בס"ד

**חלק ב' מטלה פאזינג**

הפרוטוקול שמנוטר הוא פרוטוקול dns הרשמות שיש לנו כבר בפרוטוקול הם:

* A- רשומה זו היא כתובת [IPv4](https://he.wikipedia.org/wiki/IPv4) (Address) המשויכת לשם דומיין מסוים.
* AAAA - בדומה לטיפוס A, רשומה זו היא כתובת [IPv6](https://he.wikipedia.org/wiki/IPv6).
* - NS רשומה אשר מציינת שרת אשר משמש כאחראי למסירת מידע על הדומיין המבוקש.
* - PTR רשומה זו מכילה דומיין אשר משויך לכתובת IP מסוימת (על מנת ששרת ה-DNS יוכל לחפש דומיינים על פי כתובות IP).
* - MX מכילה את כתובתו של השרת המשמש את הדומיין לקבלה של [דואר אלקטרוני](https://he.wikipedia.org/wiki/%D7%93%D7%95%D7%90%D7%A8_%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%A0%D7%99).
* CNAME – "Canonical name" - שם נוסף לאותו הדומיין.
* - TXT רשומה זו מאפשרת לצרף לכתובת ה-IP של הדומיין גם טקסט חופשי (משמשת למימוש שירותים שונים הקשורים בדומיין, כגון [DomainKeys](https://he.wikipedia.org/w/index.php?title=DomainKeys&action=edit&redlink=1)).
* [SPF](https://he.wikipedia.org/wiki/Sender_Policy_Framework)- סוג מיוחד של רשומת TXT המציינת את שמות ה־hosts מהם מותר למסור מייל בשם אותו דומיין.
* Start Of Authority – SOA - הרשומה אשר מצביעה על הימצאותו של ה־ ZONE.
* ANY

אלה הדברים הבסיסים שיש בפרוטוקול אז ישנם 2 אפשרויות:  
1. או שהם ישתמשו ב wireshark וכבר יראו אותם.  
2. נוסיף אותם לכלי שינטר מידע , ונוסיף אליו את השדות בהמשך בשביל נוחות שיראו את כל השדות באותו מקום.

החולשה העיקרית של המערכת היא בכך שמצד אחד היא מהווה תשתית קריטית ב[תקשורת מחשבים](https://he.wikipedia.org/wiki/%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA_%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D) הן ברמת פנים הארגון והן ברמת האינטרנט כולו; ומצד שני הפרוטוקול כמעט ואינו תומך באבטחה. ההתקפה הנפוצה והיחסית פשוטה היא "הרעלה" והתחזות (spoofing, poisoning) על ידי השתלת ערכים זדוניים לשמות חוקיים. דוגמה לשימוש לרעה יכולה להיות [דיוג](https://he.wikipedia.org/wiki/%D7%93%D7%99%D7%95%D7%92" \o "דיוג): השתלת כתובת של אתר זדוני תחת שם של אתר פופולרי. כך מופנה המשתמש שעושה שימוש ב-DNS ה"מורעל" לאתר אחר, אשר נראה בדיוק כמו האתר המקורי ומוסר את ססמתו שם.

בכדי להוסיף אבטחה ולמנוע man in the middle ו dns poisoning אנחנו צריכים בעצם להוסיף את השדות הבאים אשר יעזרו לוודא אבטחה(תכלס זה בדיוק אותם שדות שיש כבר ב  
(DNS Security Extensions :

* RRSIG – Resource Record Signature
* DNSKEY – DNS Public Key
* DS – Delegation Signer
* NSEC – Next Secure

ולכן את השדות האלה אנחנו נוסיף לכלי שלנו מה שיעזור לחוקרים לוודא בקלות את סוגי ההתקפות שנאמרו למעלה.