Network Security and Forensics – EECS 4482
DNS Rebinding Attack
Prepared by: Dr. Ruba Al Omari[1]
Fall 2024

Contents

Disclaimer

- This assignment is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have written permission to hack.
- Creating or deploying malware, or engaging in any malicious activities is against ethical guidelines and is illegal.
- Always ensure that you have proper authorization and are acting within the bounds of the law and ethical guidelines in a controlled environment.

[1] Lab is developed by Dr. Kevin Du at www.SEEDLABS.com

Instructions

- **Uploading of course material, assignments, labs, sample solutions, or tests to online sites is prohibited. No reuse of this assignment is allowed in part or in full without my written permission.**
- This assignment should be completed individually.
- When a question asks for a screenshot, your screenshot must:
  - Include the full window (the application window, or the terminal window, etc… but not the whole display),
  - have the PROMPT setup as per the instructions, including your name, and the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
  - be clearly readable,
  - include all the information required by the question, and
  - **not** include extra commands, failed attempts, and/or error messages. Providing more than what is required will result in a penalty of:
    a. -5 Marks per extra screenshot.
    b. -5 Marks per extra command/answer/comment.
    c. -5 Mark per screenshot with error messages.
- You should type the commands below and not copy them from this document. Copying text from a .pdf or .docx file into a terminal doesn't always (almost NEVER) work as intended.
- The below instructions are for guidance, you are expected to search and troubleshoot any warnings or errors you run into while following lab instructions or working on your assignments.
- Sample screenshots (screenshots with the word SAMPLE) are for guidance only. You will/may need to run other commands that are not displayed in the sample screenshots.
- Operating Systems, vulnerable boxes, libraries, tools, and commands get updated frequently, if a command in this document is deprecated, find the current alternative command and use it. If a software in this document has a newer release you can use it.

Environment Setup

We will use the SEED Ubuntu 20.04 Virtual Machine available at https://seedsecuritylabs.org/. Refer to the Environment Setup documents on eClass for more information.

1- Download the **DNS Rebinding Attack Lab** document available here: https://seedsecuritylabs.org/Labs_20.04/Files/DNS_Rebinding/DNS_Rebinding.pdf We will refer to this document as **DNS-Rebinding-SEED** document.
2- Download the **Labsetup** file available at https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNS_Rebinding/ and save it to your SEED Ubuntu 20.04 Virtual Machine.
3- Read the DNS-Rebinding-SEED file, and use it to aid you in carrying out the below tasks which are mapped to the tasks in the DNS-Rebinding-SEED file.

1- Introduction

The objective of this lab is two-fold: (1) demonstrate how the DNS rebinding attack works, and (2) help students gain first-hand experience on how to use the DNS rebinding technique to attack IoT devices. In the setup, we have a simulated IoT device, which can be controlled through a web interface (this is typical for many IoT devices). Many IoT devices do not have a strong protection mechanism, if attackers can directly interact with them, they can easily compromise these devices.

The IoT device simulated in this lab is a thermostat, which controls the room temperature. To successfully set the temperature, the client needs to be able to interact with the IoT server. Since the IoT device is behind the firewall, outside machines cannot interact with the IoT device, and will therefore not be able to control the thermostat. To defeat the firewall protection, the attacking code must get into the internal network first. This is not difficult. Any time when a user from the internal network visits the attacker's website, the attacker's code (JavaScript code) runs from the user's browser, and therefore runs inside the protected internal network. However, due to the sandbox protection implemented by browsers, the attacker's code still cannot interact with the IoT device, even though it is now inside the internal network.

The objective of this lab is to use the DNS rebinding attack to circumvent the sandbox protection, so the JavaScript code from the attacker can successfully get the essential information from the IoT device and then use the information to set the temperature of the thermostat to a dangerously high value. This lab covers the following topics:

1- DNS server setup
2- DNS rebinding attack
3- Attacks on IoT devices
4- Same Origin Policy

2- Background: IoT

Our attack target is an IoT device behind the firewall. We cannot directly access this IoT device from outside. Our goal is to get an inside user to run our JavaScript code, so we can use the DNS rebinding attack to interact with the IoT device.

