LAB REPORT 7

**Name:** Sai sowmith kantipudi

**Id:** 700740976

**Lab setup:**

Bring up the terminal in Ubuntu VM and changing directory to Lab setup folder in the terminal, also dcbuild and dcup -d commands are used to bring up the container.

Build lab as shown in below screenshot.

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

**Step1: Reduce Firefox’s DNS Caching Time**

Modify the cache expiration time from 60 seconds to 10 seconds.

A screenshot of a computer

Description automatically generated

Before:

A screenshot of a computer

Description automatically generated

After:

A screenshot of a computer

Description automatically generated

**Step2: Change /etc/hosts**

Execute sudo gedit /etc/hosts and add the following entry to the /etc/hosts file and use www.seedIoT32.com as the name for the IoT server. Its IP address is 192.168.60.80.

A screenshot of a computer

Description automatically generated

Browse the URL to see thermostat and also change the temperature setting by dragging the sliding bar

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step3: Local DNS Server**

Add nameserver 10.9.0.53 and execute *sudo resolvconf -u* for the change to take effect as shown in below screenshots.

A screenshot of a computer screen

Description automatically generated

**Testing the Lab Setup:**

Use the dig command to get the IP address of www.attacker32.com and ns.attacker32.com. where IP addresses will be 10.9.0.180 and 10.9.0.153 respectively.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Successfully able to see the attacker’s website.

A screenshot of a computer

Description automatically generated

**Task1: Understanding the Same-Origin Policy Protection**

Screens screenshot of a computer

Description automatically generated

By clicking on *www.seediot32.com*, and successfully able to change the temperature because it is from the same origin.

In the below screenshot when click on ww.attacker32.com but the temperature does not change because the iot32.com origin is different, so it does not allow to change temperature because it cannot get the password.

A screenshot of a computer

Description automatically generated

To find the reason clicked on *Tools -> Web Developer -> Web Console* which displays error message as the origin request blocked the following error message explains, in order to change the temperature on the IOT server, first we need to send get request and try to get the password, because if attacker32.com, it is not from the same origin, so it cannot allow to access the password, without allowing to access the password there is no way to construct the second post request to change temperature. sop policy is blocking, so we have to manage bypass same origin policy.

As per the sop policy it blocks the request which is sent from attacker32.com

A screenshot of a computer

Description automatically generated

**Task2: Defeat the Same-Origin Policy Protection**

**Step1: Modify the JavaScript code.**

Changing the url to attacker32.com and restart the attacker container

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

we can still see the different error message as password undefined. It explains now SOP is satisfied, we can send request, we will get response because it satisfies same SOP policy, so the web browser allow to access this password from the response this request sent to malicious webserver, malicious webserver does not know the password. so, its undefine and it cannot construct this post request. SOP restrain is limited.

so, when we sent request to attacker32.com again because of change URL to attacker32.com, in that attacker webserver it did not generate the password, it generates on IOT server, not on attacker server. So, the response of the value for the password is undefined.

A screenshot of a computer

Description automatically generated

**Step2: Conduct the DNS rebinding.**

To change the DNS mapping modified the zone\_attacker32.com file inside attacker’s nameserver container.

A screenshot of a computer

Description automatically generated

reload the revised zone data.

A screenshot of a computer

Description automatically generated

clean out the cache

A screenshot of a computer

Description automatically generated

The request has been sent and it is successful, Now I can be able to change the thermostat’s temperature successfully.

A screenshot of a computer

Description automatically generated

**Task3: Launch the Attack**

Changing the Ip address of www.attacker32.com in zone\_attacker32.com to default and

reloading the zone.

So, we can have the web server which attacks automatically every 10 seconds.

A screenshot of a computer

Description automatically generated

Now change IP address to 192.168.60.80 and reload the zone file.

A screenshot of a computer

Description automatically generated

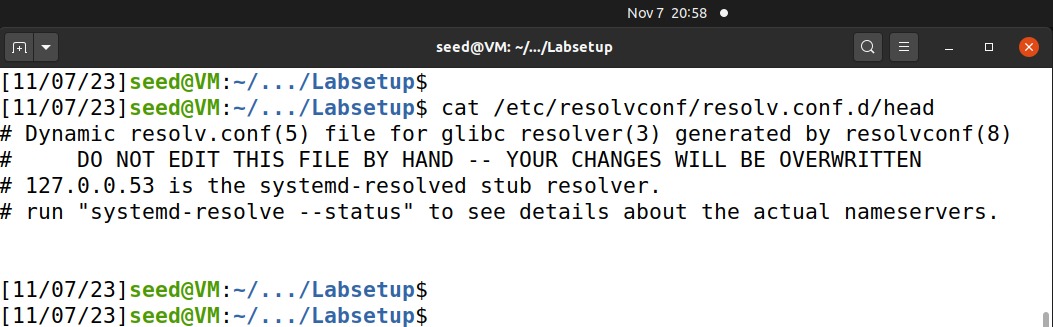
As the attacker machine sends the change request every 10 seconds to the thermostat.

We can see in the attacker32.com changed to we are now talking to IOT server. As shown below

A screenshot of a computer

Description automatically generated

**Cleaning the nameserver**



**Shutdown the lab**

# dcdown

A screenshot of a computer

Description automatically generated