Windows 7 First 15 minutes
Waldo:P@ssw0rd
http://hardenwindows7forsecurity.com/Harden%20Windows%207%20Home%20Premium%2064bit%20-%20Standalone.html

May want to start downloading updates ASAP while modifying accounts. Start-control panel-System & Security-Windows Update. Update to Windows 7 sp1 (may need to go to Microsoft directly) Also update Internet Explorer 8 to IE11

Modify accounts: Start –control panel-user accounts-user accounts-manage accounts-advanced-advanced OR start-searchbar-lusrmgr.msc
Accounts: administrator, guest, joe joe. Disable or remove, change passwords

Turn UAC to max: Control Panel-All Control Panel Items-User Accounts-Change User Account Control Settings

Set up firewall: set to public profile? Control Panel -Network and Sharing Center
- Change network location to Public.

Use only necessary network protocols:
Control Panel-Network and Sharing Center
Local Area Connection- Properties button
uncheckmark the following:
- Client for MS Networks
- File and Printer Sharing for Microsoft Networks
- QoS
- Link Layer Topology Discovery Mapper IO Driver
- Link Layer Topology Discovery Responder
- Internet protocol version 6

Select 'Internet Protocol version 4 (TCP IPv4), click Properties, click Advanced,
- click 'DNS' tab, uncheck 'register this connections address in DNS'
- click 'WINS' tab, select 'Disable NETBIOS over TCP/IP'

Disable IPv6 on a specific network adapter
You can do this by unbinding the adapter in the **Local Area Connection Properties** dialog box:
1. Click **Start**, and then click **Control Panel**.
2. Click **Network and Sharing Center**.
3. In the **View your active networks** area, click **Local Area Connection**, and then click **Properties**.
4. On the **Networking** tab, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **OK**.

Disable unused tcpip6 devices and Netbt (may need Netbt for Netbios)

Control Panel / Device Manager, View menu / Show Hidden Devices

- /Network, disable Wan Miniport IPv6
- /Network, disable Microsoft ISATAP adapter (IPv6 tunnel)
- /Network, disable Teredo Tunneling Pseudo Interface (IPv6 tunnel)
- /Non-Plug and Play Drivers /Remote Access IPv6 ARP Driver > Properties > Driver tab >: Change Startup Type from System to Disable
- /Non-Plug and Play Drivers / NETBT > Properties > Driver tab > Stop it and change Type from 'System' to 'Disabled'. (disables NETBIOS totally. partially closes port 445)

Disable port 1900 UPnP

Regedit
HKLM\Software\Microsoft\DirectplayNATHelp\DPNHUPnP
right click on right pane, new dword:32 bit,name it UPnPMode
Double click on that and set the value to 2.

Disable unneccesary services

Control panel-system and security-Administrative tools-Services-locate services-
Bluetooth-set to manual
Certificate propagation-set to manual
Remote Registry-set to manual
Network Access Protection agent
Windows Media
Homegroup listener and provider
Tablet PC Input Service
Remote Registry
http://www.techrepublic.com/blog/10-things/10-plus-windows-7-services-you-may-not-need/
http://www.digitalcitizen.life/which-windows-services-are-safe-disable-when
http://www.askvg.com/windows-7-services-that-can-be-safely-set-to-manual/
http://www.howtogeek.com/139028/which-windows-services-can-you-safely-disable/

Disabling Listening Ports

netstat –abn shows which ports are open and listening

Windows 7 firewall

If you have the Automated Configuration package, you can set the following instructions up in one step.
Control Panel / Administrative Tools / Windows Firewall with Advanced Security / Import Policy, select “Firewall Policy Win 7 Home Premium 64 Standalone.wfw”
Otherwise:
Control Panel/Administrative Tools/Windows Firewall with Advanced Security

/"Windows Firewall Properties" link
Click on each Profile (Domain, Private, Public) tab
- change Outbound connection = Block
- Specify Logging settings for Troubleshooting > Customize
-- Size Limit = 32767 KB
-- Log Dropped packets = Yes
- Specify Settings that control Windows Firewall Behavior > Customize
--Allow Unicast Response: No

Install .NET 4.5 (needed for Enhanced Mitigation Experience Toolkit)
Install Enhanced Mitigation Experience Toolkit-run it and then click the "Configure System" button. Make sure the following is configured:
DEP is set to always enabled
SEHOP is set to opt-out
ASLR is opt-in enabled

IPv6
https://support.microsoft.com/en-us/kb/929852
Autoruns
https://technet.microsoft.com/en-us/sysinternals/bb963902
process explorer
https://technet.microsoft.com/en-us/sysinternals/bb896653
currports
http://www.nirsoft.net/utils/cports.html

windows 7 security articles
http://www.windowsecurity.com/articles-tutorials/misc_network_security/Windows-7-Security-Primer-Part1.html

post by Encryptedbytes on Win7 security on wilderssecurity forum
https://www.wilderssecurity.com/threads/security-hardening-windows-7-64-bit-install.324004/

post by “david” on august 23, 2014 on superuser.com forum
http://superuser.com/questions/421558/rock-solid-hardening-of-a-windows-7-system

disabling services
http://www.askvg.com/windows-7-services-that-can-be-safely-set-to-manual/
http://www.techrepublic.com/blog/10-things/10-plus-windows-7-services-you-may-not-need/
http://www.digitalcitizen.life/which-windows-services-are-safe-disable-when