

***המשימה: ללמוד את האויב***

כחלק מחקירה של מתקפה גדולה שקרתה לפני מספר חודשים, נמצא מחשב של אחד התוקפים, אשר מסתבר שהוא חלק מקבוצה גדולה של האקרים. במחשב נמצאה תוכנה השייכת ככל הנראה לאותה קבוצה אליה משתייך התוקף, אשר מציגה את כמות המתקפות המתוכננות על ידם בכל המדינות בעולם. על מנת לנסות לגלות מידע נוסף ולחקור את פעולותיהם של קבוצה זו, אנו רוצים להצליח לגשת לתוכנה, וללמוד אותה. אנו ננסה להבין טוב יותר את השרת מולו היא עובדת ואת הפרוטוקול בו הוא משתמש. לאחר מחקר זה, נוכל לכתוב תוכנה שתפנה אליו ותשאב ממנו כל פיסת מידע שתוכל לעזור לנו להתחקות אחר פעילות ההאקרים ולהתגונן טוב יותר מפני מתקפות עתידיות.

כדי להבין את פעולת התוכנה נצטרך ללכת אל מאחורי הקלעים – בעזרת תוכנת Wireshark – כדי לגלות מה באמת שולחת ומקבלת התוכנה מהאינטרנט. באופן זה נלמד את הפרוטוקול של השרת של ההאקרים (בו משתמשת התוכנה) על מנת שנוכל בהמשך לפנות אליו בעצמנו.

**הוראות הגשה**:

לפני המענה על השאלות, הורידו את הקובץ אל המחשב שלכן (דרך File → Download As → Microsoft Word). לאחר פתיחת הקובץ שמרו אותו בנתיב לבחירתכן.

יש להעלות את הקובץ עם תשובותיכן ל-Moodle תחת השבוע המתאים.

**שלב 1 - הורדת תוכנה**

הורידו את הקובץ של תוכנת ההאקרים (Attacks.zip) מהתיקייה. עשו Extract לתיקייה משלכן ופתחו את התיקייה.

**שלב 2 - בדיקת ה-IP שלנו**

בעזרת פקודת ipconfig, בדקו מהו ה-IP של המחשב שלכם ורשמו אותו:

|  |
| --- |
| 192.168.104.49 |
| *תשובה* |

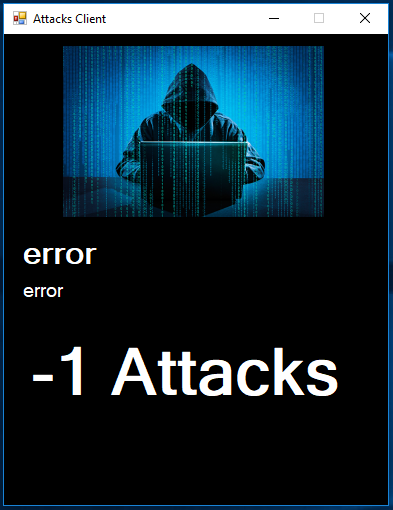
**שלב 3 - הרצה ראשונה של התוכנה**

בשלב זה נתחיל להבין איך התוכנה עובדת, וננסה לאסוף כמה שיותר מידע ונתונים על התוכנה ועל השרת איתו היא מתקשרת.

לחצו פעמיים על הקובץ AttacksClient.

**(לא להריץ את התוכנה מתוך Winrar!)**

אתן אמורות לראות את התוכנה נפתחת במסך הבא:



1. כעת ננסה להבין מדוע התוכנה לא פועלת. סגרו את התוכנה, ופתחו את Wireshark. כדי לבודד את התעבורה שמעניינת אותנו, נסו לוודא שכמה שפחות תוכנות משתמשות באינטרנט במחשב. התחילו בהסנפה ומיד לאחר מכן הפעילו את התוכנה של ההאקרים. הפסיקו את ההסנפה **מיד לאחר** שהתוכנה נפתחת – כמה שיותר מהר!

