第9章实验报告

1 实验名称

实现本地 DNS 缓存中毒攻击

2 实验原理

通过污染DNS Cache，用虚假的IP地址信息替换Cache中主机记录的真实IP地址信息，可以改变域名和IP的映射关系，使得用户在访问某网站时被错误引导至攻击者的网站中，从而暴露隐私信息。

3 实验环境

本次实验使用3台Ubuntu虚拟机，分别作为DNS服务器、用户机和攻击机。环境配置如下：

3.1 DNS 服务器

Ubuntu22.04作为域名解析服务器，配置`bind9`流程如下

```
sudo apt install bind9 bind9utils bind9-doc bind9-host
# 开启53端口
sudo ufw allow 53
# 查看bind9状态
sudo systemctl status bind9
```

- 安装`bind9`后默认启动

```
❯ sudo systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-04-25 18:07:31 CST; 19min ago
       Docs: man:named(8)
    Process: 943 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 972 (named)
      Tasks: 6 (limit: 4573)
     Memory: 11.8M
        CPU: 435ms
     CGroup: /system.slice/named.service
             └─972 /usr/sbin/named -u bind

4月 25 18:07:35 Euler0525-UbuntuVM named[972]: automatic empty zone: EMPTY.AS112.ARPA
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: automatic empty zone: HOME.ARPA
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: configuring command channel from '/etc/bind/rndc.key'
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: configuring command channel from '/etc/bind/rndc.key'
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: reloading configuration succeeded
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: scheduled loading new zones
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: managed-keys-zone: Unable to fetch DNSKEY set '.': operation canceled
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: resolver priming query complete: operation canceled
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: any newly configured zones are now loaded
4月 25 18:07:35 Euler0525-UbuntuVM named[972]: running
```

```
bind 内容包括
    name DNS服务
    named-chkconfig(named.conf文件检查工具)
    named-checkzone(zone文件检查工具)
    rndc(本地和远程DNS控制工具)
bind-libs: named DNS服务库
bind-utils: 辅助工具
    host, dig, nslookup, nsupdate
bind-chroot: 切根程序用于切换到更安全的目录`/var/named/chroot`

bind 配置文件
/etc/bind/named.conf
```

```
其中引用了3个文件
    include "/etc/bind/named.conf.options";         # 默认创建
    include "/etc/bind/named.conf.local";           # 默认创建
    include "/etc/bind/named.conf.default-zones";

```

- 接下来设置`bind9`允许查询和转发，并关闭dnssec

```
// Global Profile

options {
        directory "/var/cache/bind";

        // 允许查询和转发
        forwarders { 8.8.8.8; };
        allow-query { any; };
        recursion yes;

        dnssec-validation no;  // 禁用dnssec
        auth-nxdomain no;
        listen-on-v6 { any; };
};

```

3.2 客户机

在客户机`/etc/resolv.conf`添加DNS服务器的IP地址

```
nameserver 192.168.*.*
```

3.3 攻击机

- 安装`scrapy`，编写Python程序监听DNS服务器，并伪造DNS权威服务器回复信息。代码内容见`../9/main.py`

4 实验步骤

1. 攻击机运行Python程序，伪造DNS服务器的回复信息；

2. 客户机访问某个域名，结果跳转到攻击程序指定的IP地址`10.0.0.55`，结果如下图

```
~ base with root@Euler-PC at 09:08:28
curl -L www.abcde.com
curl -L www.abcde.com
<!--A Design by W3layouts Author: W3layout Author URL: http://w3layouts.com License: Creative Commons Attribution
 3.0 Unported License URL: http://creativecommons.org/licenses/by/3.0/-->
<!DOCTYPE html>
<html lang="zh-CN">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
    <meta name="renderer" content="webkit|ie-comp|ie-stand">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="keywords" content="网络准入认证系统" />
    <title>深澜软件</title>
    <link type="image/x-icon" rel="shortcut icon" href="/static/images/basic/favicon.ico">
    <link rel="stylesheet" href="./static/bit/css/reset.css">
    <link rel="stylesheet" href="./static/bit/css/pc.css">

    <script src="/static/js/device.min.js"></script>
    <script>
        if (device.mobile()) {
            locationURI("/srun_portal_phone")
        }
        function locationURI(uri) { return location.href = uri + location.search; }
    </script>
</head>

<body>
```

并且可以看到攻击机发送了伪造数据包

```
sudo python3 main.py
sniff:  www.abcde.com.
.
Sent 1 packets.
sniff:  cname.vercel-dns.com.
.
Sent 1 packets.
```