

מיפוי פורטים פתוחים



תרגיל 6.19 בספר הלימוד:

באמצעות ביצוע Three Way Handshake, אנו יכולים לגלות אילו שרתים פתוחים אצל מחשב מרוחק. כיצד?

קודם לכן, כאשר שלחנו חבילת SYN אל פורט 80 של Google, קיבלנו בתשובה חבילת SYN+ACK. מכך למדנו שפורט 80 "פתוח" אצל Google, כלומר יש אצלו תוכנה שמאזינה על פורט 80. מכיוון שאנו יודעים שעל פורט 80 מאזינה בדרך כלל תוכנה שנותנת שרות HTTP, גילינו שכרגע שרות ה-HTTP "פתוח" אצל Google וניתן לגשת אליו.

מה יקרה אם נשלח חבילת SYN לפורט "סגור", כלומר לפורט שאף תוכנה לא מאזינה עליו? בואו ננסה זאת. נשלח חבילת SYN לשרת של Google, אך לפורט 24601:

No.	Time	Source	Destination	Protocol	Length	Info
84	24.6544140	192.168.14.51	173.194.112.242	TCP	54	ftp-data > 24601 [SYN] Seq=0 win=8192 Len=0

השרת של Google כלל לא נתן תשובה של SYN+ACK! במקרים מסויימים, שרתים מרוחקים יענו חבילה כשדגל ה-RST דולק, ומשמעותו שהשרת לא מוכן להרים את הקישור.

השתמשו בהתנהגות זאת בכדי לכתוב סקריפט אשר מקבל מהמשתמש כתובת IP, ומדפיס למסך איזה פורטים פתוחים במחשב המרוחק, בטווח הפורטים 1024-20. מכיוון שהסקריפט עתיד לשלוח תעבורה רבה, **אל תבדקו אותו** על שרתים באינטרנט, אלא רק על מחשבים נוספים בביתכם או בכיתתכם.

טיפים:

1. כדי לא למלא את המסך בהודעות של סקאפי, תוכלו "להשתיק" אותו ע"י הפרמטר verbose
2. שימו לב שחלק מהפורטים לא מחזירים שום הודעה ("blackhole"). חישבו איך למנוע מצב בו התוכנית "נתקעת" בהמתנה לתגובה?

