1. Log in
2. Change password
3. See who is domain admin (should only be you)
4. Create accounts for Windows team members
5. Policies (management console)
   1. unlink all current policies (don't delete)
6. Make your own new policy (password complexity, etc.)
   1. gpupdate force on all clients
7. Check Local users
   1. admin group (make sure there are no weird users)
   2. get list of all users on AD
      1. dsquery user \*
   3. net user all local users
8. Know which users can access in domain admins and local admin groups
   1. powershell script that finds privileged accounts
      1. 2008 and up will have powershell
   2. powershell is an add-on for 2003
   3. there are different versions of powershell
   4. copy and paste the "script" if you can't run a text file for safety reasons
9. Check running processes
   1. process explorer (look at red services)
10. Malwarebtytes
    1. only run if it will take 5 minutes or less (don't waste too much time here)
11. Have firewall on all servers
    1. gets tricky with AD server (lots of ports open). Configure to where only Windows team computers can access so people from Linux cant' get in. (Whitelist Windows team by IP addreses)
12. Tinywall (only install and use when you are console connected)
    1. blocks inbound and outbound traffic
13. Don't need RDP access for competition
    1. will be given console access
14. Network scan (internal and external)
15. Backup config files and registry
    1. won't have space to backup the entire filesystem
16. Know where everything was before you remove it
    1. you should be the only one in domain admin, but document who you remove
17. Always disable accounts, never delete them

* NTP
  + group policy, make AD the default NTP server
  + AD should be the NTP server for all of our systems
* For AD users
  + AD users and computers (ADUC) to set up accounts across all systems
  + AD must make users!
    - this server is the only one with the tools to do it
* RSAT
  + helps fix server 2003 weird AD menu
* Use Group Policy management console to set policies
  + lookup good policies for reference
* If you bring a book, bookmark pages
* Know your hostname (you should know this from inventory)
* All servers and clients need to point to internal DNS
  + should be on AD under server manager
  + AD will point to itself (primary)
    - secondary DNS is usually Linux (Ubuntu)
      * slave DNS
  + zone transfers tab will have list of IPs
    - should only be slave DNS IP. No other IP should be in there except for the slave DNS (Rupert)
  + look at network config on all servers and make sure primary DNS is set to AD and secondary is set to Linux DNS
  + never set internal DNS to google, user internal addresses (hence the name)
    - google is an external DNS server
* Ticket system
  + Hesk (free PHP script)
    - set up SQL database and web server with PHP
* Sysinternals suite
  + TCPview (what connections is your system making?)
    - AD will have a lot, others don't need a ton of open ports