**DNS Rebinding Attack Lab**

יובל בר מעוז 314878877

רז אלבז 207276775

ראשית הגדרנו את המכונה ע"פ הנדרש במטלה, ישנם 5 קונטיינרים ואת המחשב המארח (VM host).

**הגדרות:**

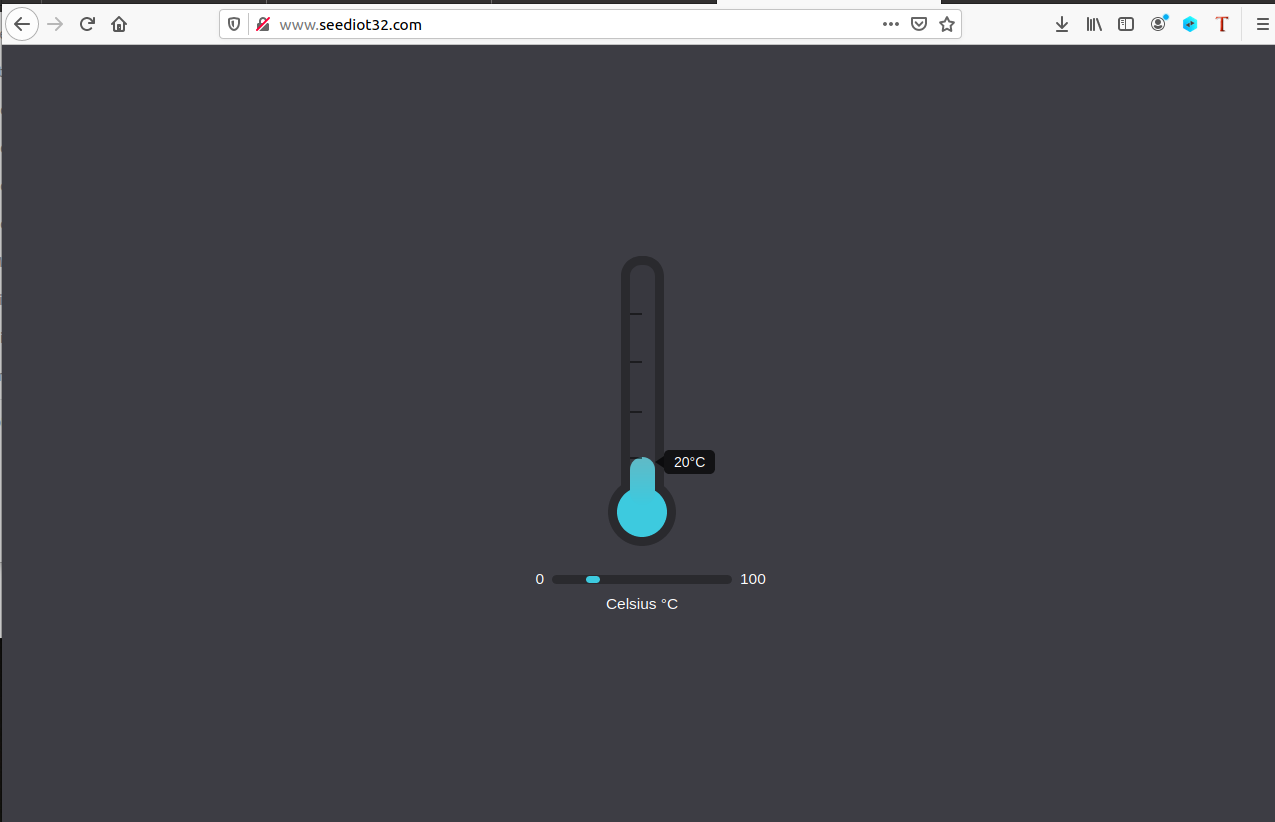
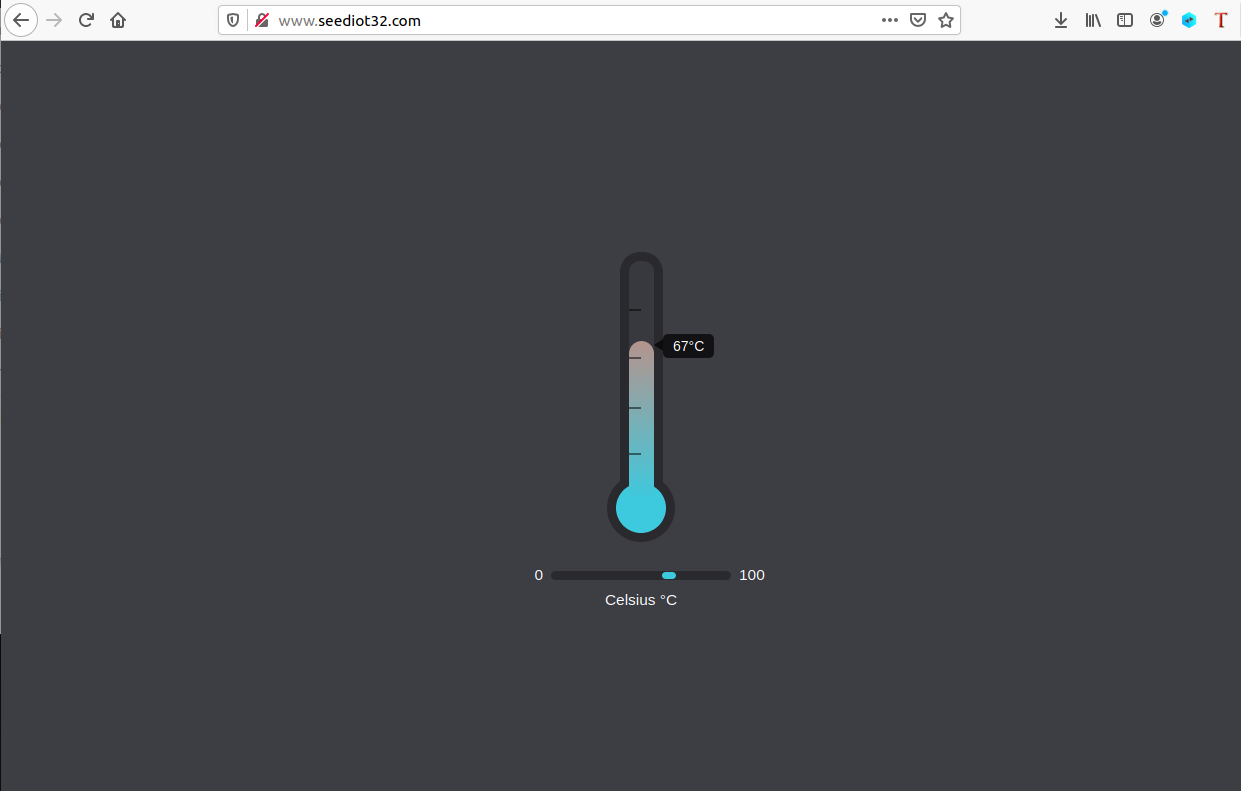
IoT - (Internet of Things) האינטרנט של הדברים הוא רשת של חפצים פיזיים ("דברים"), המשובצים בחיישנים ובתוכנה, אשר מאפשרים תקשורת בין החפצים ויכולות איסוף וניתוח מידע. האינטרנט של הדברים כולל בין השאר את תחומי "בית חכם", "עיר חכמה"' , תחבורה חכמה (כגון מכוניות אוטונומיות וכבישים חכמים).

