אלגוג'י – elgooG

- .הבוט הביס הזל שי הארנכ ,אל סאו - החיתפ טפשמב ליחתמ ליגרת לכ
- ישנם דברים שעושים בסדר הנהוג, וישנם דברים שנעשים לחלוטין הפוך. אנחנו נתחיל מהסוף, ובתקווה – נצליח לשנות אותו!
- בתרגיל זה ניצור שרת DNS, שיגרום לכך שכל פניה שלנו ל-www.google.co.il תנותב לכתובת אחרת
  *** קראו טוב את התרגיל ואת ההערות. מאוד חשוב.**

<u>הכנות:</u>

- בחלק זה ניצור הסנפה של DNS QUERY ו- DNS RESPONSE עבור www.google.co.il, כדי שנוכל בהמשך לזהות את ה-QUERY המבוקש ולגרום לשרת שלנו להחזיר תשובה תקינה
- וודאו שאתם מחוברים דרך כבל הרשת
- הריצו את שורת הפקודה הבאה (חשוב: פתחו CMD כAdministrator). השורה תגרום למחיקת ה-cache של ה-DNS שלכם, כיוון שסביר שכתובת ה-IP של גוגל כבר נמצאת שם ולכן לא תבוצע DNS QUERY אותה אנחנו רוצים למצוא
  ipconfig /flushdns && taskkill /F /IM iexplore.exe
- פתחו Internet Explorer.
- פתחו Wireshark והפעילו האזנה עם הפילטר הנ"ל: **udp.port == 53**
- גלשו ל: www.google.co.il
- עצרו ושימרו את ההסנפה בWireshark
- הורידו את הקובץ www.cyber.org.il/networks/gvahimchallenge/elgoog.rar , העתיקו את הקבצים לתיקיית התרגיל והריצו את הקובץ elgooG_set.bat בתור Administrator.
  * הסקריפט יגדיר את שרת הDNS הראשי שלכם כ127.0.0.1 ואת המשני בתור השרת הקודם. השרת המשני נכנס לפעולה אם השרת הראשי אינו מחזיר תשובה, וכך תוכלו להמשיך להשתמש באינטרנט.

<u>התרגיל:</u>

- בחלק זה יש לכתוב שרת שיקבל את בקשות ה-DNS למציאת כתובת ה-IP של www.google.co.il ויחזיר כתובת IP של אתר אחר
- מצאו בהסנפה את בקשת הA ל www.google.co.il ואת התשובה לה.
  * מומלץ להיעזר באופציה של Follow UDP/TCP Stream על הבקשה שמצאתם.
- צרו שרת UDP (הדרכה בספר הלימוד, בפרק על UDP) והאזינו על הפורט של DNS.
- גרמו לפעם הבאה שהבקשה הספציפית הזו מופיעה להחזיר את הכתובת 212.143.70.40 במקום את כתובות הIP שחזרו במקור.
- ברגע שאתם חושבים שסיימתם והכל רץ כמו שצריך, גלשו מחדש לכתובת. <u>מה קרה?</u>

<u>הערות וטיפים:</u>

- **כשסיימתם את העבודה, לפני שהולכים הביתה עליכם להריץ את הקובץ המצורף elgooG_revert.bat כAdministrator – חובה!**
- שימו לב שהשורה של flushdns עשויה להחזיר שגיאה במידה ו- Internet Explorer כבר סגור – זה בסדר גמור ומצופה מהשורה.
- מומלץ להריץ את כל התרגיל בתור Administrator, גם כשבודקים את הפייתון דרך cmd, גם כשעובדים עם PyCharm.
- מומלץ לפני שאתם עונים לבקשה הספציפית שאתם רוצים לענות לה עם התשובה שלכם – לראות שאתם מקבלים מידע כמו שצריך.
- חשבו טוב לפני שאתם רצים לכתוב – איך אתם רוצים שהקוד ייראה, מה בסופו של יום התוכנה שלכם אמורה לעשות.
- בכל פעם שתרצו לבדוק את התוכנה שלכם, מומלץ שתבצעו את ההכנות מחדש עד לשלב פתיחת הדפדפן כולל.
- בכדי להכניס מידע בינארי למחרוזת בפייתון, עליכם להוסיף x\ לפני כל בייט – ואז את ערכו ההקסאדצילמי. לדוגמא, במידה ונרצה להכניס את הערכים 0x37 0x13, נכתוב בפייתון:
  - My_binary_string = '\x13\x37'
- שימו לב שהפרוטוקול הוא לא פרוטוקול טקסטואלי. היעזרו בפונקציה hex בפייתון. לדוגמא – hex(213) = 0xD5
- שימו לב לכך שבתרגיל אין צורך לבצע פעולות על שכבת התעבורה, פרוטוקול DNS עובר בשכבת האפליקציה ולכן הדבר היחידי שצריך לבצע בקשר לשכבת התעבורה הוא פתיחת UDP socket

<u>אקסטרה:</u>

- <u>אקסטרה #1:</u> גרמו לבקשה הקודמת להפנות ל127.0.0.1, פתחו את שרת הHTTP מהתרגילים הקודמים שלכם. מה קרה?
- <u>אקסטרה #2:</u> גרמו לתוכנה שלכם להפנות IP לפי כתובת מוגדרת מראש – בצורה גנרית. כך שלדוגמא גלישה לnana10.co.il תיתן את גוגל, וגלישה לgoogle.co.il תיתן לנו את nana10.co.il, וכל כתובת שנרצה להוסיף בעתיד – נוכל ללא מאמץ רב.
- <u>אקסטרה #3:</u> ממשו את אותו התרגיל, אך במקום להאזין על פורט 53 באמצעות שרת – צרו filter בscapy שיבצע את העבודה.
- <u>אקסטרה #4:</u> גרמו לשרת הHTTP שלכם לתמוך ביותר מדומיין אחד ולהחזיר תשובות ועמודים לבחירתכם per-domain.

קרדיט: איל אבני

עריכה: ברק גונן