

***המשימה חלק ב: ללמוד את האויב***

כמו שאנחנו יודעות, קבוצת ההאקרים עדיין פועלת כדי לבצע תקיפות ברחבי העולם.

כבר הצלחנו לעלות על הפרוטוקול שלהם, הפעם הגיע הזמן לכתוב קוד ששולח בקשות אל השרת שלהם. בצורה זו נוכל לחלץ מידע חשוב על תקיפות מתוכננות, וכך אולי נוכל למנוע את המתקפות הבאות!

אבל איך נשלח בעצמנו בקשות לשרת?



מזכיר לכן משהו?

נכון! Socket!

הפעם נצטרך לבנות לקוח משלנו אשר עושה את התפקיד שעד עכשיו עשתה התוכנה. הלקוח שלנו צריך לעבוד בהתאם לפרוטוקול שגילינו, באמצעות Socket.

כדי להפיק תועלת מהמידע, התוכנית שלנו תוציא מידע מהשרת ותציג את המידע הרלוונטי בצורה של "לוח חכם" (Dashboard). מה הכוונה? התוכנית תדאג שנוכל לראות בכל רגע נתון את המידע **הקריטי ביותר והמעודכן ביותר**, בצורה נוחה לצפייה.

**שלב 1 - פניה בסיסית אל השרת**

בשלב הראשון נכתוב תוכנית צד לקוח המשתמשת ב-sockets על מנת לפנות לשרת ולקבל מידע - כמובן על פי הפרוטוקול אותו איבחנו בשלב א' של המשימה. בשלב זה נכתוב תוכנה דומה לזו שמצאנו על מחשב התוקפים, בשלבים הבאים נשכלל את התוכנה.

התוכנית תקלוט מהמשתמש:

1. שם של מדינה (למשל: Israel)
2. תאריך (בפורמט 20/02/2021)

התוכנית תדפיס את **מספר המתקפות המתוכננות** למדינה שהתקבלה בתאריך שהתקבל.

אם חזרה שגיאה מהשרת - התוכנית תציג את השגיאה בדיוק כפי שהתקבלה מהשרת.

שימו לב: בעבודה עם sockets חישבו האם אנחנו צריכים להשתמש ב TCP או ב UDP, וכתבו את הקוד בהתאם.

דגשים כלליים:

* שכחתם מהו הפרוטוקול של תוכנת המתקפות? היעזרו בחלק א' של המשימה או הריצו את התוכנה, הסניפו את התעבורה ובדקו את Follow TCP Stream.
* זכרו שחלק מהפרוטוקול הוא שדה ה-checksum שצריך להיות מחושב לפי התאריך והמדינה.
* משהו לא עובד? בדקו שאתם שולחים את ההודעה הנכונה לשרת בעזרת Wireshark.

**שלב 2 - שכלול התוכנה**

בשלב זה נשכלל את התוכנה עליה התחלנו לעבוד בשלב 1 (מומלץ להעתיק את קובץ הקוד של שלב 1, ולעבוד על הקובץ החדש, כך שתהיה לכן גרסה עובדת בצד).

כעת נרצה להשתמש בכל המידע שגילינו על הפרוטוקול איתו עובד השרת בשלב א' של המשימה, על מנת להרחיב את הפונקציונאליות של התוכנה המקורית. כפי שתיארנו, נרצה שהתוכנה שלנו תדע להציג את המידע בצורה של "לוח חכם", כלומר, תציג תמיד את המידע העדכני והרלוונטי ביותר בהתאם למדינה שמזין המשתמש.

**התוכנה תקלוט מהמשתמש שם של מדינה, ותציג לו את המידע הבא**: (שימו לב שהתוכנה תציג את כל המידע, המשתמש לא יצטרך לבחור)

### א. עדכון יומי

התוכנה תציג את כל המידע הקיים עבור המדינה, אשר רלוונטי לתאריך של היום: כמות המתקפות, יעד התקיפה וסוג המתקפה. המשתמש לא יצטרך להזין את התאריך בעצמו, התוכנה תדע לבד מהו התאריך של היום.