Many IoT devices have a simple built-in web server, so users can interact with these devices via web APIs. Typically, these IoT devices are protected by a firewall, they cannot be accessed directly from outside. Due to this type of protection, many IoT devices do not implement a strong authentication mechanism. If attackers can find ways to interact with them, they can easily compromise its security.

We emulate such a vulnerable IoT device using a simple web server, which serves two APIs: **password** and **temperature**. The IoT device can set the room temperature. To do that, we need to send out an HTTP request to the server's **temperature** API; the request should include two pieces of data: the target temperature value and a password. The password is a secret that changes periodically, but it can be fetched using the **password** API. Therefore, to successfully set the temperature, users need to first get the password, and then attach the password in the **temperature** API.

The password is not meant for authentication purposes; it is used to defeat the Cross-Site Request Forgery (CSRF) attack. Without this protection, a simple CSRF attack is sufficient; there is no need to use the more sophisticated DNS rebinding attack. For the sake of simplicity, we hardcoded the password; in real systems, the password will be re-generated periodically.

3- Lab Environment Setup Using Containers

Task 3.1 – Container Setup and Commands

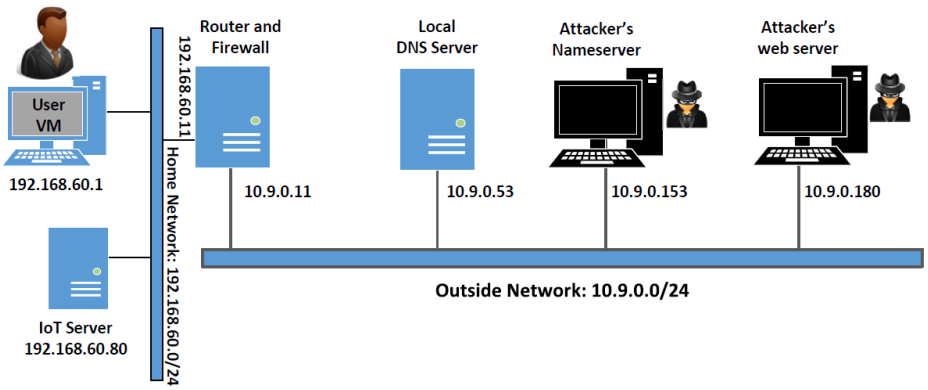
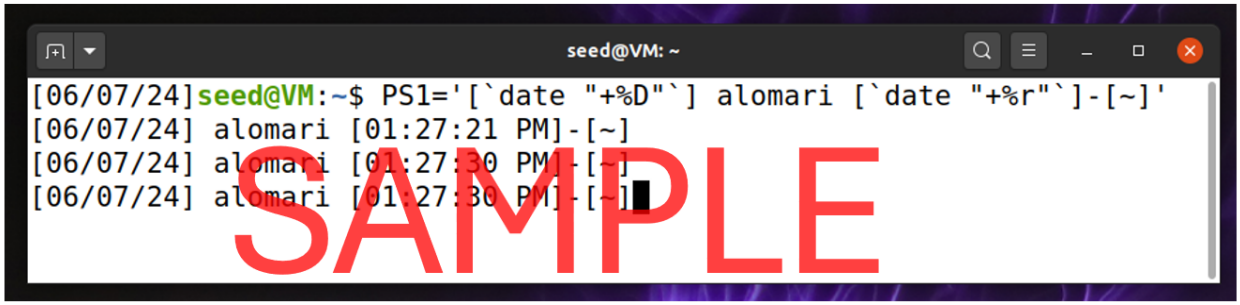
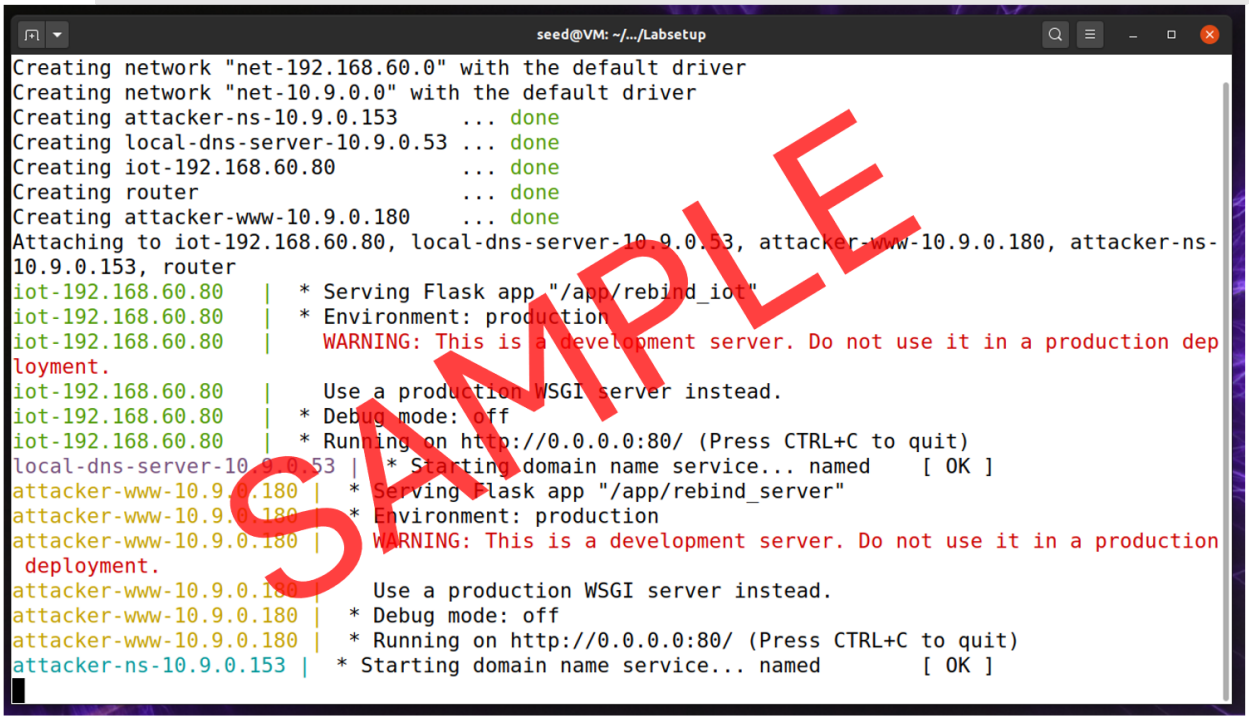


