תקשורת מטלה 3

מגישים: אריאל יפעי ת.ז 206159394, מוטי דהרי ת.ז 308212570

קישור לגיטהב:

https://github.com/ArielYifee/Computer-network-Ex 3.git

מספר commit:

b67976b63c39195dfa9a88d0de3d4caa129c076b

חלק א:

- בשיטת DoH התחבורה מתרכזת במספר מאוד קטן של שרתים כך שהטעינה בזמן קצרה,
 ועם דרך ל- DoH ש יתרון וגם DoH עובד עם פרוטוקול TCP כך שבמקרה של חבילות שאבדו בדרך ל- DoH יש יתרון בשליחה מהירה של המידע.
 - 2. נתון 4 חסרונות, ניתן לקחת את ה-2 חסרונות שאתם הכי מתחברים אליהם:
 - א. השיטה דוחה כל סוג של שיטת סינון DNS ומספקת מידע על חיבור האבטחה של המשתמש.
- ב. מכיוון שבשיטת DoH התחבורה מתרכזת במספר קטן של שרתים, ככה שחברות עם חיבור לאינטרנט פרטי (private) לא יכולות לבנות רשת בשיטת DoH, היא לא יכולה להימנע מחדירת רשת או להימנע מעובדי החברה לשימוש באתר או יישום שנבנה על DoH כך שהוא חשוף לחדירה ולא יכול להימנע מהעובדים שלהם להשתמש ביישום עם סיכון לתוכנה זדונית.
- מוסיף עוד חומה להצפנה של משתמשים, חברות האבטחה מאבדות את היכולת שלהם להתמודדות עם אנשים שיכולים לנצל לרעה את השימוש ב DoH.
 - ר. משתמש שמעוניין להשתמש במימוש של http על DNS חייב להתקין תוכנה נוספת שתאפשר לו שימוש בפרוטוקול, מכיוון שאין ל DoH תמיכה ברוב מערכות ההפעלה. ובמידה וירצו לסדר את זה הם יוכלו להתקיים plugin חומרה על על הדפדפן שיאפשר שימוש בDoH.
 - על גבי פרוטוקול DNS אפשר להתקין תוכנה http: א. פתרון ל-ד: בכדי להוסיף שימוש ב-bttp שתאפשר שימוש ב-DoH, בנוסף אין תמיכה לרוב מערכות ההפעלה ולכן יוכלו להתקין תוסף לדפדפן שיאפשר שימוש ב-DoH.
 - ב. פתרון ל-ב: אנו יכולים לגרום לרשת של החברה לאפשר לנו לבקר רק בכתובת אתר ידועה מרשימה כלשהי ולחסום את כל שאר כתובות ה- ip ואז לא תהיה גישה לשאר הכתובות.
- 4. א. מימוש DoH ברמת האפליקציות: היא מותקנת ישירות על הדפדפן והיא הפתרון הקל ביותר של התקנת DoH החיסרון של זה שלא כל הדפדפנים תומכים בזה, אלה שלא תומכים יעשו שימוש בפרוטוקול של DNS ודבר זה גורם לבעיות אבטחה.
 - ב. מימוש DoH ברמת שרת proxy* ברשת: היתרון זה שהוא ישלח שאילתות(שאילות של DNS שלא מוצפנות) בצורות קבועות לשרת המקומי אבל שרת היעד ישלח את השאילתות ע"י פרוטוקול DoH וזה ללא הצורך בשינוי הגדרות המערכת, החיסרון בזה היא עניין ההצפנה של המידע.

ג. מימוש DoH ברמת שרת proxy מקומי: אחרי התקנה שרת ה- proxy זה יוביל לשימוש דומה לשל הדפדפן שממש דומה לפרוטוקול DoH במידה ותהיה התקפה על הרשת המקומית הוא לא יצליח לקרוא את השאילתות הDNS מכיוון שהשאילתות האלה מוצפנות מהרגע שהם עוזבים את המכונה שממנו יוצא המידע, החיסרון בזה הוא שזה יכול לעלות בהמון משאבים מהמערכת.

ד. התקנת plugin המממש DoH ברמת הגדרות המחשב: התקנת התוסף במערכת הפעלה בעייתית מכיוון שאין תמיכה (מעט מאוד מערכות הפעלה תומכות בזה), היתרון בזה DoH בעייתית מכיוון שאין תמיכה (מעט מאוד מערכות הפעלה תומכות בזה), היתרוב ברמת ההגדרה של מערכת ההפעלה יוגדר, אנחנו לא צריכים להתמודד עם התקנת הרחבות נוספות ובמקום זה היא עובדת ישירות לפי סדר מערכת ההפעלה שעליה אנחנו עובדים, אך החיסרון בזה שמכיוון שלא כל מערכות ההפעלה תומכות אז יעשה שימוש בפרוטוקול DNS הלא מוצפן.

