计算机网络 · 理论作业6

20337251伍建霖

P4

P4. 考虑当浏览器发送一个 HTTP GET 报文时，通过 Wireshark 俘获到下列 ASCII 字符串（即这是一个 HTTP GET 报文的实际内容）。字符 <cr> <lf> 是回车和换行符（即下面文本中的斜体字符串 <cr> 表示了单个回车符，该回车符包含在 HTTP 首部中的相应位置）。回答下列问题，指出你在下面 HTTP GET 报文中找到答案的地方。

```
GET /cs453/index.html HTTP/1.1<cr><lf>Host: gai
a.cs.umass.edu<cr><lf>User-Agent: Mozilla/5.0 (
Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec
ko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ex
t/xml, application/xml, application/xhtml+xml, text
/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
<cr><lf>Accept-Language: en-us,en;q=0.5<cr><lf>Accept-
Encoding: zip,deflate<cr><lf>Accept-Charset: ISO
-8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>Keep-Alive: 300<cr>
<lf>Connection:keep-alive<cr><lf><cr><lf>
```

a. 由浏览器请求的文档的 URL 是什么？
b. 该浏览器运行的是 HTTP 的何种版本？
c. 该浏览器请求的是一条非持续连接还是一条持续连接？
d. 该浏览器所运行的主机的 IP 地址是什么？
e. 发起该报文的浏览器的类型是什么？在一个 HTTP 请求报文中，为什么需要浏览器类型？

答:

a）url = http://gaia.cs.umass.edu/cs453/index.html

b）是http 1.1版本

c）一条持续连接

d）http报文不包含ip地址的信息

e）Mozilla/5.0，不同浏览器收到的返回的报文是不一样的。

P15

P15. 阅读用于SMTP的RFC 5321。MTA代表什么？考虑下面收到的垃圾邮件（从一份真实垃圾邮件修改得到）。假定这封垃圾邮件的唯一始作俑者是恶意的，而其他主机是诚实的，指出产生了这封垃圾邮件的恶意主机。

```
From - Fri Nov 07 13:41:30 2008
Return-Path: <tennis5@pp33head.com>
Received: from barmail.cs.umass.edu (barmail.cs.umass.
edu
[128.119.240.3]) by cs.umass.edu (8.13.1/8.12.6) for
<hg@cs.umass.edu>; Fri, 7 Nov 2008 13:27:10 -0500
Received: from asusus-4b96 (localhost [127.0.0.1]) by
barmail.cs.umass.edu (Spam Firewall) for <hg@cs.umass.
edu>; Fri, 7
Nov 2008 13:27:07 -0500 (EST)
Received: from asusus-4b96 ([58.88.21.177]) by barmail.
cs.umass.edu
for <hg@cs.umass.edu>; Fri, 07 Nov 2008 13:27:07 -0500
(EST)
Received: from [58.88.21.177] by inbnd55.exchangeddd.
com; Sat, 8
Nov 2008 01:27:07 +0700
From: "Jonny" <tennis5@pp33head.com>
To: <hg@cs.umass.edu>

Subject: How to secure your savings
```

答：

MTA = mail transfer agent。恶意主机为"asusus-4b96 ([58.88.21.177])"。

P18

P18. 如题：

a. 什么是whois数据库？

b. 使用因特网上的各种whois数据库，获得两台DNS服务器的名字。指出你使用的是哪个whois数据库。

c. 你本地机器上使用nslookup向3台DNS服务器发送DNS查询：你的本地DNS服务器和两台你在（b）中发现的DNS服务器。尝试对类型A、NS和MX报告进行查询。总结你的发现。

d. 使用nslookup找出一台具有多个IP地址的Web服务器。你所在的机构（学校或公司）的Web服务器具有多个IP地址吗？

e. 使用ARIN whois数据库，确定你所在大学使用的IP地址范围。

f. 描述一个攻击者在发动攻击前，能够怎样利用whois数据库和nslookup工具来执行对一个机构的侦察。

g. 讨论为什么whois数据库应当为公众所用。

答：

a）whois数据库是用来查域名对应的ip地址，所有者等信息的。

b）whois数据库：[bilibili.com的Whois信息 - 站长工具 (chinaz.com)]

DNS	NS3.DNSV5.COM
	NS4.DNSV5.COM

c)

NS3.DNSV5.COM的A类型

检测结果

地区	耗时（秒）	TTL（秒）	值
中国	0.33s	5s	152.136.2.28（北京）
		5s	223.166.151.16（上海）
		5s	1.12.0.17（北京）
		5s	120.53.252.46（中国）
		5s	1.12.0.18（北京）
		5s	61.151.180.51（上海）
		5s	36.155.149.211（江苏）
香港	20.00s	DNS 错误：查询 A 时间超时	
美国	0.52s	5s	170.106.49.166（美国）
		5s	49.51.43.232（美国）
		5s	34.205.234.26（美国）
		5s	1.12.0.18（北京）
		5s	36.155.149.211（江苏）
		5s	1.12.0.17（北京）
		5s	52.52.126.139（美国）
		5s	61.151.180.51（上海）
		5s	49.51.103.88（加拿大）
		5s	223.166.151.16（上海）

NS4.DNSV5.COM的A类型

检测结果

地区	耗时（秒）	TTL（秒）	值
中国	0.19s	5s	117.89.178.200（江苏南京）
		5s	152.136.2.235（北京）
		5s	1.12.0.19（北京）
		5s	1.12.0.16（北京）
		5s	152.136.2.142（北京）
		5s	223.166.151.126（上海）
		5s	183.192.164.119（上海）
香港	0.12s	5s	150.109.248.236（韩国）
		5s	117.89.178.200（江苏南京）
		5s	183.192.164.119（上海）
		5s	108.136.87.44（美国）
		5s	35.154.34.246（印度）
		5s	1.12.0.16（北京）
		5s	101.32.104.183（中国）
		5s	1.12.0.19（北京）
		5s	52.198.159.146（日本）
		5s	183.47.126.155（广东惠州）
美国	1.11s	5s	1.12.0.19（北京）
		5s	18.223.52.147（美国）
		5s	1.12.0.16（北京）
		5s	170.106.49.118（美国）
		5s	183.192.164.119（上海）
		5s	117.89.178.200（江苏南京）
		5s	3.97.163.50（美国）

d)

www.baidu.com就有多个ip地址。

e）arin whois是美国的。。。

f）可用来确定ip地址范围，dns服务器地址，等等。

g）防范网络攻击。

P26

P26. 假定 Bob 加入 BitTorrent，但他不希望向任何其他对等方上载任何数据（因此称为搭便车）。

a. Bob 声称他能够收到由该社区共享的某文件的完整副本。Bob 所言是可能的吗？为什么？

b. Bob 进一步声称他还能够更为有效地进行他的“搭便车”，方法是利用所在系的计算机实验室中的多台计算机（具有不同的 IP 地址）。他怎样才能做到这些呢？

答：

a）是可能的，只要有人在社区中活跃地发送文件。

b）每台主机从不同的主机请求不同的数据块，再组合到一起即可。

P30

P30. 你能够配置浏览器以打开对某 Web 站点的多个并行连接吗？有大量的并行 TCP 连接的优点和缺点是什么？

答：可以。优点是下载更快，缺点是可能占用过多带宽。