2. נסו לגלות מהו ה-IP איתו מתקשרת התוכנה וכיתבו פילטר אשר יסנן לפי IP זה. זהו IP שחוזר מספר פעמים והוא לא ה-IP שלנו. אם כתבתן פילטר נכון, אתן אמורות לראות כעת רק את התעבורה של תוכנת ההאקרים. כתבו את הסינון אשר כתבתן:

|  |
| --- |
| ip.addr == 52.35.198.18 |
| *תשובה* |

**טיפ:** כדי לוודא שהפילטר שלכן באמת "תפס" את התוכנה, שימו לב שבכל הרצה מחודשת של התוכנה מתווספות חבילות לתצוגה

3. לאחר שמצאתן את ה-IP, חפשו מהו הפורט הפתוח אצל השרת איתו אנו מדברים? מהו הפורט שפתחנו אצלנו (לקוח)?

|  |
| --- |
| הפורט של השרת : 1050  הפורט שלי : 5826 |
| *תשובה* |

4. צרו סינון נוסף אשר מבודד את התעבורה של תוכנת ההאקרים בלבד, הפעם על בסיס הפורט. כלומר, פילטר נוסף אשר יציג את אותן תוצאות כמו הפילטר מסעיף ד'.

רמז: אתן יכולות להיעזר בתשובה לשאלה הנמצאת בקישור זה - <https://osqa-ask.wireshark.org/questions/41300/filter-with-destination-port>

כתבו את הסינון שביצעתן:

|  |
| --- |
| Tcp.port ==1050 |
| *תשובה* |

5. כעת אמורות להיות מוצגות כ-20 חבילות לכל היותר על המסך. נסו לעבור בין החבילות ולחפש חבילה הכוללת תוכן טקסטואלי. נסו לחפש את השגיאה אשר חזרה מהשרת וכתבו אותה כאן:

|  |
| --- |
| 500:ERROR:date illegal: date is in the past or format is invalidclosed |
| *תשובה* |

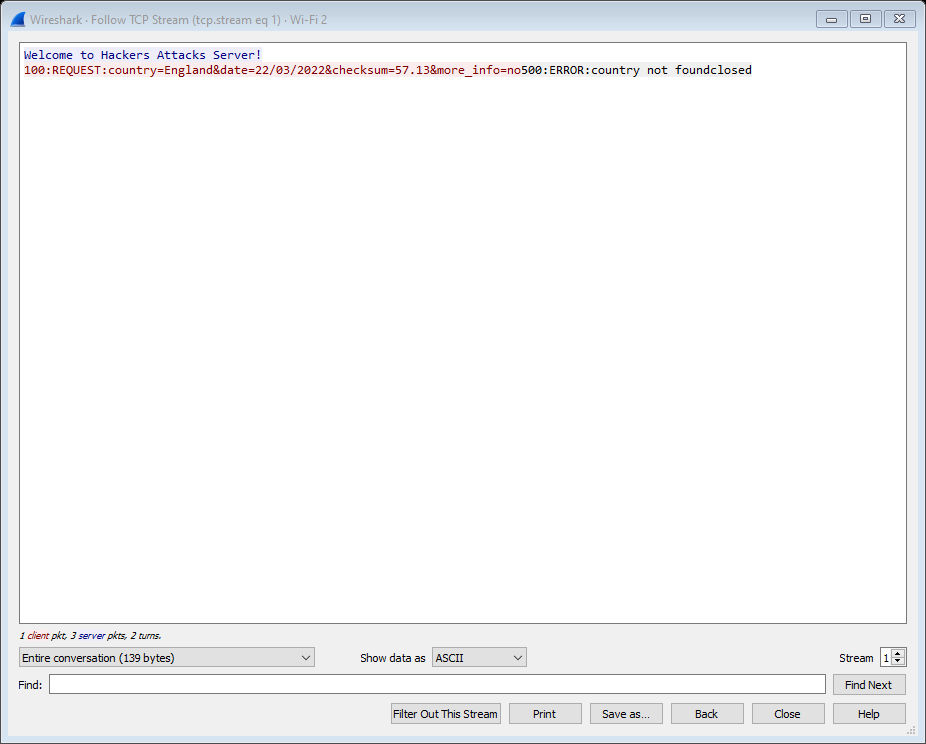
6. עדיין ב-Wireshark, נסו לחפש את החבילה הכוללת את המידע אשר נשלח מהמחשב שלנו וגרם לשרת לשלוח את השגיאה. כתבו את המידע ונסו להסביר מדוע לדעתכן התקבלה שגיאה?

