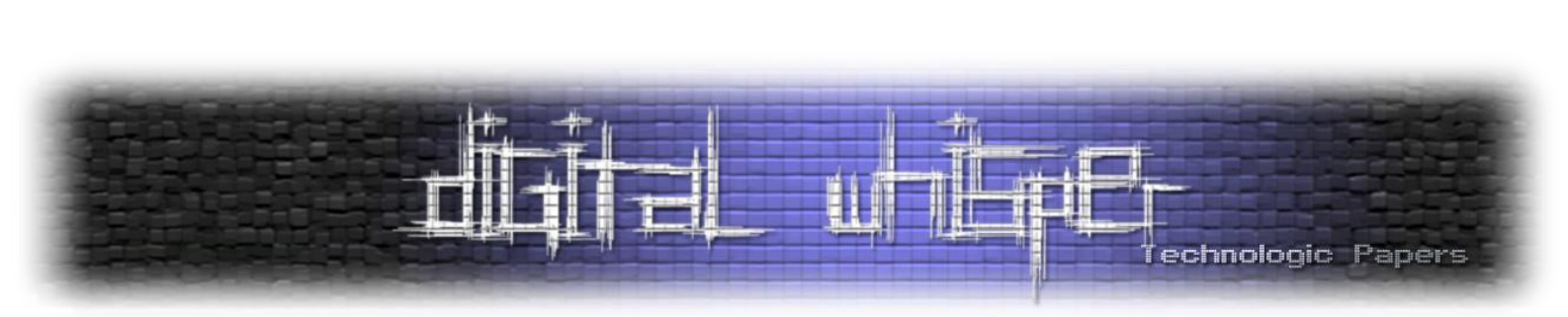


DNS Over HTTP(S) - זמן לשדרג

מאת מוטי שקורי

הקדמה

לאחרונה, חבר טוב פנה אלי להתייעצות לאחר שקיבל מייל מתוקף שדורש כופר לאחר שהשתלט לו על הנתב הביתי בעזרת חולשת 1day, ביצעו DNS Poisoning, גרמו לו להוריד backdoor, וגנבו לו קבצים מהמחשב.

מעבר למתקפה מורכבת מהרגיל, שמזכירה לכולנו שאסור לנתב הביתי שלנו להיות פתוח לאינטרנט הקר והאפל, יש פה סיבה טובה לכולנו להיזכר בהצהרה של ה-NSA ב-21 לינואר, בה הארגון מדבר על DNS Over HTTP ועל איך כדאי להטמיע אותו בצורה נכונה בארגונים.

במאמר זה נעבור בקצרה על מה זה DNS, מה זה DNS Over HTTP ויתרונות וחסרונות בפרוטוקול.

DNS - הצצה לספרי ההיסטוריה

בשנת 1983 הומצא פרוטוקול ה-DNS לראשונה לאחר ניסיונות להקל על הגלישה באינטרנט, ולהפוך אותו לנגיש.

הפרוטוקול מספק המרה בין כתובות של דומיינים המיוצגות כטקסט קריא, לכתובות IP השייכות לארגון. בשנות ה-80-90 של המאה הקודמת אבטחת המידע לא היתה בסדר העדיפויות של מפתחי וממציאי הפרוטוקולים, ולכן הפרוטוקול, כמו הרבה פרוטוקולים אחרים סובל מחולשות כאלו ואחרות.

הפרוטוקול הינו אחד הפרוטוקולים המרכזיים היחידים שעד לפני מספר שנים לא קיבל "עדכון אבטחה" ולכן עד היום מהווה משטח תקיפה מרכזי עבור תוקפים.

DNS בקצרה

אז הבנו מה זה DNS, אבל איך הוא עובד? הפרוטוקול הינו פרוטוקול רחב למדי, ולכן נכנס למה שרלוונטי לנושא המאמר בלבד, אך אני ממליץ בחום לקרוא את המאמר שנכתב על ידי קיריל לשצ'יבר ב-2011. פרוטוקול ה-DNS הינו פרטוקול שרת-לקוח, כאשר הלקוח מבקש המרה של URL אל כתובת ה-IP שלו.

