Project 1: Firewall and iptables

February 22, 2014

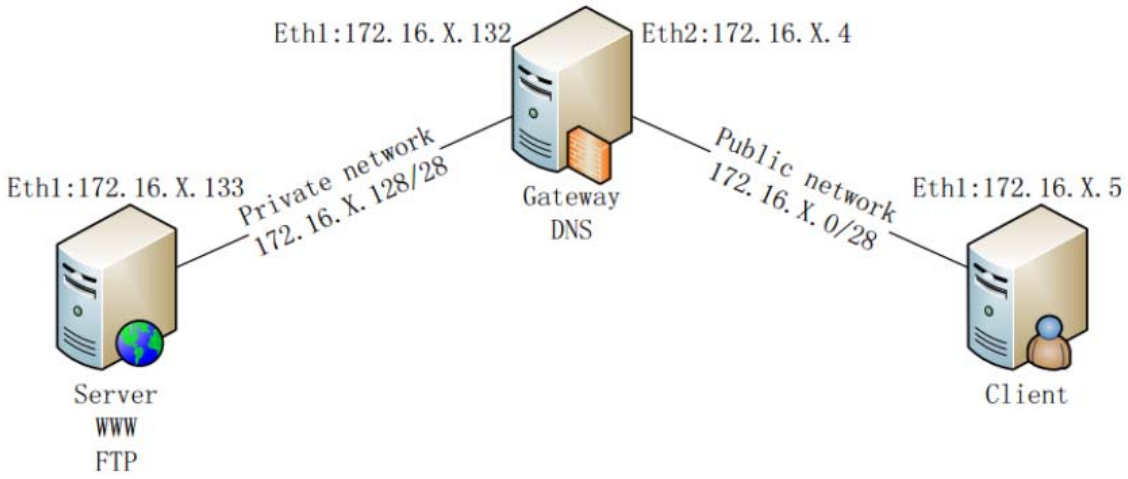
Bing Hao

Project description

The goal of this project is to gain hands-on experiences with the usage and functionality of iptables. The server student27vmg is supposed be configured as the gateway. The open source DNS server bind 9 and the sniffer tool Wireshark is installed on the gateway. Web server apache and FTP Server vsftpd is installed on the server student27vms. Gateway, Client, and Server simulate a typical network application scenario: the Server resides in a private network; the Client resides in a public network; the Gateway protects the Server from public access by using iptables.

Network set up of the project

The network topology is illustrated as follows:



(X represents your project number in vLab. Your current IP address should be 172.24.x.x/28)

For the client:

The client's IP address is 172.24.27.6 and its DNS is configured to 172.24.27.133.

For the Server:

The server's IP address is 172.24.27.134 and its DNS is configured to 8.8.8.8.

For the GW:

```
eth0      Link encap:Ethernet  HWaddr fa:16:3e:b6:bd:57
          inet addr:172.24.27.197  Bcast:172.24.27.207  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:feb6:bd57/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75664 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76827049 (76.8 MB)  TX bytes:5978729 (5.9 MB)

eth1      Link encap:Ethernet  HWaddr fa:16:3e:59:41:f7
          inet addr:172.24.27.5  Bcast:172.24.27.15  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:fe59:41f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35256 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5515111 (5.5 MB)  TX bytes:25314342 (25.3 MB)

eth2      Link encap:Ethernet  HWaddr fa:16:3e:99:72:a2
          inet addr:172.24.27.133  Bcast:172.24.27.143  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:fe99:72a2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:90060 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6708065 (6.7 MB)  TX bytes:27100898 (27.1 MB)
```

