מעבדת סייבר - הגנה  
מטלת תכנות Fuzzing

במטלה זו תצטרכו לזהות תוקף שמייצר תקשורת מלאה בתוכן חסר משמעות על פרוטוקול SSH.

מוזמנים לחפש מידע באינטרנט בנושא Fuzzing כדי להבין גישות, סוגים וכו'.

עליכם לבנות סקריפט פייטון(קוד בפייטון) גרסא 3.7 המבצע זיהוי של תקיפה זו, ומדפיס למסך: "Fuzzing detected".

ישנן שתי אפשרויות לביצוע:

1. שימוש בספריית scapy לפייטון על מנת להאזין לתקשורת הנ"ל ולזהות את התקיפה.

2. שימוש בתוכנת tshark שמאפשר להאזין לתקשורת. האזנה זו תיוצא לקובץ טקסט לבחירתכם. סקריפט הפייטון יקרא כל זמן מסוים את קובץ הטקסט ויזהה אם ישנה תקיפה.

לאחר שזיהיתם את התקיפה, אפשר לבצע יציאה מסודרת(כלומר, לבצע exit).

במידה וישנן שאלות, יש לכתוב בפורום הקורס.

במידה ואתם רוצים לבדוק את עצמכם, אתם יכולים לפתוח מכונה נוספת בה תבצעו את התקיפה. מכונה זו תייצר תקשורת חסרת תוכן על פרוטוקול SSH.

ניתן לבנות סקריפט תוקף בscapy שמייצר חבילות SSH תוקפות כנ"ל.

על המטלה תתבצע בדיקה פרונטלית בתאריך שיקבע בהמשך. הגשת המטלה היא עד 26.4.21.

רמז: זבל יכול להיות מיוצג ע"י רצף אותיות לא הגיוני בעליל או שימוש לא נכון בפרוטוקול.