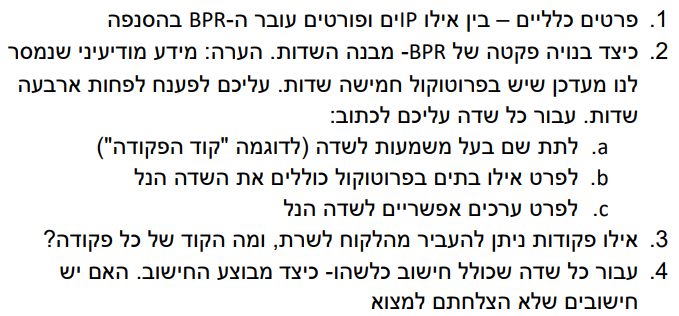
בס"ד

ישי לוטוק 304909864

**מחקר על פרוטוקול BPR**



**תשובות לשאלות:**

(תהליך המחקר המלא נמצא למטה)

1. בין כתובות הIP 192.168.1.113 ו- 192.168.1.118 והפורטים 50450 ו1400



1. הודעה לדוגמא BPR0000010981

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | שדה 1 | שדה 2 | שדה 3 | שדה 4 | שדה 5 |
|  | BPR | 00 | 0001 | 098 | 1 |
| A | שם הפרוטוקול | מספר ההודעה. בכל תגובה של השרת יהיה אותו מספר של הודעת הלקוח | אורך ההודעה | שדה מורכב – קוד האסקי של המספר שמייצג את אורך ההודעה + קוד האסקי של תוכן ההודעה.  וכל זה מודולו 256 | קוד הפקודה שיש לבצע.  שדה זה קיים רק בהודעות מהלקוח לשרת |
| B | בתים  54-56 | בתים  57-58 | בתים  59-62 | בתים  63-65 | בית  66 |
| C | BPR בלבד | בין 0 ל31 - אחרי 31 הוא חוזר ל0 | בין 1 ל9999 | בין 0 ל255 | בין 0 ל4 |

1. ניתן להעביר מהלקוח לשרת 5 פקודות

קוד הפקודה 0 – יציאה

קוד הפקודה 1 – בקשת תאריך ושעה

קוד הפקודה 2 – בקשת מספר רנדומלי בין 0 ל99

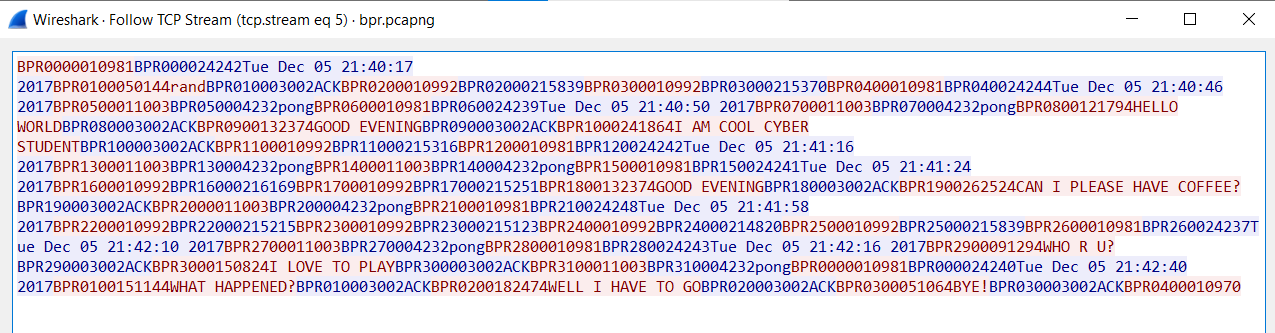
קוד הפקודה 3 – בקשת ping מצפה לקבל מהשרת pong

קוד הפקודה 4 – שליחת מחרוזת לשרת וקבלה בתגובה של ACK

1. השדה השני שמסומן בצבע ירוק הוא מספר ההודעה. השדה השני שמסומן בצבע צהוב הוא אורך ההודעה

השדה הרביעי מורכב מחישוב מסובך יותר – קוד האסקי של המספר שמייצג את אורך ההודעה (שדה 3 בלי קוד האסקי של האפסים שלפני המספר) + קוד האסקי של תוכן ההודעה, כלומר כל מה שמעבר לשדה הזה עצמו (זה כולל כמובן את קוד ההודעה במידה ויש). ולסיום יש לקחת את התוצאה שהתקבלה ולעשות לה מודולו 256.

**תהליך המחקר המלא:**



מהצילום מסך ניתן לראות כי השדה הראשון בכל ההודעות הוא BPR אחר כך השדה השני הוא מספר שמיוצג על ידי שתי ספרות והוא נע בין 00 ל31. ניתן לראות בקלות כי מדובר בשדה שמייצג את מספר ההודעה, מספר התגובה של השרת זהה למספר ההודעה. הספירה מתחילה מ0 ומגיעה עד 31 לאחר מכן היא חוזרת ל0.

