שיעור 9 – שכבת הרשת ו-IP

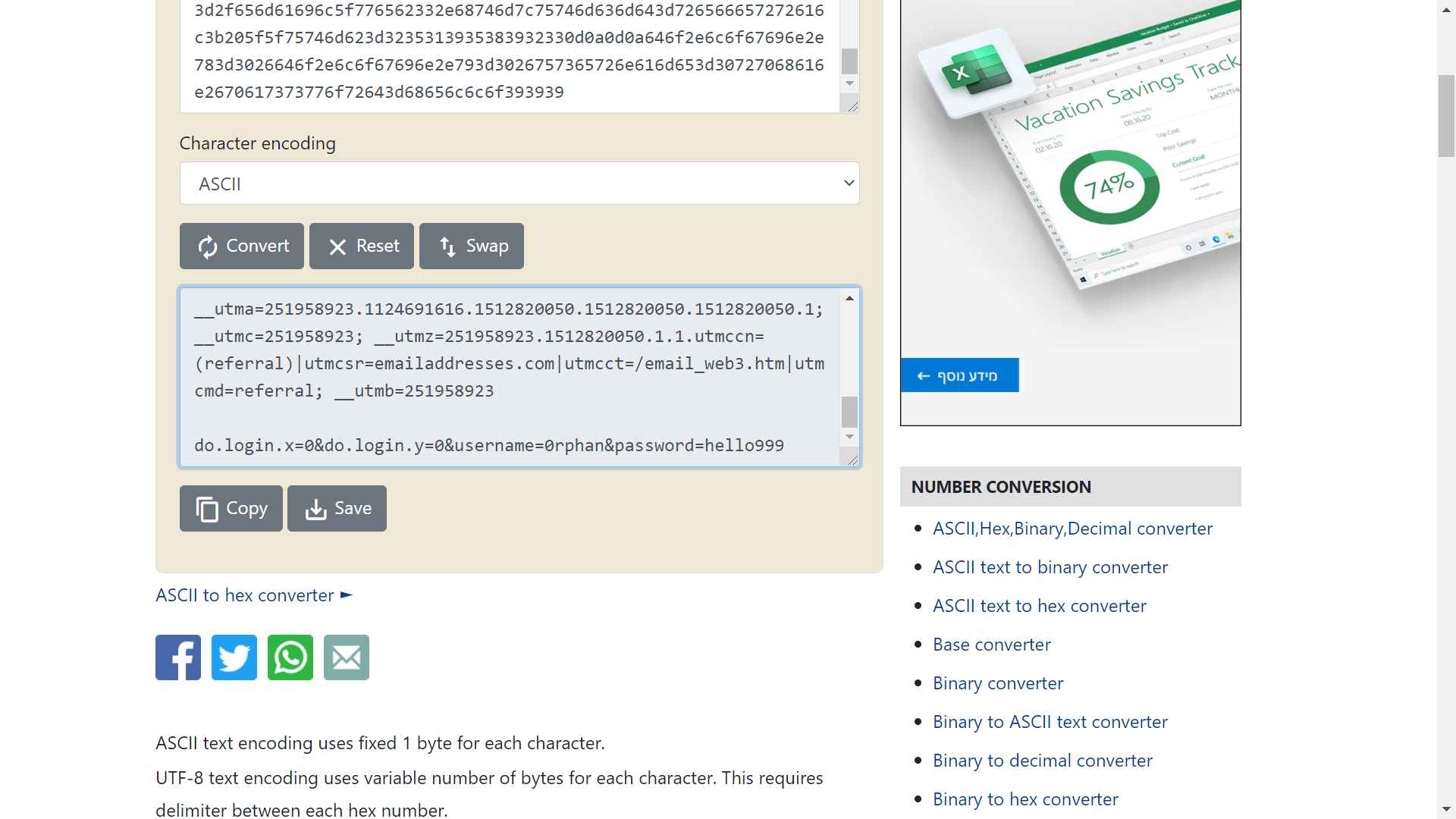
**תרגיל: הפעילות החשודה של 0rphan**

קהילת הסייבר הבינלאומית כולה במרדף אחר פושע הסייבר הבינלאומי 0rphan, שעל פי החשד גנב מאות אלפי דולרים מאנשים ברחבי העולם בעזרת מתקפות מסוג כופר (Ransomware). ידוע ל-FBI כי 0rphan בעל ידע נרחב במחשבים וכנראה עובד בחברת מחשבים, עם זאת הם לא יודעים מהי זהותו האמיתית והיכן הוא עובד. לאחרונה התרחשה פריצת דרך בחקירה - החוקרים הצליחו להשיג גישה למחשבו האישי של 0rphan ולהסניף בו תעבורה העוברת דרכו, אך למרבה הצער ההסנפות מעט משובשות. נסו לעזור לחוקרים לגלות מידע מההסנפות ולהבין איפה עובד 0rphan.

