Windows Checklist

# General

* Run CyLR
* Rotate Administrator Password

net user administrator <password>

* Create new Admin-level account

net user /add <new account> <password>

net localgroup administrators <new account> /add

* Disable Administrator and Guest accounts

net user administrator /active:no

net user guest /active:no

* Enable Firewall (Ensure RDP and scored services are Allowed)

wf.msc

firewall.cpl

* Remove non-privileged users from Administrators

compmgmt.msc

* Check startup programs and Scheduled Tasks

msconfig.msc (win8+ ctrl+shft+esc)

taskschd.msc

* Check for SMB shares and review/adjust permissions – disable if unscored

File system *and* Network level

* Disable administrative shares

for %i in (C$ IPC$ ADMIN$) do net share %i /delete

* Identify externally available services – disable/remove if unscored
* Disable IPv6

ncpa.cpl

* Disable SMBv1 where possible (single line cmd)

reg add HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG\_DWORD /d 0

* Begin service hardening

# DC Specific

* Roll Kerberos twice (krbgt)
* Remove all accounts from Domain Admins (except Administrator)