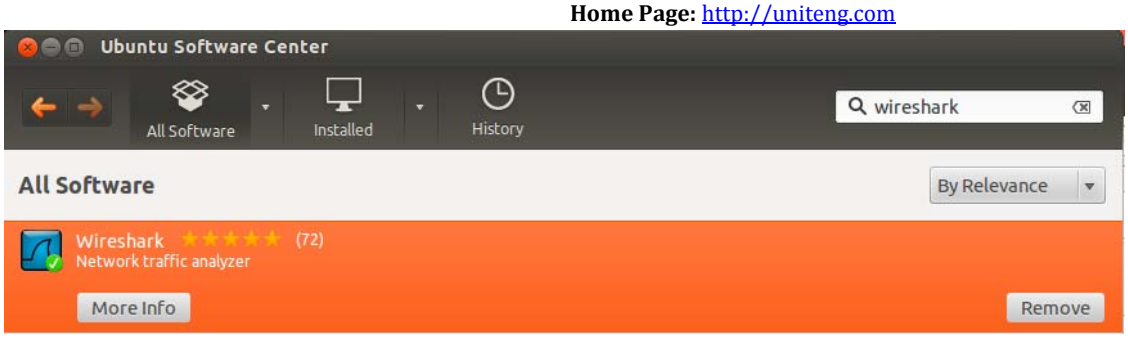
GW has 3 network cards, 172.24.27.133 will be used as the DNS server and the Gateway for other 2 machines.

Software packages used in the project

- Apache web server
- Bind9 DNS server
- VIM
- Iptables
- Wireshark
- Vsftpd
- Openssh-server

Step-by-step project description

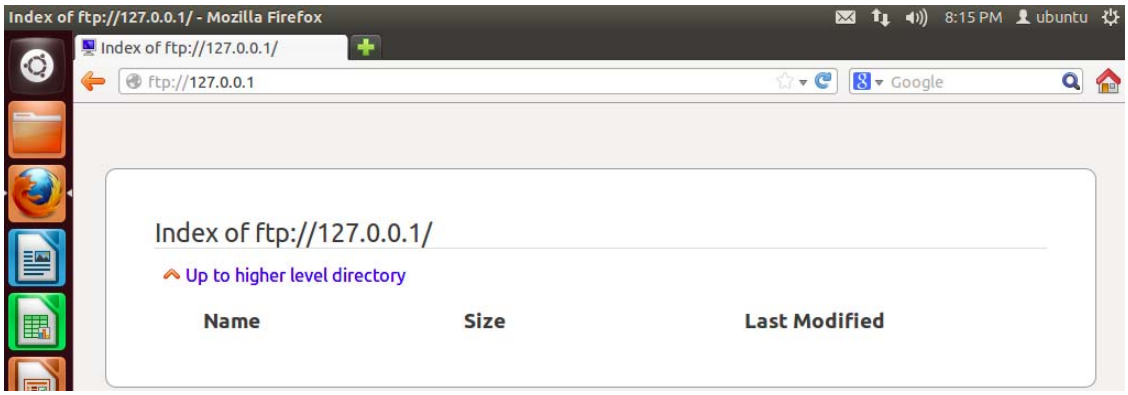
1. Install Wireshark on the server student27vmg



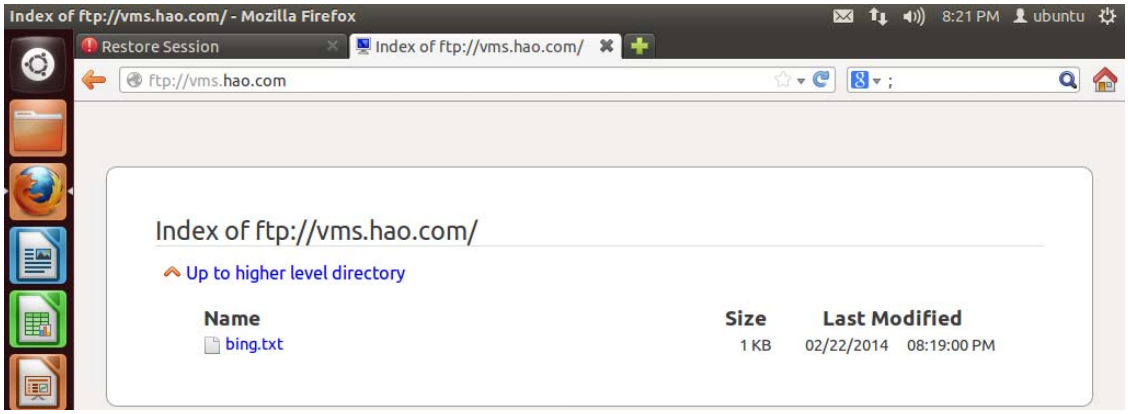
Wireshark could be installed using Ubuntu software center

