

# Pass-the-Hash

---

Martin Stanek

2025

## Net-NTLMv2 protocol

- NTLMv2 (Net-NTLMv2) is a challenge/response authentication protocol
- the protocol uses password hash as a secret to validate the response
  - hash is the actual password in this case
  - NT hash –  $\text{MD4}(\text{UTF-16-LE}(\text{password}))$
- the attacker need to steal just the hash
  - no password cracking necessary

# Mitigations

- “easy”: remove NTLMv2, move to Kerberos
  - see *pass the ticket* for Kerberos
- reality: defense in depth (prevention, detection, response)
- Microsoft, *Mitigating Pass-the-Hash and Other Credential Theft*, version 2, 2014