**חלק א'** – **ההסנפות החשודות**  
המשטרה הצליחה להשיג גישה למחשבו האישי של 0rphan ולהסניף את התעבורה העוברת דרכו, אך עקב החיבור הבעייתי חלק מההסנפות נפגמו והפרוטוקולים לא פוענחו על ידי Wireshark.  
  
בהסנפה מוצגת רק שכבה 2 (שכבת הקו עליה עוד לא למדנו ואפשר להתעלם ממנה), וה-Data שלה. **נסו לחשוב מהו ה-Data של שכבה זו (רמז – אנקפסולציה...).**  
  
פתחו את ההסנפה בקובץ 0rphan.pcap וענו על השאלות הבאות.

1. מצאו את החבילה בה יש נסיון כניסה לאתר אינטרנט. מה מספר החבילה ברשימה? כיצד זיהיתם את החבילה הזאת?

|  |
| --- |
| 5, דבר ראשון היא החבילה הכי גדולה מה שהפך אותה לחשודה, דבר שני כשמתרגמים את הHEX לASCII יוצא חבילת HTTP |

1. האם תוכלו למצוא את פרטיו האישיים של 0rphan בתוך הודעת ה-HTTP? צלמו היכן מצאתם אותם, וכתבו את הפרטים. 

|  |
| --- |
| username=0rphan&password=hello999  do.login.x=0&do.login.y=0& |

1. בעזרת ניתוח של שכבת הרשת (IP), נסו למצוא את כתובת ה-IP בה נמצא האתר אליו 0rphan מנסה להיכנס. כתבו את הכתובת. אם נמצא אתר בכתובת הזאת, נסו להיכנס אליו, וכתבו מהו האתר.

|  |
| --- |
| בהתחלה יש פקטה שמגיעה אל פייסבוק, אחריה רוב הפקטות הן ל <http://173.8.224.33/> שזה אתר שמציג את עצמו כsofthome.net, שזה כנראה מה שאתם רוצים... |

1. כעת נסו למצוא את כתובת ה-IP ממנה שלח 0rphan את הודעה זו. כתבו את הכתובת, והסבירו כיצד מצאתם אותה.

|  |
| --- |
| 10.200.0.1 זו הכתובת הפרטית, שמתי את הפקטה באתר לפירוק פקטות מסוג כזה וזה הfrom IP שיצא. |

1. האם תוכלו למצוא את מיקומה של כתובת IP זו בעולם? אם לא, מדוע?

|  |
| --- |
| לא, כי זו כתובת IP פרטית ולא ציבורית (היא מתחילה ב10...). |

1. האם בכל זאת תוכלו למצוא רמז כלשהו למיקומו הנוכחי של 0rphan מבקשת ה-HTTP?

|  |
| --- |
| אפשר לדעת לפי האזור זמן שהוא כנראה ב+1 מגריניץ', חוץ מזה לא הצלחתי למצוא כלום ואני עצוב ☹ |

1. בהסנפה קיימת גם בקשת DNS אשר נשלחה ממחשבו של 0rphan. חוקרי המשטרה מאמינים שהיא מצביעה על אתר כלשהו ברשת פנימית אליו נכנס 0rphan. האם תוכלו למצוא אותה? מהי כתובת האתר אליו מנסה 0rphan להיכנס?

|  |
| --- |
| bgworkers.com |

**חלק ב'** – **הרשת החשודה**

בעוד אתם מנתחים את ההסנפה החשודה, הצליחה יחידת הסייבר של ה-FBI להתחבר **מרחוק** למחשבו האישי של 0rphan ברשת פנימית כלשהי. בעזרת המידע שהשגתם מההסנפה, המשטרה בטוחה שתוכלו לסייע בהשגת מידע ממחשבו האישי, ואולי לגלות - **איפה עובד 0rphan?**

כדי לעשות זאת המשטרה שלחה לכם את כתובת ה-IP דרכה ניתן להתחבר למחשבו של 0rphan ברשת הפנימית. "תתחברו אליה ב-SSH, אתם בטח יודעים לעשות זה, הרי אתם מגשימיסטים, לא?..."