2. Install vsftpd on the server student27vms
   sudo apt-get install vsftpd
   sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original

   Accessing ftp://127.0.0.1 in the firefox on student27vms:



   Accessing ftp://vms.hao.com in the firefox on student27vmc:



3. Configure vsftpd to be passive mode
   Add following contents to the end of the file /etc/vsftpd.conf:
   pasv_enable=YES

pasv_min_port=40000
pasv_max_port=40080
pasv_promiscuous=YES

4. Use NAT to hide Server VM from Client VM on the gateway student27vmg
   #Use NAT to hide Server VM from Client VM, change forward policy
   $IPTABLES -P FORWARD DROP

5. Install openssh-server on the gateway student27vmg
   sudo apt-get install openssh-server

   Accessing the gateway student27vmg from student27vms:

```
ubuntu@ubuntu-virtual-machine:/etc$ ssh vmg.hao.com
ubuntu@vmg.hao.com's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri Feb 21 00:49:04 2014 from ubuntu-virtual-machine-2.local
ubuntu@ubuntu-virtual-machine:~$
```

6. Install openssh-server on the server student27vms:
   On the student27vmg:
   sudo iptables-P FORWARD ACCEPT

   On the student27vms:
   sudo apt-get install openssh-server

   On the student27vmg:
   sudo iptables-P FORWARD DROP

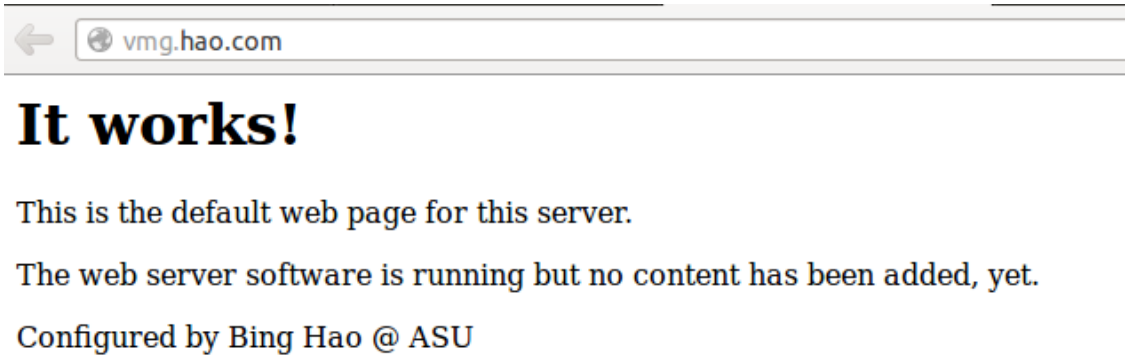
7. Execute following iptables rules on the gateway