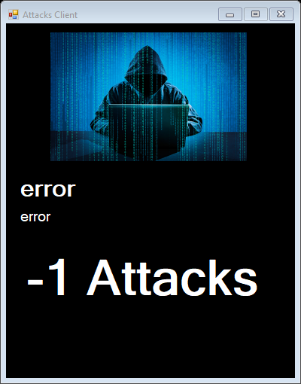
|  |
| --- |
| country=Israel&date=25/06/2020&checksum=64.17&more\_info=no  לדעתי, השגיאה התקבלה מאחר והפרוטוקול של המחשב ושל השרת שלנו לא התאימו אחד לשני. |
| *תשובה* |

7. חזרו לתיקיית התוכנה. נסו לחפש מאיפה מגיע המידע אשר גורם לשגיאה. נסו לשנות אותו ולגרום לתוכנה לעבוד ולהחזיר נתונים הגיוניים. צרפו כאן צילום מסך של התוכנה כאשר היא פועלת כהלכה (ב-Word ניתן לצלם את המסך בעזרת תפריט הוספה->צילום מסך).



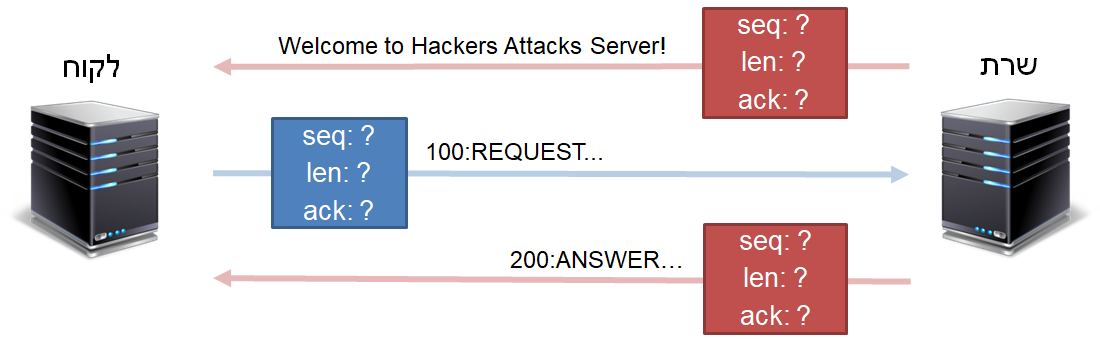


8. התחילו הסנפה חדשה. נסו לשנות את המדינה למדינה אחרת לבחירתכן וצרפו צילום מסך.





9. לחצו לחצן ימני על אחת הפקטות השייכות לשיחה בין התוכנה לשרת, ובחרו ב-   
Follow → TCP Stream, אשר מציג את השיחה עם השרת. היכנסו לפקטות הרלוונטיות (על פי המידע הנשלח בכל פקטה המתוארת בתרשים), הוסיפו צילומי מסך שלהן, וענו - מהם ערכי ה- Sequence, Acknowledgment ו- Length עבור כל פקטה:



**הכניסו תשובותיכן כאן:**



|  |  |
| --- | --- |
| **Welcome to….** | Seq: \_\_1\_\_\_\_\_  Len: \_\_\_35\_\_\_\_  Ack: \_\_1\_\_\_\_\_ |
| **100:REQUEST...** | Seq: \_\_1\_\_\_\_\_  Len: \_\_\_\_\_71\_\_  Ack: \_\_36\_\_\_\_\_ |
| **200:ANSWER...** | Seq: \_\_\_36\_\_\_\_  Len: \_\_72\_\_\_\_\_  Ack: \_\_27\_\_\_\_\_ |

10. בשיעור TCP דיברנו על כך שה-header מכיל פעמים רבות דגלים (Flags) אשר מעבירים מידע נוסף. עברו על החבילות השונות בשיחת ה-TCP שלכן עם השרת וכתבו, אילו דגלים דלוקים במהלך השיחה? מה המשמעות של כל דגל?

|  |
| --- |
| SYN –לחיצת היד המשולשת  RST- צריך לסיים את התקשורת  ACK – גם משמש לחיצת יד משולשת(מאשרת הגעה של הודעה)  PSH- השולח מבקש שהמידע בהודעה זו יועבר מיד לאפליקציה ולא יחכה לחלקים נוספים  FIN – סיום השיחה |
| *תשובה* |

11. האם דגל ה-PSH דלוק בחלק מהחבילות? אם כן, כתבו למה לדעתכן הוא דלוק דווקא בחבילות אלה?

|  |
| --- |
| כן, הוא דלוק דווקא בחבילה שבה התוכנה אומרת שלום ללקוח, ובחבילה שבה התוכנה שולחת שגיאה ללקוח, לדעתי הוא דלוק דווקא בחבילות האלו מאחר וחשוב למי שכתב את התוכנה שההודעות האלו יגיעו מיידית ללקוח בעתו עושה שגיאה/ בעתו נכנס לתוכנה מבלי שיחכה. |
| *תשובה* |

12. בשיעורים האחרונים דיברנו על מודל חמשת השכבות, וראינו כיצד ניתן לראות את ה-header של שכבת התעבורה ב- Wireshark (בין אם בפרוטוקול UDP ובין אם בפרוטוקול TCP). אך כיצד ניתן לראות את שאר השכבות? קראו על כך בקובץ הנמצא בתיקייה הנקרא "**מודל השכבות בWireshark**".

