OS Credential Dumping

Credential Access - T1003.001

Summary of Actions

- Authenticate as local admin through RDP
- Load Mimikatz
- Execute Mimikatz and Locate com.service ntlm hash
- Utilize Mimikatz to over-pass-the-hash to gain privileges as a domain admin
- Create domain admin account