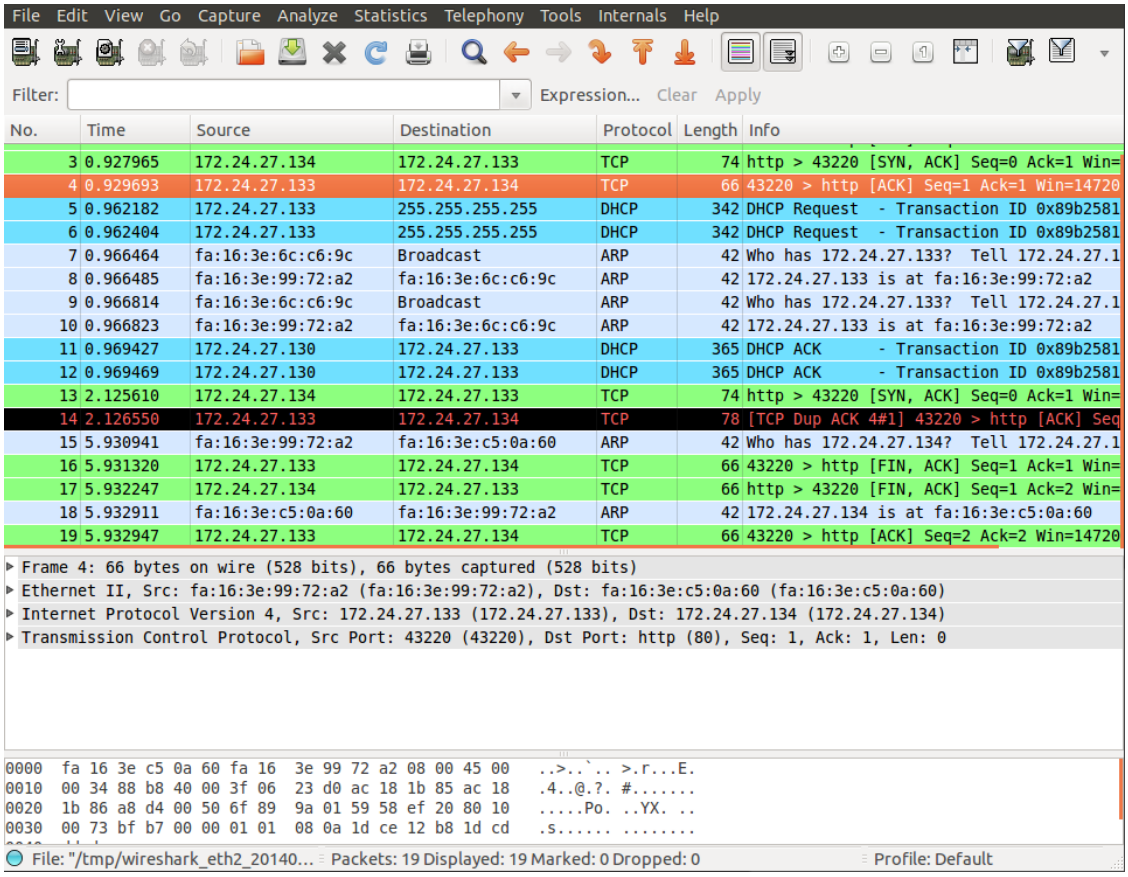
```
#!/bin/sh
iptables -F
iptables -F -t nat

iptables -P FORWARD DROP
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#comming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
```

Accessing http://vmg.hao.com (Gateway's IP) in the firefox on student27vmc:





This means the forwarding is working

8. Modifying the iptables rules as following for FTP

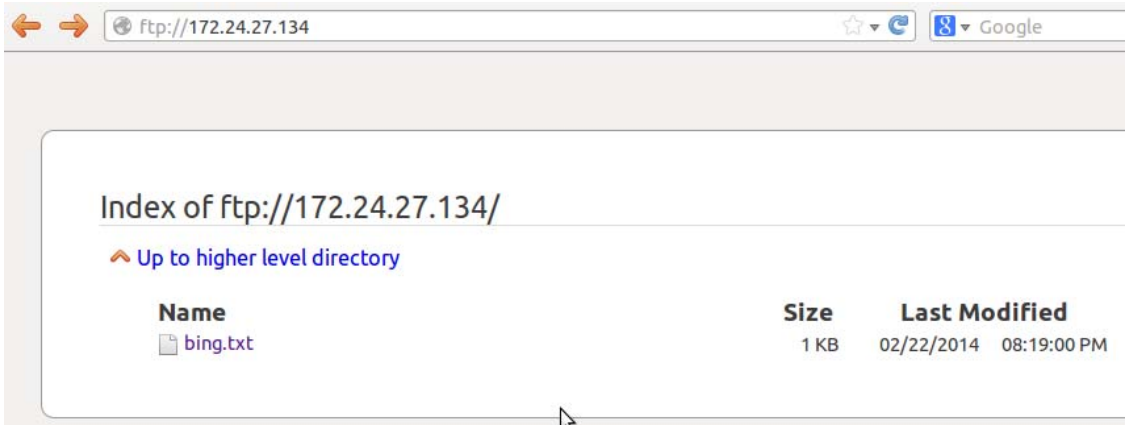
```
#!/bin/sh
iptables -F
iptables -F -t nat

iptables -P FORWARD DROP
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

#For HTTP
#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#comming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT

#For FTP
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 21 -j DNAT --to 172.24.27.134:21
iptables -t nat -A POSTROUTING -p tcp --dport 21 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 21 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 21 -j ACCEPT
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 20 -j DNAT --to 172.24.27.134:20
iptables -t nat -A POSTROUTING -p tcp --dport 20 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 20 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
```