Figure 1: Lab environment setup

1. Start by changing the terminal prompt as shown in the command below:
   ```
   $PS1='[`date "+%D"`] yourname [`date "+%r"`]-[~]'
   ```
   Your terminal should look like the screenshot below.

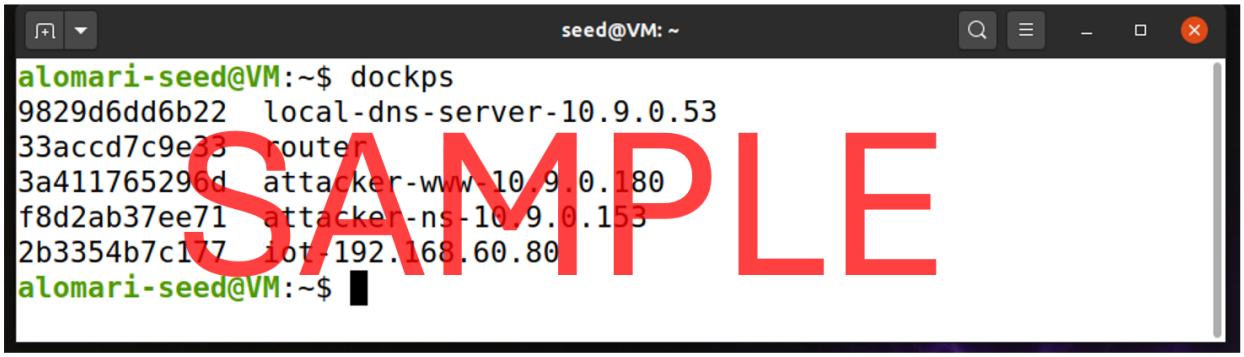


2. Build and start the containers:
   ```
   $ docker-compose build
   $ docker-compose up
   ```



Important Note: For the remaining screenshots, my terminal prompt is set up with my name only without the date and time. But your terminal prompt should include the date, time, and format from the previous step.