13. לחצו על החבילה המכילה את התשובה שקיבלתן מהשרת (ANSWER:200), כתבו את תשובת השרת אליה אתן מתייחסות, ובדקו עבור חבילה זו, מהו האורך (בבתים) של כל אחת מהשכבות:

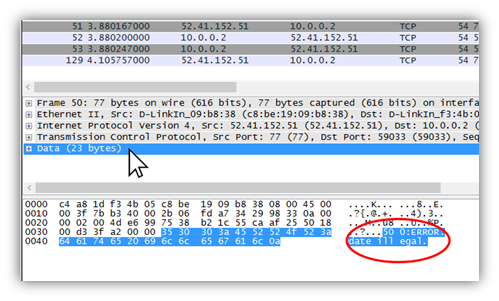
|  |
| --- |
| תשובת השרת: ERROR:date illegal: date is in the past or format...  אפליקציה = 35  תעבורה = 35  רשת = 20  קו = 20 |
| *תשובה* |

**עכשיו כשאספנו מספיק נתונים, בואו נתחיל להבין איך באמת עובד השרת איתו מתקשרת התוכנה… רק כך נוכל בהמשך לתקשר איתו בעצמנו!**

**שלב 4 - אבחון הפרוטוקול**

כפי שלמדנו, פרוטוקול הוא למעשה שפה הכוללת סט מוגדר של חוקים לשיחה ברשת. כעת ננסה ללמוד את הפרוטוקול בו משתמשת תוכנת ההאקרים, על מנת שנבין כיצד ניתן לעשות בקשות לשרת וכך נוכל לגשת אליו בעצמנו.

עזרה: לשם כך נמשיך להתמקד בחלק התחתון ביותר של Wireshark המציג את תוכן החבילה. כדי לפשט את העבודה, נוכל להגיד ל-Wireshark לסמן לנו את החלק הרלוונטי בכחול. כדי לעשות זאת, בכל חבילה שנבחר, נעבור למסך האמצעי (מסך השכבות) ונלחץ על השורה התחתונה ביותר בו, Data. כעת נוכל לראות שהחלק המעניין מסומן למטה מצד ימין בכחול.



כתבו הסבר על ההודעות של הפרוטוקול:

בסעיף **"כיצד היא נראית"** יש לכתוב בדיוק את ההודעה כפי שהיא. אם זיהיתן חלק בהודעה שמשתנה ואינו קבוע, תוכלו לציין אותו בעזרת <>. למשל:

date:<DATE>

בסעיף **"הסבר"** יש להסביר את מטרת ההודעה לדעתכן, ולהסביר את כל השדות ששמתם ב-<>.

|  |  |
| --- | --- |
| **הודעת פתיחה (שרת -> לקוח)** | |
| כיצד היא נראית? | Welcome to Hackers Attacks Server! |
| הסבר | הודעה בתבנית קבועה, הודעת "שלום" ללקוח הפונה לתוכה |
| **בקשה (לקוח -> שרת)** | |
| כיצד היא נראית? | 100:REQUEST:country=Israel&date=23/03/2022&checksum=64.13&more\_info=no |
| הסבר | הבקשה מסומנת במספר 100 יש "כותרת" לפני כל תשובה , למשל: "ארץ" : ישראל ולפני שם הארץ/ התאריך וכד, יש את הסימן = , כל "קטגוריה" בהודעה מחוברת בסימן & |
| **תשובה (שרת -> לקוח)** | |
| כיצד היא נראית? | 200:ANSWER:country=israel&attacks=6&date=22/03/2022 |
| הסבר | ההודעה בנויה בדומה להודעת בקשה, היא מראה לנו כמה מתקפות קיימות, על איזה ארץ, ובאיזה תאריך. |
| **הודעת שגיאה (שרת->לקוח)** | |
| כיצד היא נראית? | date illegal: date is in the past or format is invalidclosed |
| הסבר | הודעת שגיאה בתבנית קבועה |

**שלב 5 - פענוח שדה ה-Checksum**

1. כפי שלמדנו, שדה ה-checksum הוא שדה אשר מהווה בדיקה שכל המידע בבקשה עבר כהלכה. כדי לעשות זאת הוא מבצע פעולה מתמטית על המידע של הבקשה ושולח את התוצאה הזאת יחד עם המידע. במקרה שלנו ה-checksum מורכב משני חלקים שמופרדים ע"י נקודה – החלק הראשון מבצע פעולה מתמטית על שדה המדינה, והחלק השני מבצע פעולה מתמטית על התאריך.

