**Windows**

1. Kill Networking (in powershell) and firewall rules (CLI)
   1. Disable-netadapter
   2. $wmi = gwmi –class win32\_networkadapter –filter “Name LIKE ‘%<name>%’” [enter] $wmi.disable()
   3. Netsh advfirewall set currentprofile firewallpolicy blockinboundalways,allowoutbound
   4. Netsh advfirewall firewall add rule name=”Open <Service>” dir=in action=allow protocol=<tcp | udp> localport=<port number> remoteip=<scoring server ip>
   5. Netsh advfirewall set currentprofile logging <filepath>
   6. Netsh advfirewall set allprofile logging droppedconnections enable
   7. Netsh advfirewall set allprofile logging allowedconnections enable
2. Rotate Creds and delete unnecessary accounts (CLI)
   1. Net user
   2. Net user <username> <new password>
   3. Net user <username> /delete
   4. Net localgroup administrators <username> /delete
   5. Net group “Domain Admins”
   6. Net share <sharename> /delete
   7. Create own administrator and delete default admin and guest
   8. Net group
3. What services are running and stop unnecessary (powershell)
   1. Get-service
   2. Stop-service <service-name>
   3. Turn off file sharing and remote desktop
4. Backup configs (CLI)
   1. Copy <file path> <new file path>
5. Check environ for suspicious (both)
   1. $PATH
   2. Event viewer
   3. Task Scheduler
   4. Get-EventLog
6. Check Service configs
   1. Server Manager
      1. AD
      2. DNS
      3. DHCP
      4. HTTP (IIS)
7. Restart services and turn interfaces back on (powershell)
   1. Enable-netadapter
   2. $wmi = gwmi –class win32\_networkadapter –filter “Name LIKE ‘%<name>%’” [enter] $wmi.enable()
   3. Restart-service <service-name>
8. Audit Logs
   1. In Local Security Policy > Local Policies > Audit Policy, audit all for failure
      1. Block failures
   2. Disable netbios
   3. Netdom query WORKSTATION
   4. Netdom query SERVER
   5. Host file
      1. C:\%SystemRoot%\System32\Dns
9. Check for other bads
   1. Watch processes
   2. Disable sticky keys
      1. Reg add “HKCU\Control Panel\Accessibility\StickyKeys” /v Flags /t REG\_SZ /d 506 /f