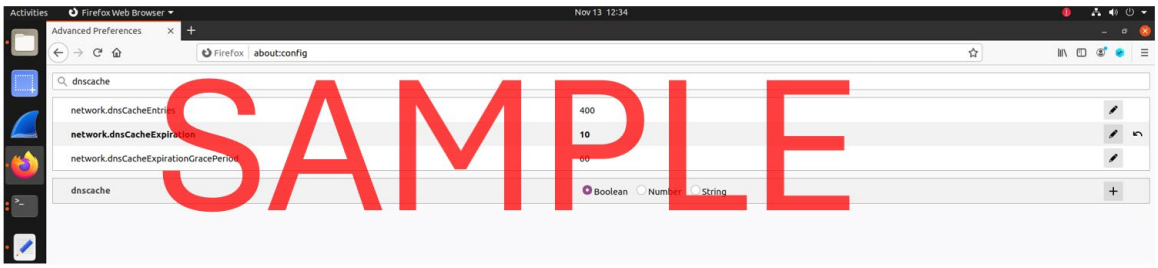
3. Leave the containers running in this terminal**.** Open a new terminal, change the prompt similar to what you did in step 1, and check the container IDs.



4. Take a screenshot of your containers' IDs similar to the one shown above, and place it under **Screenshot#1** in the answer file.

Task 3.2 – Configure the User VM

1. Follow section 3.2 in the DNS-Rebinding-SEED file to configure the user VM.
2. Take a screenshot of your Firefox browser showing the change of the **`network.dnsCacheExpiration`** to **10**. Place your screenshot that is similar to the screenshot below under **Screenshot#2** in the answer file.



3. Restart Firefox, double-check that the setting from the last step is changed to 10.
4. Change the **`/etc/host`** file and the Local DNS Server head file as per the instructions under steps 2 and 3 in the DNS-Rebinding-SEED file.
5. Browse to http://www.seedIoT32.com and verify that your screen looks like the screenshot below.

Task 3.3 – Testing the Lab Setup

1- Test the Lab Setup as per the instructions in the DNS-Rebinding-SEED file (step 3.3).
2- Ensure your lab is configured properly, and the results of the dig command are correct as per the instructions.