לדעתי השיטה המועדפת ביותר היא התקנה על המחשב כי אז אנחנו לא צריכים להתמודד עם התצורה מכיוון שזה מגיע ישר עם המערכת הפעלה וה-plugin שעובדת עם פרוטוקול DoH ודבר זה עוזר בהצפנת המידע בשימוש בפתרון זה הבעיה היחידה היא שאין תמיכה בכך בהרבה מערכות הפעלה.

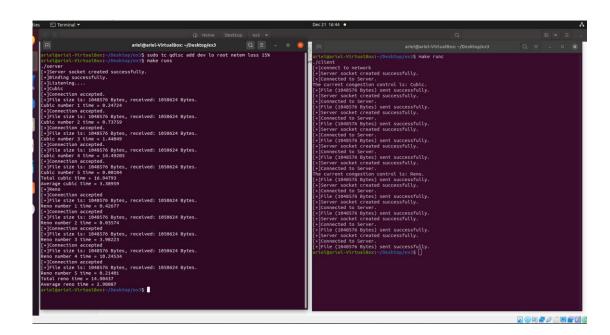
5. מכיוון שב- DoH משתמש עם פרוטוקול TCP והפרוטוקול הזה אמין, בנוסף קיימת בקרה על החבילות,, מכיוון שהוא אמין ושולט על החבילות שאבדו במהלך הבקשה. במידה וחבילה נאבדת יש מנגנון ששולח 3 סינגלים (ping) לחבילות לפני שהיא נאבדת, ואז הוא יודע לשלוח מחדש את החבילה האבודה, באופן שונה DO53 שולח באמצעות פרוטוקול UDP ששולח את כל המידע בערוץ בלי תגובה ואם חבילה נאבדת נצטרך לשלוח מחדש את כל החבילות.

חלק ב:

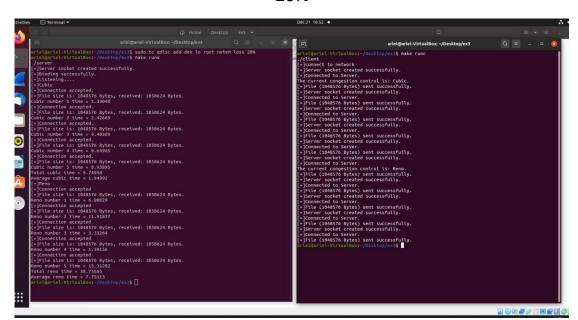
| Reno | | | Cı | ubic | אחוזי איבוד פאקטות |
|--------------------|--------------------|--|--------------------|--------------------|--------------------|
| Total = 2.57950 | Average = 0.51590 | | Total = 2.50270 | Average = 0.50054 | 10% |
| Total = 14.90437 | Average = 2.98807 | | Total = 16.94793 | Average = 3.38959 | 15% |
| Total = 38.75563 | Average = 7.75113 | | Total = 9.74958 | Average = 1.94992 | 20% |
| Total = 163.41555 | Average = 32.68311 | | Total = 61.17447 | Average = 12.23489 | 25% |
| Total = לא רץ | Average = לא רץ | | Total = לא רץ | Average = לא רץ | 30% |

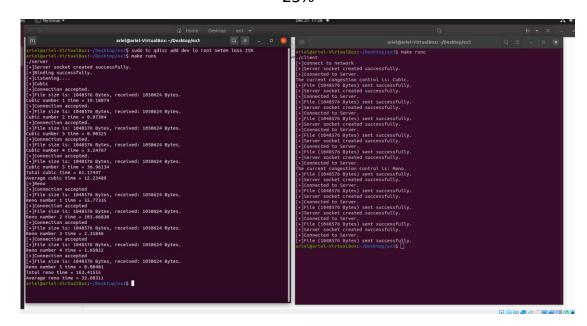
כאשר אנו מנסים להריץ את השליחה ב – 30% מצליחים להגיע רק 3 קבצים (לעיתים 4), ניסינו להריץ כמה פעמים אך תוצאה זהה בכל פעם. פתחנו את ה – wireshark בכדי לנסות להבין איפה זה נופל ולמה זה לא נשלח כמו שצריך לשרת, ראינו כמה תופעות הראשונה היא הודעת Keep-Alive שמשמעותה לבדוק אם החיבור עדיין קיים ועובד. השנייה היא מסוג Out-of-Order שבתכלס אומר שהפקטה הגיע בסדר אחר ממה שהיא נשלחה, השלישית היא Cero-Window שכוונתה היא להגיד לצד השולח שאנחנו לא מספיקים לקבל את המידע כי הבאפר מלא ולכן יש להאט את השליחה או להפסיק לשלוח עד שנפנה מקום בזיכרון (נסינו להגדיל את הגודל של הבאפר שלנו בתקווה שזה יפתור את הבעיה אך ללא הצלחה), לבסוף נשלחה הודעת Fin-Ack , seq = 1 בכדי לסגור את הקשר ולהתנתק.

10%



20%





30%

