מטלה 3- תקשורת

שם: עמית חג'ג'

ת.ז: 205837727

חלק א':

1. בנוסף לנושא האבטחה שDoH מייעלת, ניתן לראות שיש יתרון נוסף לשימוש DoH והוא האפשרות לעקוף את ה-ISP שמנתב את הבקשות של המשתמש.
2. חסרון אחד לשימוש בשיטה זאת היא שהרשת שלנו נעשית קל יותר לfishing. ז"א, אם במצב של שאילתת DNS רגילה הקלדתי בטעות bannk.com ה-ISP שמנתב את השאילתות שלי יודע שיש טעות ומנתב אותי ל-bank.com. אבל כאשר אנחנו משתמשים בשאילתות DoH התיקון הזה לא יתבצע וניתן לזייף במדויק את האתר bannk.com שיתאים ל-bank.com וכך הפרטים האישיים שלנו ייגנבו.

חסרון נוסף לשימוש בשאילתות מסוג זה נובע באופן ישיר מהיתרון הפרטיות והאבטחה. מכיוון שהבקשה עצמה מוצפנת בתוך תוכן ההודעה, קורה מצב שגם אם נגדיר מערכת סינון תכנים בתוך רשת ביתית, שימוש בשאילתות מסוג DoH יעקפו את הסינון הזה.

1. אני אציע דרך לעקות את החיסרון השני אותו הצגתי. כאמור יש בעיה בסינון תכנים לרשת ביתית, הדרך לשלוט שוט בתכנים שנכנסים לרשת הביתית היא ע"י הקמץ שרת פרוקסי מקומי לרשת הביתית. כך בעצם, הבקשות בתוך הרשם הביתית יצאו כשאילתת DNS רגילה וכך נשלוט עליהן. לאחר שסיננו את הבקשות בתוך הרשת הביתית, נוכל לשלוח אותן החוצה ע"י DoH.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| סוג  המימוש | ברמת האפליקציה | Proxy ברשת | Proxy מקומי | Plug-in בהגדרות המחשב |
| הסבר כללי | בדרך זו, אנו מגדירים לדפדפן בו אנו משתמשים, לשלוח מעתה והלאה רק שאילתות DoH. | בדרך זו אנחנו מתקינים DoH Proxy ברשת שלנו ומעתה והלאה כל הבקשות יעברו בשאילתת DNS בתוך הרשת שלנו, אבל שהן ייצאו זה יהיה ע"י DoH. | להתקין שרת Proxy באותה מוכנה שאנו מריצים את הדפדפן שלנו. |  |
| יתרונות | קל למימוש, מכסה את כל הבקשות של אותו דפדפן ללא קשר לתוכן הבקשה. | מאפשר להשתמש בדרך זו בלי להגדיר מחדש את ההתנהלות בתוך הרשת הביתית.  כל בקשה שיוצאת החוצה עדיין תהיה מוצפנת. | בדרך זו, גם אם יש תוקף בתוך הרשת הביתית שלי, אין לו גישה לתוכן ההודעות שאני שולח כיוון שהן מוצפנות. |  |
| חסרונות | תקף רק עבור אותו דפדפן ולבקשות העוברות דרכו. ז"א, ברגע שנשתמש בדפדפן אחר הבקשות יישלחו דרך DNS רגיל. כמו כן גם אפליקציות שונות במחשב יעבדו באותה דרך. | הבקשות אינן מוצפנות בתוך הרשת הביתית כך שפורץ יכול לגשת לתוכן שלהן אם הוא בתוך הרשת הביתית. | צריך להתקין פיזית במערכת ההפעלה ודורש הרבה עבודה כדי לממש, מכיוון שאנחנו רוצים לאבטח כל בקשה שיוצאת מהמכונה עצמה. |  |
|  |  |  |  |  |

1. כאשר נעבוד ברשת שקיים בה איבוד פקטות, נעדיף להשתמש בפרוטוקול DoH שלעומת Do53 הוא יכול לתזמן את השליחה מחדש של הפאקטות שנפלו בדרך.

בעזרת תזמון כזה, נחסך זמן ונקבל טעינה מהירה יותר של הדף.