שיעור 6 – שכבת התעבורה - UDP

**תרגיל: הסנפות מתקדמות**

בתרגיל זה נעיין בהסנפות תוך התמקדות בשתי השכבות אותן אנחנו מכירים - שכבת התעבורה ובשכבת האפליקציה.

**1. פרוטוקולים**

1. התחילו הסנפה חדשה ב-Wireshark, גלשו לאתר **רשות העתיקות http://www.antiquities.org.il,** ולאחר שהאתר נטען עצרו את ההסנפה.
2. השתמשו בפילטר udp או tcp כדי לסנן חבילות אשר כוללות בתוכן את אחד מהפרוטוקולים בשכבת התעבורה.
3. רשמו ארבעה פרוטוקלים שאתם מוצאים בטבלה, ומלאו את המידע שאתם מוצאים על כל פרוטוקול (את כל המידע ניתן להסיק מההסנפה בלבד ללא צורך בגוגל).

(שימו לב – חבילות שבשדה פרוטוקול כתוב רק UDP או TCP – התעלמו מהן בשלב זה. אלו חבילות ללא שכבת אפליקציה או שהפרוטוקול אינו מזוהה).

|  |  |  |  |
| --- | --- | --- | --- |
| פרוטוקול | טקסטטקסטואלי / בינארי? | בשכבת התעבורה יש.. | Port (בצד השרת) |
| SSDPSSDP | בינארי | UDP | 239.255.255.250 |
| QUIC | בינארי | UDP | 216.58.212.227 |
| HTTP | טקסטואלי | TCP | 199.203.52.31 |
| TLSv1 | טקסטואלי | TCP | 52.109.12.23 |

1. הסבירו כיצד יתכן שבחבילה אחת יש גם את פרוטוקול UDP וגם פרוטוקול נוסף?

|  |
| --- |
| אולי אפשר לקרוא את החבילה בשתי דרכים. אולי שלחו אותה פעמיים פעם בדרך המהירה פעם בדרך הבטוחה כדי לבדוק את הקודם |
| *תשובה* |

1. באיזו שכבה כל הפרוטוקולים שרשמתם בעמודה הימנית טבלה?

|  |
| --- |
| שכבת האפליקציה |
| *תשובה* |

**2. DNS**

1. הציגו רק את חבילות ה-DNS שיצאו מהמחשב שלנו. כתבו שני פילטרים שונים שיבצעו את הסינון הזה:

|  |
| --- |
| dns  ip.src == 10.100.102.145 |
| *תשובה* |

1. כתבו 3 דומיינים שונים אותם ביקש הדפדפן שלנו (ב-DNS):

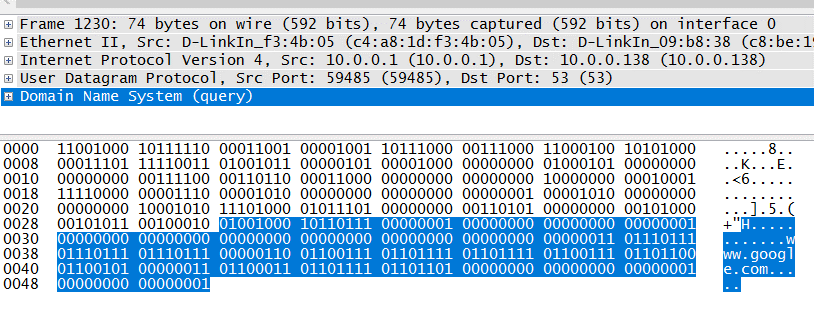
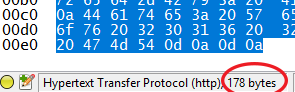
|  |
| --- |
| nexus.officeapps.live.com  זה היה החבילת dns היחידה שהמחשב שלי שלח. |
| *תשובה* |

1. בחרו את אחת מחבילות ה-DNS. כתבו את האורך שלה המופיע תחת העמודה Length:

|  |
| --- |
| 85 |
| *תשובה* |

1. באיזה פרוטוקול בחר DNS להשתמש בשכבת התעבורה?

|  |
| --- |
| UDP |
| *תשובה* |

1. כאשר אנחנו מסמנים את אחת השכבות במסך השכבות, בשורה התחתונה מוצג האורך של השכבה הזו בלבד (בתוך החבילה).
2. בחבילה שבחרתם, כתבו מהו האורך (בבתים) של כל אחת מהשכבות:

|  |
| --- |
| אפליקציה = 43 תעבורה = 8 רשת = 20 קו = 14 |
| *תשובה* |

1. מהי השכבה הארוכה ביותר? האם זה מצב הגיוני לדעתכם? מדוע?

|  |
| --- |
| שכבת האפליקציה היא הארוכה ביותר. וזה די הגיוני לדעתי- זה אומר שהמידע עצמו הוא החלק הארוך ביותר, זה מצב די לגיטימי לדעתי |
| *תשובה* |

1. מהו פורט המקור (Src Port) שבחר המחשב שלי לשיחת DNS זו? כיצד הוא בחר את ה-Port הזה?