במעבדה הבאה אנחנו נדמה מתקפה אפשרית על שרת IoT בדוגמא שלנו נתקוף תרמוסטט, שמחובר כביכול לבית חכם, ושולט על הטמפרטורה בחדר מסוים. כיוון שמכשיר הIoT נמצא מאחורי חומת אש, מכשירים שאינם ברשת לא יכולים לתקשר עם מכשור זה, ולכן לא יוכלו לשלוט בטמפרטורת התרמוסטט.

לכן על מנת להתגבר על ההגנה של חומת האש, על התוקף קודם כל להצליח להיכנס לרשת הפנימית.

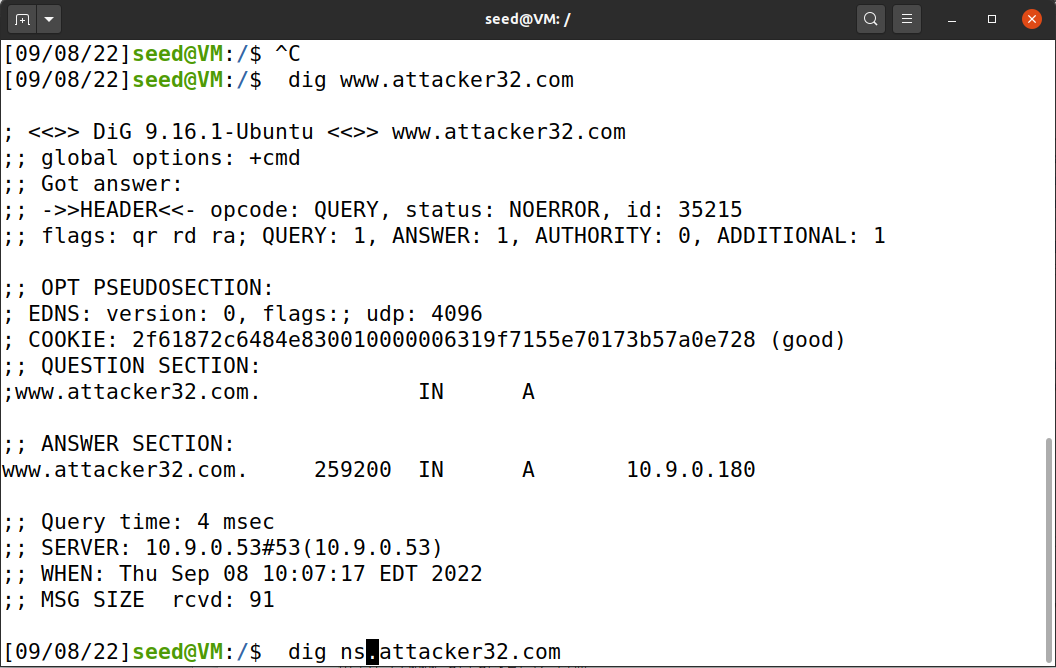
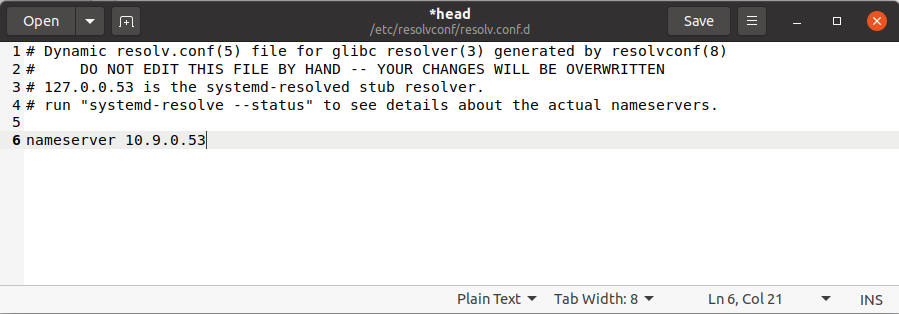
בכל זמן שבו משתמש ברשת הפנימית מבקר באתר האינטרנט של התוקף, הקוד של התוקף (קוד JavaScript) פועל למעשה מהדפדפן של המשתמש, ולכן פועל בתוך הרשת הפנימית המוגנת. עם זאת, בשל הגנות של הדפדפנים (ארגז חול וכדומה), ה- הקוד של התוקף עדיין לא יכול לקיים אינטראקציה עם מכשיר ה-IoT, למרות שהוא נמצא כעת בתוך הרשת הפנימית. המטרה של מעבדה זו היא להשתמש במתקפת ה-DNS rebinding כדי לעקוף את הגנת ארגז החול, אז קוד JavaScript מהתוקף יכול לקבל בהצלחה את המידע החיוני ממכשיר ה-IoT ו לאחר מכן השתמש במידע כדי להגדיר את הטמפרטורה של התרמוסטט לערך גבוה מסוכן.

