山东大学 计算机 学院

计算机网络 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202400130039 | 姓名：张汇智 | | 班级：智能 |
| 实验题目：  Wireshark\_DNS | | | |
| 实验学时：2h | | 实验日期： 2025. | |
| 实验目的： 深入研究 DNS 的客户端 | | | |
| 硬件环境： AMD ryzen R9 7900HX ; NVIDIA RTX4070LAPTOP ; RAM SAMSUNG 16GB\*2 ; ROM WD770 1T+2T; | | | |
| 软件环境：Windows11 23H2 (KB5056580) | | | |
| 实验步骤与内容：  尝试PDF的三个指令  问题：  1.运行 nslookup 获取亚洲某台 Web 服务器的 IP 地址。该服务器的 IP 地址是多少？  A:  2.运行 nslookup 来确定欧洲某所大学的权威 DNS 服务器。  A:    3.行 nslookup，查询问题 2 中获取的其中一个 DNS 服务器，获取 Yahoo! 邮件的邮件服务器。它的 IP 地址是什么？  A:      **\*\*牛津找不到我佛，谷歌找得到。\*\***  4.找到 DNS 查询和响应消息。然后通过 UDP 还是 TCP 发送？    **用TCP发送**  **很迷？怎么这么大？？**  **重启电脑试试。**  **再抠一次，这次干净了。**  **UDP发送**    5.DNS 查询报文的目的端口是什么？DNS 响应报文的源端口是什么？  **53；53**  6.DNS 查询消息发送到哪个 IP 地址？使用 ipconfig 确定本地 DNS 服务器的 IP 地址。这两个 IP 地址相同吗？  **192.168.254.245；相同。**  7.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？  \*\*A类型查询。Answerrrs是空的\*\*    8.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？  \*\*2。NAME;TYPE;CLASS;TIME TO LIVE;DATA LENGTH;ADRESS\*\*    9.考虑主机随后发送的 TCP SYN 数据包。SYN 数据包的目标 IP 地址是否与 DNS 响应消息中提供的任何 IP 地址相对应？  这次抓包只有UDP和TSL1.3 何意味？？？      //为什么不走TCP SYN 啊啊啊啊啊我是集美我要互搏了  又抓了一次，这次成功了。    ANSWER:\*\***是的。**\*\*  10．此网页包含图片。在检索每张图片之前，您的主机是否会发出新的 DNS 查询？  域名不同的 会发出新的查询。    这里有analytic 应该是登录的JS Script请求  11. DNS 查询报文的目的端口是什么？ DNS 响应报文的源端口是什么？    **53;53.**  12.DNS 查询消息发送到哪个 IP 地址？这是您的默认本地 DNS 服务器的 IP 地址吗？  192.168.254.245 是的。  13.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？  AAAA类型。无答案。  14.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？  4答案。2CNAME2AAAA地址。每个答案包含name type class timetolive datalength  15.提供截图。      16.DNS 查询消息发送到哪个 IP 地址？这是您的默认本地 DNS 服务器的 IP 地址吗？  192.168.254.245貌似无法访问。切谷歌吧。  8.8.8.8 是的。  17.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？  NS.无答案。（用自己的DNS服务器是A类型查询，发生什么了？）  18.检查 DNS 响应消息。响应消息提供了哪些 MIT 域名服务器？该响应消息是否也提供了 MIT 域名服务器的 IP 地址？  给出了上一级域的权威服务器，无mit服务器。提供了IP地址。此为自己DNSserver  提供了 8 个 MIT 域名的权威名称服务器，没有IP地址。  19.提供截图。      20.DNS 查询消息发送到哪个 IP 地址？这是你的默认本地 DNS 服务器的 IP 地址吗？如果不是，那么这个 IP 地址对应的是什么？  BITSY.MIT.EDU SEEMS NOT AVAILABLE AT PRESENT.  SO I CHOSE 180.76.76.76.  NO IT CORRESPONDS TO BAIDU’S DNS SERVER.  21.检查 DNS 查询消息。它是什么类型的 DNS 查询？查询消息包含任何“答案”吗？  //THERE ARE 2 QUERY AND THE IPV4 ONE RESPONDING WITH FAILURE.LATER THE IPV6 ONE WOULD BE DISPLAYED.  AAAA TYPE WITH NO ANSWER.  22.检查 DNS 响应消息。它提供了多少个“答案”？每个答案包含什么？  2.NAME TYPE CLASS ADDRESS(HERE IST IPV6 ADDR.)  **23.提供截图。** | | | |
| 结论分析与体会：  （1）如果想要访问一个网站，那么计算机要知道 DNS服务器的 IP 地址  （2）本机只向自己的 DNS 服务器查询；  （3）DNS 服务器查询到每个域名的 IP 地址是通过分级查询的方式；域名的层级结构如下：主机名.次级域名.顶级域名.根域名 | | | |