שיעור 12

**תרגיל: 0rphan - הסוף**

המשטרה ממשיכה לחפש את ההאקר 0rphan, פושע ה-Ransomware המפורסם. כעת מתברר כי הוא ישראלי, עונה לשם אור פנדובסקי ועבד בעבר כאיש מכירות בחברת BUG, סניף רעננה. כדי למצוא איתו חברת BUG הסכימה לתת למשטרה גישה למערכת ניהול העובדים של החברה. על פי הדיווחים, המערכת שומרת את המיקומים המדויקים מהם התחבר 0rphan לשרת, אך אבוי - התוכנה של BUG לא עובדת ואף אחד לא יודע למה. עזרו למשטרה למצוא פרטים על מיקומו הנוכחי של 0rphan שיעזור להם למצוא אותו.

**שלב א'**

פתחו את תוכנת העובדים של BUG המצורפת בקובץ BugClient.zip ונסו לדלות ממנה מידע אודות הכניסות של 0rphan למערכת.

לצורך הפתרון עליכם להשתמש בכל הכלים אשר למדנו השנה –

Wireshark, Putty, קובץ hosts

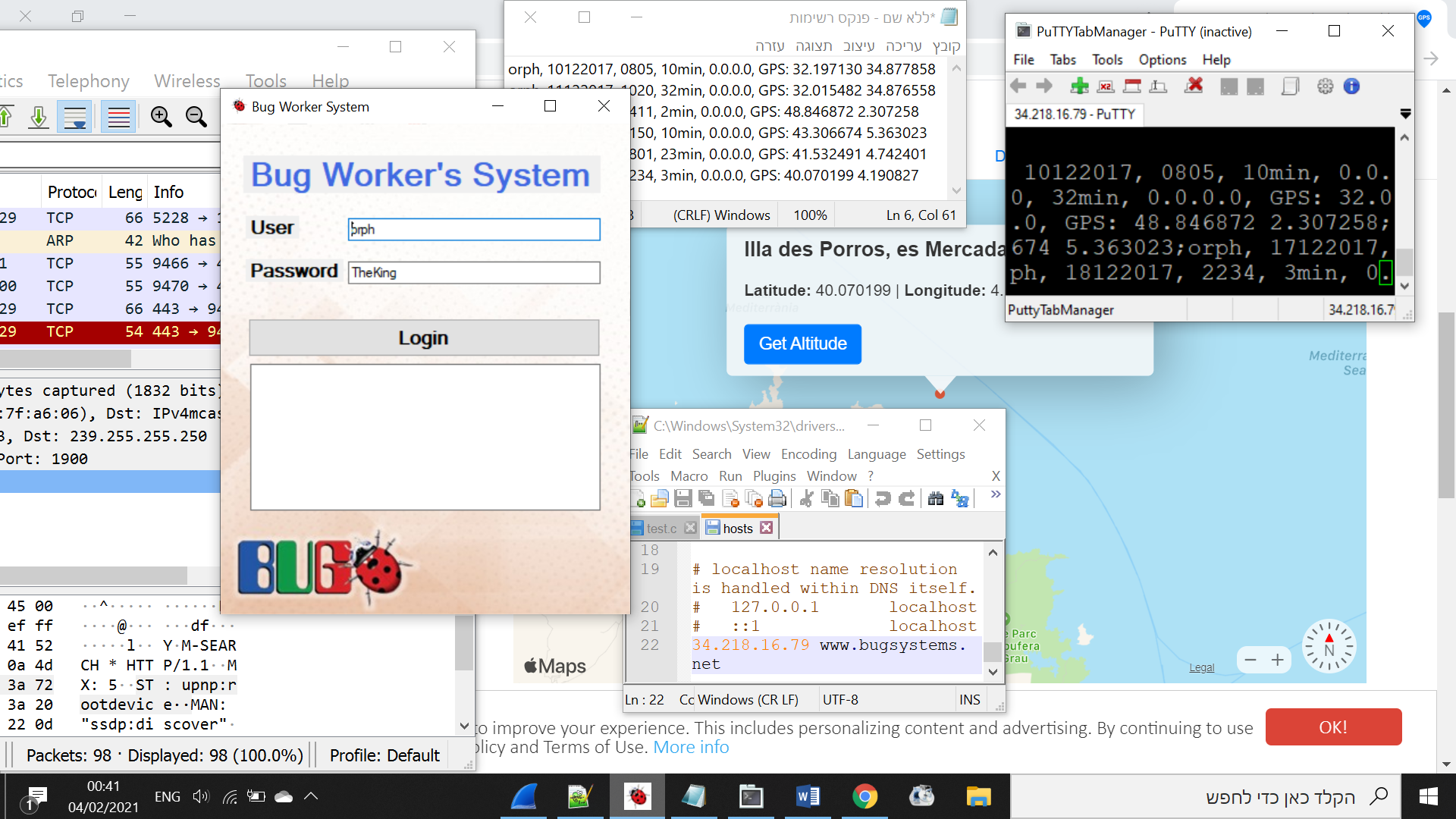
משימתכם היא למצוא את מסלול הבריחה של 0rphan (בתחנות).

