

Kathy First 15 Mins

1. Check that all outside services are running and working correctly, sign off on them
 - VLANs
 - Projector use
2. Delegate and get people working on the correct things
3. Harden Ubuntu 6.06 so that we have it secured until we rebuild.
4. Collect reports, look for baselines, ports, services, accounts disabled or changed. MBSA
5. Remind everyone to monitor their services and ports throughout competition
6. Check outside facing services constantly
7. Ossec server and agents

VPN for branch office http://articles.techrepublic.com.com/5100-10878_11-5805260.html

First things to ask the white team:

1. Can we set up a vlan to the branch office
2. We need a list of all the users and credentials of everyone in the branch office
3. Send them all our password changes

Windows Hardening

[Page history](#) last edited by [Daniel Zweber](#) 11 months, 4 weeks ago

start with patching the operating system with service packs and all security updates. this is done through the windows update option in the

control panel.

make sure the automatic updates are turned on to update automatically and the firewall turned on. done through the control panel install anti-virus software.

run the microsoft security baseline analyzer. if the machines do not have internet access download a cab file.

change the administrator password to something different from the default. this is done through the user accounts option in the control panel

change the name of the administrator account this is done through the user accounts option in the control panel

make sure that the guest account is turned off. this is done through the user accounts option in the control panel

check to see if there are any other user accounts on the machine and if there is disable them. this is done through the user accounts option in the control panel.

turn off all unnecessary services. services to turn off include fax, iphlpsvc, msftpsvc, p2pimsvc, simptcp, tlntsrvc

Configure Audit policy as described.

Set minimum password length.

Enable Password Complexity.

Configure event Log Settings.

Configure User Rights to be as secure as possible.

Ensure all volumes are using the NTFS file system

Configure file system permissions.

Configure registry permissions.

Set the system date/time and configure it to synchronize against campus time servers.

Install software to check the integrity of critical operating system files.

If RDP is utilized, set RDP connection encryption level to high.

turn on data execution prevention. done through system properties advanced performance settings data execution prevention turned on.

scan for vulnerabilities through the secunia.com site

How to set up auditing for the C: Drive

modify the local security policy,

Administrative tools -> local Security Policy -> security settings -> audit policy -> modify the ones you want to change

<http://www.5starsupport.com/tutorial/hardening-windows.htm>

Server Hardening Checklist <http://security.utexas.edu/admin/win2003.html>

Step 1 - Malware Removal

Malware infection is the #1 security issue facing Windows users.



[Malware Removal Guide](#) - Clean Adware, Rootkits, Spyware, Trojans, Viruses and Worms. Malware is short for malicious software. It is a general term that refers to any software or program code designed to infiltrate or damage a computer system without the owner's informed consent. This guide will show you how to remove these infections and protect yourself from future infections using free software.

FACT: [89% of consumer PCs are infected with spyware](#)

[^ TOP](#)

Step 2 - Windows Update



- [Steps to take before you install Windows XP Service Pack 3](#)

Windows Update - [Home Page](#)

Install **All** of the critical updates. This may have to be run multiple times. Run it over again until it says **0** critical updates available.

Notes - Windows Update requires the following services be enabled:

- **Automatic Updates** - Automatic

- **Background Intelligent Transfer Service** - Manual or Automatic

[^ TOP](#)

Step 3 - Software Updates

One of the most overlooked areas in terms of security is updating everyday applications. The majority of applications installed on your system have had updates released for them at some point. These updates not only address bugs and additional features but also security updates.



Secunia Software Inspector - [Home Page](#)

A free service that detects insecure versions of software that you may have installed in your system. When insecure versions are detected, the Secunia Software Inspector also provides thorough guidelines for updating the software to the latest secure version from the vendor.