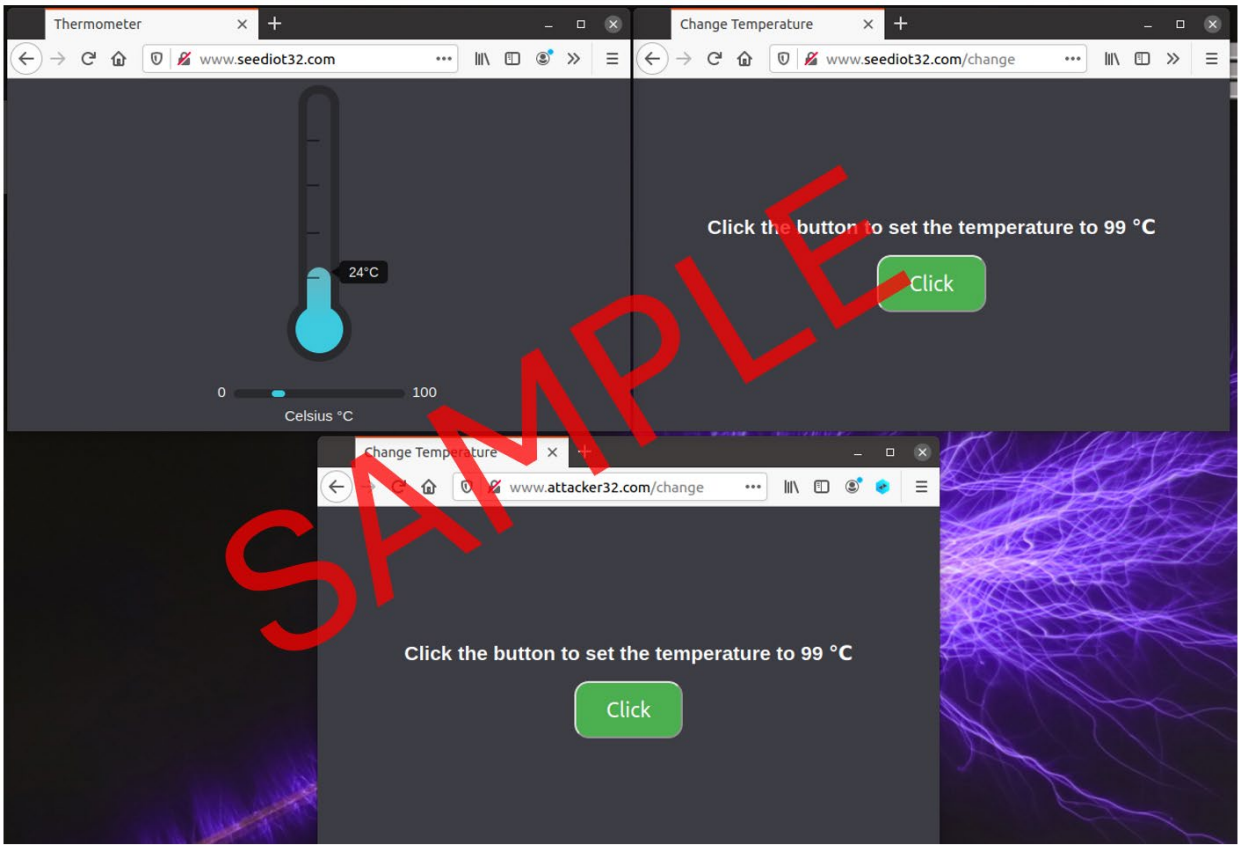
4 - Launch the Attack on the IoT Device

Task 4.1 – Understanding the Same-Origin Policy Protection

1- Follow the steps in Task 1 in section 4, and take a screenshot of the browsers showing the three URLs:

URL 1: http://www.seedIoT32.com/
URL 2: http://www.seedIoT32.com/change
URL 3: http://www.attacker32.com/change

2- In your screenshot set the initial temperature to a **random number** (not 24 Celsius, but any other temperature).



3- Place your screenshot that is similar to the one above under **Screenshot#3** in the answer file, and make sure the three URLs are showing.

Question#1: Try changing the temperature from URL2, were you successful? Why?

Question#2: Try changing the temperature from URL3, were you successful? Why?

Task 4.2 – Defeat the Same-Origin Policy Protection

1- Follow the instructions under **Step 1: Modify the JavaScript code** in the DNS-Rebinding-SEED file.
2- Conduct the DNS rebinding in **Step 2: Conduct the DNS rebinding.**

Question#2: What did you set TTL to?

Question#3: Where did you get the www entry to point to?

3- Record a video while changing the thermostat from the www.attacker32.com/change website.
   1- Start with a **random temperature** set at the IoT device.

2- Have a folder with your name showing on the desktop while recording the video.
3- Record your full screen, where the date and time are showing, similar to the sample videos.
4- Name your video **Video#1-FirstName** and upload it to the assignment dropbox.
5- Make sure your video is in .mp4 format, and doesn't require the download of any codecs.
6- Your video should **not** exceed 30 seconds.

Note a sample video has been attached to this assignment dropbox.

Task 4.3 – Launch the Attack

1- Follow the instructions to launch the attack from www.attacker32.com .
2- Record a second video showing the launch of the attack.
3- Follow the exact video recording instructions in Task 4.2.
4- Name your video **Video#2-FirstName** and upload it to the assignment dropbox.

Note a sample video has been attached to this assignment dropbox.