|  |  |
| --- | --- |
| **SSH – תעודת זהות** | |
| **שם מלא** | Secure Shell |
| **פותח ע"י** | טאטו ילונן (פינלנד) |
| **שנת פיתוח** | 1995 |
| **RFC** | [RFC 4253-4254](https://tools.ietf.org/html/rfc4253) |
| **שכבה** | אפליקציה |
| **פורט מוכר** | 22 |
| **טקסטואלי / בינארי** | בינארי |
| **Stateful / Stateless** | Stateful |

**אז מה זה SSH?**

**SSH** הוא פרוטוקול מאובטח המאפשר לקבל שליטה על מחשב מרוחק. השליטה מתבצעת באמצעות העברת פקודות בכתב במסוף שנקרא Shell. במילים אחרות, זהו למעשה מסך CMD שאפשר דרכו לבצע כל פעולה על המחשב. SSH היא הדרך הנוחה והנפוצה ביותר כיום לנהל שרתים מרחוק. כל התקשורת ב-SSH מוצפנת כך שזו גם נחשבת דרך בטוחה לעשות זאת. למזלנו, התוכנה האהובה Putty יודעת גם לנהל שיחות ב-SSH.

**התחברות לשרת**

1. השתמשו בפרטים שגיליתים בחלק א' אודות 0rphan ונסו להתחבר לשרת ה-SSH בכתובת **54.71.128.194** בפורט **2222** (הפורט המוכר של SSH הוא 22, אבל במקרה זה השרת בחר בפורט אחר). זכרו לסמן את האופציה של SSH במקום Raw.

**\*** לא מצליחים להתחבר? נסו להשעות באופן זמני את הפיירוול של חלונות. הוראות [כאן](https://www.wikihow.com/Disable-Windows-7-Firewall)

1. לאורך כל התרגיל תוכלו להשתמש בפקודות ה-CMD אשר היכרנו לאורך הסמסטר – **nslookup, ping, tracert, ipconfig**. בנוסף אם תרצו לגשת ב-telnet לשרת השתמשו בפקודה **telnet.**

**חוקרים את הרשת**

1. כעת אנחנו נמצאים **בתוך רשת פנימית.** ראשית כל בואו ננסה לברר איפה אנחנו נמצאים ברשת הזאת. נסו לגלות את ה-IP של המחשב, את מסכת הרשת שלו וכמה מחשבים יש בתת רשת הזאת (במקסימום). הסבירו כיצד ביצעתם כל פעולה.

|  |
| --- |
| כתבתי בSSH ipconfig וקיבלתי את הפרטים - 10.200.0.1 אייפי, 255.255.255.0 סאבנט מאסק, 256 מקסימום מחשבים – זה כמות האייפים שיכול להיות עם הסאבנט מאסק. |
| *תשובה* |

1. האם תוכלו למצוא מחשבים נוספים אשר בוודאות קיימים באותה תת הרשת? איך מצאתם הוכחה לקיומם?

|  |
| --- |
| לא, לא מצאתי הוכחה לקיומם למרות שנראלי שיש ואני עצוב שוב, אבל כן יש כאלה שמתחילים ב10.1.1.x או משהו כזה. אבל אחר כך מצאתי אותו - 10.200.0.100 שהוא כנראה הנתב שלי מצאתי אותו ע"י tracert |
| *תשובה* |

1. האם תוכלו למצוא את כתובת ה-IP של האתר הפנימי אליו ניגש0rphan בבקשת ה-DNS בהסנפות? כיצד? מי ענה לכם?

|  |
| --- |
| 10.1.1.36, 10.1.1.5 זה מי שענה לנו |
| *תשובה* |

1. האם bgworkers.com נמצא באותה תת רשת כמו המחשב שלנו? הסבירו את תשובתכם.

|  |
| --- |
| לא כי הוא מתחיל ב10.1.x.x ואנחנו ב10.200.0.1 והסאבנט הוא שרק האחרון הוא משתנה, כנראה שנינו נמצאים בתתי רשתות שונות תחת אותה רשת פרטית |
| *תשובה* |