[^ TOP](#)

Step 4 - Firewall

Firewalls are systems designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both Hardware and Software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Everyone connected to the Internet should be using a Firewall. The Windows XP Firewall is more than sufficient for most users. Those seeking more advanced features should get ZoneAlarm. Certain routers come with a built-in Hardware Firewall, you can use a Software Firewall in conjunction with this for added security. **Do not use more than one Software Firewall, since this can cause various problems.**



Windows XP Firewall - [Home Page](#)

Windows XP has always come with a firewall built-in that is highly recommended for most users since it offers the best performance and is the easiest to use. However, it was not enabled by default pre-SP2 but is automatically enabled if SP2 or higher is installed. SP2 or higher includes significant security enhancements to the original Windows XP Firewall such as boot time protection.

Instructions - Go to "Start", "Settings", "Control Panel", "Windows Firewall", select "On (recommended)". In the exceptions tab uncheck all of them unless you are sharing Files or Printers, then leave "File and Printer Sharing" enabled.

Notes - The Windows XP Firewall is more than sufficient for most users with full inbound protection. Advanced users may find it lacks any outbound monitoring, logging and other advanced features found in ZoneAlarm. If you do not need these features stick with the Windows XP Firewall since all third party firewall solutions will reduce performance and are harder to use. In Windows XP there is no way to guarantee 100% outbound protection once your system is compromised. - [Source](#) - [Source 2](#)



ZoneAlarm Firewall - [Download](#) - [Home Page](#)

Includes full inbound protection, outbound monitoring, logging and other advanced features. Recommended for advanced users only.

Instructions - Download and install, then disable the Windows XP Firewall.

Notes - The free version provides solid Firewall protection. The Pro version includes enhanced privacy, e-mail and security controls. If you are interested in purchasing an enhanced version compare them using the [ZoneAlarm Security Feature Comparison Chart](#).



GRC Shields Up! - [Shields Up!](#) - [Home Page](#)

The Internet's quickest, most popular, reliable and trusted, free Internet security checkup and information service. After you have properly configured your Firewall, use Shields Up! to test your Internet security.

Instructions - Select "Proceed", on the next page select "File Sharing", then "Common Ports" and finally "All Service Ports". Check for any security breaches and if found, check your Firewall to make sure it is enabled and configured correctly.

Notes - If you have a Router with a Hardware Firewall, Shields Up! will show results relating to it, not your Software Firewall. Any security issues can usually be rectified by updating the Router's Firmware or by properly configuring the Router's Firewall. Direct all inquiries to the documentation or manufacturer of the Router.

[^ TOP](#)

Step 5 - Utilities



Autoruns - [Download](#) - [Home Page](#)

Utility to display and control startup applications. Disabling unnecessary startup applications improves boot up time and overall system performance.

Instructions - Unzip and launch Autoruns.exe, wait until it says "Ready" in the bottom left corner, then select the "Logon" Tab. Next select "Options", check "Hide Microsoft Entries" and press the refresh button or press the "F5" key. The remaining items are third party applications. Uncheck all that are not needed, this will disable them from loading at Windows startup. AntiVirus and Firewall applications are necessary applications that should be running on startup. If you are unsure of what something is, highlight it, select "Entry" then "Google" to launch a search for more information regarding the highlighted application. You can permanently remove items by deleting them. Do not "Delete" anything unless you are 100% positive you do not need it. Disabled (Unchecked) items can be activated again by rerunning Autoruns, checking the item and restarting Windows.

Notes - You can control the startup applications for separate user accounts by selecting "User" and the account you want to edit. This is a much more powerful tool then the built-in System Configuration Utility (msconfig).



TCPView - [Download](#) - [Home Page](#) - [Port Authority Database](#)

An advanced monitoring utility that will show you detailed listings of all open TCP and UDP ports on your system, including the local and remote addresses and the connection state. On Windows 2000 and XP, TCPView also reports the name of the process that owns the open port.

