תרגיל 6.19 – אילו שירותים פתוחים על המחשב

באמצעות ביצוע Three Way Handshake, אנו יכולים לגלות אילו שירותים פתוחים אצל מחשב מרוחק.

כיצד?

כאשר שלחנו חבילת SYN אל פורט 443 של שרת אינטרנט קיבלנו בתשובה חבילת SYN+ACK. מכך למדנו שפורט 443 "פתוח" אצל השרת, כלומר יש אצלו תוכנה שמאזינה על פורט 443. מכיוון שאנו יודעים שעל פורט 443 מאזינה בדרך כלל תוכנה שנותנת שירות HTTPS גילינו שכרגע שירות ה-HTTPS "פתוח" אצל השרת וניתן לגשת אליו.

מה יקרה אם נשלח חבילת SYN לפורט "סגור", כלומר לפורט שאף תוכנה לא מאזינה עליו?

חלק מהשרתים לא יענו לנו ואילו חלקם יחזירו תשובה שדגל ה-RST דלוק, אך אף שרת לא יענה בתשובה שדגלי ה-SYN+ACK דלוקים.

השתמשו בהתנהגות זאת כדי לכתוב סקריפט אשר מקבל מהמשתמש כתובת של מחשב מרוחק ומדפיס למסך אילו פורטים פתוחים במחשב זה, בטווח הפורטים 20 1024 .

מכיוון שהסקריפט עתיד לשלוח תעבורה רבה, **א ל תבדקו אותו** על שרתים באינטרנט, אלא רק על מחשבים נוספים בביתכם או בכיתתכם. ניתן להשתמש בשרתים וירטואליים.

- על מנת שהשירות אכן יעבוד בזמן סביר על כמות פורטים גדולה, יש לתת timeout לא ארוך מידי, אך עדיין כזה שיאפשר לנו לקבל את התשובה, במידה והיא נשלחת אלינו. הזמן המומלץ הוא 0.5 שניות, אך מומלץ להגדירו כקבוע ולבדוק את הזמן המתאים לסביבה שלכם.