

计算机网络实验二(2)报告

马成 20307130112

1. 使用python的SMTP(区别SMTP_SSL), 登录邮件服务器(例如, 学邮), 并发送一个纯文本邮件, 体会用户层发送邮件的过程
 1. 好像网上找到SMTP_SSL()方法使用了安全socket层
 2. 使用python自带的库, 首先给出服务器用户和密码, 登录之后给出一封邮件的几个基本信息随后使用python的接口投递即可
2. 在发送邮件的过程中, 通过wireshark抓包, 分析SMTP发送邮件的过程

```
138 S: 220 newxmesmtplgicsvrsza31.qq.com XMail Esmtpl QQ Mail Ser...
109 C: ehlo USER-20200908RA.fudan.edu.cn
244 S: 250-newxmesmtplgicsvrsza31.qq.com | PIPELINING | SIZE 734...
135 C: AUTH PLAIN ADExNDA00TI4MjBACXEuY29tRjB29md2Fue...
105 S: 235 Authentication successful
114 C: mail FROM:<1140492820@qq.com> size=262
82 S: 250 OK
110 C: rcpt TO:<20307130112@fudan.edu.cn>
82 S: 250 OK
80 C: data
112 S: 354 End data with <CR><LF>.<CR><LF>.
339 from: =?utf-8?b?6ams5oiQUVE=?=, subject: =?utf-8?b?UHl0aG9uIF...
94 S: 250 OK: queued as.
80 C: quit
84 S: 221 Bye.
```

可以看到SMTP发送的步骤是

1. 显示请求连接服务器, 服务器回复连接成功, 客户给出一个类似IP的地址信息和服务器沟通
 2. 客户尝试登录并给出用户名和口令(应该使用base64加密的)服务器回复登录成功
 3. 客户设置mail from、rcpt、data等邮件信息其中服务器返回OK代表设置成功, data的时候服务器告诉客户端给出一个单行的.表示结束
 4. 断开连接
3. 使用python的POP3, 登录邮件服务器, 实现接收邮件的功能
 4. 抓包使用wireshark抓包, 分析POP3接收邮件时与服务器的交互过程

```
128 S: +OK XMail POP3 Server v1.0 Service Ready(XMail v1.0)
98 C: USER 1140492820@qq.com
79 S: +OK
97 C: PASS aovdcoof...
79 S: +OK
80 C: LIST
173 S: +OK
82 C: RETR 1
1494 S: +OK 3287
1494 S: DATA fragment, 1420 bytes
536 S: DATA fragment, 462 bytes
80 C: QUIT
83 S: +OK Bye
```

可以看到步骤如下

1. 显示请求连接服务器，服务器回复连接成功，客户给出一个类似IP的地址信息和服务器沟通
2. 给出用户名和口令尝试登录
3. LIST可以用于获取所有邮件的编号
4. RETR 1获取第一封邮件的信息，返回三个信息
5. 断开连接
5. 使用dig命令查询DNS，使用+trace参数，观察并分析DNS查询过程，指出使用+trace参数后，查询采用的是递归查询还是迭代查询

```
mc020207@USER-20200908RA:/mnt/c/WINDOWS/system32$ dig www.bilibili.com +trace
; <<> DiG 9.16.1-Ubuntu <<> www.bilibili.com +trace
;; global options: +cmd
324483 IN NS k.root-servers.net.
324483 IN NS l.root-servers.net.
324483 IN NS m.root-servers.net.
324483 IN NS a.root-servers.net.
324483 IN NS b.root-servers.net.
324483 IN NS c.root-servers.net.
324483 IN NS d.root-servers.net.
324483 IN NS e.root-servers.net.
324483 IN NS f.root-servers.net.
324483 IN NS g.root-servers.net.
324483 IN NS h.root-servers.net.
324483 IN NS i.root-servers.net.
324483 IN NS j.root-servers.net.
;; Received 811 bytes from 202.120.224.26#53(202.120.224.26) in 3 ms

com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS i.gtld-servers.net.
com. 172800 IN NS a.gtld-servers.net.
com. 172800 IN NS d.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS c.gtld-servers.net.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS f.gtld-servers.net.
com. 172800 IN NS e.gtld-servers.net.
com. 172800 IN NS m.gtld-servers.net.
com. 172800 IN NS l.gtld-servers.net.
com. 172800 IN NS g.gtld-servers.net.
com. 86400 IN DS 30909 8 2 ED3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
com. 86400 IN RRSIG DS 8 1 86400 20221019200000 20221006190000 18733 . w2um4ys/mtgFwLzJ2AnNeoTnkvalZReeP6VJ/TjzEW1gqILPFMpn13+ 9
CqW1AuN1ZQJh+2FDQd1QtaBT+Aq1uId7heZt/gUsBA81BebMVfQsGt s848qTYEeCyDuuMw0gwMeJF10/RjbQn69zHDetIWMRQ3+P1+Y0U95/Lo tPaCaoPFQWuB1/G25Axt9ARCuT+bmPkVCZ1N3QFQBmI7
aUQ17j/4/DpR KB164aylKHMGG4FIDGxvwZG4uzTIO2MhFLLw319qYvWIXg/BbcK7OLWp q3x5r1qKArY+prFe7rYdLayU0/kTYgkOxay701oyDhtaaSF4+G9jwhcj FfcX9A==
;; Received 1204 bytes from 199.79.1.13#53(d.root-servers.net) in 32 ms

bilibili.com. 172800 IN NS ns3.dnsv5.com.
bilibili.com. 172800 IN NS ns4.dnsv5.com.
CKOPQJMC874LJREF7EPN8430QVIT8BSM.com. 86400 IN NSecs 1 1 0 - CKOQ2D6NI4I7EQH8NA3ONS61048UL8G5 NS SOA RRSIG DNSKEY NSecs3PARAM
CKOPQJMC874LJREF7EPN8430QVIT8BSM.com. 86400 IN RRSIG NSecs3 8 2 86400 20221018042431 20221011031431 32298 com. kMyWcyQJMHYeykwwKREGp1QaYBgahpEae4uzIMk1cnbHaTH
```

