|  |
| --- |
| 实验目的：  了解DNS 域名系统、nslookup及ipconfig  实现使用 Wireshark 追踪 DNS  实现nslookup 的 DNS 查询  实验结果：  实验一：  1、运行nslookup查找以获取亚洲的服务器的IP地址。该服务器的IP地址是什么？  屏幕截图 2023-03-17 162321  该服务器的ip地址为110.242.68.4 110.242.68.3   1. 运行nslookup查找以确定欧洲大学的权威DNS服务器。   剑桥大学：<https://www.cam.ac.uk/>  屏幕截图 2023-03-17 162739   1. 运行 nslookup，使用上一个操作中一个已获得的 DNS 服务器，来查询 Yahoo! 邮箱的邮件服务器。它的 IP 地址是什么？雅虎邮箱的域名为 “mail.yahoo.com”，   选择服务器 “dns0.cl.cam.ac.uk” 来找，发现没有捕获到，如下图所示：  屏幕截图 2023-03-17 163104  使用递归方法获得雅虎邮箱的 IP 地址如下图所示：  屏幕截图 2023-03-17 163140  实验二：访问http://www.ietf.org  查看本机的无线局域网适配器：  屏幕截图 2023-03-17 165048  4.找到DNS查询和响应消息，是通过UDP还是TCP发送的？  屏幕截图 2023-03-17 175234  通过UDP发送的  5.DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？都是53  屏幕截图 2023-03-17 175353  屏幕截图 2023-03-17 175405  6.DNS查询消息被发送到哪个IP地址？使用ipconfig来确定本地DNS服务器的IP地址。这两个IP地址相同吗？  屏幕截图 2023-03-17 175353  屏幕截图 2023-03-17 164721 相同的  7.检查DNS查询消息。DNS查询的“类型”是什么？查询消息是否包含任何“答案”？  屏幕截图 2023-03-17 175604  查询类型是A,查询信息不包含答案  8.检查DNS响应消息。我们提供了多少个“答案”？这些答案都包含了什么？  屏幕截图 2023-03-17 175653  提供了4个答案，type A表示访问网址的ip地址，cname类型为原域名的别名 |
| 9.请考虑由您的主机发送的后续TCP SYN数据包。SYN数据包的目标IP地址是否对应于DNS响应消息中提供的任何IP地址？  屏幕截图 2023-03-17 213022  是相对应的，返回地址后，主机就一直与其发送消息交互  10.这个网页包含图片。在检索每个图像之前，主机是否会发出新的DNS查询？  不会，因为本机的DNS已经进行缓存了  实验三：nslookup 的 DNS 查询  查询网址 [www.mit.edu](http://www.mit.edu) 查询窗口  屏幕截图 2023-03-17 175849  11.DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？都是53  屏幕截图 2023-03-17 213538  屏幕截图 2023-03-17 213550  12.DNS查询消息被发送到哪个IP地址？这是默认的本地DNS服务器的IP地址吗？  屏幕截图 2023-03-17 213752  屏幕截图 2023-03-17 162321 是  13.检查DNS查询消息,DNS查询的“类型”是什么？查询消息是否包含任何“答案”？  查询类型是A，不包含任何信息   1. 检查 DNS 响应消息。提供了多少个 "answers"？这些答案包含什么？   屏幕截图 2023-03-17 215027  提供了3个answers,其中两个cname是别名，最后一个是目标网址的ip地址  15.截图如上图所示  实验四：  查询nslookup –type=NS mit.edu  屏幕截图 2023-03-17 175858  16.DNS查询消息被发送到哪个IP地址？这是默认的本地DNS服务器的IP地址吗？  屏幕截图 2023-03-17 215605  屏幕截图 2023-03-17 162321  发送到192.168.254.245，对比以上两图发现是本地DNS服务器的IP地址  17.检查DNS查询消息。DNS查询的“类型”是什么？查询消息是否包含任何“答案”？  屏幕截图 2023-03-17 215909  类型为NS，表示查询权威DSN服务器，没有任何回答  18检查DNS响应消息。响应消息提供了什么MIT名称服务器？此响应消息是否也提供了MIT命名者的IP地址？  屏幕截图 2023-03-17 220153  是NS类型，没有提供MIT命名者的IP地址   1. 提供一个截图 如上图所示   实验五：  查询nslookup www.aiit.or.kr bitsy.mit.edu  由于此网址访问超时，故换了一个网址  屏幕截图 2023-03-17 175912   1. DNS查询消息被发送到哪个IP地址？这是您默认的本地DNS服务器的IP地址吗？如果没有，那么IP地址对应于什么呢？   屏幕截图 2023-03-17 220937  发送到的网址为96.7.49.64，为use2.akam.net的ip地址不是本地DNS服务器的IP地址，表示此查询请求发送到DNS服务器use2.akam.net，不是默认服务器；  21.检查DNS查询消息，DNS查询的“类型”是什么？查询消息是否包含任何“答案”？  屏幕截图 2023-03-17 221210  查询的类型是A，不包含任何答案  22.检查DNS响应消息。我们提供了多少个“答案”？这些答案都包含了什么？  屏幕截图 2023-03-17 221255  包含一个回答，是该域名的ip地址   1. 提供截图如上图所示   问题及收获：  一、查询消息的目标端口和响应消息的源端口一样吗？  一般情况下，查询消息的目标端口和响应消息的源端口一样；   1. 如何查看DNS查询的“类型”？   屏幕截图 2023-03-17 175604  三、如何查看端口号？  屏幕截图 2023-03-17 175353 |