הפרוטוקול משתמש בפורט 53 udp, או tcp במידה והפקטה גדולה מ-512 בתים, או במהלך zone transfer.

לפרוטוקול שתי דרכי פעולה אפשריות: שאילתה רקורסיבית ושאילתה איטרטיבית.

שאילתה רקורסיבית:

בשאילתה זו, הלקוח מבקש מהשרת את כתובת ה-IP של השרת המבוקש, ובמידה ולשרת ה-DNS אין את כתובת ה-IP של השרת המבוקש, הוא יפנה בעצמו לשרתים הנמצאים מעליו בהיררכיה, אשר עשויה להיות להם את הרשומה של השרת הנדרש.

שאילתה רקורסיבית נוחה מאוד למשתמש, הוא רק צריך לבקש את הכתובת ולא לעשות שום דבר נוסף, השרת שלו כבר ידאג לכל. בנוסף לכך, אם השרת הוא זה שמחזיר לי את התשובה הסופית, במידה ומחשב אחר באותה הרשת המקומית יבקש את אותה הכתובת, הוא יוכל להחזיר לה אותה מבלי לתשאל שוב שרתים אחרים. אך ביחד עם הנוחות, מגיע גם הסיכון כמובן. בשאילתה רקורסיבית, במידה ושרת ה-DNS יפול למתקפות שונות כמו DNS cache poisoning, הוא ישמור את ה-DNS Record הנגוע במטמון שלו, וישפיע על כל המשתמשים תחתיו.

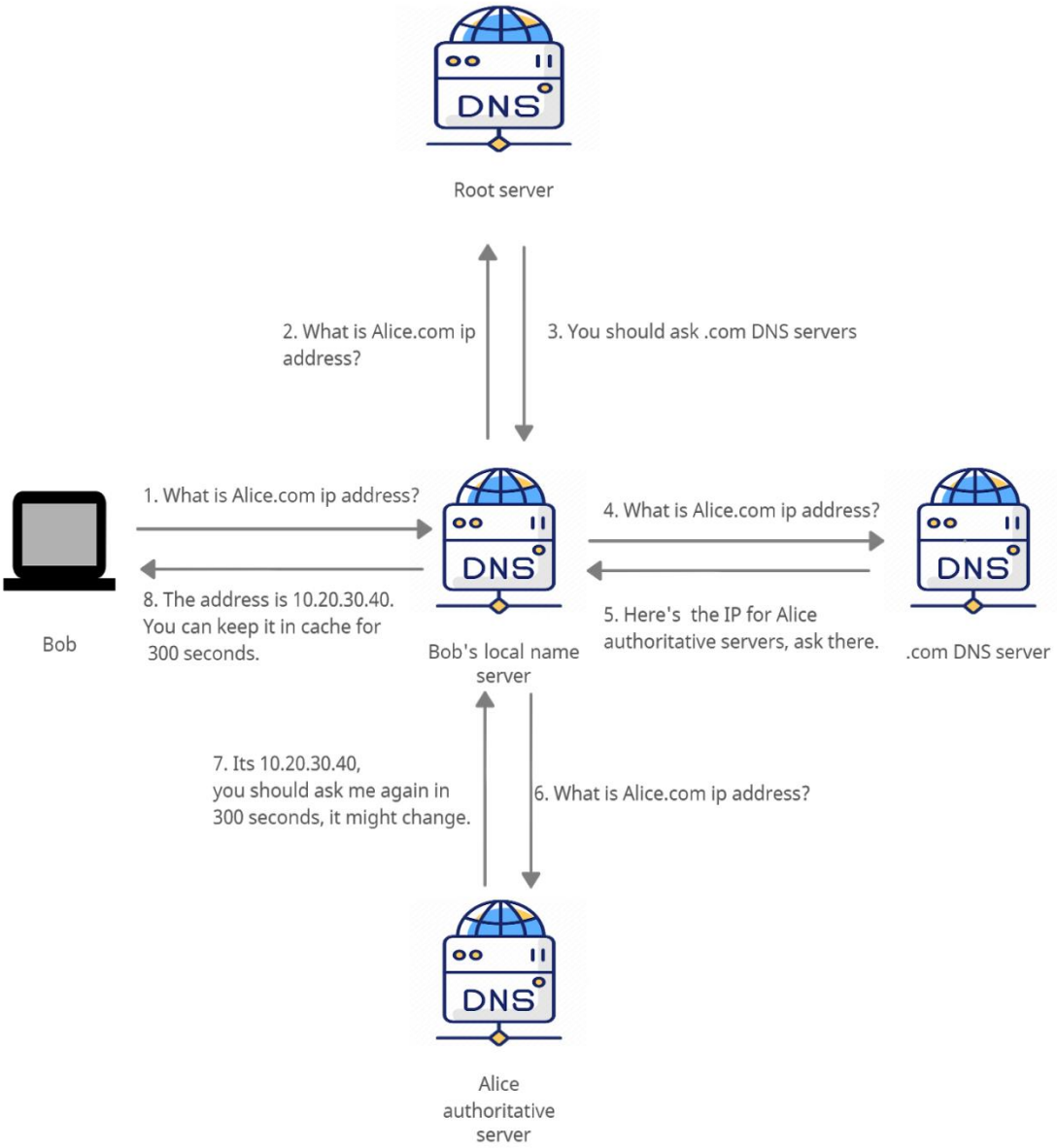
שאילתה איטרטיבית:

