

**מעבדה מספר 2**

**תשובות**

**Reset-Attack**

**פתרונות לשאלות חזרה בנושא Reset-Attack:**

1. תאר את כלל האפשרויות לסגירת התקשרות TCP. הסבר מדוע נחוצה הודעת ה – Reset בקשר TCP.

תשובה:

ניתוק "מסודר" של קשר TCP: כאשר לאחד הצדדים ( צד A) בקשר TCP לא נותר עוד דאטה להעביר, הוא שולח פאקטת FIN, בה ביט ה – FIN הינו "למעלה". FIN הינו אחד מששת הביטים ב – TCP header, עליהם הסברנו במעבדה הראשונה. בקבלת הפאקטה, צד B עונה עם פאקטת ACK ובצורה זו נסגר הקשר מצד A לצד B. יש לשים לב כי הקשר מצד B ל- A עדיין הינו פתוח בשלב זה. במידה וירצה גם צד B לסיים את הקשר, הוא ישלח פאקטת FIN משלו שצריכה להיענות על ידי פאקטת ACK מצד A. משזה נעשה, קשר ה-TCP בכללו, יחשב כסגור.

ניתוק "לא מסודר" של קשר TCP: אחד הצדדים שולח פאקטת RST לצד השני וסוגר את את הקשר באופן מיידי. RST הינו אחד מששת הביטים שנלמדו במעבדה הקודמת. אופן סגירת קשר זה מתבצע בעיקר בעיתות חירום כאשר אין זמן לביצוע הפרוטוקול ה"מסודר".

פאקטת ה-RST נשלחת גם לעיתים במקרה של שגיאות. למשל, במקרה של מתקפת SYN-Flood, אם אחת הפאקטות המזוייפות, נשלחת לכאורה מכתובת IP קיימת, ישלח השרת לכתובת זו פאקטת SYN + ACK. המחשב היושב באותה הכתובת, לא ניסה ליצור שיחה עם השרת ולכן עם קבלת הפאקטה, כחלק מהפרוטוקול, הוא ישלח לשרת כתשובה פאקטת RST, אשר מודיעה לשרת כי יש לסגור את הקשר החצי-פתוח ועל ידי כך לשחרר את המשאבים המוקצים לקשר זה. זו דוגמא אחת לנחיצות פאקטת ה–RST בקשרי TCP.

2) תאר את אופן ביצוע Reset attack. מהם הפרטים הנחוצים לתוקף עבור ביצוע המתקפה? כיצד ניתן להשיגם?

תשובה:

כפי שראינו, כל שצריך על מנת לסגור תקשורת TCP הינו פאקטת RST אחת. לכן, כל שצריך תוקף לעשות הינו לזייף ולשלוח פאקטת RST מצד אחד לשני. יחד עם זאת, על מנת להצליח במתקפה, יש למלא חלק מהשדות בפאקטה במידע עדכני ונכון. כל תקשורת TCP מאופיינת על ידי השדות source IP address, source port, destination IP address, destination port. על כן, הפאקטה המזוייפת צריכה להכיל את השדות הנ"ל התואמים לקשר. בנוסף, על שדה ה – sequence number להיות בעל ערך עדכני, כדי שהפאקטה תחשב עדכנית בצד המקבל. מכאן, לצורך קבלת המידע הנחוץ לזיוף הפאקטה, תחילה יש להאזין על קשר קיים ו"לדוג" פאקטה מבין התקשורת המועברת. בכאשר הושגה פאקטה כזו, יש לזייף את הפאקטה ושולחה מהר מספיק, טרם תגובת הצד המקבל, על מנת שהמספר הסידורי שזייפנו יחשב עדכני.

1. מהי נקודת התורפה המנוצלת עבור ביצוע המתקפה וכיצד ניתן למנוע ביצוע Reset Attack על התקשרות TCP? הסבירו והביאו דוגמאות.

תשובה:

זיוף פאקטות בקשר TCP מתאפשר מאחר וקידוד המידע בקשר מתבצע מתחת לשכבת ה – IP. לכן, המידע המכיל את הכתובות, הפורטים וביטי הבקרה, הנמצא ב – TCP header הינו חשוף ואינו מוצפן. אם נוכל להצפין את המידע כך שאך ורק כל אחד משני הצדדים שהקימו את הקשר יוכלו לאשר את אמינות הפאקטה, נוכל למנוע מתקפות RST עתידיות על הקשר המיוסד. לצורך כך נוצר פרוטוקול ה – Internet Protocol Security – Ipec, הכולל פרוטוקולים המאפשרים הצפנה ווידוא בין הצדדים בעת הקמת הקשר ובמהלכו. בעזרת IPsec, ניתן להעביר מידע באופן בטוח ויציב בין שני מחשבים, בעזרת קשר TCP.: