**דוח – תרגיל 4**

**מבוא לרשתות תקשורת**

**עידו ברקאי 326629987**

**יוגב אברבנאל**

**חלק א – שרת אינטרנט**

**משימה 1: התחברות לשרת apche2 מאותו המחשב**

בשלב זה הפעלנו את שרת apache2 על המחשב והתחברנו מהדפדפן לשרת על מנת לקבל את דף האינטרנט:

Graphical user interface, text, application

Description automatically generated

ניתן לראות שנפתח חיבור יחיד אשר לא נסגר בשורות 1-3 יש את מנגנון פתיחת החיבור של tcp (3 way handshake)

על החיבורים עבר מידע של שכבת האפליקציה בפרוטוקול tcp.

Graphical user interface, text, application, email

Description automatically generatedכאשר הלקוח (הדפדפן( מתחבר לשרת הוא שולח הודעת GET כדי לקבל את הhtml של העמוד, ניתן לראות אותה בתעבורה בהודעה 4, תוכנה הוא:

Graphical user interface, text, application, email

Description automatically generatedרואים שהוא מבקש את הקבצים הבאים:

את הhtml, תמונות מסוימות וכו’.

בשורה 5 מוחזר ACK על הודעה 4.

בשורה 6 ניתן לראות את תגובת השרת לדפדפן, הוא מחזיר הודעה בסטטוס OK עם תוכן הודעה שהוא הhtml של העמוד, ה-header שבו סטטוס ההודעה כפי שניתן לראות:

Graphical user interface, text, application, email

Description automatically generated

תוכן ההודעה כנראה דחוס ולכן לא ברור:

Graphical user interface, text, application, email

Description automatically generated

**משימה 1.2 : ביטול מנגנון ה segmentation offload**

בשלב זה ביטלנו את מנגנון ה segmentation offload ובדקנו את ההבדלים בין גלישה ממחשב שונה לגלישה מהמחשב בו השרת מורץ, וכן את ההבדלים בין גלישה בסתר לגלישה "רגילה".

השתמשנו בפקודה ifconfig על מנת למצוא את כתובת ה-ip של המחשב בו השרת מורץ ולפנות אליו מהדפדפן:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כאמור, ניתן לראות שהשרת מורץ על מחשב עם כתובת ip 192.168.1.189.

ראשית, נציג את התעבורה שהסנפנו מהמחשב השני בגלישה "רגילה":

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

ניתן לראות תחילה את החיבור TCP הרגיל בין שני המחשבים, ע"י 3 way handshake – כמובן בדומה לחיבור לעיל מהמחשב בו השרת הורץ.

מצד שני, אנו רואים שינוי במספר הפקטות שהוסנפו לאורך החיבור בין שני המחשבים – התעבורה גדלה לעומת התעבורה שהייתה בהרצה לעיל.

ההבדל נובע מכיבוי מנגנון ה segmentation offload – כעת, ניתן לראות שהפקטות שלמעלה נשלחו בפעם אחת הופרדו למספר פקטות שונות ונשלחו אחת לאחר השנייה כמו שציפינו, הדבר מתבטא גם ע"י תשובת השרת continuantion:



ניתן לראות שהפעם בניגוד להרצה מאותו מחשב התחברנו להוסט שונה 192.168.1.189:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

ובתגובה קיבלנו את המשאב המבוקש מהשרת, ניתן לראות זאת ע"י סטטוס תשובה 200 OK:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**גלישה בסתר**

כעת, ביצענו בקשת HTTP עי גלישה לשרת מהדפדפן גלישה בסתר, נציג את התעבורה שהוסנפה עי wireshark:

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

ניתן לראות תחילה את החיבור TCP הרגיל בין שני המחשבים, ע"י 3 way handshake – כמובן בדומה לחיבור מהגלישה הרגילה.

כמו כן, לא חל שינוי מיוחד במספר הפקטות שהוסנפו לאורך החיבור בין שני המחשבים.

ניתן לראות שגם הפעם בדומה להרצה מהדפדפן הרגיל התחברנו להוסט 192.168.1.189:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

ובתגובה קיבלנו את המשאב המבוקש מהשרת, ניתן לראות זאת ע"י סטטוס תשובה 200 OK:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

חוסר-ההבדל נובע מכך שבשני החיבורים התבצעה קריאה בפעם הראשונה אל השרת, ולכן לא נשמר שום מידע ב cache , ובפרט השרת היה צריך לשלוח בשני החיבורים את המידע כולו.

כמו כן, לאחר עוד בדיקה, שמנו לב כי אם הייתה מתבצעת בקשת HTTP לשרת בפעם השנייה מהדפדפן הרגיל, הוא היה לוקח את המידע המבוקש מה cache (בעזרת מנגנון cookies).

**חלק ב – שרת DNS**

**משימה 2.1 : שרת DNS לא אוטורטיבי:**

בהתחלה עשינו nslookup ל-meta, קבלנו את התעבורה הבאה:

Graphical user interface, text, application

Description automatically generated

בשורה 7 ניתן לראות את הפניה לשרת הdns שהגדרנו, לאחר מכן נשים לב שהוא פונה לגוגל (עם כתובות בipv6), בשורות 5-6,8-11, ואז בשורה 13 השרת dns המקומי מחזיר את התשובה שקיבל מגוגל.

Graphical user interface, text, application, email

Description automatically generatedכעת הרצנו שוב nslookup ל-meta, וקבלנו את התעבורה הבאה:

נשים לב שהפעם כמו קודם בשורה 1, אנו פונים לשרת dns המקומי, אך הפעם שמור לא כבר בcache הכתובת של meta ולכן הוא לא פונה לגוגל וישר מחזיר לנו תשובה בשורה 2.

הסבר על השדות בפרוטוקול DNS:

Graphical user interface, text, application, email

Description automatically generatedבקשת הDNS:

נעבור על השדות:

Graphical user interface, text, application

Description automatically generatedכלומר מספר השאילתות-1

נכנס לשאילתה,

Graphical user interface, text, application, email

Description automatically generated

ניתן לראות שמבקשים את כתובת הIPv4 לפי type A, של הdomain: meta.com

תשובת הDNS:

Graphical user interface, text, application

Description automatically generated

נעבור על השדות:

נשים לב שהID זהה-Graphical user interface, text, application

Description automatically generated

יש תשובה אחת-Graphical user interface, text, application

Description automatically generated

כעת נשים לב שהשאלה שעליה הוא ענה היא מה ה-IP של meta, כלומר ענה לשאלה שלנו:

Graphical user interface, text, application, email

Description automatically generated

בנוסף ניתן לראות שאכן היא ה-IP.

בדיקת הcache:

בהתחלה היה בקאש רק את meta שחיפשנו קודם לכן:

Text

Description automatically generated

אחר כך הרצנו שוב, הפעם עם mako וראינו שה-IP נוסף לקאש:

Text

Description automatically generated

**משימה 2.2 : שרת DNS אוטורטיבי**

בשלב זה הגדרנו את שרת ה DNS להיות שרת אוטורטיבי – הגדרנו לשרת קובץ שיכיל את הניהול של הדומיין biu.ac.il וכן הגדרנו רשומות מתאימות שימפו לנו בין דומיינים מסוימים לכתובת ה ip של המחשב שלנו.

נדגים עבור כל אחת מהרשומות שהשרת אכן עונה את התשובות הנכונות בהתאם לרשומות שהגדרנו בקובץ.

**רשומת NS**

ברשומה זו מיפינו בין שרת השמות של הדומיין biu.ac.il לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט, כתום, צילום מסך, הגדר

התיאור נוצר באופן אוטומטי

**תצלום 2.1 : מיפוי בין שרת השמות של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג NS לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת השמות האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

נשים לב שאף התבצע A על מנת לדעת את כתובת ה ip של שרת השמות (כפי שציפינו), עבורה מופתה כתובת הip של המחשב שלנו – כפי שהגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**רשומת MX**

ברשומה זו מיפינו בין השרת המשמש את הדומיין biu.ac.il לקבלה של דואר אלקטרוני לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**תצלום 2.2 : מיפוי בין שרת הדואל של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג MX לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת הדואל האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

נשים לב שאף התבצע A על מנת לדעת את כתובת ה ip של שרת הדואל (כפי שציפינו), עבורה מופתה כתובת הip של המחשב שלנו – כפי שהגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**רשומת A**

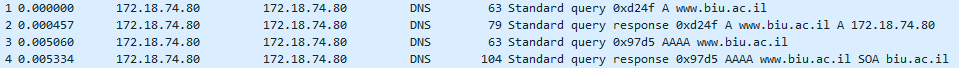
ברשומה זו מיפינו בין השרת המשמש את הדומיין [www.biu](http://www.biu).ac.il לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**תצלום 2.3 : מיפוי בין שרת הדואל של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג A לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת הדואל האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

עוד נוכל לשים לב, כי התבצעה אף בקשת AAAA לזיהוי כתובת בגרסה ipv6

אם נשים לב טוב יותר, נוכל לראות כי השרת מחזיר תשובת SOA (start of authority) – רשומה שמצביעה על המצאותו של ה zone.

אכן, בתשובה השרת מחזיר את הפרטים שהיו כתובים ברשומת ה SOA שהגדרנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**חלק ג – שרת proxy**

Graphical user interface, text, application

Description automatically generatedגלשנו לאתר http, בכתובת <http://info.cern.ch>., ניתן לראות את הבקשה של עמוד הhtml של האתר משרת הפרוקסי: (שורה 4)

כעת, שרת הפרוקסי שלנו ביצע שאילתת DNS משרתי גוגל על מנת לדעת כתובת IP של העמוד:Application

Description automatically generated with medium confidence

Application

Description automatically generated with medium confidence

ניתן לראות כי השרת מחזיר תשובת DNS בו הוא מודיע שהאתר שלנו נמצא בכתובת 188.184.21.108.

כעת, שרת הפרוקסי מבצע בקשת HTTP על מנת לקבל את התוכן שנמצא בעמוד:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

הפרוקסי מקבל מהאתר את העמוד וכל התמונות ודברים נוספים שלהם הוא זקוק להצגת מסך הבית.

ואז שרת הפרוקסי מחזיר למחשב ממנו גלשנו לאתר את התשובות שהוא קיבל. כלומר השרת פרוקסי הינו שרת מתווך:

Graphical user interface, text, application

Description automatically generated

כלומר, יש חיבור tcp אחד לחבר בין השרת פרוקסי למחשב הגולש לאתר,וחיבור tcp נוסף נפרד בין שרת הפרוקסי לאתר אליו גלשנו (וכן בוצעה שאילתת DNS משרת הפרוקסי).