כפי שניתן לראות בשני התמונות הבאות, באתר הבא ניתן לשלוט בטמפרטורת התרמוסטט.



נעדן את השם של השרת במיקום /etc/resolvresolv.conf ואת כתובת הip

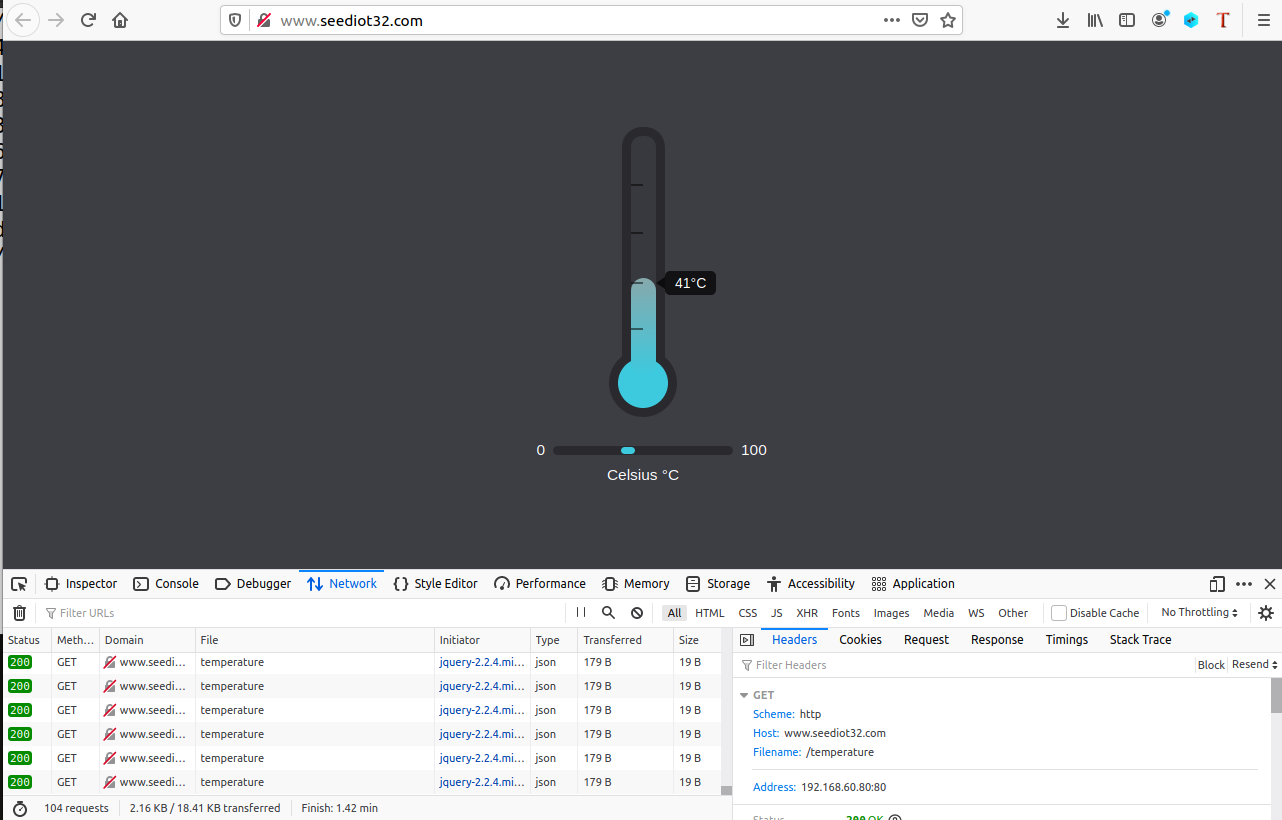
נעשה dig לכתובת השרת של האתר התוקף (המטרה של פקודת dig היא לאסוף מידע על הDNS)

