Solution Guide: Security+ Sample Questions

Question 1

- Which of the following threat actors or threat actor groups is most likely to have the best funding to hire and sustain a group of hackers?
    - **Solution**: Nation states
- Extended Explanation:
    - Nation states have tax revenues, backing from large companies, and/or wealthy benefactors who fund malicious activities.
    - Well-funded organized criminals do not have the resources of an entire nation behind them.
    - Script kiddies do not have any funding because they are typically young and inexperienced and do not qualify for any backing.
    - Hacktivist groups might have minor funding from opposing viewpoint factions but the funding is not significant or comparable to nation states.

Question 2

- Which feature of insider threat actors makes them especially dangerous to an organization?
    - **Solution**: They have unrestricted access to sensitive data and information.
- Extended Explanation:
    - Insider actors are so dangerous because they have unrestricted access to sensitive data and information. That data can then be easily stolen or leaked by someone with appropriate access.
    - Insiders prefer to stay in stealth mode and an advanced persistent threat (APT) would give away their intent.

- A hacktivist would oppose the organization's political or ideological goals. An insider would never reveal this oppositional nature.
- Script kiddies use prebuilt or canned programs for attacks. Such attacks would likely give away the insider's position and intent.

Question 3

- Of the several types of threat actors, which one is a novice with little experience as a hacker?
  - **Solution**: Script kiddie
- Extended Explanation:
  - Script kiddies have very limited knowledge of security but use automated tools, such as scripts, to hack systems.
  - A hacktivist is a hacker who gains access to systems or other resources to disrupt operations based on ideological differences with the target.
  - An insider is someone who hacks internal systems in a company who has or had access to restricted materials.
  - A competitor may attempt to hack, compromise, or sabotage another company or an individual's work to gain a competitive edge.

Question 4

- Which threat actor is most likely to be highly skilled in launching attacks involving APTs against targets?
  - **Solution**: Nation state
- Extended Explanation:
  - A nation state has the most sophisticated and highly skilled hackers available for launching APTs.
  - A script kiddie is not highly skilled nor capable of launching APTs against targets.
  - An insider can be highly skilled but does not use APTs because these would give away their positions and intent.

- Organized crime rings are highly skilled but they do not launch APTs against a target.

Question 5

- A group known as Takedown hacked into your political action committee website and defaced it. Which type of threat actor is most likely responsible for the attack?
  - Solution: **Hacktivist**
- Extended Explanation:
  - Takedown is a hacktivist group. Its motivations seem political and it is interested in defacing websites of those who have opposing viewpoints from their own.
  - Script kiddies typically do not deface websites, only using scripts and applications that help them break into systems or applications with known vulnerabilities.
  - Although a malicious insider might have the ability to deface the site, it's unlikely that they would do so. Insiders usually exfiltrate data rather than deface sites.
  - It's unlikely that a competitor would deface the site. They would more likely look for a list of donors or other sensitive information.

Question 6

- What aspect of cybercrime often motivates script kiddies to hack into systems or into a company?
  - **Solution**: Bragging rights, publicity, or some other form of notoriety.
- Extended Explanation:
  - Script kiddies generally only want to be able to tell their friends that they have hacked some company, or hear their names on the news.
  - Script kiddies are not generally profit seekers because they do not have the resources to acquire or sell stolen items.
  - Script kiddies are not involved with government entities or agencies and therefore do not seek this type of information or activity.
  - Private or secret information motivates insiders to become threats. Script kiddies do not gain profits by having access to private or secret information.

Question 7

- Which of the following motivates a hacktivist to perpetrate a website for defacing or an informational breach?
    - **Solution**: Reputation damage to the target.
- Extended Explanation:
    - Hacktivists are interested in damaging or exposing their ideological opposition but not generally for monetary gain or other accolades.
    - Hacktivists are primarily concerned with damaging the reputations of their targets.
    - Hacktivists have no interest in military tactics or political upheaval. Their interest is purely ideological.
    - A boost in recognition is only important to script kiddies who want to show off to friends or rival script kiddie groups.