Chi Zhang & Yuyang Zhang
CS6740 Network Security

Lab report for Firewall

1) *All of the files modified in /etc/iptables.*

   We modified the /etc/iptables/ipv4/start.sh and /etc/iptables/ipv4/filter.sh.
   Please check them in the folder for more details.

2) *Why does the File Transfer Protocol (FTP) pose a problem for firewalls? If you had blocked all traffic on your firewall, what iptables commands would you use to allow outgoing FTP connections from your VM?*

   Because the FTP protocol has two sessions: control session and data session. The FTP protocol first opens up a connection in the control session, then it will use other ports to create a data session to transfer the actual data.
   Since the port numbers are determined by either client or server in the control session (depending on whether the connection is active or passive), they cannot be known by the firewall in advance. Thus, it requires the firewall to analyze the traffic data and set the rules dynamically.

   We will use the **ip_conntrack_ftp** module to track the FTP connection and set the filter rule to allow traffic of data session dynamically.

```
# First load the module
modprobe ip_conntrack_ftp
# Allow outgoing connections for the control session
iptables -A OUTPUT -p tcp --dport 21 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 21 -m conntrack --ctstate ESTABLISHED -j ACCEPT
# Allow traffic for active connections
# The server will initiate the data session with a fixed source port 20 and the destination port given by client
iptables -A INPUT -p tcp --sport 20 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 20 -m conntrack --ctstate ESTABLISHED -j ACCEPT
# Allow traffic for passive connections
# The client will initiate the data session with a random source port and the destination port given by server
iptables -A OUTPUT -p tcp --sport 1024: --dport 1024: -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --sport 1024: --dport 1024: -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

3) *The standard port for RDP on Windows is 3389/TCP. Suppose you change the port for RDP on your Windows server to 13889/TCP. How could you use iptables to forward any packets from the outside network destined for your Windows server at port 3389/TCP to port 13889/TCP instead? What iptables commands would you use? Hint: read about the NAT table in iptables.*

   We will use the following command:
   Use nat table for Network Address Translation.
   Use PREROUTING chain to alter request packets as soon as they get into the firewall.
   Use DNAT to do the port forwarding: change tcp traffic at port 3389 to port 13889.
   Use POSTROUTING chain to alter response packets just as they are about to leave the firewall.
   Use SNAT to restore the source IP address so that the response packets will not be refused by the client.

   The final rules are:

```
$IPTABLES -t nat -A PREROUTING -p tcp -i $OUTSIDE_IF --dport 3389 -j DNAT --to-destination 10.0.100.1:13389
$IPTABLES -t nat -A POSTROUTING -o eth0 -j SNAT --to-source $OUTSIDE_IP
```