2. כעת ננסה יחד לפענח את **החלק השני** (מימין לנקודה), הקשור לתאריך. נסו להבין אילו תאריכים ניתן להזין? מה גיליתן? מה המידע הזה יכול לתת לנו?

|  |
| --- |
| אפשר להזין את התאריכים : 22.3/23.3/24.3/25.3/26.3  התוכנה חוזה את המתקפות שלה 5 ימים קדימה, ה checksum , כנראה מוסיף 5 ימים לתאריך הנוכחי |
| *תשובה* |

3. שלחו בעזרת התוכנה מספר בקשות שונות, שבכל אחת יהיה הבדל קטן בתאריך. כתבו עבור כל תאריך את הצ'קסאם שהוא יצר:

|  |
| --- |
| 26.3.2022 – 17  25.3.2022-16  24.3.2022- 15  23.3.2022 - 14 |
| *תשובה* |

4. נסו לבחון את ההבדלים בין ה-Checksums וכיצד הם קשורים לתאריכים השונים. הצלחתן להבין כיצד הוא מחושב? לאחר שהבנתן כיצד מחושב החלק השני של ה-checksum, הסבירו זאת:

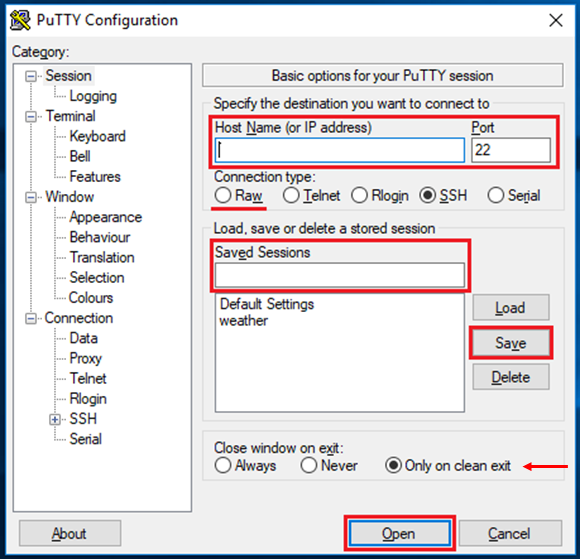
|  |
| --- |
| ככל שהתאריך הוא מאוחר יותר, כך ה checksum גדל – המספר "ברירת המחדל" ממנו התחלתי הוא 17 ובהתאם לתאריכים הוא יורד או עולה – הקבועים שלנו הם החודש והשנה(ובחודש המספר 0 לפני הספרה)  הcheacksum מחושב באופן שבו הוא מחבר את כל הספרות בתאריך |
| *תשובה* |

**הצלחנו לפענח כמעט את כל הפרוטוקול של השרת! אנחנו כבר ממש מתחילות להבין איך הוא עובד. עכשיו נתחיל לנסות לתקשר איתו בעצמנו...**

**שלב 6 - התחברות לשרת ב-Telnet**

1. כעת נרצה להתחיל לעבוד על להחליף את תפקיד התוכנה ולדבר בעצמנו עם השרת. לשם כך אנו זקוקות ל-IP ולפורט בו התוכנה פונה אל השרת (הפורט שמעניין אותנו הוא הפורט **בצד השרת** אשר נשאר תמיד קבוע ולא הפורט שנפתח אצלנו שהוא אקראי). באמצעות מידע זה נוכל ליצור חיבור חדש אל השרת של ההאקרים.

