CWL
CyberWarFare Labs

Certified Enterprise Lateral Movement Specialist (CELMS)

@CyberWarFare Labs

External Lateral Movement:

Windows :

- **User / Pass**
  - WMI
  - PSEXEC
  - SCShell
  - WSMAN (PSREMOTE)
    - winrs
- **Hash**
  - Pass the hash
- **Kerberos**
  - PTK (AES keys)
- **Remote Desktop Gateway**
  - Myrtille

Linux :

- **User / Pass**
  - SSH
  - VNC
- **SSH Keys**
  - Agent
- **Hash**
  - NTLM Relaying
- **Kerberos**
  - Kerberoasting
- **Remote Desktop Gateway**
  - Guacamole

Internal Lateral Movement:

Windows :

- **User / Pass**
  - Network Share
- **Hash**
  - Pass the Hash
- **Kerberos**
  - **Ticket**
    - Silver Ticket
    - Golden Ticket
    - Diamond ticket
  - **Delegation**
    - Unconstrained
    - Constrained
    - RBCD

Linux

- **User / Pass**
  - Kinit (Ex : access machine resources)
  - SMB
- **Hash**
  - Over Pass the Hash
- **Kerberos**
  - Hijacking Kerberos ticket (ccache)
  - Keytab
  - Sapphire ticket

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live