בשאילתה זו, הלקוח מבקש את כתובת ה-IP של השרת המבוקש, במידה ולשרת ה-DNS אין את כתובת ה-IP של השרת המבוקש, הוא יפנה את הלקוח לשרת DNS אחר בהיררכיה, שלו עשוי להיות את הרשומה הנדרשת.

ברוב המקרים, ממומשת הגישה הרקורסיבית, מכיוון שכאשר אנחנו מאפשרים לשרת ה-DNS המקומי שלנו לשמור את הרשומות במטמון, אנחנו "עוזרים" לשאר המחשבים ברשת לגשת לאתרים בקלות יותר.

במידה ועמדה תיפול ל-DNS cache poisoning בשאילתה איטרטיבית, היא היחידה שתושפע מכך, מכיוון ששרת ה-DNS המקומי שלה לא קיבל את התשובה בעצמו.

להלן תרשים זרימה על אופן פעולתה של שאילתא רקורסיבית:



[איור הממחיש שאילתה רקורסיבית של בוב, המחפש את האתר של אליס]

רגע, איפה מנגנוני האבטחה?

אז כמו שאמרנו, בשנות ה-80 אבטחת המידע לא הייתה בראש סדר העדיפויות של המפתחים, ולכן DNS בגרסתו המקורית לא קיבל שום מנגנון אבטחה אמיתי. בשנת 2005 פרסם ה-IETF את התקן הראשון של DNSSEC, מנגנון אבטחה שנועד לוודא את תקינותן של התשובות שחוזרות משרת ה-DNS.