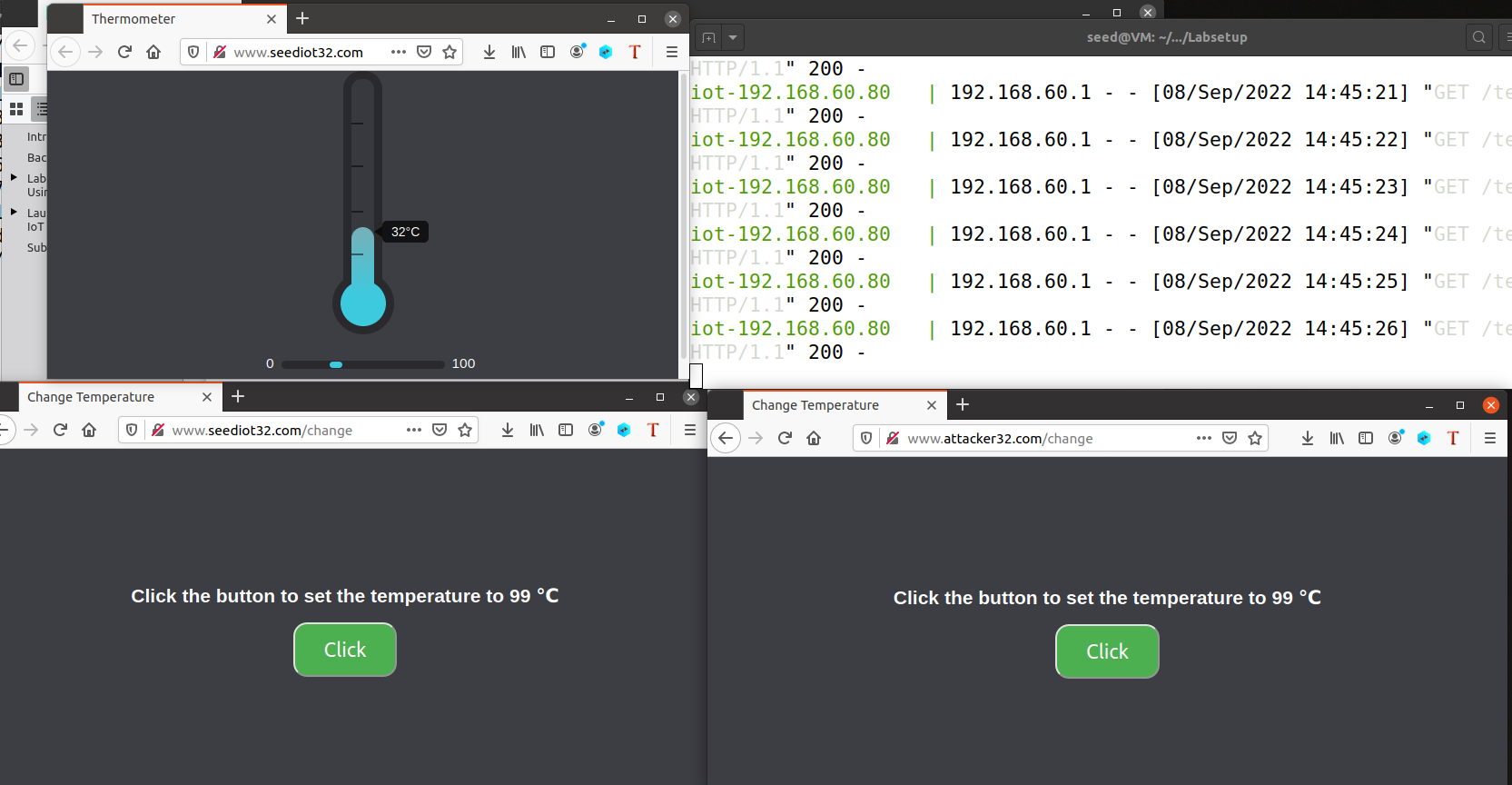


נעשה dig לname server של השרת התוקף.תמונה שמכילה טקסט

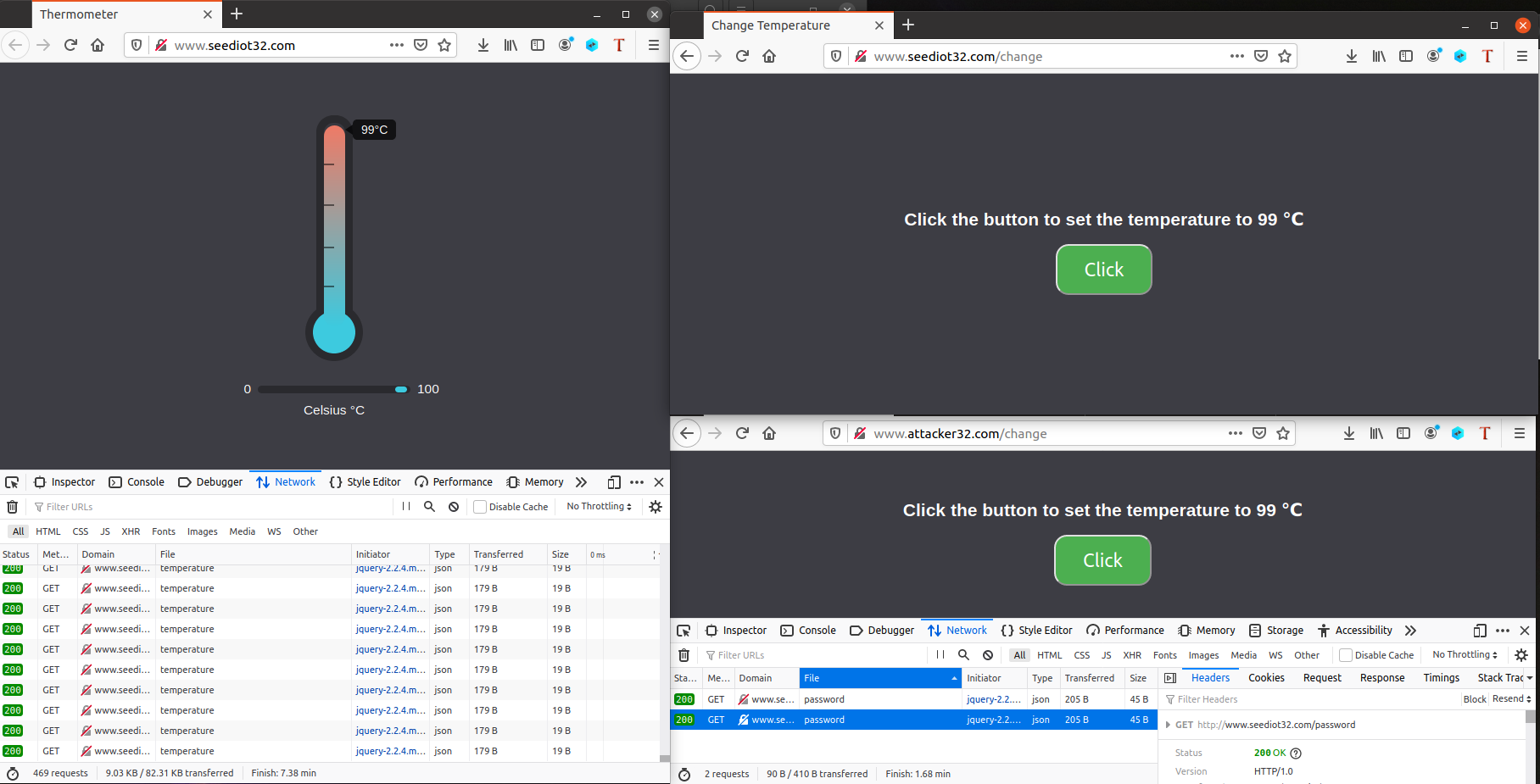
התיאור נוצר באופן אוטומטי

כאשר נפתח את הגדרות המפתח בדפדפן נוכל לראות את נתוני התעבורה של האתר, את הקוד בjavascript ובאופן כללי, עוד כלים נוספים שיוכלו לעזור לנו לנתח את האתר.

