CyberPatriot Notes – Summary and Checklist [v.4 - 2013-11-09]

This is a collection of notes, tips, etc. from the discussions and training we've had up to this point, which has been fairly basic. Don't trust the system! Stick with the basics and follow a simple, logical plan and you'll be able to discover and fix the issues on any system whether it's Windows or Linux.

Take good notes while you're checking out each system! Keep track of what you find, both good and bad, including:

- Programs / services that you must keep running, depending on the function of the system (typically found in the CyberPatriot rules & notes)
- User accounts and passwords (both good and bad)
- Suspicious-looking programs / services
- Additional items to look at after your initial system survey

Getting Started

Windows Commands and Utilities	System Survey / Checklist Item	Linux Commands and Utilities
CTRL-ALT-DEL and choose "Change Password" (or use Command Prompt or Control Panel / User Accounts)	Change your password (at least 8 characters with a combination of upper, lower, number, and special characters)	'passwd' (follow prompts)
Open the "Folder Options" window, then be sure to set the following: ▪ Show hidden files, folders, and drives ▪ (uncheck) Hide extensions for known file types ▪ (uncheck) Hide protected operating system files	Set file and folder viewing options By default, Windows tries to make file listings simpler for end users. But since you are cyber ninjas, you want to see everything on the system.	
Check to see what Service Pack (if any) has been applied and if any additional patches have been installed: ▪ Control Panel → Add/Remove Programs (select the "include updates" option) ▪ Current Service Packs include: ○ Windows XP = SP3 ○ Windows 7 = SP1 ○ Windows Server 2003 = SP2 ○ Windows Server 2008 = SP2 ○ Windows Server 2008 R2 = SP1 (more on this in the "Digging Deeper" section below)	Service Packs, updates, and patches Some of the service packs take a while (maybe up to an hour or so) to install, so it would be wise to begin installing the current service pack early in the round. While the service pack is installing, you can still continue through the checklist and take notes on things you see, or even begin fixing issues found, if possible.	To update Ubuntu, run the following: ▪ sudo apt-get update ▪ sudo apt-get upgrade This may require several runs and reboots, but run until no more updates are available.

Computer Management applet (Admin Tools → Computer Management), a single point to view the following: ▪ Event Viewer (system logs) ▪ Shared Folders ▪ Local Users and Groups ▪ Services System Configuration Utility (msconfig): ▪ Services ▪ Startup (things that start up when Windows starts and/or a user logs on) ▪ Tools (a launching point for a bunch of other useful utilities)	These are all good tools to start with	▪ 'dpkg -l' will list all installed packages on a Ubuntu system
▪ netstat.exe -an (netstat -anb to show executables) ▪ Admin Tools → Services	See what's "listening" and/or running on the system. Watch for remote access programs! (i.e., Telnet server, netcat, backdoors, etc.)	▪ lsof –i ▪ netstat -an ▪ ps -ef
▪ Administrator, Guest, Support_###### are standard on a Windows system ▪ Watch for spelling and unknown accounts, especially ones in the Administrators group (i.e., AdmlnIstrator instead of Administrator, etc.) ▪ Make sure Administrator and Guest accounts have strong passwords, and disable the Guest account ▪ Create a new account for your routine use that has admin rights and set a strong password. Don't use the Administrator account for routine use!	User Accounts: which ones exist and are they legitimate? When in doubt, check a reference (Google, MS docs, etc.) before removing anything!	▪ cat /etc/passwd ▪ cat /etc/group

Shared folders on the system: ▪ Computer Management applet ▪ Check who has access, and whether it's read-only or read-write (full access) ▪ If a shared folder isn't necessary, stop sharing it ▪ A $ (dollar sign) after the share name hides the share in folder view (but not from the command line using the 'net view \\<hostname>' command)	Shared folders / directories: Check to see what's being shared from the system	On Linux systems, directories are typically shared using either NFS (Network File System) or Samba. NFS would be used if the folder is going to be accessed by other Linux/Unix systems, and Samaba would be used if the directory is going to be accessed by Windows systems. Shares can be listed/viewed as follows: NFS: 'exports', or 'cat /etc/exportfs' Samba: (search Google)
▪ Right-click the desktop, select Properties, and then choose the screen saver tab. This only sets it for the currently logged in user, though. ▪ To set the screen saver for all users, set it using the Local Security Policy utility.	Screensaver / Screen Lock: Make sure the screensaver is set to activate after a given time (10 minutes is good) and it requires a password before unlocking.	Ubuntu server doesn't usually have a pretty GUI (Graphical User Interface) on it, so make sure the shell (command prompt) is configured to automatically log out the user after 10 minutes of inactivity.
Digging A Little Deeper		
▪ Enable the Automatic Updates feature ▪ If you know that the latest Service Pack for your version of Windows hasn't been installed yet, install it manually before running Windows Update wizard. ▪ As one of the final things you do, run Windows Update (on Start Menu) and apply the updates. Run this several times until no more updates are identified to ensure you get all of the updates! THIS MAY TAKE A LONG TIME, so save this for near the end of the competition, because you probably won't need to do it.	Service Packs, updates, and patches	