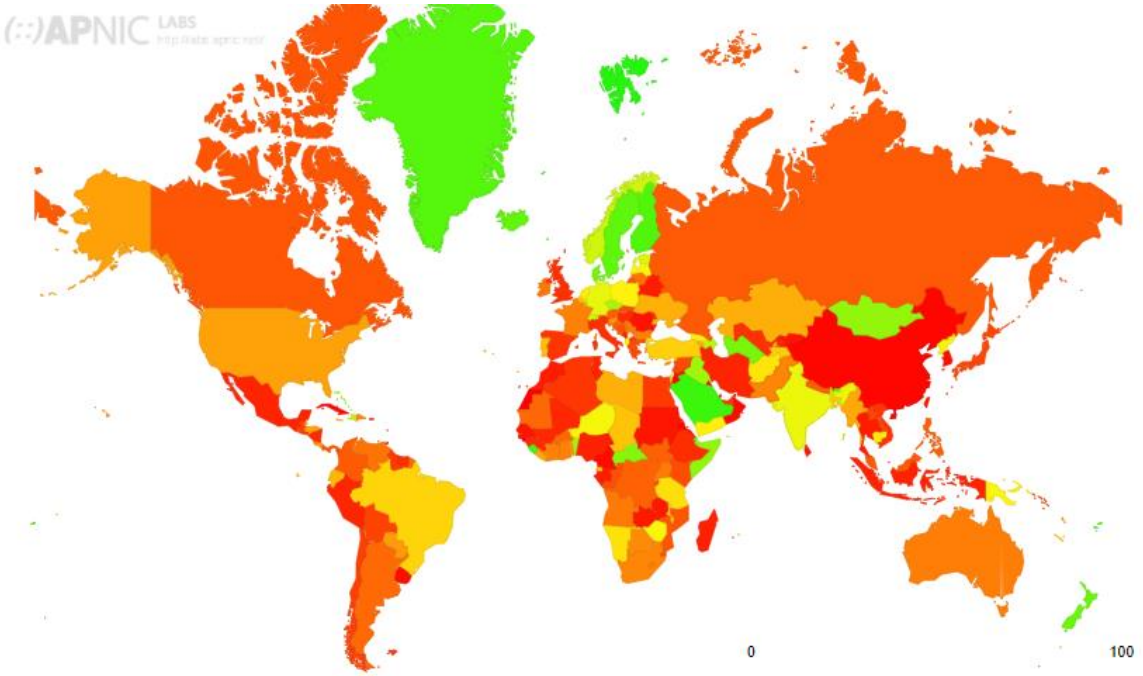
מנגנון ה-DNSSEC לא מצפין את המידע שעובר, אלא דואג לכך שכל שרת DNS יחתום את התשובה שלו, ובעזרת מפתחות ציבוריים ופרטיים השייכים לשרתים, ניתן יהיה לאמת שהתשובה מגיעה באמת מהשרת הרצוי.

המנגנון לא דואג להצפין את המידע שנשלח, אלא רק לחתום אותו על מנת לוודא את אמינותו.

לא נכנס לעמקי התקן מעבר לכך במאמר זה, אך אני ממליץ בחום לקרוא את ה-RFC המתאר על פעולת המנגנון בהרחבה, למי שמעוניין בכך. סטטיסטיקה של APNIC, רשם האינטרנט של אוקיאניה ואסיה, מציינת כי גם היום בשנת 2020, תקן ה-DNSSEC ממומש רק ב-24.5% מכלל שרתי ה-DNS בעולם.

ישראל, לצורך ההשוואה, עומדת במקום ה-71 עם אחוזי שימוש של 43.7% שימוש בתקן.

אם כך, ניתן לראות כי עדיין עומדות בפנינו שתי בעיות עיקריות - האחת היא אימות מקור המידע, והשניה היא העובדה שהמידע עובר כ-plain text:



[מתוך הסטטיסטיקה של Apnic, פברואר 2020]

אז מה זה בעצם DNS Over HTTP (או DoH)?

מדובר בהטמעה חדשה של הפרוטוקול המוכר והאהוב תחת כל היתרונות של HTTP. בשנת 2018 ה-IETF פרסם את RFC 8484 המתאר את אופן הפעולה של הפרוטוקול החדש, יתרונות, וכמובן חסרונות.

אז מה, זה סתם Tunnel?