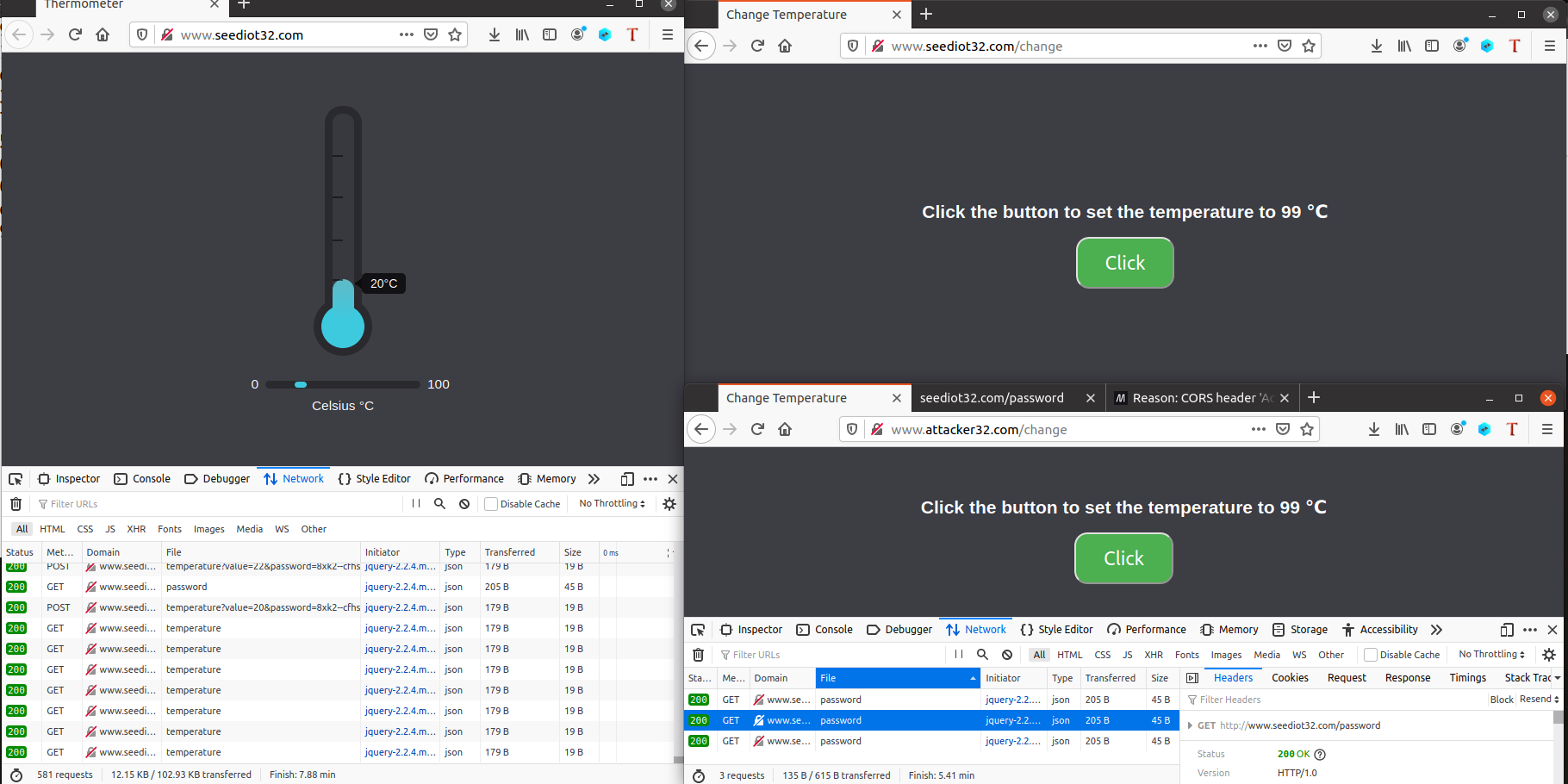


כעת פתחנו את שלושת כתובות הURL כך, משמאל למעלה נמצא השרת של IoT, משמאל למטה נמצא הכפתור ששולט על שינויים של התרמוסטט, מימין למטה נמצא האתר הזדוני שמבחינת נראות נראה זהה לאתר שאחראי על השינוי של הטמפרטורה, כעת ננסה ללחוץ על הכפתורים ונראה איך האתרים מגיבים ללחיצות על שני הכפתורים וננסה לנתח את הפעולות שהכפתורים עושים.

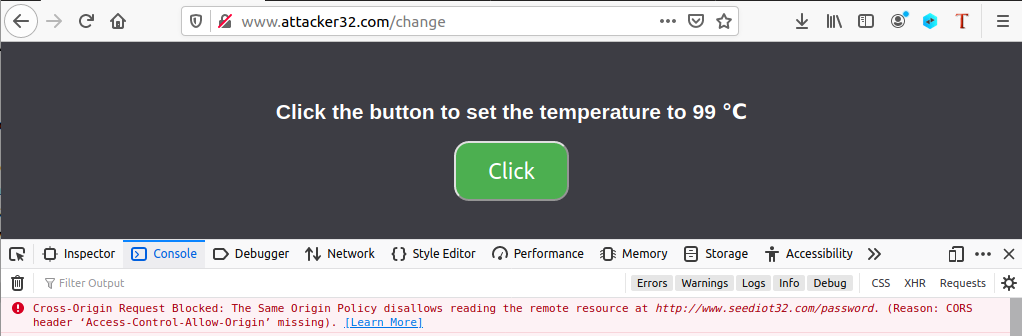
עמוד הURL השני (http://www.seedIoT32.com/change), בחלק העליון של התמונה מטה, שינה את הטמפרטורה בתרמוסטט בצורה טובה.



