**שאלה 1:**

**חלק 1:**

1. שיטת התקפה זו בקיצור "מרעלה את ה DNS" על ידי השתלטות על authority records, כך שהתוקף מקים שרת שהוא authoritative ל domain שהוא רוצה לתקוף ומציף את הקורבן עם פקיטות מזויפות שאומרות לעשות authority delegation לשרת שהתוקף הקים, וכך כאשר הקורבן מקבל את הפקטה הזו הוא יאמין שהשרת הזה שנמצא בשליטת התוקף הוא authoritative ל domain שהוא מנסה לגשת אליו ויאמין לתשובות שלו אך לצערו הרב התוקף יכול להפנות אותו לאן שהוא רוצה. ההבדל מההתקפה שתוארה בהרצאה נובע מזה שבהרצאה ראינו איך מזייפים record אחד של אתר ספציפי אבל כאן ניתן להשתלט על domain שלם בגלל שבמקרה שההתקפה מצליחה הקורבן מאמין לתשובות של שרת שהתוקף הקים והוא יכול לשלוח לקורבן כל תשובה שהוא רוצה ב domain הזה ולא רק לאתר ספציפי כמו שראינו בכיתה וזה הרבה יותר חזק!
2. היתרונות של התקפה זו שהיא מאפשרת התשלטות על domain שלם ולא רק על אתר ספציפי כך שאחרי הצלחת ההתקפה התוקף יכול לתקוף הקורבן בכל פעם שהוא ניגש לאתר ב domain וכמובן שזה מעלה את הסיכויים שהתוקף יצליח בהשגת מטרותיו (למשל אם הן גניבת מידע מהקורבן).
3. כדי להגן מפני התקפה זו, הוצע להפוך את ה source port לרנדומלי וגם את ה query id לרנדומלי כך שכאשר שניהם רנדומליים יש בערך אפשרויות שונות לקומבנציה של שניהם וזה מנמיך את הסיכויים שכאשר תוקף מנסה לשלוח query להשתלט על domain הוא יצליח כי זה כבר מספר עצום בהשוואה למה שהיה קודם שאפשר לתוקף להצליח בערך פעם ב 10 שניות.

**חלק 2:**

1. ש
2. ש
3. ש

**שאלה 2:**

1. ש