האמת, שלא. DoH מאפשר לנו לקחת את כל ההיררכיה והמנגנון המעולה של DNS, ולהשתמש בו בשילוב של כל הפיצ'רים האהובים עלינו מ-HTTP, כמו Redirect, Compression, Caching ו-Authentication. מומלץ להשתמש ב-DoH על גבי HTTP/2, על מנת שנוכל לנצל באופן מלא את הפיצ'רים השונים שלו, כגון HTTP Pipelining ודחיסה של המידע העובר על הטווח.

במידה ונשתמש ב-HTTP/1.1, הדבר עלול להשפיע עלינו מבחינת מהירות וביצועים, שלזה כמובן יש חשיבות רבה בפרוטוקול.

בקשת DoH

ניתן לשלוח בקשת DoH על ידי שימוש במתודות GET ו-POST. כאשר נשתמש בבקשת GET, נעביר את הבקשה בלי גוף הבקשה, אלא נשתמש בפרמטר DNS, אליו נצמיד את הדומיין המבוקש מקודד ב-base64url.

שתי בקשות DoH עבור שרת המקבל בקשות ב-url הבא:

https://dnsserver.example.com/dns-query

בקשת DoH בעזרת GET עבור www.example.com תראה כך:

```
:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-message
```

ניתן לראות שימוש בדחיסה ו-padding של HTTP/2.

בקשת DoH בעזרת POST עבור אותו הדומיין תראה בצורה הבאה:

```
:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query
accept = application/dns-message
content-type = application/dns-message
content-length = 33

<33 bytes represented by the following hex encoding>
00 00 01 00 00 01 00 00  00 00 00 00 03 77 77 77
07 65 78 61 6d 70 6c 65  03 63 6f 6d 00 00 01 00
01
```

במקרה של בקשת POST, ניתן לראות את 33 הבתים של הבקשה בhex, לאחר שעברו על הטווח. בשני המקרים, ניתן לראות כי יש שימוש ב-content-type של application/dns-message. הדבר הינו חובה, ואי אפשר לוותר עליו בעת השימוש.

כל בקשת DoH מוצמדת לבקשת HTTP נפרדת, וגם פה, ניתן לבצע שימוש משמעותי ב-multiplexing של HTTP/2 על מנת להגיע למהירויות גבוהות יותר של התשובה.

תשובת DoH

כחלק מתשובת השרת, DoH משתמש ב-header בשם cache-control של HTTP על מנת להודיע לשרת/לקוח שישמור את הרשומה החדשה במטמון שלו, הערך הינו בשניות. תשובת DoH לבקשה מסוג AAAA (בקשת כתובת IPv6 של דומיין מסויים):

```
:status = 200
   content-type = application/dns-message
   content-length = 61
   cache-control = max-age=3709

   <61 bytes represented by the following hex encoding>
   00 00 81 80 00 01 00 01  00 00 00 00 03 77 77 77
   07 65 78 61 6d 70 6c 65  03 63 6f 6d 00 00 1c 00
   01 c0 0c 00 1c 00 01 00  00 0e 7d 00 10 20 01 0d
   b8 ab cd 00 12 00 01 00  02 00 03 00 04
```

במקרים בהם הבקשה מכילה מספר רשומות IP של אותו הדומיין, כאשר כל רשומה בעלת TTL שונה, מומלץ לשים ב-cache-control את הערך הנמוך ביותר, על מנת למנוע מצב בו השרת יגיש למשתמש כתובת לא נכונה.

רגע, אבל זה לא איטי מדי?

DNS חייב להיות פרוטוקול מהיר, ולכן המימוש של DoH חייב להיות מהיר גם הוא, אך יש מספר דברים שלא ניתן להתעלם מהם. פרוטוקול ה-DNS משתמש ב-UDP, אשר עצמו נוצר בשביל פקטות מהירות הדורשות פחות אמינות, מכיוון שאם הפקטה משובשת, פשוט נשלח עוד אחת.

