Real-World Exercises

1. Imagine that a disaster, such as a fire, has befallen your home, damaging your belongings and some of the interior walls. What would your priorities be in assessing the damage and working to reoccupy your home? Create a prioritized list and timetable to accomplish this task.
2. This chapter listed several natural disasters that routinely occur in various parts of the United States. Using a Web browser or library research tool, identify the disasters that occur regularly in your area. Prioritize this list based on probability of occurrence and potential damage. What should organizations in your area do to prepare for these disasters?
3. Using a Web browser, search for organizations in your area (and nearby areas) that offer DR training. What topics do they cover in their training? Create a list of the topics covered by each organization and look for topics covered across the offerings.
4. Using a presentation tool such as PowerPoint, create a short DR training presentation that gives an overview of the key points found in Exercise 3. Bring it to class to share with your peers.
5. Using a Web browser or local directory, search for organizations that provide DR services. Make a list, then scratch out those that only provide data backup services or provide only alternate site services (BC services). How many are left? Why is this list so much shorter than the first? What services do the remaining organizations offer?

Hands-On Projects

In this project, we will take a look at reassembler, a Python script that reassembles fragmented packets in multiple methods so that analysts can view questionable traffic exactly as an IDS saw it, thus helping them determine whether the IDS made a proper decision regarding the traffic in question. Additionally, we will use reassembler to write the traffic to disk, so that binary payloads can be examined in the same form that the potential target operating system would view it.

1. Start your Security Onion distro.
2. Open a terminal session by double-clicking the **Terminal** icon on the desktop.
3. The version of Security Onion we are running does not have reassembler installed, so you will have to upgrade to the most recent version. Type **sudo -i curl -L http://sourceforge.net/projects/security-onion/files/security-onion-upgrade.sh >~/security-onion-upgrade.sh && bash ~/security-onion-upgrade.sh** and press **Enter**. If prompted, enter your administrative password. You may experience a delay as Security Onion downloads and installs updates.
4. To have fragmented packets to work with, you will use the scapy application. Normally, you would extract the suspect packets from an existing pcap of valid network traffic for further examination. Type **scapy** and press **Enter**.
5. Type **pkts=scapy.plist.PacketList()** and press **Enter**.