רמז: לצורך כך תצטרכו להשתמש בטיפוס חדש מסוג תאריך. חפשו באינטרנט כיצד ניתן להשיג את **התאריך של היום** באמצעות האובייקט **datetime** (הקיים בפייתון). כמו כן, קראו על פונקציה שיש לו הנקראת **strftime**, לצורך התאמת הפורמט של התאריך לפורמט בו אנחנו צריכים להשתמש עם השרת שלנו.

פלט לדוגמה:

Daily Update for country Israel:

date:07/03/2021 attacks:4 target:Hospital attacks\_type:DDos

**ב. מידע על מדינות בסיכון גבוה**

כפי שיגילינו בשלב א' של המשימה, השרת מחזיק מידע על מדינות רבות. אנו נרצה לנצל את המידע הזה כך שנוכל ב"לוח החכם" לראות בנוסף למדינה עליה מוצג המידע כרגע, את המדינות אשר נמצאות בסיכון גדול למתקפות מרובות מצד קבוצת ההאקרים.

בקובץ הנמצא בתיקייה - countries20.txt, תמצאו רשימה של 20 מדינות בעולם. עליכן להציג מתוכן רק את המדינות אשר מתוכננות בהן מעל ל-20 מתקפות (נכון להיום). עבור כל מדינה הציגו את שמה ואת **כמות המתקפות המתוכננות בה נכון להיום** (אין צורך בנתונים הנוספים).

שימו לב כי הקובץ מכיל מידע נוסף מעבר לשמות המדינות. חלצו מתוכו את המידע אותו אתן צריכות.

פלט לדוגמה:

Countries with more then 20 attacks today:

country:china attacks:45

country:indonesia attacks:38

country:iran attacks:40

דוגמה **לפלט מלא** של התוכנה:

Please enter a country name: Israel

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Daily Update for country Israel:

date:07/03/2019 attacks:4 target:Hospital attacks\_type:DDos

Countries with more then 20 attacks today:

country:china attacks:45

country:indonesia attacks:38

country:iran attacks:40

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**הוראות הגשה עד לשלב זה:**

יש להגיש את קובץ הקוד של שלב 2 בלבד, שמרו אותו בשם dashboard.py, והעלו אותו יחד עם הקבצים האחרים אותם תצטרכו להגיש (בסיום השלב הבא) תחת השבוע המתאים.

**וואו! תראו כמה מידע נוסף התוכנה שלנו מציגה לעומת התוכנה המקורית שמצאנו! אין ספק שמידע זה יהיה קריטי בלמידת האויב ובמניעת מתקפות עתידיות!**

**שלב 3 - ביטול תקיפות שמתרחשות בזמן אמת**

חקרנו את התוכנה שנמצאה במחשב של ההאקר והבנו איך הפרוטוקול עובד, גילינו מידע על התקיפות הבאות של קבוצת ההאקרים! אבל המשימה לא הושלמה וכעת הגיע אלינו **מידע חדש!**! נתרכז רק בו בשלב הזה.

סוכני ה-FBI מצאו על המחשב של התוקף קבצים נוספים, והצליחו להבין שהקבצים קשורים למערכת נפרדת שההאקרים משתמשים בה כדי לנהל את התקיפות ש**מתבצעות ממש ברגע זה**!! קובץ אחד נראה כמו גישה מרחוק אל מערכת הניהול, דרך פקודות CMD. יתר הקבצים מכילים קוד, נראה שהוא קשור למערכת, אבל הקוד לא שלם. מעבר לקבצים, נמצא המייל האחרון שנשלח מהמחשב. זהו המייל שנמצא:

|  |  |  |
| --- | --- | --- |
|  | **מאת** | SmAri0 |
| **אל** | $LuIg1 |
| **נושא** | הודעה דחופה!! לקרוא הכל |
| **קבצים מצורפים** | **^^^.py, @@@.py, &&&.py, ATTACKS\_CMD.exe** |
| שומע, נראה לי שה- FBI עלו על הפעילות שלנו וראו מה נמצא על המחשב שלי. אין לי הרבה זמן!  לא הספקתי לכתוב את המודול החדש עד הסוף אז אני מצרף את הקבצים למייל.    כמה דברים חשובים:   * בדקנו כבר את צד הלקוח וקיבלנו אישור, אז לא צריך לשנות אותו * מהרתי לכתוב את השרת, אז אולי יש בו קצת טעויות. כתבתי בהערות בקוד מה לא עובד כרגע, לפחות ממה שהצלחתי להבין * אם הצלחת לעשות את בקשת ה-TEST, תנסה את הפעולות האחרות * כדי שהתקשורת תהיה מוצפנת ברשת, הצפנתי חלק מהמידע     אני מקווה שלא יפסיקו את הפעילות שלנו, אחרי שנסיים המערכת תהיה סוף סוף מוכנה ונוכל לראות ולשלוט בכל מה שרץ כרגע בקלות  להתראות חייב לרוץ  SmAri0 | | |

**המטרה שלנו:**

**אם נצליח להבין איך להשתמש בניהול המערכת דרך כלי ה-CMD, נוכל לבטל את כל התקיפות שפעילות כרגע! כלומר להפוך אותן להיות בסטטוס "canceled".** בשביל לעשות את זה נדרשת חקירה מעמיקה. כאן אתן נכנסות לתמונה- חקרו את הקבצים ונסו להבין מה יש בהם ומה הם עושים, ואיך ניתן לבטל את כל התקיפות הפעילות במערכת דרך הגישה המרוחקת ב-CMD.

**דגשים:**

* **הקבצים נמצאים בתיקיות שלכן, תחת תיקיית "שלב 3" בתוך זיפ בשם live\_attacks.zip.** בשלב זה נשתמש רק בקבצים האלו, ללא שימוש בקוד משלבים 1-2
* **הוראות הגשה לשלב זה:** יש להגיש את קובץ הקוד של השרת של המערכת, לאחר תיקונים ותוספות. בנוסף יש לשמור את המסמך הנוכחי כ-word, לענות על השאלות הבאות, ולשלוח בשבוע המתאים.
* אין צורך לשנות או להגיש את קבצי הקוד של צד הקליינט, אבל כן ניתן ורצוי לשנות אותם ולהעזר בהם כדי לתקשר עם השרת, כדי לחקור וכדי לשלוח דברים שונים ולקבל מידע מהשרת.
* התרגיל הוא בעל אופי מחקרי, זה אומר שלא נבין ונדע את הכל מההתחלה וזה בסדר. אם לא נבין מאיפה יש לנו מידע מסויים או מה לעשות עכשיו, נחזור להסתכל על מה שכן יש לנו ולנסות כל מיני כיוונים.

**יצירת תקשורת**

קודם ננסה ליצור תקשורת בין השרת ללקוח. כדי לעשות את זה נצטרך לתקן או להוסיף קוד לשרת, כך שיצליח לתקשר עם הקליינט. העזרו בהערות שהשאיר ההאקר בקובץ. ניתן גם להעזר בקוד מתרגילים קודמים.

קודם נגרום לכך שקריאת TEST תצליח ותחזיר תשובה לקליינט. ענו על השאלות:

1. כאשר קריאת TEST אל השרת מצליחה, מהי התגובה שהקליינט מקבל מהשרת?

|  |
| --- |
| Connected successfully |
| *תשובה* |

2. האם השרת, כפי שההאקר כתב אותו, יכול להמשיך להאזין לבקשות, אחרי שכבר שלח תגובה לקליינט אחד?

|  |
| --- |
| לא |
| *תשובה* |

3. וודאו שלאחר תיקון השרת אצלכם בקוד, הוא מסוגל לענות למספר קליינטים, ולא רק לאחד בכל ריצה שלו. איך עשיתן את זה?

