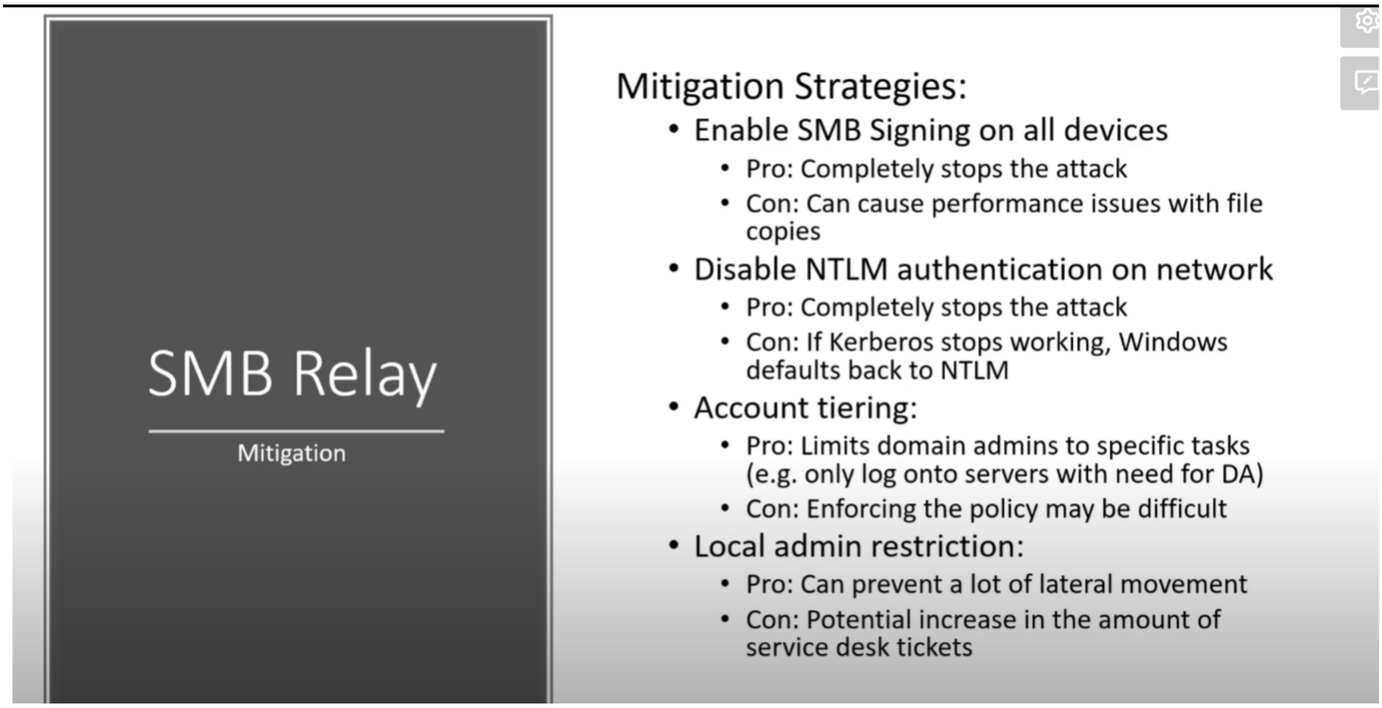
ENABLE SMB SIGNING

ENABLE SMB SIGNING



SMB Relay

Mitigation

Mitigation Strategies:

- Enable SMB Signing on all devices
  - Pro: Completely stops the attack
  - Con: Can cause performance issues with file copies
- Disable NTLM authentication on network
  - Pro: Completely stops the attack
  - Con: If Kerberos stops working, Windows defaults back to NTLM
- Account tiering:
  - Pro: Limits domain admins to specific tasks (e.g. only log onto servers with need for DA)
  - Con: Enforcing the policy may be difficult
- Local admin restriction:
  - Pro: Can prevent a lot of lateral movement
  - Con: Potential increase in the amount of service desk tickets