בהצלחה!

1. מהם המיקומים בהם שהה 0rphan? איפה הוא נמצא כיום לדעתכם?

|  |
| --- |
| רעננה – קניון רננים, ישראל  רמלה, ישראל  פריז, צרפת  ארונדיסמנט(?), צרפת  הים התיכון  חופי ספרד  אני חושב שהוא נמצא בספרד |

1. ספרו מהו התהליך אותו עשיתם כדי להגיע לפתרון. נסו לפרט ככל האפשר. צרפו צילום מסך רלוונטי.

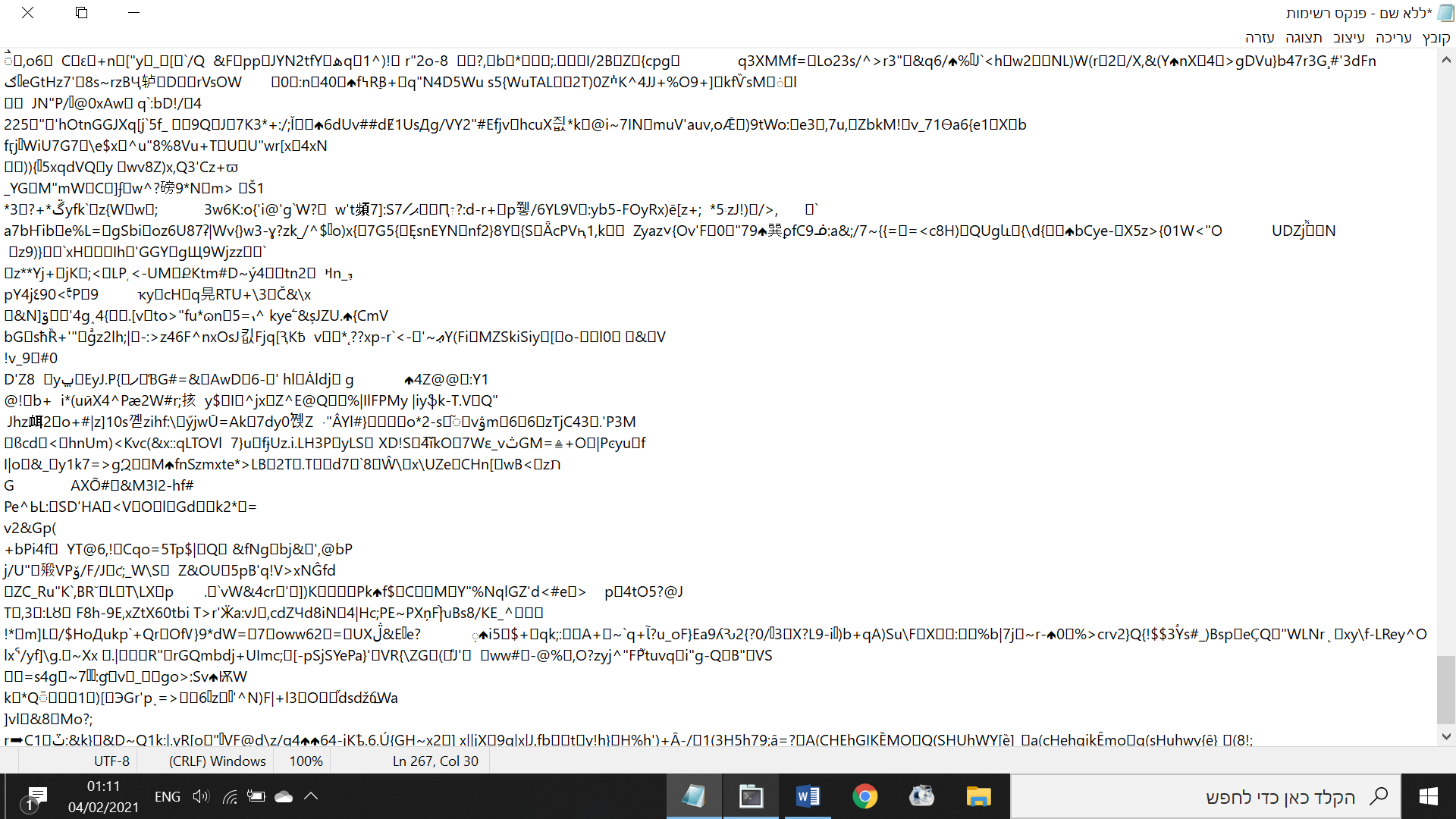


|  |
| --- |
| פתחתי את התוכנה, (נתקעתי (אחבג עזר לי)), חיפשתי בגוגל את bugsystems.net, ראיתי שצריך טלנט, ניסיתי להתחבר אבל משום מה ניסיתי את זה עם פורט 80 וHTTP, אחבג עזר להבין שזה לא דווקא 80, הסנפתי שזה 333, פתחתי טלנט מחדש, אמר לי להחליף IP, התעכבתי על מה לכתוב, ואז הבנתי מה צריך לעשות, שיניתי את הקובץ הוסטס ככה שהאייפי החדש יהיה לכתובת הישנה גם לתכנה, פתחתי את התכנה מחדש, לא מצאתי מיקום, הסנפתי, עקבתי אחרי ההוראות בהסנפה, הוספתי FULL לאחת הפקודות כדי לקבל מיקום, תרגמתי גי פי אס למיקום במילים, כתבתי אותו. |

