1. You have just been hired to conduct a security audit of a small business network. When you looked at their network closet, you noticed that they did not have a hardware firewall installed. You do see two servers in the closet, so you log into them to see if they have a software firewall enabled. Both machines are running a version of Linux on them. What application should you use to check if their software firewall is configured properly?
   1. Windows Firewall
   2. IPFW
   3. **iptables**
   4. PF

Explanation: The program iptables is used to configure the firewall on Linux servers. Windows Firewall is only available on Windows servers and desktops. PF and IPFW are available on FreeBSD and OS X. (Lesson 04\_02 Software Firewalls)

1. You are a security analyst who is reviewing the alerts and logs from your company’s intrusion detection system. You find an alert in the IDS that states that a data exfiltration was occurring. You analyze the logs and determine that the data being sent was just the nightly backup of your company’s database to its offsite facility. How should you classify this alert in the IDS?
   1. True positive
   2. **False positive**
   3. True negative
   4. False negative

Explanation: Since you were able to verify that the alert is erroneous (the event was not malicious but was instead expected), this is an example of a false positive. A false positive occurs when the IDS creates an alert which states that legitimate activity was malicious. (Lesson 04\_04 IDS)

1. You have been asked to evaluate several different DLP solutions at an IT trade show and determine which one will best meet your company’s needs. Your boss has told you that he wants a solution that can be installed on the file server to inspect data at rest. Which type of DLP should you consider first?
   1. **Storage DLP**
   2. Endpoint DLP
   3. Network DLP
   4. Cloud DLP

Explanation: A storage DLP is typically installed on a file server or in the data center to monitor the data at rest. An endpoint DLP is installed on an individual computer to monitor data in use. A network DLP would best be installed at the perimeter of the network and inspect the data in transit. A cloud-based DLP would best be used if your organization has a large cloud presence. (Lesson 04\_06 DLP)