ב-DoH אנו משתמשים ב-TCP, דבר המאט את אופן יצירת החיבור, ומשפיע על המהירות. כמובן שיש גם את נושא ההצפנה של המידע, אשר מוסיף תקורה לביצועים. במבחני ביצועים שפורסמו באתר SamKnows, ניתן לראות כי אמנם ברוב המוחלט של המקרים אכן ל-DoH יש השפעה על הביצועים, אך ההשפעה מזערית וזניחה, מכדי לא להשתמש בפרוטוקול ברשת הביתית.

ניתן לראות את מבחני הביצועים בטבלה הבאה:

Country	ISP	ISP Do53	Cloudflare Do53	Cloudflare DoH	Google Do53	Google DoH
Germany	Deutsche Telekom	15.66	34.57	38.03	33.97	33.01
Germany	Kabel Deutschland	20.67	20.41	23.03	35.58	37.55
Germany	Telefonica	17.82	19.73	21.61	49.43	49.1
Greece	CYTA	59.07	47.78	25.82	79	76.14
Greece	Cosmote	18.41	19.97	22.57	75.03	73.02
Greece	Forthnet	26.45	65.48	75.22	81.97	88.49
Italy	Fastweb	21.28	14.54	16.77	46.1	48.73
Italy	Telecom Italia	40.53	39.19	37.55	60.06	61.46
Italy	Vodafone	57.87	22.1	26.62	57.04	62.85
Portugal	MEO	33.65	20.83	21.92	62.73	66.04
Portugal	Vodafone	26.12	18.29	8.52	48.1	50.31
Spain	Orange	15.24	15.2	19.84	48.79	48.97
Spain	Telefonica	20.2	12.83	15.93	45.15	45.08
Spain	Vodafone	12.27	5.11	9.82	47.65	51.73
UK	BT	29.63	21.61	28.42	41.91	43.44
UK	Plusnet	26.24	19.88	24.65	37.86	40.59
UK	Sky	13.83	13.95	27.23	13.82	41.43
UK	TalkTalk	9.86	16.32	21.88	35.38	36.97
UK	Virgin	14.57	17.6	21.4	39.2	38.73
UK	Vodafone	32.44	22.62	17.97	37.77	33.53

[מקור: https://samknows.com/blog/dns-over-https-performance]

מדהים! אני רץ להטמיע את זה בארגון שלי

רגע, הלוואי שזה היה כזה פשוט.DoH מספק לנו הגנה על הפרטיות שלנו מפני ספקיות התקשורת, ומאפשר רק לשרת ה-DoH שלנו לראות למי אנחנו פונים, אבל הדבר לא תמיד טוב בשביל הארגונים הפרטיים. מערכות סינון תוכן רבות היום מסתמכות על העובדה הפשוטה ש-DNS אינו מוצפן, הן יכולות לראות בדיוק לאן אנחנו ניגשים, לשמור את זה, ובהתאם לפוליסות מסויימות, לחסום או לדווח על כך.

על מנת שמערכות פרטיות יוכלו לבצע סינון תוכן תוך כדי שימוש ב-DoH, יש צורך לבצע SSL/TLS stripping לפקטה, דבר העשוי להשפיע על מהירות המשתמשים בצורה משמעותית, ויכול להפוך את השימוש בו ללא כדאי בכלל. אלו לא רק מערכות לסינון תוכן, אלא גם מערכות SOC וחומות אש שנפגעות, וכתוצאה מכך גם בטיחות הארגון. במסמכם של ה-NSA, מדובר על הסוגיה. במידה ולא ניתן להשתמש בשרת DoH ארגוני, אשר מסוגל להתמודד עם מידע מוצפן ולפעול בהתאם, המלצתם של ה-NSA היא שלא להשתמש ב-DoH בכלל, על מנת שלא לסכן את בטיחות הארגון.

בנוסף לכך, ה-NSA ממליצים לחסום כל שרת DoH חיצוני, שאינו מאושר לשימוש בארגון.