בעוד שעמוד הURL השלישי לא שינה את הטמפרטורה כלל, כנראה שקיימת תקלה כלשהי שעלייה לא חשבנו, אנו רואים שבפירוט של הגדרות המפתח רשומה לנו שגיאה המופיעה בתמונה הבאה.



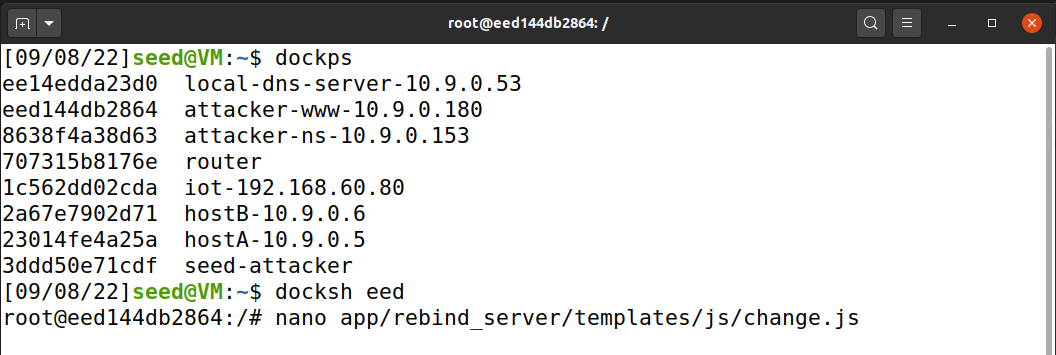
כמוכן נכתבה האזהרה הבאה



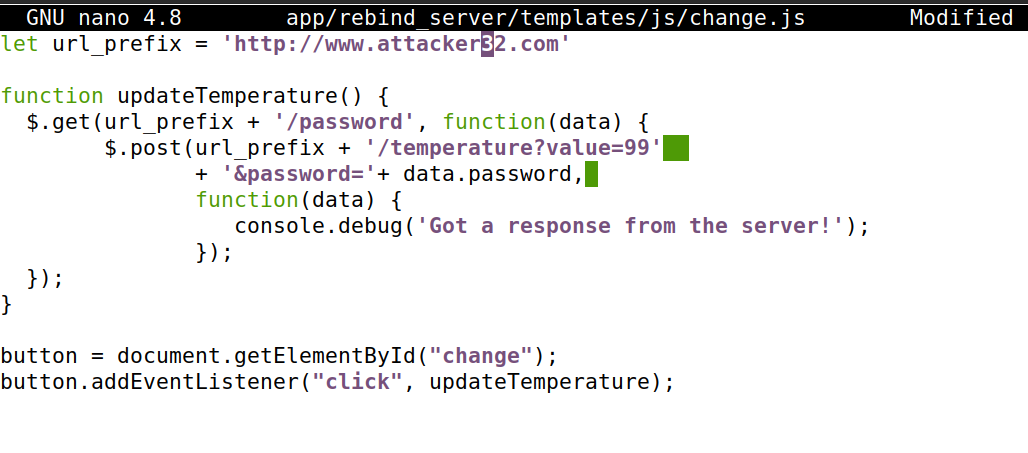
כלומר יש בעיה עם הheader של CORS – שאחראי על העברת בקשות ומידע בין שרתים ודפדפנים בצורה מאובטחת, ככל הנראה אין הרשאה לאתר זה לשלוח בקשות לכתובת הURL הראשונה (<http://www.seedIoT32>.). שזה הגיוני בהתחשב בזה שבקשת הrequest נשלחה על ידי אתר זדוני שאינו קשור באמת לאתר התרמוסטט.

