות פתיחת קשרים חדשים. בצורה זו, על אף שצד השרת פעיל, הוא מנוע ממתן שירות עבור לקוחות.

1. תחת אילו תנאים מתרחשת הוצאת קשר חצי-פתוח מן התור המיועד לה?

פתרון:

הוצאה של קשר חצי פתוח מהתור נעשית בשלושה מקרים:

1. בקבלת הודעת ה – ACK מהלקוח וסיום לחיצת היד המשולשת.
2. לאחר חלוף הזמן המוקצה לקבלת הודעת ה – ACK מהלקוח. זמן זה יכול להיות מאוד ארוך במונחים של זמן CPU.
3. קבלת הודעת איפוס (RST) עבור קשר חצי פתוח.
4. תאר את שיטת המנע SYN – cookies.

פתרון

שיטה יעילה להגנה מפני המתקפה נקראת SYN cookies. השיטה הומצאה על ידי דניאל ג' ברנשטיין בשנת 1996. שיטה זו כיום מהווה חלק סטנדרטי ממערכות ההפעלה השונות. העיקרון המרכזי בשיטה הינו לא להקצות משאבים כלל בצד השרת, עבור הקמת הקשר, עד קבלת הודעת ה – ACK מהלקוח, בשלב השלישי בלחיצת היד המשולשת.

1. מהו העיקרון המנחה בשיטת המנע SYN – cookies?

פתרון:

העיקרון המרכזי בשיטה הינו לא להקצות משאבים כלל בצד השרת, עבור הקמת הקשר, עד קבלת הודעת ה – ACK מהלקוח, בשלב השלישי בלחיצת היד המשולשת.

6)טיפול במתקפת SYN Flooding עלול לפתוח שער למתקפה נוספת. תאר את המתקפה הזו וכיצד שיטת SYN cookies מתמודדת אתה. האם מתקפה זו מסוכנת יותר מ – SYN – Flooding?

פתרון:

שיטה זו פותרת אמנם את בעיית ההצפה אך פותחת שער למתקפה אחרת. מאחר ולא מוקצים משאבים כלל, אין דרך לדעת האם הודעת ה – ACK שנתקבלה בשרת הינה כמשוב לשלב השני של לחיצת היד המשולשת או הודעה מזויפת. כתוצאה מכך, ניתן יהיה להציף את השרת בהודעות ACK מזויפות שיגררו הקמת קשרי TCP ריקים. למתקפה זו פוטנציאל הרס גדול משל המקורית, שכן המשאבים המוקצים לקשר שלם גדולים מאשר לקשר חצי פתוח.

SYN cookies פותרת זאת בצורה הבאה: לאחר קבלת בקשה לפתיחת קשר מהלקוח, השרת מחשב ערך, H, בעזרת מפתח האש, הידוע רק לו, מהכתובת ממנה נשלחה ההודעה, מספר הפורט והמספר הסידורי. H ישלח כמספר הסידורי בהודעת ה – SYN+ACK, שתשלח כתגובה ללקוח, מהשרת. אם ההודעה המקורית הגיעה מתוקף, הודעת התגובה תגיע לכתובת מזויפת ולא נקבל הודעת ACK לסיום לחיצת היד המשולשת. אולם, השרת טרם הקצה משאבים כלשהם לקשר ולכן לא נגרם כל נזק. אם ההודעה המקורית נשלחה מלקוח רלוונטי, הוא יקבל את הודעת ה – SYN+ACK, עם המספר הסידורי H, ויחזיר הודעת ACK עם הערך H+1, בשדה מספר האישור. בקבלת הודעה זו, השרת יכול לחשב חזרה את ערך ההאש ולבדוק האם ההודעה הגיע מלקוח רלוונטי או מתוקף. רק אם החישוב יראה על לקוח רלוונטי, יקצה השרת משאבים לקשר ה – TCP. מפתח ההאש בו משתמש השרת ידוע רק לו ועל כן, יהיה קשה מאוד לתוקפים לזייף הודעות ACK שיגררו הקמת קשרי סרק.