- 使用的是迭代查询
- 过程
 1. 访问202.120.224.26获得了若干根服务器的主机名
 2. 访问d.root-servers.net获得了.com的顶级域名对应的主机名
 3. 访问m.gtld-servers.net或者了bilibili.com的主机
 4. 从权威服务器获得了IP
- 6. 使用wireshark抓取DNS请求与应答包，解释DNS报文中各个字段的含义以及标志(flag) 字段中，各个flag位的含义

1. 请求包

```

▼ Flags: 0x0120 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  .... ..0. .... = Truncated: Message is not truncated
  .... ..1 .... = Recursion desired: Do query recursively
  .... ..0.. .... = Z: reserved (0)
  .... ..1. .... = AD bit: Set
  .... ..0 .... = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
▼ Queries
  > www.bilibili.com: type A, class IN
▼ Additional records
  > <Root>: type OPT
\[Response In: 60\]

```

- 事务ID是0x8bca
- 第一位表示这个报文是请求报文
- 操作码是标准询问
- Truncated: 表示报文没有被阶段

- Recursion Desired: 期望递归
- 其余均为保留字段
- 有一个询问有一个附加RR
- 询问 www.bilibili.com 的地址

2. 响应包

```
Transaction ID: 0xf168
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
....0... .. = Authoritative: Server is not an authority for domain
....0... .. = Truncated: Message is not truncated
....1... .. = Recursion desired: Do query recursively
....1... .. = Recursion available: Server can do recursive queries
....0... .. = Z: reserved (0)
....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0... .. = Non-authenticated data: Unacceptable
....0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 7
Authority RRs: 2
Additional RRs: 17
Queries
> www.bilibili.com: type A, class IN

Answers
> www.bilibili.com: type CNAME, class IN, cname a.w.bilicdn1.com
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.5
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.6
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.7
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.2
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.3
> a.w.bilicdn1.com: type A, class IN, addr 61.156.196.4
Authoritative nameservers
> bilicdn1.com: type NS, class IN, ns ns4.dnsv5.com
> bilicdn1.com: type NS, class IN, ns ns3.dnsv5.com
Additional records
> ns3.dnsv5.com: type A, class IN, addr 36.155.149.211
> ns3.dnsv5.com: type A, class IN, addr 49.234.175.103
> ns3.dnsv5.com: type A, class IN, addr 61.151.180.51
> ns3.dnsv5.com: type A, class IN, addr 223.166.151.16
> ns3.dnsv5.com: type A, class IN, addr 1.12.0.17
> ns3.dnsv5.com: type A, class IN, addr 1.12.0.18
> ns3.dnsv5.com: type A, class IN, addr 1.12.0.18
> ns3.dnsv5.com: type A, class IN, addr 1.12.0.20
> ns3.dnsv5.com: type AAAA, class IN, addr 2402:4e00:1430:1102:0:9136:2b2b:ba61
> ns4.dnsv5.com: type A, class IN, addr 106.55.82.76
> ns4.dnsv5.com: type A, class IN, addr 117.89.178.200
> ns4.dnsv5.com: type A, class IN, addr 183.47.126.155
> ns4.dnsv5.com: type A, class IN, addr 183.192.164.119
> ns4.dnsv5.com: type A, class IN, addr 223.166.151.126
> ns4.dnsv5.com: type A, class IN, addr 1.12.0.16
> ns4.dnsv5.com: type A, class IN, addr 1.12.0.19
> ns4.dnsv5.com: type AAAA, class IN, addr 2402:4e00:1020:1264:0:9136:29b6:fc32
> <Root>: type OPT
[Request In: 41]
[Time: 0.002356000 seconds]
```

- 事务ID是0xf168
- 第一位表示这个报文是响应报文
- 操作码是标准询问
- 授权应答, 该字段在响应报文中有效。表示不是权威服务器
- Truncated: 表示报文没有被截断
- Recursion Desired: 期望递归
- Recursion Available: 允许递归
- 其余均为保留字段
- 最后表示没有出现错误
- 有一个询问, 7个回答RR, 有2个权威RR和17个附加RR

- 以下均为查询过程