|  |
| --- |
| הוספת לולאת לעולמים |
| *תשובה* |

4. אילו תיקונים או שינויים נוספים עשיתן כדי להצליח לקיים תקשורת בין שרת ללקוח?

|  |
| --- |
| היה צריך להמיר את ההודעה שהשרת קיבל decode(), לשנות את הפורט לפורט שעליו השרת עובד (1050) , לשנות מ sent ל )send בקבלת הודעה מהשרת), לשנות מ client ל conv |
| *תשובה* |

**הבנת הלוגיקה**

5. כעת שחקו קצת עם התקשורת בין צד לקוח לשרת, ועברו על הקוד. מה עושה כל קובץ? כתבו תאור כללי במשפט - מה מטרת הקוד של כל קובץ? כתבו בטבלה הבאה:

|  |  |
| --- | --- |
| מטרת הקוד | שם קובץ הקוד |
| השרת, מודיע לנו אם הצלחנו להתחבר אליו או לא, מראה לנו את "מאחורי הקלעים" | ^^^.py |
| הלקוח מבקש מאיתנו שם של מדינה ונותן לנו פרטים עליה, למשל:  תעודת הזהות שלה ,חבר קבוצה,סוג מתקפה | @@@.py |
| נותנת לנו קוד שבעזרתו אנחנו יכולים לבטל את התקיפה על אותה המדינה  ב CMD | &&&.py |

6. נתמקד בצד השרת- באילו פעולות צד השרת תומך? עבור כל פעולה איזה מידע הוא מקבל, ואיזה שולח חזרה? תארו את ההודעה הנשלחת לשרת בכל פעולה ואת הפלט שחוזר, והוסיפו דוגמאות, בטבלה הבאה (אין צורך לתאר תשובה במקרה של שגיאה, ואין צורך לפרט את אופן ההצפנה של השרת)

|  |  |  |
| --- | --- | --- |
| שם פעולה | מה השרת מקבל  **(הוסיפו דוגמא לקלט)** | מה השרת מחזיר  **(הוסיפו דוגמא לפלט)** |
| התחברות(TEST) | **תיאור**:הרצה של אחת הלקוחות  **דוגמא**: TEST:Connection | **תיאור**: הודעה הצלחת התחברות  **דוגמא**: Connected successfully |
| ID(INFO) | **תיאור**: ID של מדינה מסוימת, כלומר הודעת ביטול מתקפה  **דוגמא**: CANCEL\_COMMAND:102 | **תיאור**: תוכן מוצפן  **דוגמא**: <))<:2+0}p:}A1kddj |
| שם מדינה(INFO) | **תיאור**: השרת מקבל שם של מדינה  **דוגמא**: ISRAEL | **תיאור**: תוכן מוצפן  **דוגמא**: ihq\*N/TRqM54\*54/6 |

7. מי מחברי קבוצת ההאקרים אחראי על התקיפה שמתרחשת בספרד?

|  |
| --- |
| CorAl |
| *תשובה* |

8. מהי פקודת הביטול של התקיפה שמתרחשת בצרפת?

|  |
| --- |
| -c Al2993 |
| *תשובה* |

**אז מה המשימה? מה צריך לעשות?**

אנחנו רוצים לבטל את כל התקיפות שראינו שפעילות כרגע.

