Windows AD Playbook

Enumeration and Preliminary Setup:

* Run the two scripts to gather information about who the local administrators are and remove them
* Rename the Administrator account
* Run script to change the passwords of all users
* Check to make sure self is the DNS server and the forwarder is set to google or Cloudflare
* Turn off IPv6 and disable NetBios over TCP (old style Network Settings)
* Audit GPOs and disable malicious group policies
* Create a password policy GPO with the following settings
  + Enforce password history 6
  + Maximum password age 60 days
  + Minimum password age 15 days
  + Minimum password length audit 10
  + Password must meet complexity requirements
  + Store password using reversible encryption false
* Create an Audit logon/logoff policy
  + Audit logon success;failures
  + Audit logoffs success;failures
  + Audit special logons success;failures
  + Audit other logon/logoff events success;failures