

# מבחן רשתות מגמת סייבר

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

הנחיות:

מותר בשימוש כל חומר עזר (אינטרנט)  
אסורה תקשורת עם תלמידים אחרים  
משך המבחן 90 דקות.

בהצלחה!

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

הורידו את קובץ ההסנפה מהקישור הבא:

[http://www.lamed-oti.com/school/rs/networks/downloads/test\\_sniff.pcapng](http://www.lamed-oti.com/school/rs/networks/downloads/test_sniff.pcapng)

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

1. גלישת אינטרנט (2.5 נקודות כל סעיף)

- a. באיזה פילטר תשתמשו ב Wireshark כדי לסנן גלישה לאתרי אינטרנט?
- b. מה ה IP של המחשב ממנו בוצעה ההסנפה?
- c. מהו ה IP של אתר האינטרנט אליו בוצעה הגלישה הראשונה? (המשך השאלות מתייחסות כולן לגלישה הראשונה)
- d. מהו ה URL המלא אליו בוצעה הגלישה?
- e. מהו פורט היעד?  
80
- f. האם הגלישה צפויה לעבוד תקין אם הלקוח יבחר פורט יעד אקראי אחר?
- g. מיצאו את תשובת השרת. מהו ה status code?
- h. 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.
- i. אילו המשאב היה לא זמין מסיבה כלשהי, מה היה ה status code שהיה מתקבל? מיצאו בהסנפה פקטה כזו ורישמו מה המספר הסידורי שלה.
- j. מיצאו פקטה שמכילה בקשת GET עם פרמטרים ורישמו מה המספר הסידורי שלה.

2. ביצוע nslookup (2.5 נקודות כל סעיף)

- a. באיזה פילטר תשתמשו כדי לסנן פקטות שנוצרו בעקבות הרצת nslookup?
- b. מיצאו את הפקטה הראשונה מסוג QUERY. רישמו את מספר הפקטה. מה כתובת ה IP של השרת אליו נשלחה ה QUERY?
- c. מהו הפורט אליו נשלחה ה QUERY?
- d. האם ה QUERY היא reverse mapping? איזה שדה מאפשר לכם לדעת זאת?
- e. אילו ה QUERY היה נשלח לפורט יעד אחר, האם היינו מצפים לקבל תשובה?
- f. מיצאו את התשובה לפקטת ה QUERY הראשונה. רישמו את מספר הפקטה. רשמו את הצירוף של כתובת IP ו domain name שאפשר להסיק מתשובה.
- g. מיצאו את הפקטה השניה מסוג QUERY. רישמו את מספר הפקטה. הסיקו ממנה, מה ה domain name עליו בוצע ה nslookup?
- h. מהו ה TLD של ה domain name שמצאתם?
- i. האם ה QUERY (הפקטה השניה) היא רקורסיבית או איטרטיבית?
- j. 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?



שאלה 2: כתיבת שרת מחשבון (פייתון + סוקטים)

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

[http://www.lamed-oti.com/school/rs/networks/downloads/calc\\_client.py](http://www.lamed-oti.com/school/rs/networks/downloads/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 (**30 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

2. 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 (**20 נקודות**), למשל קלטים לא נומריים, פעולת חשבון לא מזהה וכו'.

בהצלחה!