An on-path attack involves an adversary intercepting communication between two parties. How do on-path attacks differ from man-in-the-middle (MitM) attacks, and what common tools or techniques are used by attackers to facilitate these interceptions?

Answer: On-path attacks and man-in-the-middle (MitM) attacks both involve intercepting communication, but on-path attacks specifically refer to situations where the attacker positions themselves along the communication path, whereas MitM attacks encompass a broader range of interception techniques, including on-path attacks. Common tools and techniques for on-path attacks include ARP spoofing, DNS spoofing, and session hijacking to manipulate or eavesdrop on the communication between two parties.

Considering the subtlety of password spraying attacks, how can organizations effectively detect and thwart them? What indicators of compromise should system administrators monitor to identify such attempts?

Answer: Organizations can effectively detect and thwart password spraying attacks by implementing account lockout policies, monitoring for anomalous login patterns, and utilizing multi-factor authentication. System administrators should closely monitor failed login attempts, especially those targeting multiple accounts with a few password attempts each, and analyze authentication logs for unusual access patterns or repeated failed login activity from specific IP addresses.

Both password spraying and credential stuffing are attack methods that target user authentication. What are the main distinctions between the two, and are there scenarios where one method might be favored over the other by attackers?

Answer: Password spraying involves attempting a few commonly used passwords across many user accounts, while credential stuffing involves using a large set of username-password pairs obtained from previous data breaches to gain unauthorized access. The main distinction is in the scale and approach. Password spraying is more subtle and targeted, making it suitable for avoiding detection, while credential stuffing relies on a massive number of credentials and is more brute-force in nature. Attackers might favor password spraying when trying to evade account lockout mechanisms, whereas credential stuffing is effective when attackers have a large database of compromised credentials and aim for widespread account access.