**שלב ב'**

על פי הדיווחים, בחשבונו של 0rphan ב-BUG אוחסן קובץ שעשוי להיות משמעותי למציאתו. נסו להוריד אותו.

1. צרפו צילום של הקובץ והסבירו כיצד השגתם אותו.



|  |
| --- |
| נכנסתי לחשבון של אורפן שוב, ועשיתי את הרשימת קבצים, מצאתי שם את הקובץ גיפ, והורדתי אותו כמו שהם אמרו, אחרי זה פשוט תרגמתי אותו בבייס64 |

**בונוס - שלב ג'**

בחקירה התברר כי מנהל המשמרת בסניף BUG בו עבד 0rphan, דידי רם, שיתף איתו פעולה בתכנון הפשעים. נסו למצוא בפרוטוקול **חולשה** שתאפשר לכם להשיג מידע מפליל אודות.

1. הסבירו מהי החולשה בפרוטוקול וכיצד ניתן לנצל אותה. צרפו צילום של הקובץ שמצאתם.

|  |
| --- |
| החולשה היא שאם אתה כבר מחובר למשתמש אחד, אתה יכול להתחבר לכל משתמש בלי הסיסמא(!)  אבל- לא הצלחתי להפוך את הטקסט לתמונה ואני מאוד עצוב בנוגע לזה ☹, אבל כן הצלחתי להוריד את כל הקבצים |