DNS REBINDING ATTACK LAB

NT140.O11.ANTT\_nhom14

Thành viên:

Nguyễn Đình Luân – 21521105

Trần Thanh Triều - 21522713

Trần Đức Trí Dũng - 21520748

Setup:

Step 1. Reduce Firefox’s DNS caching time

A screenshot of a computer

Description automatically generated

Step 2. Change /etc/hosts.

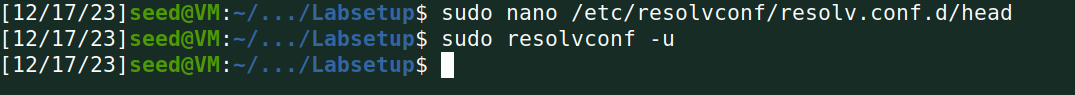
A screenshot of a computer

Description automatically generated

Step 3. Local DNS Server.

A screen shot of a computer

Description automatically generated



Đã vào được trang attacker

A screenshot of a computer

Description automatically generated

Task 1. Understanding the Same-Origin Policy Protection

Vào 3 trang trong bài lab yêu câu:

A screenshot of a computer

Description automatically generated

Ta nhận thấy rằng ở trang <http://www.seediot32.com/change> nút bấm có thể thay đổi nhiệt độ nhiệt kết còn ở trang <http://attacker32.com/change> thì không được

A screenshot of a computer error message

Description automatically generated

Mở console ra ta thấy lỗi như sau ở trang attacker32.com/change

Khi giao thức, tên miền và cổng của hai tên miền giống nhau, trình duyệt coi chúng là cùng một nguồn gốc. Điều này được thiết lập bởi trình duyệt để đảm bảo rằng tài nguyên trong một ứng dụng chỉ có thể được truy cập bởi các tài nguyên thuộc về ứng dụng đó. Trong thí nghiệm này, nhiệt độ của bộ điều khiển nhiệt độ không thể được sửa đổi vì [www.attacker32.com/change](http://www.attacker32.com/change) đến từ nguồn khác so với [www.seedIoT32.com](http://www.seediot32.com/).

Task 2. Defeat the Same-Origin Policy Protection

Step 1: Modify the JavaScript code.

A computer screen shot of a program code

Description automatically generated

Sau khi restart container: lỗi khi nãy đã thành lỗi khác

A screenshot of a computer error message

Description automatically generated

Step 2: Conduct the DNS rebinding.

A computer screen with white text

Description automatically generated

Reload trên máy attacker dns server:



Rndc flush trên máy local dns:

A group of white text

Description automatically generated

Task 3. Launch the Attack

Đã thành công:

A screenshot of a computer

Description automatically generated