192.168.1.0:80 - IP Address

192.168.1.0:**80** - Port Number

iexplorer.exe:1000 - Process Name

iexplorer.exe:**1000** - PID

Instructions - Unzip and launch TCPView.exe. You can use the "A" toolbar button to toggle the display between IP Addresses and their Domain Names. By default, TCPView updates every second, ports that change state from one update to the next are highlighted in yellow, those that are deleted are shown in red, and new ones are shown in green. Use this to quickly see what is accessing the Internet and on what ports. General port information can be looked up in the [Port Authority Database](#). It is common to have certain ports open such as Port 80, the primary port used by the world wide web (www) system, it will be open any time a web browser such as Internet Explorer is running. Ports can be open for various legitimate reasons, some pose an unnecessary security risk and others are open for malicious reasons (Spyware and Viruses). [Firewalls](#) such as the Windows XP Firewall or ZoneAlarm will secure all open dangerous ports. It is still a good idea to close all unnecessary ports.

Notes - Svchost.exe is related to various Windows Services. A Remote Address of *.* means the port is open but not connection to anything. TCPView may show that the System Idle process (PID 0) is using some TCP ports. This behavior may occur if a local program connects to a TCP port, and then stops. The program's TCP connection to the port may be left in a "Timed Wait" state even though the program is no longer running. In this case, TCPView may detect that the port is in use. However, TCPView cannot identify the program that is using the port because the program has stopped and the PID was released.



TweakUI - [Download](#) + [Control Panel](#) - [Home Page](#)

This Windows XP PowerToy lets you disable AutoPlay. The Windows AutoPlay feature is the method Sony's Music CD [Rootkit](#) used to install itself. Disabling this will protect you from these sorts of exploits in the future. This has the added benefit of bypassing most [DRM](#) systems on Audio and Video CDs/DVDs. Data CDs can still be accessed through Windows Explorer. DRM Audio CDs can be

played in Windows Media Player by going to "Play", "DVD, VCD or CD Audio", "CD Drive (X:)". In Winamp select the Main Menu Icon in the top left corner, "Play", "Audio CD X:".

Instructions - Download, install, add to the Control Panel and run. Go to "My Computer", "AutoPlay", "Drives" then uncheck each drive letter for each drive you want AutoPlay disabled on. It is recommended to do this on all Optical Drives.



XP-AntiSpy - [Download](#) - [Home Page](#)

Disables all the known 'Suspicious' Functions in Windows XP.

Instructions v3.97 - Install and run. Go to "Profiles", select "Neutral", then check all but the following:

[MediaPlayer Functions]

_ **Do not acquire licenses automatically** - This prevents Windows Media Player from downloading any necessary licenses.

_ **No automatic updates** - This prevents Windows Media Player from automatically updating.

_ **Disable automatic codec downloads** - This prevents Windows Media Player from downloading required codecs.

_ **Don't get meta data from the internet** - This prevents Windows Media Player from getting CD/DVD information.

[Miscellaneous Settings]

_ **Don't synchronize with internet time** - This prevents Windows from automatically keeping your clock accurate.

_ **Clear pagefile at shutdown** - This will cause Windows XP to take much longer to shutdown but increases security for the paranoid.

_ **Deny starting regedit.exe** - This prevents future use of the very useful regedit tool.

_ **Deactivate Scripting Host** - This will cause features to stop working in web browsers and e-mail.

_ **Always show *.lnk suffixes** - This adds .lnk to desktop shortcuts.

_ **Always show *.url suffixes** - This adds .url to web browser bookmarks.

_ **Don't autostart CD's** - This prevents CD's from running automatically when put in the CD/DVD drive.

_ **Disable Java Script in the PDF-Reader** - Security vulnerability is patched in Adobe Reader v8.1.2

[Network]

_ **Disable integrated Firewall** - This will disable the Windows XP firewall.

_ **Hide Computer in Network** - This prevents your Computer from showing up in Network Neighborhood.

_ **Disable Network crawling** - This prevents Windows from searching your network for network resources.

[Internet Explorer 6] (This will not show up if IE7 is installed)

_ **Disable automatic updates** - This prevents Windows Update from checking for and downloading updates.

_ **Disable scheduled updates** - This prevents Windows Update from installing updates.

_ **Disable Integrated Windows Authentication** - Disables Kerberos authentication, which is more secure than NTLM.

_ **Disable Javascript** - This will cause some web pages to lose their menus or functionality completely.