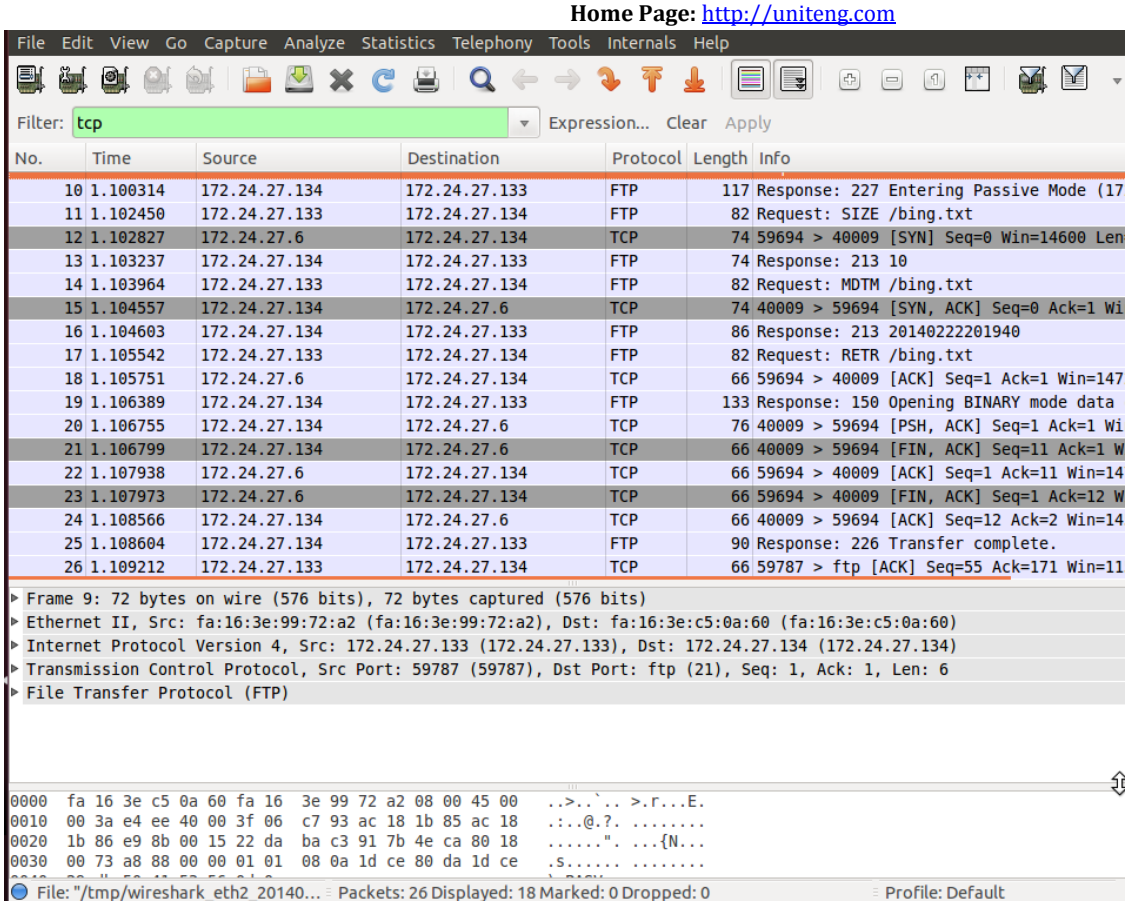
Accessing http://vms.hao.com in the firefox on student27vmc:



9. Allowing DNS on Gateway

```
#DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT
```

10. Downloading a file from ftp from client



Conclusion

The project have been finished successfully. The client and server have been configured properly.

Attached files

File name: rc.firewall

```
#!/bin/sh
iptables -F
iptables -F -t nat

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#For HTTP
#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#comming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT

#For FTP
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 21 -j DNAT --to 172.24.27.134:21
iptables -t nat -A POSTROUTING -p tcp --dport 21 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 21 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 21 -j ACCEPT
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 20 -j DNAT --to 172.24.27.134:20
iptables -t nat -A POSTROUTING -p tcp --dport 20 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 20 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 172.24.27.6 -j ACCEPT

#DNS
```

```
#DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT
```