**תשובות לחלק תיאורטי מעבדה 3**

1. אם תוקף חיצוני יוכל להתחבר גם הוא להעברת התקשורת בקשר, כלומר לקבל את הפאקטות הנשלחות ולשלוח פאקטות בעצמו, אזי נאמר כי הקשר "נפרץ" ואמינותו נפגעה.
2. מאחר ומחשב יכול להיות חלק מכמה קשרי TCP, בעת קבלת הודעה עליו לדעת לאיזה קשר היא שייכת. לצורך כך, משתמש המחשב בארבעה שדות: source TCP address, source port, destination IP address, destinaion port. נהוג לקרוא לארבעה שדות אלו ה"חתימה" של קשר ה – TCP.
3. לזייף פאקטת TCP עם חתימה של קשר קיים ולשולחה, כך שהצד המקבל לא יוכל להבדיל באם נשלחה פאקטה מהצד השני או מתוקף חיצוני. מלבד חתימת הקשר, התוקף צריך בנוסף לזייף ולשמור על עקביות ה – seqence number – המספר הסידורי בקשר.
4. בתקשורת TCP אנו מתייחסים לדאטה כאל מחרוזת – string, כך שלכל בייט בדאטה ישנו מספר סידורי בלעדי, המאפיין את מיקומו במחרוזת. בפאקטת הTCP ישנו שדה בן 32 ביט המכיל את מיקום הבייט הראשון במידע הנשלח. בעת קבלת הפאקטה, המחשב שומר את המידע בבאפר המסודר על פי המספרים הסידוריים ובצורה זו, גם אם סדר קבלת ההודעות שונה, סדר המידע הנשלח נשמר. לכן, לצורך העניין, אם המחשב קיבל מידע עד הבייט ה- x, הוא מצפה לקבל את הבייט ה- x+1 בהודעה הבאה. אם המספר הסידורי המזוייף יהיה x + d, אזי ההודעה תחשב כהודעה שהגיעה מחוץ לסדר והמידע ישמר בבאפר, במידה וישנו מקום, בעמדה ה – x+d, כאשר נשארו לפניו d-1 ביטים ריקים עבור המידע המתחיל במקום ה – x+1. במקרה זה, המידע המזוייף לא יעבור לשכבת האפקליקציה עד להשלמת המידע החסר בהודעה ולכן לא יהיה לו כל אפקט. אם הערך של d גדול מדי, המידע עלול להיזרק אל מעבר לגבולות הבאפר. לעיתים, עקב הקושי בדיוק במספר הסידורי, הוא מזוייף מראש עם מרווח טעות קטן, כך שהפאקטה המזויפת תשמר בבאפר ואף על פי שלא תיושם מיד, לאחר שליחת כמה הודעות בין הצדדים ומילוא המרווח עד המידע המזוייף, תשלח ההודעה המזויפת לשכבת האפליקציה ותוצא לפועל.
5. Session hijacking attack מתאפשרת עקב ידיעת חתימת קשר ה – TCP ועל ידי אפשרות לזייף מספר סידורי מתאים. על כן ינשן כמה גישות מנע:

* שימוש במפתח קשר ראנדומאלי ומשתנה. בצורה זו קשה יותר לזייף פאקטה שתחשב קבילה.
* יצירת חתימת קשר חדשה, לאחר הקמת הקשר, על ידי שני הצדדים. בצורה זו התוקף לא ידע לזהות את הקשר אותו הוא רוצה לתקוף.
* הצפנה ווידוא של המידע ברמת ה- IP , כלומר הרמה המכילה את מספרי הכתובות, הפורטים והמספרים הסידוריים. קיימים פרוטוקולי בטיחות רשת - IPsec המנהלים שיטת מנע זו.