_ **Disable ActiveX Controls** - This will cause some web pages to lose their menus or functionality completely.

_ **Clean website cache on shutdown** - This will cause Windows XP to take longer to shutdown.

[Services]

_ **Disable auto-updates service** - This prevents Windows Update from running Automatically.

_ **Disable time server service** - This prevents Windows from automatically keeping your clock accurate.

_ **Disable task-scheduler service** - The Windows Prefetcher, BootVis and Norton AV require this service to be running.

_ **Disable firewall/connection sharing service** - This will disable the Windows XP firewall.

_ **Disable Security Center** - This prevents necessary security warnings.

[Microsoft Messenger]

_ **Uninstall completely** - If you use or plan on using Microsoft's Instant Messenger leave this unchecked.

[Regsrv32 dll's]

_ **licdll.dll** - Only select this if Windows is already activated.

_ **Disable ZIP Functionality** - Only select if you have another .Zip program installed such as IZArc or WinZip.


[Tweaks]

_ **Disable the Desktop Cleanup Wizard** - This helps people keep their desktop clean.

_ **Don't Search Windows Update for device drivers** - Windows Update includes thousands of 100% compatible drivers.

_ **Do not cache thumbnails** - Only select this if you do not view a lot of photos.

Then select "Apply"

 - It is highly recommended to leave the profile on "Neutral" and adjust the values manually. The presets included such as the "Suggested" profile will disable important Windows features such as Windows Updates, the Security Center and Internet Explorer settings like Javascript and ActiveX. This will break common web page features such as menus and forms and prevent critical security patches from being applied. The color coding of check boxes can be further explained in the Help file under "Signs and Symbols".

[^ TOP](#)

Step 6 - Services

Windows XP has a lot of extra services running by default that can be a security concern. By disabling these services you will limit the number of security vulnerabilities on your system.



Shoot The Messenger - [Download](#) - [Home Page](#)

Disables Windows Messaging service. This will prevent online spammers from abusing this and causing message Pop-ups during normal system operation.

Notes - Installing SP2 or higher will disable the messenger service for you.



Unplug n' Pray - [Download](#) - [Home Page](#) - [Details](#)

Disables Windows potentially dangerous and exploitable Universal Plug and Play networking capability.




BlackViper's Windows XP Services Guide - [Home Page](#) - [Mirror](#) - [PDF File](#) ([Acrobat Reader](#) Required)


Using this guide will improve security by disabling useless Services turned on by default in XP. Run XP-AntiSpy, Shoot The Messenger and Unplug n' Pray first before going through this guide since those utilities will disable some of these Services for you.


The following is a list of Services that you can **Disable** on most systems for added security:

 **Alerter**

 **Distributed Link Tracking Client**

 **Help and Support** (If you use Windows Help and Support leave this enabled)

 **Indexing Service**

 **Messenger** (Shoot the Messenger and installing SP2 or higher will disable this)

 **Net Logon**

 **Netmeeting Remote Desktop Sharing**

 **Portable Media Serial Number**

 **Remote Desktop Help Session Manager**

 **Remote Registry Service**

 **Routing and Remote Access**

❌ **Secondary Logon**

❌ **SSDP Discovery Service** (Unplug n' Pray will disable this)

❌ **Telnet**

❌ **Terminal Services**

❌ **Universal Plug and Play Device Host**

❌ **Upload Manager**

❌ **Wireless Zero Configuration** (If you are on a wireless network leave this enabled)

The following is a list of Services that should always be set to **Automatic** for increased Security:

✅ **Automatic Updates**

✅ **Background Intelligent Transfer Service**

✅ **Cryptographic Services**

✅ **Protected Storage**

✅ **Security Accounts Manager**

✅ **Security Center**

✅ **System Event Notification**

✅ **System Restore Service**

Notes - Windows Updates can enable services that you have previously disabled. Check which services are running after a future Windows Update is completed. If applications stop working after using this guide it is usually due to being too aggressive with disabling services. Enable the services you disabled one at a time until the application works. In the future leave this service on automatic. If you run into any problems set all services back to their [Defaults](#) and start over.