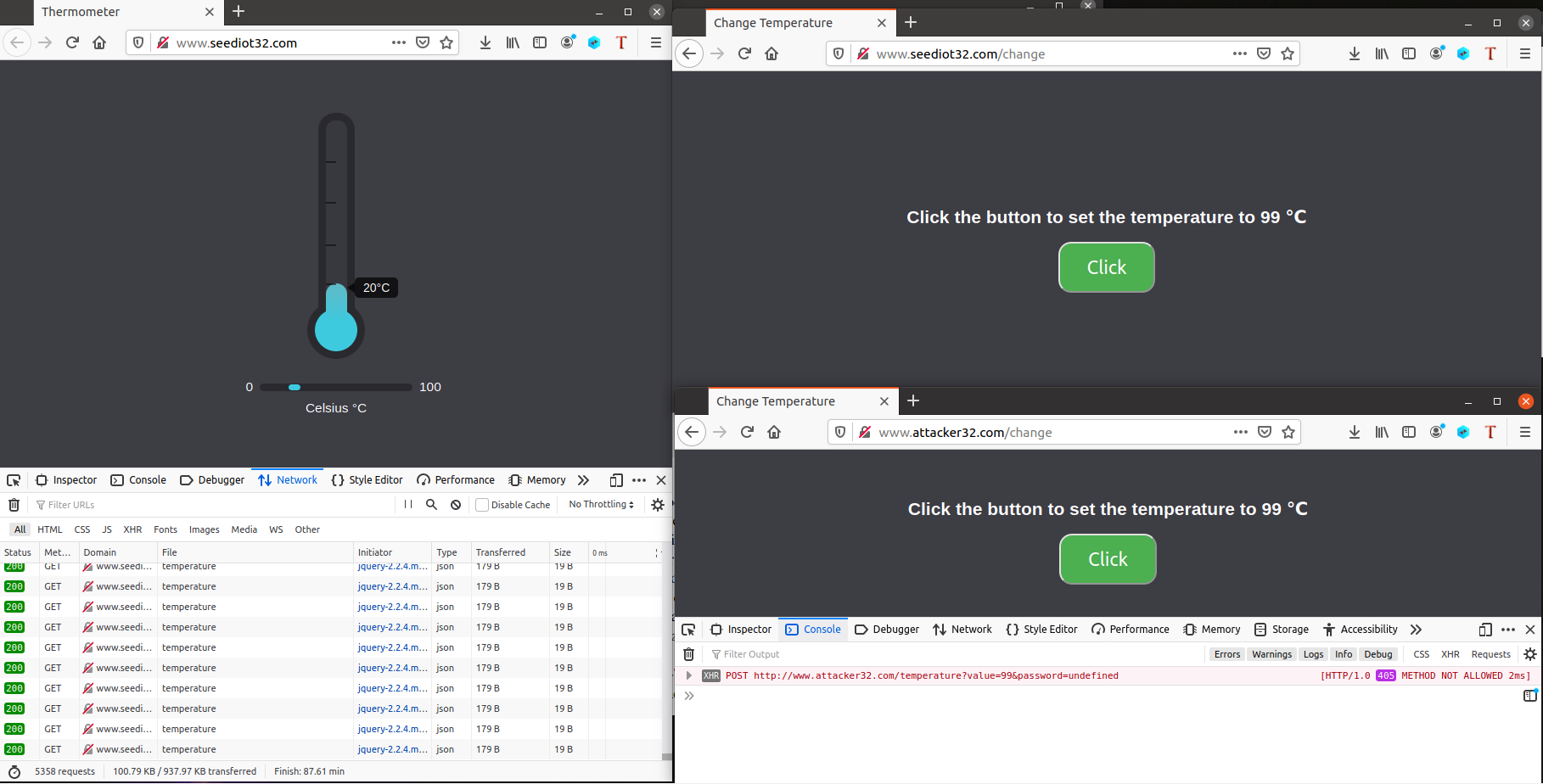
על מנת להתגבר על ה same-origin policy protection נפעל כך,

נתחבר דרך הדוקר אל השרת של התוקף (attacker-www)בכתובת 10.9.0.180 ונשנה את ההגדרות שלו



שיננו את כתובת הURL לכתובת של האתר התוקף

לאחר מכן נעשה לדוקר restart, על מנת לוודא שהנתונים עודכנו כפי הנדרש.