נסדר את הפקודות לפי סוג כדי לזהות שדות נוספים:

BPR0000010981 BPR000024242Tue Dec 05 21:40:17 2017

BPR0400010981 BPR040024244Tue Dec 05 21:40:46 2017

BPR0600010981 BPR060024239Tue Dec 05 21:40:50 2017

BPR1200010981 BPR120024242Tue Dec 05 21:41:16 2017

BPR1500010981 BPR150024241Tue Dec 05 21:41:24 2017

BPR2100010981 BPR210024248Tue Dec 05 21:41:58 2017

BPR0000010981 BPR000024240Tue Dec 05 21:42:40 2017

BPR2600010981 BPR260024237Tue Dec 05 21:42:10 2017

BPR2800010981 BPR280024243Tue Dec 05 21:42:16 2017

BPR0200010992 BPR02000215839

BPR0300010992 BPR03000215370

BPR1100010992 BPR11000215316

BPR1600010992 BPR16000216169

BPR1700010992 BPR17000215251

BPR2200010992 BPR22000215215

BPR2300010992 BPR23000215123

BPR2400010992 BPR24000214820

BPR2500010992 BPR25000215839

BPR0500011003 BPR050004232pong

BPR0700011003 BPR070004232pong

BPR1300011003 BPR130004232pong

BPR1400011003 BPR140004232pong

BPR2000011003 BPR200004232pong

BPR2700011003 BPR270004232pong

BPR3100011003 BPR310004232pong

BPR0800121794HELLO WORLD BPR080003002ACK

BPR0900132374GOOD EVENING BPR090003002ACK

BPR1000241864I AM COOL CYBER STUDENT BPR100003002ACK

BPR1800132374GOOD EVENING BPR180003002ACK

BPR1900262524CAN I PLEASE HAVE COFFEE? BPR190003002ACK

BPR2900091294WHO R U? BPR290003002ACK

BPR3000150824I LOVE TO PLAY BPR300003002ACK

BPR0100151144WHAT HAPPENED? BPR010003002ACK

BPR0200182474WELL I HAVE TO GO BPR020003002ACK

BPR0300051064BYE! BPR030003002ACK

BPR0400010970

השדה שמסומן בירוק הוא המספר של ההודעה או התגובה כפי שכבר אמרנו.

אם נתבונן בשדה הצהוב ובאורך ההודעה (החל ממה שלאחר השדה בצבע תכלת[[1]](#footnote-1)) נוכל לראות כי שדה זה מייצג את אורך ההודעה.

ניתן גם לראות כי השדה שמסומן בוורוד מייצג קוד פקודה, שכן כאשר הוא משנה גם השרת מגיב באופן שונה.

השדה שמסומן בתכלת קשור לשדה הפקודה נוכל להסיק זאת מכך שכאשר הפקודה היא 0 הוא 97, כאשר הפקודה היא 1 הוא 98, כאשר הפקודה היא 2 הוא 99 וכאשר הפקודה היא 3 הוא 100. כלומר כשקוד הפקודה עולה ב1 גם השדה בצבע תכלת עולה ב1.

להלן המחשה:

BPR0400010970

BPR0000010981 BPR000024242Tue Dec 05 21:40:17 2017

BPR0200010992 BPR02000215839

BPR0500011003 BPR050004232pong

כמו כן הוא קשור למחרוזת של ההודעה במידה ויש. נמחיש זאת על ידי ההודעות הבאות:

BPR0200010992 BPR02000215839

BPR0300010992 BPR03000215370

BPR1100010992 BPR11000215316

ניתן לראות שהשדה שמסומן בצבע תכלת משתנה בהתאם למספר למחרוזת ההודעה שמסומנת באדום. המספר הבסיסי כאן הוא 146 כאשר מוסיפים לו 3+9 מקבלים 158, כאשר מוספים לו 7+0 מקבלים 153 וכאשר מוסיפים לו 1+6 מקבלים גם כן 153.

אם נסתכל רק על ההודעה BPR0000010981 ונחפש משמעות למספר 98 נוכל לראות שקוד האסקי של 1 הוא 49 ולכן נראה שהשדה הזה מתייחס גם לאורך ההודעה שכן אז נחשב את קוד האסקי של אורך ההודעה + קוד האסקי של תוכן ההודעה שבמקרה זה הוא קוד הפקודה ונקבל 98. אם נחזור להודעות האחרות וננסה להבין את המשמעות של השדה הזה נוכל לראות שהוא בעצם קוד האסקי של אורך ההודעה + קוד האסקי של תוכן ההודעה כאשר תוכן ההודעה הוא כל מה שמעבר לשדה הזה עצמו (המסומן בצבע תכלת). בהודעות מצד הלקוח קוד הפקודה נכלל בתוך תוכן ההודעה וכן אם יש לאחר מכן מחרוזת אז גם היא נכללת בתוכן ההודעה. בהודעות מצד השרת כל מחרוזת שמופיעה אחרי השדה הזה בין אם מדובר במספר ובין אם מדובר בטקסט הוא בעצם תוכן ההודעה.

נשים לב שיש הודעות שבהן הערך של שדה זה הופך להיות קטן יותר מקוד האסקי של המספר של אורך ההודעה ושל תוכן ההודעה. למשל: BPR080003002ACK. כאן לכאורה היינו צריכים לקבל 65 + 67 + 75 + 51 שזה שווה ל258. אם נסתכל על כל ההודעות נראה שהמספר הכי גבוה שקיים בשדה הזה הוא 248 (בהודעה: BPR210024248Tue Dec 05 21:41:58 2017). נראה שמעבר לסף מסוים מתחילים לספור מהתחלה. נוכל לתת חוקיות שתסביר את כל ההודעות על ידי שנוסיף לחישוב הקודם שאמרנו מודולו 256, כך נקבל מהמספר 258 את המספר 2 שכן

1. השדה האחרון שקיים גם בהודעות של הלקוח וגם בהודעות של השרת. [↑](#footnote-ref-1)