2. נפתח את תוכנת ה-Telnet שלנו (נכתוב putty, בשורת ה-run), יפתח לנו החלון הבא שאנו מכירות:



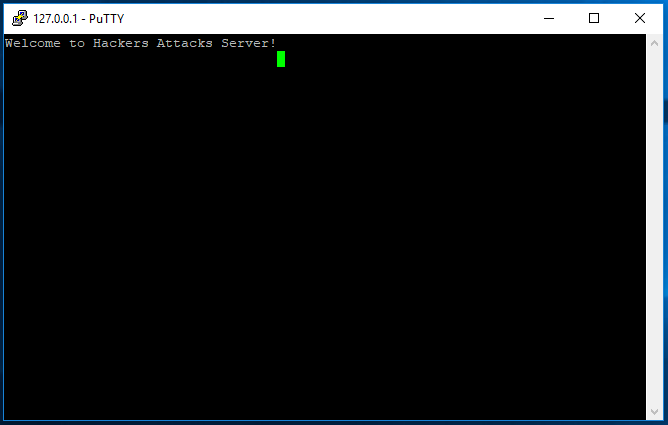
3. בחלון נמלא את השדות הבאים:

* **Host Name** - ה-IP של השרת
* **Port** - מספר ה-Port אליו מאזין השרת
* **Connection type** - נבחר ב-Raw
* **Saved Session** - ניתן שם חדש לבחירתנו ל-session שיצרנו
* **Close window on exit** - נבחר ב"Only on clean exit" (כך שחלון השיחה לא יסגר לנו)

לאחר מילוי השדות נלחץ על: Save.

4. נפתח את ה-Session שיצרנו שאמצעות הכפתור Open. לחיצה על Open תיצור את החיבור לשרת באמצעות הפרטים שהזנו.

אם הצלחתן להתחבר כמו שצריך אתן אמורות לראות את הודעת הפתיחה של השרת:



אם לא הצלחתן להתחבר בדקו שבחרתן את ה-IP והפורט הנכונים שוב.

5. שלחו לשרת את ההודעה "Hello" וכתבו מה התשובה שהוא שלח:

|  |
| --- |
| 500:ERROR:arguments invalid |
| *תשובה* |

**טיפ:** כדי להעתיק טקסט ב-Putty יש לסמן את הטקסט וללחוץ על כפתור ימני בעכבר.

כדי להדביק נלחץ על כפתור ימני בעכבר.

6. התחברו שוב והפעם כתבו לשרת הודעה חוקית (הודעה זהה לחלוטין לאחת שהסנפתן מהפעולה של התוכנה). אם לא קיבלתן תשובה נסו מספר פעמים נוספות. אם הצלחתן לקבל תשובה, כתבו את ההודעה ששלחתן וצרפו צילום מסך של התשובה של השרת.



|  |
| --- |
|  |
| *תשובה* |

7. כתבו הודעה זהה מלבד שדה אחד: בקשו את התאריך של מחר. זכרו, כעת גם ה-Checksum צריך להתעדכן. כתבו מה ההודעה שהשרת החזיר:

|  |
| --- |
| 200:ANSWER:country=israel&attacks=8&date=23/03/2022 |
| *תשובה* |

8. בחרו מדינה אחרת, ובקשו את תחזית המתקפות שלה ב-telnet. שימו לב, כדי לעשות זאת תצטרכו לחשב את החלק הראשון של ה-Checksum בעצמכן, ללא עזרת התוכנה! אבל איך נחשב סכום לשדה המורכב מאותיות? לפני הסכימה נמיר כל אות למספור שלה ב-ABC, למשל את האות A נמיר ל-1, את האות B ל-2 וכן הלאה (אין משמעות לאותיות גדולות/קטנות). כתבו את הבקשה ששלחתן והוסיפו תצלום מסך של התשובה שהחזיר השרת.



|  |
| --- |
|  |
| *תשובה* |

9. שלחו בקשה חדשה לשרת, נסו לשנות את הבקשה כך שנוכל לקבל מידע חדש נוסף. הוסיפו תצלום מסך של התשובה של השרת וכתבו מה לדעתכן מידע זה אומר.



|  |
| --- |
| 100:REQUEST:country=Israel&date=26/03/2022&checksum=64.17&more\_info=yes  ב more\_info במקום no שמתי yes  זה הציג לי את סוג המתקפה, ומיקום ספציפי שלה |
| *תשובה* |

**זהו! סיימנו לאבחן את כל הפרוטוקול של השרת ואפילו הצלחנו לתקשר איתו בעצמנו ולגלות עוד המון מידע חדש!**

**עכשיו אנחנו מוכנות לשלב הבא - נשתמש בכל מה שגילינו על מנת להוציא כמה שיותר מידע מהשרת באמצעות תוכנה משלנו..!**

**(המשך בחלק ב' של המשימה)**