1. You are at the doctor’s office and waiting for the physician to enter the room to exam you. You look across the room and see a pile of patient records on the physician’s desk. There is no one in the room and your curiosity has gotten the better of you, so you walk across the room and start reading through the other patient records on the desk. Which tenant of security have you just violated?
   1. Authentication
   2. **Confidentiality**
   3. Integrity
   4. Availability

Explanation: Confidentiality ensures that data or information has not been disclosed to unauthorized people. In this case, you are not the doctor or the patient whose records you looked at, therefore confidentiality has been breached. (LESSON 01\_03 CIA TRIAD)

1. You have just walked up to the bank teller and requested to withdraw $100 from checking account #7654123 (your account). The teller asks for your name and driver’s license prior to conducting this transaction. After she looks at your driver’s license, she thanks you for your business, pulls out $100 from the cash drawer, and hands you back the license and the $100 bill. What category best describes what the bank teller just did?
   1. Accounting
   2. Authorization
   3. **Authentication**
   4. Availability

Explanation: Authentication occurs when a person’s identity is established with proof and confirmed by a system. In this case, the bank teller verified you were the account holder by verifying your name and looking over your photo identification (driver’s license) prior to giving you the cash being withdrawn. (LESSON 01\_04 AAA OF SECURITY)

1. You have just registered as a penetration tester in a bug bounty contest and begin to scan the company’s website. You find a known vulnerability in their Apache web server, document the finding, and submit it to the bug bounty program hoping for a cash reward for your efforts. Which hat best describes you?
   1. Black
   2. Grey
   3. White
2. **Blue**

Explanation: A blue hat hacker is someone who attempts to hack into a network with permission of the company but are not employed by the company. This most commonly occurs as part of a bug bounty program or contest. If you were hired or contracted directly by the company, though, then you would be a white hat hacker. (LESSON 01\_07 HACKERS)

1. You are in the kitchen cooking dinner while your spouse is in the other room watching the news on the television. The top story is about how hackers have been able to gain access to one of the state’s election systems and tamper with the results. Unfortunately, you only heard a fraction of the story, but your spouse knows that you have been learning about hackers in your Security+ course and asks you, “Which type of hacker do you think would be able to do this?”
   1. Hacktivists
   2. Organized crime
   3. **APTs**
   4. Script Kiddies

Explanation: An APT is the most likely candidate to be able to successful hack a well-defended government computer network like the election system. Advanced Persistent Threats (APTs) are highly organized, well-funded, and often part of a nation state’s larger foreign policy and influence campaigns. Hacktivists are usually political, but they are disorganized and don’t have the level of sophistication needed to hack into a well-defended government computer network like the election system. While organized crime groups may have the sophistication to conduct the hack, they are usually more interested in conducting criminal actions to make money instead of getting involved in politics. Script kiddies are low skilled hackers who can only use other peoples tools, and therefore an unlikely choice. (LESSON 01\_08 Threat Actors)