מבחן רשתות – מגמת סייבר / ברק גונן

פייתון, sockets, מודל השכבות, wireshark, HTTP, DNS

הנחיות:

* מותר בשימוש כל חומר עזר (אינטרנט)
* אסורה תקשורת עם תלמידים אחרים
* את קבצי הפתרון יש לשמור בתיקיה בשם שלכם באנגלית

- קובץ וורד עם תשובות

- קובץ של לקוח (פייתון)

- קובץ של שרת (פייתון)

* משך המבחן 90 דקות.

בהצלחה!

שאלה 1: עבודה עם קובץ הסנפה, פרוטוקולי HTTP, DNS (50 נקודות)

הורידו את קובץ ההסנפה מהקישור הבא:

[www.cyber.org.il/networks/test\_sniff.pcapng](http://www.cyber.org.il/networks/test_sniff.pcapng)

הערה: כל התשובות לשאלות הבאות אמורות להיות קצרות ביותר- כמה מילים או מספרים.

1. גלישת אינטרנט (2.5 נקודות כל סעיף)
   1. באיזה פילטר תשתמשו ב-wireshark כדי לסנן גלישה לאתרי אינטרנט? פילטר http
   2. מה ה-IP של המחשב ממנו בוצעה ההסנפה? 192.168.2.203
   3. מהו ה-IP של אתר האינטרנט אליו בוצעה הגלישה הראשונה? (המשך השאלות מתייחסות כולן לגלישה הראשונה) 92.122.135.44
   4. מהו ה-URL המלא אליו בוצעה הגלישה? <http://www.haaretz.co.il/captain>
   5. מהו פורט היעד? 80
   6. האם הגלישה צפויה לעבוד תקין אם הלקוח יבחר פורט יעד אקראי אחר? לא
   7. מיצאו את תשובת השרת. מהו ה-status code? 200 OK
   8. אילו הלקוח היה ממתין מספר שניות וגולש שוב לאותו אתר. לאיזה status code הייתם מצפים בתשובת האתר? מיצאו בהסנפה פקטה כזו ורישמו מה המספר הסידורי שלה. הייתי מצפה לסטטוס קוד 304 Not Modified, ופקטה מספר 600 היא כזאת (היא כוללת את הסטטוס קוד הזה)
   9. אילו המשאב היה לא זמין מסיבה כלשהי, מה היה ה-status code שהיה מתקבל? מיצאו בהסנפה פקטה כזו ורישמו מה המספר הסידורי שלה. הסטטוס קוד שהיה מתקבל הוא 404 Not Found, ופקטה 617 היא כזאת.
   10. מיצאו פקטה שמכילה בקשת GET עם פרמטרים ורישמו מה המספר הסידורי שלה. פקטה מס. 150
2. ביצוע nslookup (2.5 נקודות כל סעיף)
   1. באיזה פילטר תשתמשו כדי לסנן פקטות שנוצרו בעקבות הרצת nslookup? פילטר dns
   2. מיצאו את הפקטה הראשונה מסוג QUERY. רישמו את מספר הפקטה. מה כתובת ה-IP של השרת אליו נשלחה ה-QUERY? מספר הפקטה הוא 10, וכתובת ה-IP של השרת היא 192.115.106.31
   3. מהו הפורט אליו נשלחה ה-QUERY? פורט 53
   4. האם ה-QUERY היא reverse mapping? איזה שדה מאפשר לכם לדעת זאת? כן, והשדה שמאפשר לנו לראות זאת הוא Type, שהערך שלו הוא PTR (Pointer DNS, שזה מה שמשמש בReverse Mapping)
   5. אילו ה-QUERY היה נשלח לפורט יעד אחר, האם היינו מצפים לקבל תשובה? לא.
   6. מיצאו את התשובה לפקטת ה-QUERY הראשונה. רישמו את מספר הפקטה. רשמו את הצירוף של כתובת IP ו-domain name שאפשר להסיק מתשובה. מספר הפקטה הוא 11, כתובת ה-IP היא 31.106.115.192, וכתובת ה-domain היא dns1.bezeqint.net
   7. מיצאו את הפקטה השניה מסוג QUERY. רישמו את מספר הפקטה. הסיקו ממנה, מה ה-domain name עליו בוצע ה-nslookup? מספר הפקטה הוא 12, והדומיין הוא www.cnn.com
   8. מהו ה-TLD של ה-domain name שמצאתם? .com
   9. האם ה-QUERY (הפקטה השניה) היא רקורסיבית או איטרטיבית? רקורסיבית
   10. פקטה מספר 1621 היא DNS QUERY לגוגל. השתמשו בה ליצירת פילטר שמסנן רק פקטות שבהן ה-QUERY NAME הוא [www.google.com](http://www.google.com). מהו הפילטר?

הפילטר הוא dns.qry.name == "www.google.com"

שאלה 2: כתיבת שרת מחשבון (פייתון + סוקטים)

כיתבו שרת בשם calc\_server.py, שמבצע פעולה של מחשבון. השרת יעבוד מול לקוח שנמצא בקישור:

[www.cyber.org.il/networks/calc\_client.py](http://www.cyber.org.il/networks/calc_client.py)

אסור לשנות את קוד הלקוח, אפשר להשתמש בקוד הלקוח כדי לבדוק את השרת.

1. השרת יחזיר תוצאת חישוב נכונה עבור בקשות תקינות של הלקוח (**40 נקודות**)

בקשה תקינה היא בפורמט הבא:

number, space, operation, space, number

כאשר operation יכול להיות רק +-\*/ (חיבור, חיסור, כפל או חילוק)

ו-number הוא מספר חיובי שלם בלבד, שקטן מ-65,536

דוגמה לבקשה תקינה:

100 + 14

1. שפרו את השרת כך שהוא יהיה יציב, כלומר לא יתרסק כאשר הלקוח שולח לו בקשות מסוגים שונים, גם בקשות תקינות וגם בקשות לא תקינות. מומלץ לבדוק באמצעות הכנסת קלטים שונים מהלקוח (**10 נקודות**)

הערה: יש להקפיד על קונבינציות כתיבת קוד בפייתון.

בהצלחה!