|  |
| --- |
| 54720. אולי סתם כי זה פורט פנוי??? |
| *תשובה* |

1. לחצו פעמיים על השכבה של UDP במסך השכבות כדי לפתוח את הפירוט שלה. הסבירו על כל אחד מארבעת השדות שכולל ההדר – מה שמו, מה האורך שלו ומה התפקיד שלו.

|  |
| --- |
| Sourcw port. 2 bytes. To hold the sorce port  Destination port. 2 bytes. To hold the destination port  Length. 2 bytes. To hold the length of the message  Checksum. 2 bytes. To check if the message was successfully sent, using the sum of the message. |
| *תשובה* |

1. מה המספר המקסימלי שיכול להיכנס בשדה Length? הסבירו כיצד חישבתם זאת.

|  |
| --- |
| 65536. 2 בחזקת 16, 2 = כמות האפשריות לכל יחידה (0/1), 16 = כמות היחידות (16 ביטים). |
| *תשובה* |

1. סמנו במסך השכבות את השדה Source Port. שימו לב לקטע ההקסא שמסומן במסך התחתון. העתיקו את הקטע לאתר שממיר ממספר הקסא למספר דצימלי (hex to dec). מהו המספר שקיבלתם? האם הוא המספר שציפיתם?

|  |
| --- |
| Hex = d5c0 Dec = 54720  כן זה מה שציפיתי כי זה הsrc port. |
| *תשובה* |

**3. HTTP**

1. כעת נבצע סינון לחבילות HTTP בלבד.
2. באיזה פרוטוקול משתמש HTTP בשכבת התעבורה?

|  |
| --- |
| TCP |
| *תשובה* |

1. מדוע לדעתכם הוחלט ש-HTTP ישתמש דווקא בפרוטוקול זה?

|  |
| --- |
| כי ככה קל יותר להעביר את המידע בעיקר את הhtml. וחשוב מאוד שיצא בדיוק כמו ששלחנו – אם חסר < אחד הקוד יכול לא לעבוד |
| *תשובה* |

1. גלו כיצד ניתן לסנן HTTP ע"פ Response Code. ניתן לעשות זאת בעזרת גוגל או ע"י כתיבת http ולאחריו נקודה בשדה הפילטר. כתבו פילטר אשר מציג רק תשובות של 200 OK:

|  |
| --- |
| http.response.code == 200 |
| *תשובה* |

1. כתבו פילטר אשר מציג רק את התגובות שאינן 200:

|  |
| --- |
| http.response.code != 200 |
| *תשובה* |

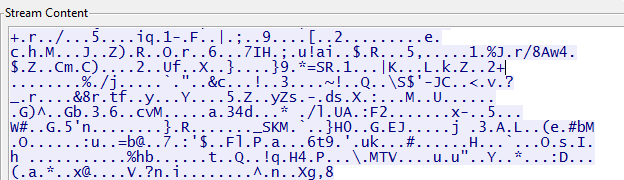
1. חזרו לפילטר שמציג את התשובות של 200. כעת אנו למעשה רואים את כל הקבצים אשר קיבלנו מהשרת. כמה קבצים מוצגים?

|  |
| --- |
| 4 |
| *תשובה* |

1. אילו סוגי קבצים אתם רואים בבקשות HTTP? כתבו לפחות 5.

|  |
| --- |
| לא הבנתי את השאלה, סוגי פרוטוקולים יש 2 (אחד SSDP) |
| *תשובה* |

\* הידעת? עד היום לא דיברנו על כך, אבל כאשר HTTP מעביר תמונות או קבצים אחרים הוא מעביר אותן בצורה בינארית. כך ש-HTTP, למרות שבמהותו הוא פרוטוקול טקסטואלי, מסוגל להעביר גם מידע בינארי לפעמים.

1. **בונוס:** ידוע לנו ש-HTTP הוא פרוטוקול טקסטואלי, ובאתר העתיקות לא מתבצעת הצפנה (אין סימן של מנעול בגלישה, והפורט הוא 80 ולא 443 של HTTPS). אם כך, מדוע חלק מהתשובות של השרת מגיעות אלינו בצורה בינארית, גם כאשר אנחנו מבקשים קובץ טקסטואלי כמו HTML?   
   רמז – התשובה נמצאת בהדרים...

|  |
| --- |
| יש הדר בשכבת האפליקציה בשם content encoded entity body שהוא מוצפן – יכול להיות שהוא מעביר חלקים מוצפנים בשכבת האפליקציה לדוג' PHP ששם נמצאות סיסמאות וקוד מקור שאפשר להשתמש בהם לפרוץ לדאטאבייס וכו' |
| *תשובה* |

1. **בונוס:** בצעו כמה טעינות רצופות של אתר רשות העתיקות עם Reload. לאחר מכן הסניפו טעינה נוספת של אתר רשות העתיקות. כעת הדפדפן שלכם אמור לזכור חלקים מהאתר (למשל תמונות) ולא להוריד אותם מחדש, כדי לחסוך בתעבורה. מצאו תגובות HTTP שתומכות בטענה זו, והסבר מה הן אומרות.

|  |
| --- |
|  |
| *תשובה* |