[^ TOP](#)

Step 7 - Measures

The following are necessary measures that should be taken to further secure Windows XP.



1. Use NTFS on all your partitions - [Home Page](#)

"NTFS provides security enhancements in the form of Access Control Lists (ACL)s for files and directories. ACLs are security descriptors attached to all files and directories on an NTFS file system. Any file, directory, or other object in the file system can have multiple levels of access permissions. Before a process is allowed to access a file, the security system verifies that the process has the appropriate authorization to do so. FAT file systems do not implement security, and all user accounts have equal access to files and directories on the system." - [Source](#)

Instructions - Go to "My Computer", right-click on each partition, left-click "Properties". Look under "File System", if it does not say NTFS use the built-in utility [convert.exe](#) to change them to NTFS.

Notes - The conversion to NTFS is a one-way process. After you convert a drive or a partition to NTFS, you cannot convert it back to FAT or to FAT32. To restore the volume to the previous file system, you must reformat it as FAT or as FAT32. This action erases all existing data including your programs and personal files. In this case, you must either restore your data from a backup, or reinstall your operating system and programs. - [KB307881](#)



2. Password Protect All User Accounts

Windows XP Professional and Home Edition allow user accounts to utilize blank passwords. Blank password accounts cannot be accessed remotely by means such as a network or the Internet. A blank password (no password at all) on your account is more secure

than a weak password such as "1234" on a network or the Internet. However this offers no physical security. Many people store personal and financial information on their computer and would not want everyone who has physical access to the computer access to this information. Laptop users are at an even greater risk. Regardless it is highly recommend to use strong passwords for all user accounts, especially the Administrator account.

Instructions - Go to "Start", "Control Panel", "User Accounts", select the account you wish to password protect, then select "Create a password". Use a minimum eight character or more password for all user accounts. A simple easy way to do this is to use two four letter words in combination. Passwords are case sensitive. For added security you can use "Pass Phrases" of three or more words, mixing in numbers and symbols. For the Administrator account use a very [strong password](#). Make sure to use passwords you can remember or write them down in a physically secure location not on a computer.

Notes - Windows XP Home does not password protect the Administrator account by default and it can only be accessed from safe mode in the Home Edition. Reboot your computer into safe mode by pressing the F8 key down during boot up and selecting "Safe Mode" from the Windows Advanced Options menu. Go to "Start", "Control Panel", "User Accounts", select the "Administrator" account, then select "Create a password". Again make sure to use a [strong password](#).



3. Remove Useless User Accounts

Windows XP Creates additional User accounts that are of no use to the average user. **aspnet_wp** and the **ASP.NET** account can be removed if you do not do .NET development work. Delete any other accounts that are no longer required. If you do not use or recognize the account, delete it.

Instructions - Go to "Start", "Control Panel", "User Accounts", select the account, then "Delete the account".



4. Disable the Guest Account

The Guest account should be disabled for added security.

Instructions - Go to "Start", "Control Panel", "User Accounts", select the "Guest" account, then select "Turn off the guest account".

Notes - Windows XP Home does not allow you to truly disable the Guest account. Disabling the Guest account in Windows XP Home only removes it from the Fast User Switching and Log on screens. For security set a very strong password for the Guest account.



5. Disable Simple File Sharing - [Home Page](#)

By default, simple file sharing is enabled on a Microsoft Windows XP based computer if the computer is not a member of a domain. There are no permissions or passwords set on shares this way. If you do not have a firewall enabled, anyone with network access to your PC can access these shares with no restrictions.

Instructions - Go to "Start", "My Computer", "Tools", "Folder Options", "View" tab, select "Advanced Settings", uncheck "Use Simple File Sharing", select "Apply".

Notes - Windows XP Home doesn't allow you to disable Simple File Sharing and is unable to join a domain. For security make sure you set your shared folders to be read only or if your using the NTFS file system, use the "Make Private" option in the folder properties. If you cannot select this see [KB307286](#). For any issues accessing these folders later see [KB308421](#).