This is like the holy grail of Windows security settings. You can configure a lot of stuff in here, but you can also make your system unusable. Make sure you understand what a particular setting does before you change it! (Admin Tools → Local Security Policy) Some basic things to set here include: ▪ Password policies ▪ Account lockout settings	Local Security Policy	To make security-related tweaks in Linux, you usually have to make modifications to startup and/or configuration files. The startup files are in /etc/rc* and configuration files are everywhere, depending on the application or service.
This is a helpful tool from Microsoft you can download and run to check the status of updates, accounts, and more.	MBSA (Microsoft Baseline Security Analyzer)	(N/A for Linux systems)

It's almost essential these days to have an antivirus and anti-malware program on your system. There are several free ones, but the one we're going to use for our CyberPatriot exercises is from Microsoft because we know that they work and are supported.
 	
Windows XP/Vista/7:
MS Security Essentials
(http://windows.microsoft.com/en-US/windows/security-essentials-all-versions)
 	
Windows Server 2000/2003/2008:
Windows Defender
(http://www.microsoft.com/en-us/download/details.aspx?id=17)
	Antivirus	There are a couple of Antivirus packages out there, however, which could be installed. The one we've used and practiced with is AVG, and can be downloaded from http://free.avg.com/us-en/download. For Ubuntu Linux systems, make sure you download the ".deb" version. Install and run it as follows:
		`$ dpkg -i <filename>`
		`$ sudo /etc/init.d/avgd start`
		`$ sudo avgupdate`
		`$ sudo avgscan /`

	Rootkits	Install and run rootkit detection utilities (chkrootkit, rkhunter, etc.). You can usually just run 'apt-get install chkrootkit' and 'apt-get install rkhunter' from a command line. Run rkhunter as follows:
		`$ sudo rkhunter --update`
		`$ sudo rkhunter --check`
		`$ sudo rkhunter --check --enable apps`

Terminal Services is typically a service and can be found in the Services applet. Remote Desktop Services can be disabled by: Right-click on “My Computer” or “Computer”, then click “Properties”, then go the “Remote” tab (on WinXP or earlier) or “Remote Settings” (on Win7 and later). Uncheck the “Allow Remote Assistance” option and check the “Don’t allow connections to this computer” option.	Remote Access Unless required on the system as a critical or required service, you should DISABLE any remote access technologies. On Windows, these include Terminal Services and/or Remote Desktop Services and typically listen on TCP port 3389.	You can remotely access Linux systems using a free utility called PuTTY and can be downloaded from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html. On the Linux server, it’s not a good idea to let the root user log in remotely. To disable this, add the following line in the configuration file (/etc/ssh/sshd_config): PermitRootLogin no Most Linux distributions set this to ‘no’ by default, but always verify it.
	Drivers: Hardware drivers contain the code the computer needs to make components work, including video cards, modems, network cards, and more. If these drivers get corrupted or if one that contains malicious code is installed, you may see weird symptoms on the system. Remember the second CyberPatriot qualification round? Our mouse was acting screwy and we had to update the VMware tools, which includes drivers for use in the VMware application. As part of your patching process, update the VMware drivers to avoid potential issues.	If you’re running the command-line-only Ubuntu server, you probably won’t have much of a need for the VMware tools.
	Unnecessary software: We discussed the fact that these systems are typically considered to be servers, and typically have specific functions (i.e., web serv, DNS server, FTP server, etc.) Accordingly, users wouldn’t log into and surf the web on these systems. On Windows systems it’s nearly impossible to uninstall Internet Explorer, but if Firefox (or Opera, or Chrome, etc.) is installed, remove it. Use a web browser on another computer (like the host system/laptop, in our virtualized CyberPatriot environment).	