Windows 8

1. Print & read Readme…!!! REMEMBER TO READ SECURITY Q’S!!!
2. 5 minute look around
3. Locked out of TaskMng
   1. Fixed with easy google OR Process Hacker
4. Accounts
   1. Remove unwanted
   2. Set password
   3. Authorization (IE: Admin should be user)
   4. Secure password for all
5. Start Windows Defender/MalwareBytes/TDSKiller
   1. Found and deleted DarkComet RAT
6. Services - found nothing?
   1. Forgot to campare to baseline… whoops
7. Install/Uninstall software
   1. Unistalled zoomify – points
8. Password policies
   1. Minimum characters
   2. 30 day max - admin
   3. 90 day max - non-admin
   4. Password age warning 10-30 days
   5. History set to 5
   6. Complexity Requirements
   7. Disable reverse encryption
9. Security Policies0
   1. Compare to Server2008 baseline (Ferris doc.)
      1. GET POINTS ALMOST ALWAYS
         1. Last username not displayed
         2. Ntlm hash not stored
10. Updates
    1. IE – points
    2. Notepad++ - points
    3. Didn’t finish Windows/Security updates…?
       1. No service pack.
11. Misc.
    1. Bitlocker
       1. Had to enable and change some policies
    2. Security Q’s
       1. IP of comment?
          1. Logged into local site web

DIDN’T KNOW HOW TO DO SERVER STUFFL

TEAM BRAVO: 60-70 points? TEAM ALPHA: 40 -50 points?

Windows Vista

ALL WINDOWS RELATIVELY SAME…

Points for:

* Deleted User Sbaski -6
* Deleted User Rairn – 2
* User Mmag no longer admin - 2
* User Vhand is enabled – 7
* Password history – 3
* Lockout threshold – 3
* Malwarebytes – 13
* Remove wire shark – 4
* UAC enabled – 6
* Service Pack 2 – 10ish
* Security Q 1 – 10 ; Types of character coding
* Security Q2 – 7 ; Extract hidden file out of jpeg and “Q Code”

Ubuntu

* Read readme
* Installed rkhunter + Clamtk
  + Found root ssh access enabled, noted
  + Password file/group file changes
* Looked at services with sysv-rc-conf
* User accounts
  + Deleted accounts - 8pt
    - Deleted user we needed for security question - 8pt
  + Changed permissions - 8pt
  + Changed insecure root password – 4pt
  + Disabled guest account – 7pt
* Updated through terminal
  + System not vulnerable to shellshock – 7pt
  + OpenSSL updated – 9pt
* Configured auto update – 7pt
* Removed unnecessary software
  + Games
  + Magic secret password finder that I don’t know the name of
  + Python crypto
  + Disabled apache – 6pt
  + Went through installation history
  + Someone uninstalled rtkit, looks like we needed that
  + Also found netcat, malware? Uninstalled (bleached anything with name in filesystem) but no points
  + Deleted Transmission (default torrent client)
* Enabled firewall – 7pt
* Disabled ssh root logon – 7pt
* Removed mp3 files – 5pt
* Deleted background image – 4pt
* Password policy but no points
  + Min and max length
  + Min and max age
  + Complexity
* Readme said Firefox to be default, did so, but no points