DEFENSIVE

DEFENSIVE

Pass the Hash / Pass the Password

Mitigation

Hard to completely prevent, but we can make it more difficult on an attacker:

- Limit account re-use:
  - Avoid re-using local admin password
  - Disable Guest and Administrator accounts
  - Limit who is a local administrator (least privilege)
- Utilize strong passwords:
  - The longer the better (>14 characters)
  - Avoid using common words
  - I like long sentences
- Privilege Access Management (PAM)
  - Check out/in sensitive accounts when needed
  - Automatically rotate passwords on check out and check in
  - Limits pass attacks as hash/password is strong and constantly rotated