使用telnet进行HTTP头部解析

笔记本: 我的第一个笔记本
创建时间: 2019/3/18 16:35 **更新时间:** 2019/3/25 18:51
作者: 13611377816@163.com
URL: https://blog.csdn.net/rentian1/article/details/78835566

实验二 用TELNET观察HTTP协议

安装telnet

- **安装telnet工具**

```
yum list |grep telnet   //列出当前可用的rpm包
yum install telnet-server    //安装telnet-server 服务端
yum install telnet        //安装telnet 客户端
#安装xinetd
yum install -y xinetd systemctl enable xinetd.service  //设置xinetd开机自启动
```

```
[root@VM_0_15_centos ~]# clear
[root@VM_0_15_centos ~]# rpm -qa | grep tenet
[root@VM_0_15_centos ~]# rpm -qa | grep telnet
[root@VM_0_15_centos ~]# yum install telnet-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
---> Package telnet-server.x86_64 1:0.17-64.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch          Version                  Repository  Size
================================================================================
Installing:
 telnet-server        x86_64        1:0.17-64.el7            os          41 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 41 k
Installed size: 55 k
Is this ok [y/d/N]: y
Downloading packages:
telnet-server-0.17-64.el7.x86_64.rpm                       |  41 kB   00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:telnet-server-0.17-64.el7.x86_64                          1/1
  Verifying  : 1:telnet-server-0.17-64.el7.x86_64                          1/1

Installed:
  telnet-server.x86_64 1:0.17-64.el7

Complete!
```

- **开启xinetd服务**

```
systemctl enable xinetd.service
systemctl status xinetd.service
systemctl start xinetd.service
```

- **测试telnet是否可用**

```
 telnet localhost
 #发现错误
#Trying 127.0.0.1...
#telnet: connect to address 127.0.0.1: Connection refused
#需要开启23端口
netstat -tunlp #查看当前网络状态下的可用连接
firewall-cmd --query-port=23/tcp#查看端口是否开启
firewall-cmd --zone=public --add-port=23/tcp --permanent#开启23端口
```

```
[root@VM_0_15_centos xinetd.d]# telnet localhost
Trying 127.0.0.1...
telnet: connect to address 127.0.0.1: Connection refused
Trying ::1...
telnet: connect to address ::1: No route to host
[root@VM_0_15_centos xinetd.d]# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
698/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*
887/dhclient
udp        0      0 172.21.0.15:123         0.0.0.0:*
553/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*
553/ntpd
udp        0      0 0.0.0.0:56043           0.0.0.0:*
887/dhclient
udp        0      0 0.0.0.0:38704           0.0.0.0:*
12407/ntpdate
udp6       0      0 :::49592                :::*
887/dhclient
[root@VM_0_15_centos xinetd.d]# systemctl enable telnet.socket
Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to /
usr/lib/systemd/system/telnet.socket.
[root@VM_0_15_centos xinetd.d]# systemctl start telnet.socket
[root@VM_0_15_centos xinetd.d]# systemctl start xinetd
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
FirewallD is not running
[root@VM_0_15_centos xinetd.d]# firewall-cmd --zone=public --add-port=23/tcp --p
ermanent
```

- **修改配置文件 /etc/xinetd.d/telnet**

```
#default:yes
# description: The telnet server servestelnet sessions; it uses \
# unencrypted username/password pairs for authentication.
service telnet
{
    flags = REUSE
    socket_type  = stream
    wait = no
    user = root
    server =/usr/sbin/in.telnetd
    log_on_failure  += USERID
    disable = no
}
```

修改后测试生效

```
Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64
VM_0_15_centos login: root
Password:
Login incorrect

VM_0_15_centos login: Connection closed by foreign host.
[root@VM_0_15_centos xinetd.d]# vi /etc/pam.d/remote
[root@VM_0_15_centos xinetd.d]# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64
VM_0_15_centos login: root
Password:
Last failed login: Mon Mar 18 15:50:36 CST 2019 from VM_0_15_centos on pts/1
There was 1 failed login attempt since the last successful login.
Last login: Mon Mar 18 15:21:24 from 60.247.41.94
```