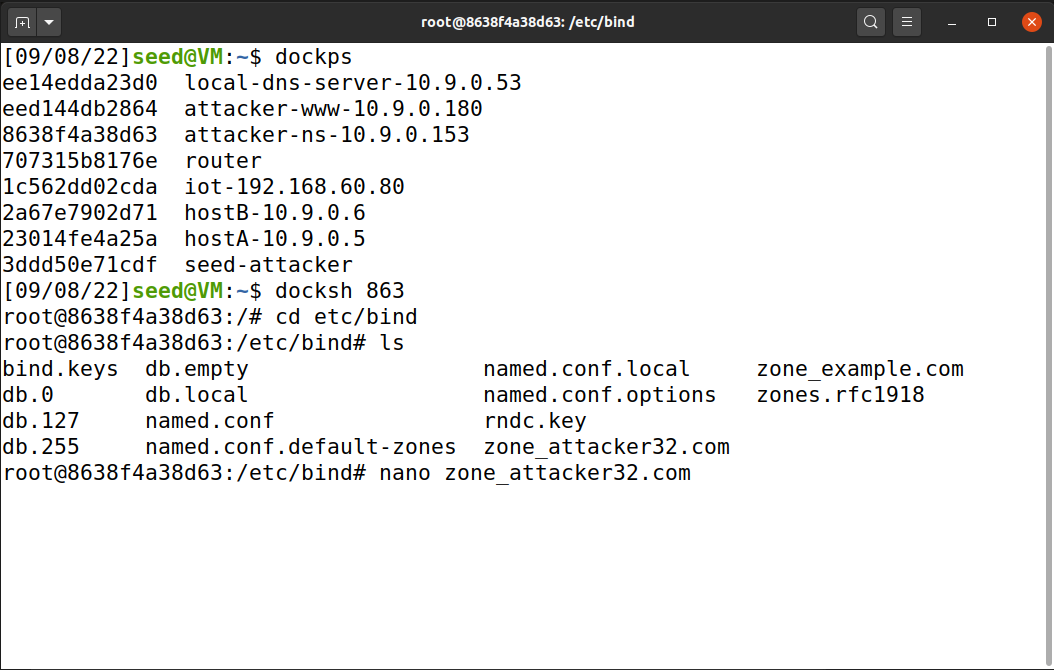


כעת רעננון את העמוד של האתר התוקף וניסנו ללחוץ שוב על הכפתור, הטמפרטורה עדיין לא משתנה (בחלון התחתון) אבל הפעם הסיבה השתנתה. הבעיה הפעם היא שגיאה 405 בפרוטוקול HTTP, שגיאה זו נוצרת כאשר השרת מכיר את סוג הבקשה, אבל מטרת המקור, האתר המותקף, אינו תומך במתודה.

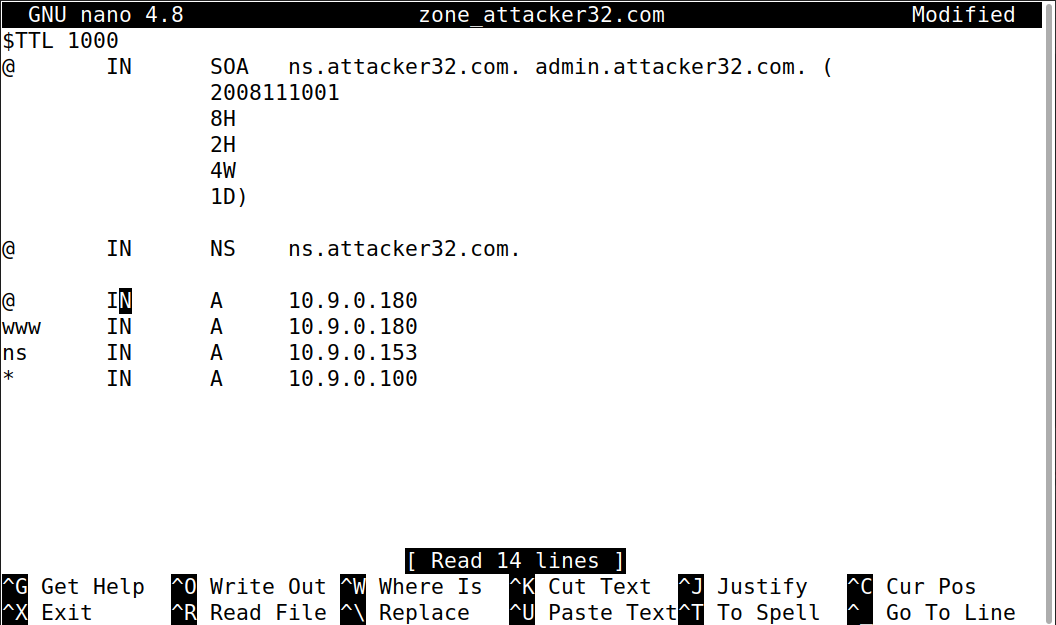
קוד הJS שלנו שלח את הבקשה לאתר <http://www.attacker32.com/> והתשובה חוזרת בחזרה לשרת הweb שלך התוקף, שזה לא מה שרצינו שיקרה. אנו רצינו שהבקשה תחזור לשרת הIoT. דבר זה יכול לקרות באמצעות שימוש בDNS rebinding.

ראשית נמפה את הכתובת <http://www.attacker32.com/> לכתובת הIP של שרת הweb של התוקף, כך שהמשתמש יוכל לקבל את הדף של <http://www.attacker32.com/change>, ולפני שנלחץ על הכפתור בדף אנחנו נחליף את כתובת הIP ושם המארח (hostname) לשרת הIot. כך שהrequest שיופעל על ידי הכפתור יגיע לשרת הIoT וזה בדיוק מה שאנו רוצים שיקרה.

על מנת לשנות את מיפוי הDNS, בתוך הדוקר של התוקף נשנה את הקובץ כך:



בקובץ הזה שיננו את הTTL והגדלנו אותו ל1000 כך שהוא ישאיר את הבקשה "בחיים" להרבה זמן.





כעת נרען את הדפדפן, וכאשר נלחץ על הכפתור בכתובת <http://www.attacker32.com/change>, נראה שהתרמוסטט עלה ל99 מעלות. כלומר ההתקפה עבדה.