בסדר, אבל זה מונע מספקית התקשורת שלי לעקוב אחרי...

אז זהו, שלא ממש. ספקיות התקשורת לא יוכלו יותר לראות את תעבורת ה-DNS שאנחנו מעבירים, אבל זה לא עוצר בעדם לדעת לאיזה אתרים אנחנו פונים. אמנם את רשומת ה-DoH הספקיות לא יוכלו לראות, אבל הן יוכלו לבצע Reverse DNS Lookup על מנת להבין לאיזה דומיין אנחנו פונים. כדי למנוע גם את זה, יש צורך לעשות שימוש בשרת פרוקסי שיעביר את המידע שלנו בשבילנו.

אוקי, אבל אני לא ארגון, איך אני משתמש ב-DoH?

נכון להיום, בפברואר 2020, ניתן להגדיר DNS Over HTTP ברמת ה-Windows אך ורק אם אתם חלק מפרויקט ה-Windows insiders, המאפשר לכם לקבל את היכולות החדשות של מערכת ההפעלה לפני כולם, מעין בטא. אראה כיצד ניתן לעשות את זה כיום, בתקווה וזה ישאר ככה, ויוכל גם לשמש אתכם בעתיד - כל מה שנדרש על מנת לעבור ל-DoH ב-Windows, זה פשוט שינוי קטן ב-registry.

נכנס ל-regedit ומשם ננווט להיררכיה הבאה:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
```

לאחר מכן נוסיף ערך DWORD בשם "**EnableAutoDoh**" ונגדיר את ערכו **2**.

לבסוף, ניתן להשתמש בכלי כגון pktmon כדי לוודא שמערכת ההפעלה שלנו לא משתמשת ב-DNS רגיל.

```
pktmon filter remove
pktmon filter add -p 53
pktmon start --etw -l real-time
```

אם הכל עובד כראוי, איננו אמורים לראות פקטות יוצאות.

סיכום

במאמר זה הבנו מה הוא הפרוטוקול DNS, מה הם סכנותיו וכמה הוא חשוב. ראינו את התחליף החדש והנוצץ שלו - DNS Over HTTP, אך האם באמת כדאי לעבור אליו ישר?

למשתמש הפשוט שיכול להרשות לעצמו את זה, אני לא רואה שום סיבה שלא לעבור, מדובר בשדרוג לאבטחה של המשתמש מבלי לפגוע יותר מדי בנוחות שלו. אך כיום, בעוד שהפרוטוקול החדש בחיתוליו, כנראה שלא הייתי רץ להעביר את הארגון שלי ל-DoH, דבר אשר יכול להזיק יותר מאשר להועיל.

whoami

מוטי שקורי, בן 21, מפתח backend, חוקר אבטחת מידע בזמני הפנוי, וסטודנט למדעי המחשב. אוהב לפתור CTF-ים ולחקור מערכות, כמו כל אדם נורמלי כמובן. לשאלות, הערות, הארות וסתם לדבר, ניתן לפנות אלי במייל:

motishaku@gmail.com

מקורות וקישורים לקריאה נוספת

- Adopting Encrypted DNS in Enterprise Environments - NSA:
  https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/
- RFC 4033 (DNS):
  https://tools.ietf.org/html/rfc4033
- RFC 8484 (DNS Over HTTP):
  https://tools.ietf.org/html/rfc8484#section-5.1
- מאמר על DNS מתוך הגליון ה-18 של Digital Whisper:
  https://www.digitalwhisper.co.il/files/Zines/0x12/DW18-4-DNS.pdf
- איך להגדיר את Windows לעבוד עם DNS Over HTTP מתוך BleepingComputer:
  https://www.bleepingcomputer.com/news/microsoft/windows-10-gets-dns-over-https-support-how-to-test/
- מבחני הביצועים מתוך האתר SamKnows:
  https://samknows.com/blog/dns-over-https-performance