DNS欺骗

一、实验环境搭建

一台Kali Linux攻击主机，一台Windows Server 2016服务器，一台Windows 10主机。

二、实验内容

1.设置Kali Linux主机、Windows Server 2016服务器与Windows 10在同一个可以上网的网段。分别记录各个主机的IP地址，并检查他们之间能否ping通。配置Windows Server 2016打开其IIS的Web服务。

2.在Kali Linux的root终端中输入以下指令打开并编辑ettercap工具执行dns欺骗时的参数文件

vim etc/Ettercap/etter.dns

在文件中编辑以下内容并保存：

IPv4地址的域名 A 错误的IPv4地址（Windows Server 2016的IP地址，或者一个第三方网站的IP地址）

3.图形化界面打开Kali Linux的ettercap应用程序，点击accept后跳转到操作界面。点击放大镜（scan for hosts）扫描Kali Linux相同网段的其他主机，点击右边按钮（Hosts list）列出主机列表。通过指令查看Kali Linux网段的网关地址，将Windows 10列为Target 1，网关列为Target 2，点击操作界面右边MITM menu下的ARP Poisoning对目标主机与网关进行ARP欺骗。

4.在Windows 10上查询ARP欺骗是否成功。

5.在Kali Linux的ettercap界面右边点击Ettercap menu下的Plugins，选择Manage Plugins，并双击弹出的界面中的dns\_spoof开始dns欺骗。

6.在Windows 10上通过浏览器以http的方式访问目标域名，同时打开wireshark进行抓包，观察访问到的网页并通过报文分析该过程。

7.尝试以https进行访问，观察结果并结合报文分析。

8.在服务器上IIS里开启https服务，为其开启443端口，并为其添加一个证书（请自行查询如何获取虚假证书）。同样在Windows 10上以https访问域名，观察结果并结合抓取的报文分析。