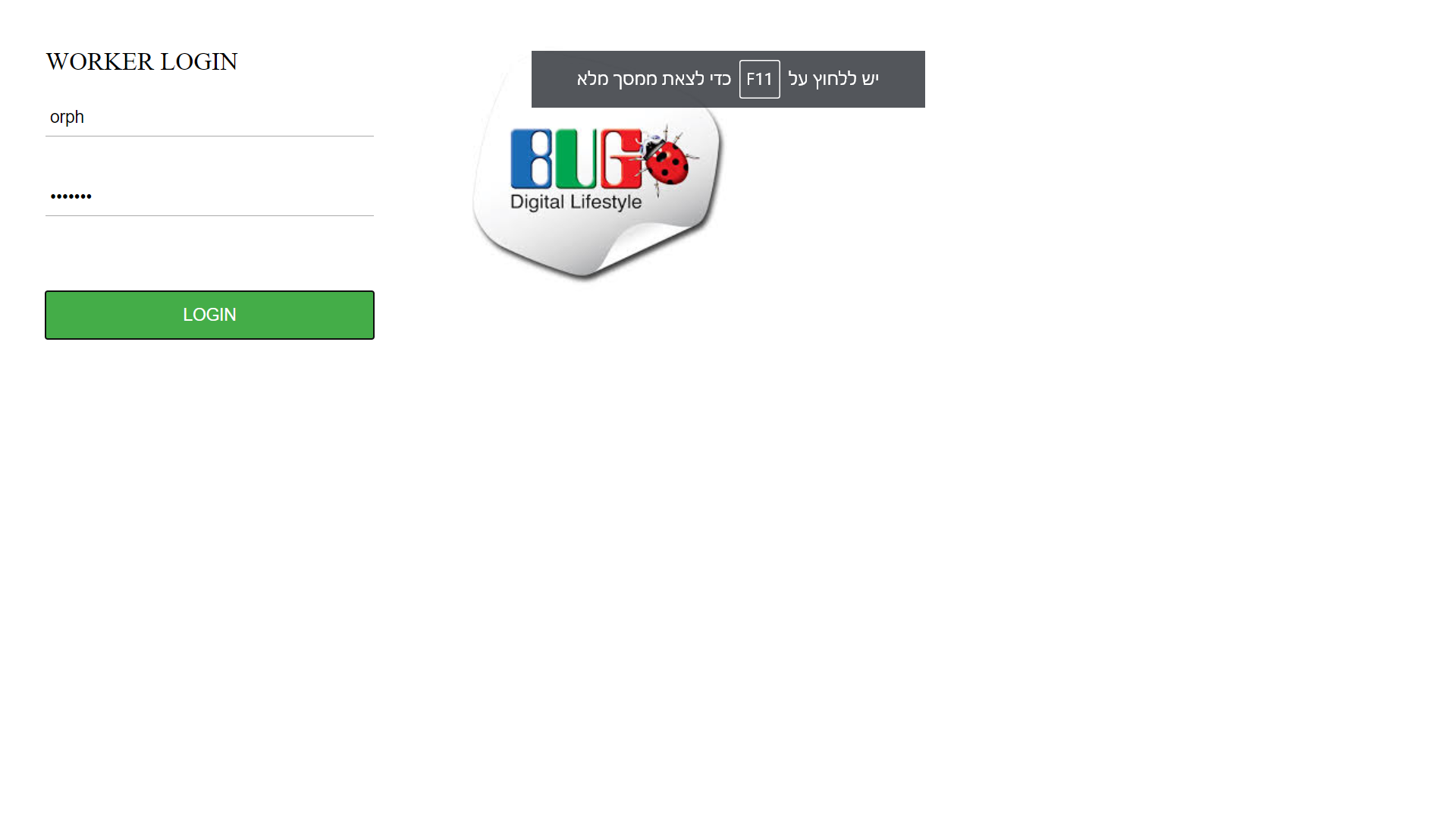
1. האם יש תחנות נוספות ביניכם לבין bgworkers.com? הסבירו מה עשיתם. עבור כל תחנה כתבו האם היא מחשב או נתב.

|  |
| --- |
| יש אותנו ואז 10.200.0.100 שהוא כנראה הנתב שלנו ואז - 10.1.1.100 שהוא כנראה הנתב של bgworkers.com, ואז את bgworkers.com שהוא לא נתב |
| *תשובה* |

1. כפי שכבר הבנתם, על bgworkers.com יושב שרת HTTP. נסו להשתמש בפריט המידע הזה כדי לגלות **איפה עובד 0rphan.** הסבירו מה עשיתם וצרפו צילום מסך. אם גיליתם פרטים נוספים (לא חובה) כתבו גם עליהם.

עשיתי טלנט על bgworkers.com, ואז עשיתי בקשת HTTP פשוטה, וקיבלתי את האתר הבא:

**חניכים יקרים, שימו לב!!**



**תזכרו שסין כרגע סגורה בגלל הקורונה ולא ניתן להגיע לשם. לאורפן אין עדיין דרכון ירוק 😞.**

**לכן אם הגעתם לשם, צאו מהר!! אחרת תצטרכו להיכנס לבידוד. אורפן עובד במקום אחר, מקום הרבה יותר קרוב 🙂**

|  |
| --- |
| כנראה שאורפן עובד בבאג, לא בסין (לא הגעתי לשם אגב) |
| *תשובה* |