CCDC Debrief

Windows Server 2008 R2

Active Directory

DNS

Responsibilities

- Manage Active Directory
- Manage DNS Server

Server Hardening

- Not enough time for all updates
  - Only ran those related to Security
- Reboot required
  - Timed to coincide with Router reboot
- Active Directory
  - Disabled all other users
- Deployed Group Policy Objects according to checklist
  - Kept Red Team out later.

Injects

- Sync time across computers
- Implemented a GPO to enforce this.

Red Team Attacks

- Attacks were monitored in real time via router
  - Most focused on SMB vulnerabilities
    - SMB was already locked down via GPO
- Repeated Attackers blocked via Firewall rules on Router