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 –

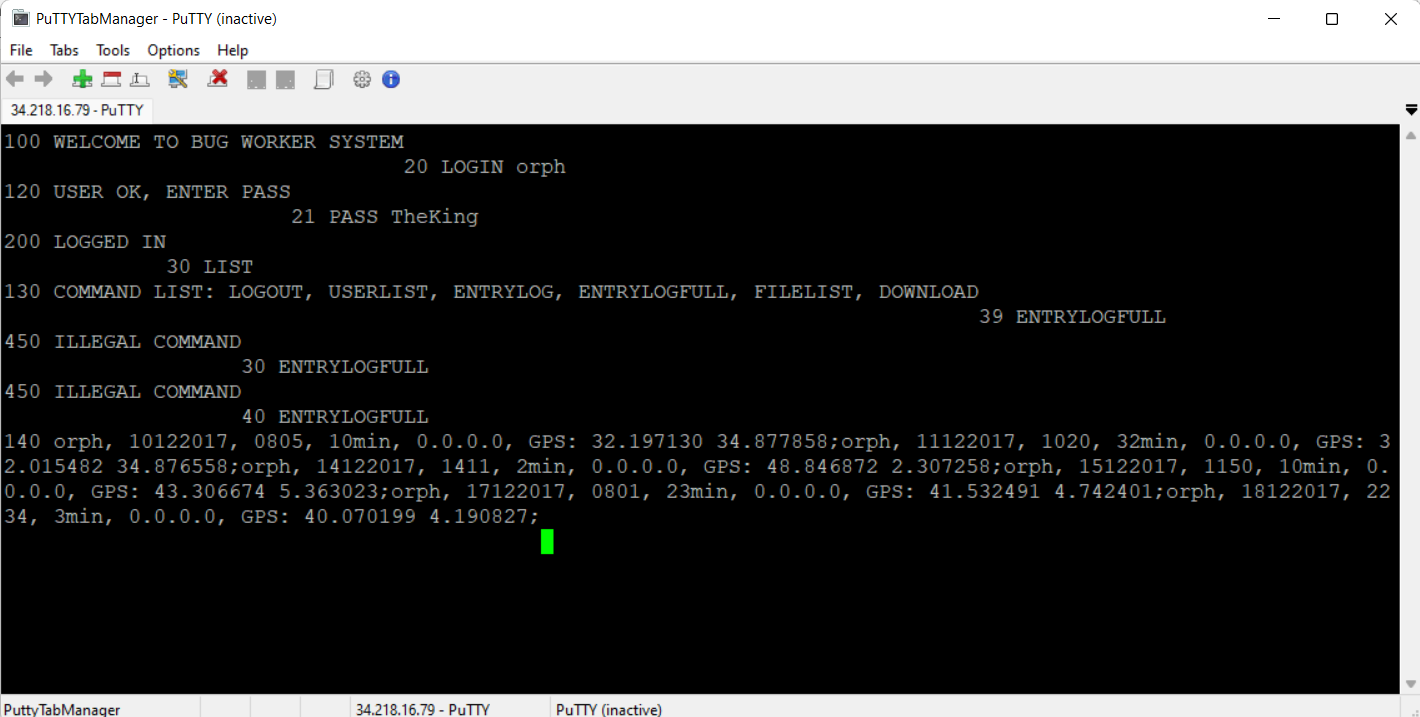
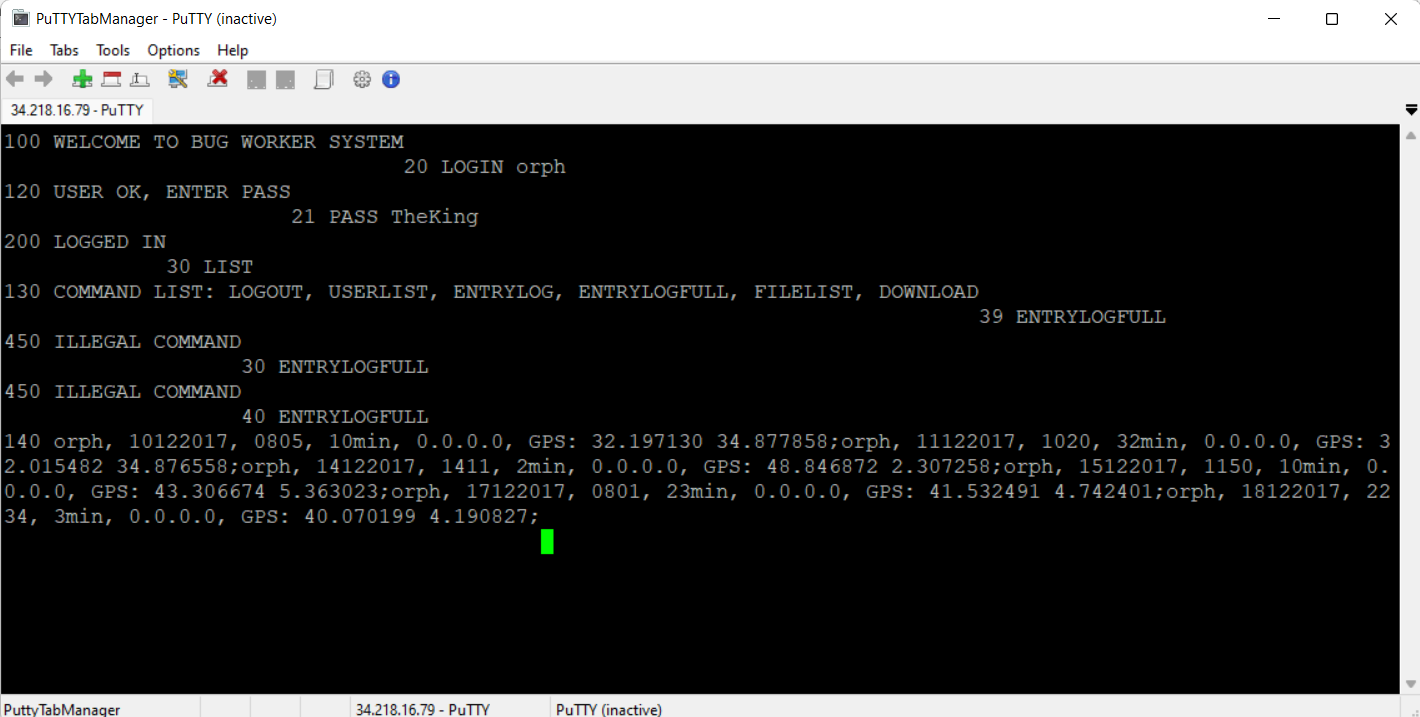
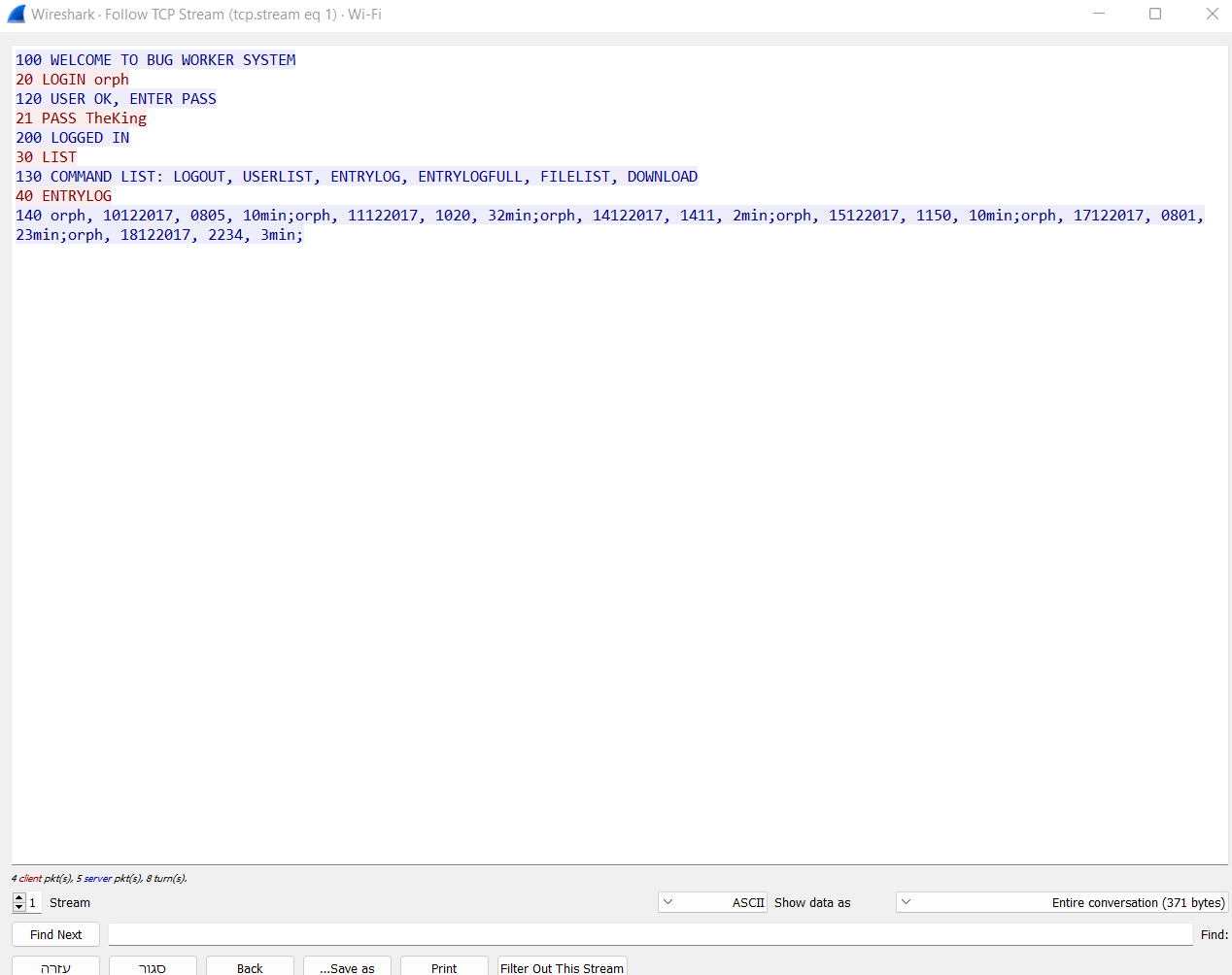
Wireshark, Putty, קובץ hosts

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

בהצלחה!

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

|  |
| --- |
| 1. קניון רננים ברעננה  2. במסלול 26\8 בנתבג  3. בפריז.  4. נמל מרסיי  5. באמצע הים  6. בים ליד מנורקה |

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

|  |
| --- |
| יצרנו רשומת DNS מעודכנת על פי התגובה של השרת שהפנה אותנו לכתובת IP אחרת  נכנסתו בפותי לשרת על פי ההסנפה שעשינו בחיבור בווירשארק אחר שזה עבד  ואמרנו לו להביא לנו את הרשימה המורחבת |

**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.

|  |
| --- |
| בPUTTI שיחקתי ומצאתי פקודה לרשימת הקבצים ופקודה להורדה  השתמשתי בממיר אונליין להמרה מ BASE64 לתמונה |

**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.

|  |
| --- |
|  |