שיעור 9 – שכבת הרשת ו-IP

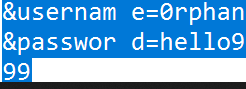
**תרגיל: הפעילות החשודה של 0rphan**

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 כי בדאטה שלה מוזכר HTTP/1.1 |

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

|  |
| --- |
| username=0rphan password=hello999 |

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.

|  |
| --- |
| 173.8.223.33 וזה איזה שהו אתר שקוראים לוsoft home |

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 לפי ההדר זה נמצא ב בדאטה שורה לפני הIP של האתר |

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

|  |
| --- |
| זה IP פרטי, ולכן לא נוכל למצוא את המיקום שלו |

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

|  |
| --- |
| יש לנו 3 רמזים בבקשת ה-HTTP בנוגע למיקום. אלו הם: google.fr (יענו צרפתי), יש לנו בשפה העדפה לצרפתית, וגם ה-timezone שבו נשלחת הבקשה הוא צרפתי |

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.

|  |
| --- |
| 10.200.0.1 הIP של המחשב  255.255.255.0 מסכת רשת  253 מחשבים כי מחשב לא יכול לקבל את 0 ואת 255 |
| *תשובה* |

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

|  |
| --- |
| 10.200.0.100  10.200.0.3  Tracert עשיתי ל IP שנמצא בתוך התווך |
| *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 עשיתי NSLOOKUP  ובשורה הראשונה כתוב מי ענה Server: 10.1.1.5 |
| *תשובה* |

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

|  |
| --- |
| לא כי ה SUBNET MASK לא תואם |
| *תשובה* |

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

|  |
| --- |
| עשיתי tracert לIP של האתר  1 10.200.0.100 (10.200.0.100) 18 ms 67 ms 24 ms  נתב  2 10.1.1.100 (10.1.1.100) 135 ms 127 ms 64 ms  נתב  3 10.1.1.36 (10.1.1.36) 67 ms 117 ms 59 ms  מחשב(האתר) |
| *תשובה* |

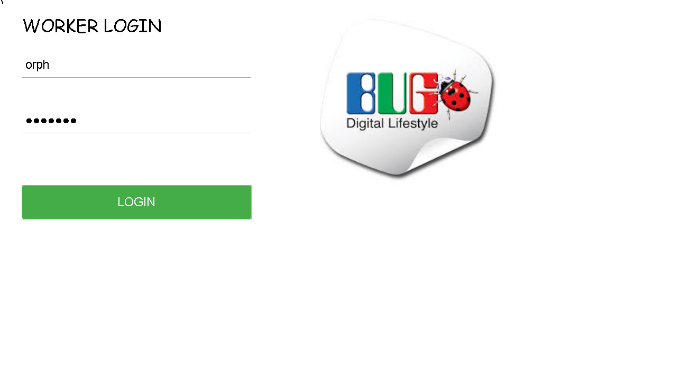
1. כפי שכבר הבנתם, על bgworkers.com יושב שרת HTTP. נסו להשתמש בפריט המידע הזה כדי לגלות **איפה עובד 0rphan.** הסבירו מה עשיתם וצרפו צילום מסך. אם גיליתם פרטים

בתוך ה SSH התחברתי ל HTTP דרך80 10.1.1.36 TELNET

ואז עשיתי את הפקודה הזאת GET / HTTP/1.1 Host: bgworkers.com

וקיבלתי דפ HTML אז פתחתי אותו



נוספים (לא חובה) כתבו גם עליהם.

וגם במידע של הדף היה בכתוב את השם משתמש והסיסמה שלו

value="orph">

value="TheKing">

**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 🙂**

|  |
| --- |
|  |
| *תשובה* |