Active Directory Attacks

Vernon Andrade
CyberHoos 2018
What is the Active Directory?

- A directory service that Microsoft developed for Windows domain networks.
- A centralized and standardized system that automating many functions
  - Management of user data
  - Security
  - Network Resources
- Used for distributed networking environments
Why attack the active directory?

- Part of critical infrastructure for many businesses and governments
- Acts as a gateway to organization’s information
- Makes privilege escalation very easy
- Grants control of all machines on a network to the administrator
- Fake domain controller to distribute malware and create back doors
Active Directory Attack Vectors / Weaknesses

- Stealing hashed credentials and tricking the authenticator (nerfed)
  - Security policies only allow certain computers access to AD
- General privilege escalation
  - Unprivileged accounts having access to reset privileged accounts passwords
Tools for

- Mimikatz
  - Grabs LM hashes / creates Kerberos tickets
- Powersploit
  - Powershell toolkit
- Bloodhound
  - Finds path of users that can get you to admin
- Death Star
  - Uses information from Bloodhound and automates elevation to Admin
Basic Attack Path

- Build attack path with Bloodhound (admin mapper)
- Leveraging Active Directory permissions and password resets
- Reset passwords following attack paths
- Once privileged access is achieved, use Mimikatz to extract NTLM password history for all compromised accounts
- Apply previous NTLM hash to the accounts, reverting the passwords to previous values
How to protect against AD attacks

- Limit “Reset Password” permissions
- Limit admin logins to trusted computers