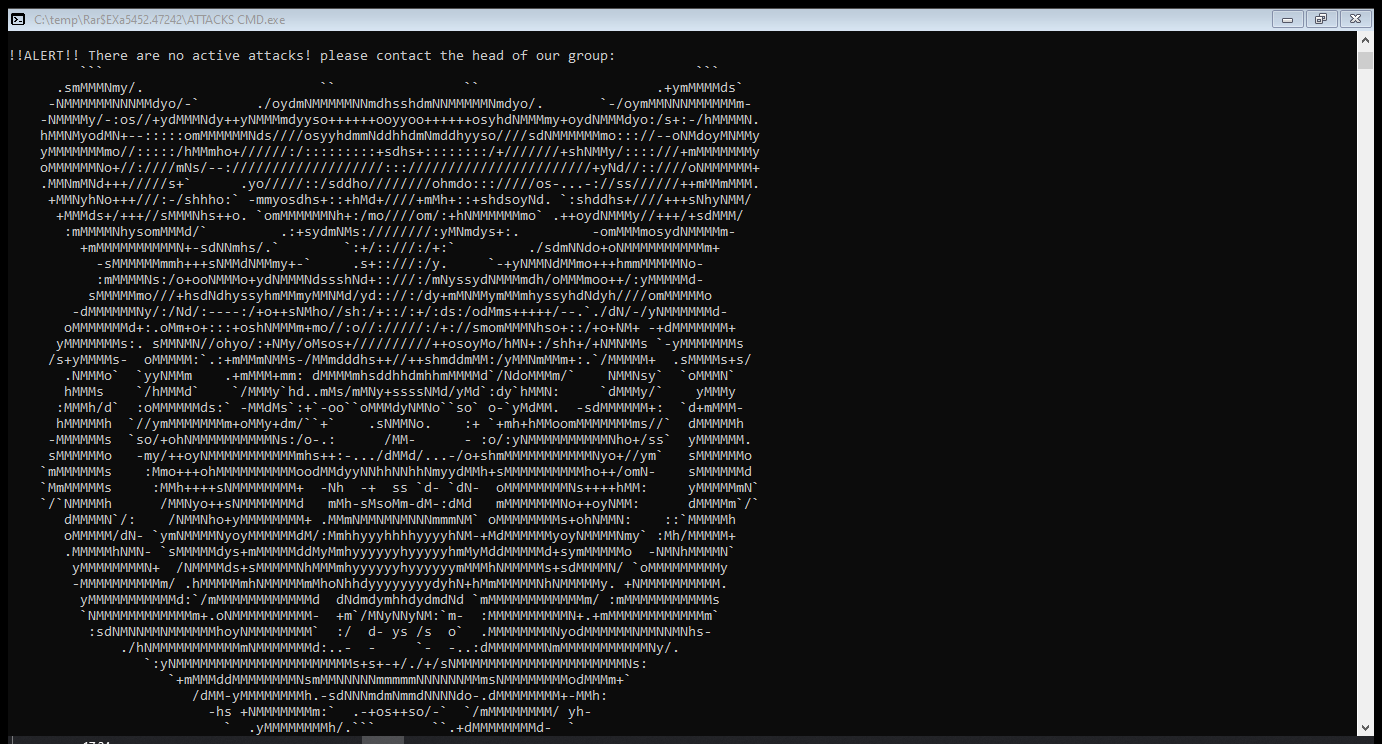
9. לפי החקירה וכל המידע החדש שגילינו, אילו פקודות אפשריות להרצה ב- ATTACKS\_CMD? ענו בעזרת הטבלה הבאה:

|  |  |
| --- | --- |
| פקודה | מה היא עושה |
| show -s active | מראה לנו את המתקפות שקורות עכשיו |
| פקודת ביטול מתקפה(משתנה מ ID ל ID של מדינה, דוגמה: ב 8) | מבטלת מתקפה של מדינה ספציפית |
| show -s canceled | מראה לנו את המתקפות שהתבטלו |
| show -all | מראה לנו את כל המידע |

10. בצעו קריאות לשרת לפי הצורך ולבסוף בטלו תקיפה אחת ב-CMD. מה עשיתן על מנת לבטל תקיפה? תארו לא רק פעולות של השרת אלא כל פעולה שהייתן צריכות לעשות, כולל לפני/אחרי קריאות לשרת וכולל פקודות בכלי ה-CMD.

|  |
| --- |
| ביקשתי מהלקוח @@@ מידע על מדינה, למשל SPAIN, קיבלנו את ה ID של המדינה וביקשנו מהשרת &&& שיביא לנו את הפקודה לביטול המתקפה, לאחר מכן את ההודעה שקיבלנו מהשרת הרצנו בcmd והמתקפה התבטלה. |
| *תשובה* |

