25

Answers to Even-numbered Exercises

2. What is firestarter? How is it related to iptables?

   The firestarter utility is a user-friendly, graphical tool that you can use to create a firewall that protects a system from malicious users and to set up NAT (Network Address Translation), which can allow several systems to share a single Internet connection. In addition, firestarter can control a DHCP server.

   The iptables utility builds and manipulates network packet filtering rules in the Linux kernel.

4. How would you list all current iptables rules?

   The following command lists all iptables rules:

   ```
   $ sudo iptables -L
   ```

6. Define an iptables rule that will reject incoming connections on the TELNET port.

   The following command rejects incoming connections on the TELNET port:

   ```
   $ sudo iptables --append FORWARD --sport telnet --jump REJECT
   ```

8. What does the **conntrack** module do?

   The **conntrack** module implements the connection tracking machine, which provides information on the state of a packet, allowing you to define rules that match criteria based on the state of the connection the packet is part of.

10. What do packet match criteria do? What are they used for?

    Packet match criteria identify network packets and implement rules that take action on packets that match the criteria.

12. Define a rule that will silently block incoming SMTP connections from **spmr.com**.

    The following command blocks incoming SMTP connections from **spmr.com**:

```
$ sudo iptables --append FORWARD --dport smtp --source spmr.com --jump DROP
```