- **查看xinetd启动成功**

```
ps -ef | grep xinetd
```

```
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
no
[root@VM_0_15_centos xinetd.d]#  firewall-cmd --complete-reload
success
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
no
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
no
[root@VM_0_15_centos xinetd.d]# systemctl start telnet.socket
[root@VM_0_15_centos xinetd.d]# systemctl start xinetd
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
no
[root@VM_0_15_centos xinetd.d]# firewall-cmd --zone=public --add-port=23/tcp --p
ermanent
success
[root@VM_0_15_centos xinetd.d]#  firewall-cmd --complete-reload
success
[root@VM_0_15_centos xinetd.d]# firewall-cmd --query-port=23/tcp
yes
[root@VM_0_15_centos xinetd.d]# vi /etc/xinetd.d/telnet
[root@VM_0_15_centos xinetd.d]# vi /etc/xinetd.d/telnet
[root@VM_0_15_centos xinetd.d]# ps -ef | grep xinetd
root     12328     1  0 15:40 ?        00:00:00 /usr/sbin/xinetd -stayalive -pid
file /var/run/xinetd.pid
root     13574 10569  0 15:50 pts/0    00:00:00 grep --color=auto xinetd
```

使用telnet向服务器发出请求

- **请求百度页面**

```
telnet www.baidu.com 80#一定要跟80 虽然是默认但一定要加 否则没有结果
```

```
[root@VM_0_15_centos xinetd.d]# telnet www.baidu.com 80
Trying 220.181.112.244...
Connected to www.baidu.com.
Escape character is '^]'.
GET /index.html HTTP/1.1
Host: www.baidu.com

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 14615
Content-Type: text/html
Date: Mon, 18 Mar 2019 08:08:29 GMT
Etag: "5c7cdb1f-3917"
Last-Modified: Mon, 04 Mar 2019 08:00:31 GMT
P3p: CP=" OTI DSP COR IVA OUR IND COM "
Pragma: no-cache
Server: BWS/1.1
Set-Cookie: BAIDUID=2BFDA545589195E0DE05A79ABF46C75B:FG=1; expires=Thu, 31-Dec-3
7 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: BIDUPSID=2BFDA545589195E0DE05A79ABF46C75B; expires=Thu, 31-Dec-37 23
:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1552896509; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=214748
3647; path=/; domain=.baidu.com
Vary: Accept-Encoding
X-Ua-Compatible: IE=Edge,chrome=1
```

解析HTTP字段作用

- Accept-Ranges
  告诉WEB服务器自己接受什么介质类型，/表示任何类型，type/* 表示该类型下的所有子类型，type/sub-type。
- Accept-Charset： 浏览器申明自己接收的字符集
- Cache-Control：请求：no-cache（不要缓存的实体，要求现在从WEB服务器去取）
- Connection: 针对该连接所预期的选项Connection: close
- Content-Length： WEB 服务器告诉浏览器自己响应的对象的长度。
- Content-Type： WEB 服务器告诉浏览器自己响应的对象的类型。
- Date : 此条消息被发送时的日期和时间(以RFC 7231中定义的"HTTP日期"格式来表示)
- ETag: 对于某个资源的某个特定版本的一个标识符，通常是一个消息散列
- Accept-Encoding： 浏览器申明自己接收的编码方法，通常指定压缩方法，是否支持压缩，支持什么压缩方法 （gzip，deflate）
- Last-Modified所请求的对象的最后修改日期(按照 RFC 7231 中定义的“超文本传输协议日期”格式来表示)
- P3P : P3P策略相关设置
- Pragma与具体的实现相关，这些响应头可能在请求/回应链中的不同时候产生不同的效果
- Server服务器的名称
- Set-Cookie： 设置HTTP cookie, 包括公司名，时间，有效时长，域名等等
- Vary： 告知下游的代理服务器，应当如何对以后的请求协议头进行匹配，以决定是否可使用已缓存的响应内容而不是重新从原服务器请求新的内容。

> -X-Ua-Compatible: 强制浏览器的渲染方式，默认使用chrome来渲染，然后再按照IE该浏览器的最新版本来渲染