11. המשיכו ובטלו את כל התקיפות. צרפו תמונת מסך שמראה את כל התקיפות כשהן בסטטוס מבוטל





12. מה הכינוי של ראש ארגון ההאקרים שמבצע את התקיפות?

|  |
| --- |
| BlackTiger |
| *תשובה* |

13. **שאלת בונוס!**

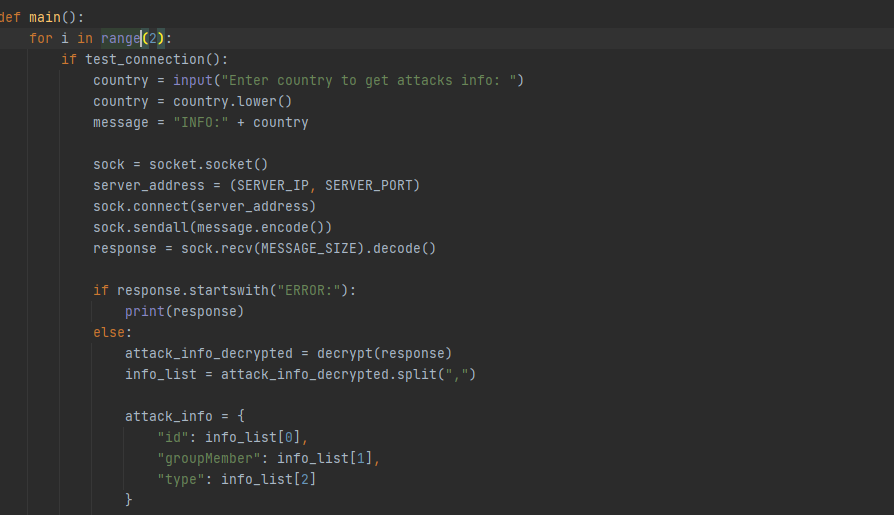
תארו את אלגוריתם ההצפנה של הנתונים בשרת. ב 1-2 משפטים ותאור כללי- איך מתבצעת ההצפנה?

|  |
| --- |
| ההצפנה עובדת על הקוד ASCI , היא לוקחת כל אות שנמצאת במחרוזת, ומחסירה ממנה את הקוד של התו ' ' ואת זה שומרת במשתנה, אחכ היא מוסיפה ל ' ' 93 ומחסירה ממנו את המשתנה. |
| *תשובה* |

14. **שאלת בונוס!**

השרת מאזין לכמה לקוחות. אבל כל לקוח מבצע רק פניה אחת אל השרת, מקבל תשובה ומיד נסגר. למה לברוח כלכך מהר? אולי יש עוד פעולות לעשות? אפשר לדמיין את זה כמו לקוח שמגיע לדואר כדי לבצע שתי פעולות- לשלוח חבילה ולקנות מעטפות. הוא ישלח את החבילה, ואז יקח מספר חדש לתור ויחכה מחדש את כל התור, כדי לקנות מעטפות! כלומר יגיע מחדש אל הנציג בדוכן כאילו היה לקוח חדש.

שנו את אחד מקבצי הלקוחות כך שיבצע פעולה מול השרת, ואחרי קבלת התשובה ישלח הודעה נוספת, בלי לסגור את הsocket. לדוגמא, נוכל לבצע פעולת TEST ומיד אחריה פעולת INFO, בלי לפתוח socket חדש.

ב main הוספתי לולאת פור שעובדת פעמיים(אפשר גם לכמות גדולה יותר של פעמים), וכך הלקוח יכול לפנות לשרת פעמיים, שניתי את שרת @@@:

**כל הכבוד!**

**הצלחתן לבטל את התקיפות הפעילות!!**

**ועל הדרך גם השגנו עוד מידע חשוב על הארגון**