6. Disable Hidden Admin Shares - [Download](#) - [Home Page](#)

Windows XP Professional automatically creates a number of hidden administrative shares (such as ADMIN\$ and C\$). These shares are designed for remote access support by domain administrators. By default, if you delete these admin shares, they will be recreated when you reboot. To disable them permanently so they will not be recreated on the next reboot, use this utility.

Instructions - Download, unzip and run. Uncheck the box, apply the changes and reboot.

Notes - Hidden shares that are created by users can be deleted, and they are not re-created after you restart your computer. Windows XP Home Edition does not create hidden administrative shares.



7. Enable DEP for all programs

"The default configuration for hardware and software DEP protects core Windows components and services and has a minimal impact on application compatibility, but you can choose to configure DEP to protect all applications and programs on your computer." -

[Source](#)

Instructions - Go to "Start", "Control Panel", "System", "Advanced" Tab, under "Performance" select "Settings", "Data Execution Prevention Tab", Select "Turn on DEP for all programs and services except for those I select". Finally remove any exceptions from the list unless you have added them there personally.

Notes - "If you configure DEP to protect all applications and programs on your computer you will have the benefit of additional protection, but it might lead to additional application compatibility issues. If you configure DEP to protect all applications and programs on your computer, you can exempt individual 32-bit applications from software DEP protection if they have compatibility issues. You cannot disable hardware DEP or exempt 64-bit applications running on 64-bit Windows XP systems with DEP compatible processors. Hardware-enabled DEP is enabled by default on computers with DEP compatible processors that run Microsoft Windows XP 64-Bit Edition. 64-bit applications will not run from "non-executable" areas of memory. Hardware-enabled DEP cannot be disabled."



SecurAble - [Download](#) - [Home Page](#)

SecurAble checks your system for the presence of Hardware DEP support, 64-bit instruction extensions and Hardware Virtualization.

[^ TOP](#)

Step 8 - Internet



Internet Explorer 7 - [Home Page](#) - [Features](#) - [Download](#)

Internet Explorer 7 maintains the most webpage compatibility of any browser and adds Tabs, Integrated Search and a much needed Anti-Phishing feature. Pop-up Blocking support was added in Windows XP SP2 for Internet Explorer 6 and is built into Internet Explorer 7. Since the single most important feature of a browser is webpage compatibility, this is an excellent choice for most users.



Opera 9 - [Home Page](#) - [Features](#) - [Download](#) - [Betas](#) - [Customize](#)

Opera invented [Tabbed like browsing](#) and was the first web browser to include an [Integrated Search](#) feature and [Pop-up Blocking](#). Other unique features include an integrated BitTorrent Client and Voice control. Opera is the [Fastest](#), most [Secure](#) and most Compliant ([Acid2](#)) Graphical Web Browser for Windows. An excellent choice for advanced users.

Notes - Opera is not compatible with all webpages.



Firefox Myths - [Firefox Myths](#)

Firefox is **not** being recommended here for many reasons. Some of those reasons are that it is slower than Internet Explorer, insecure and not completely compatible with **10-15%** of all web sites. [Get the facts.](#)

[^ TOP](#)

Advanced



Microsoft Baseline Security Analyzer - [Download](#) - [Home Page](#)

"Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance."



Process Explorer - [Download](#) - [Home Page](#)

"Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process."



Process Monitor - [Download](#) - [Home Page](#)

"An advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements."



Windows XP Security Console - [Download](#) - [Home Page](#)

"Windows XP Security Console allows you to assign various restrictions to specific users, whether you're running XP Pro or XP Home. XP Home leaves you completely without the Group Policy Editor, while XP Pro lacks the ability to use the Group Policy Editor to selectively apply policies to specific users."

Downloads

[Page history](#) last edited by beha0017@go.inverhills.edu 19 hours, 35 minutes ago

MBSA (1.54 MB): <http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c>

7zip (1.05 MB): <http://sourceforge.net/projects/sevenzip/files/7-Zip/9.20/7z920.exe/download>

Nmap (18.9 MB): <http://nmap.org/dist/nmap-5.51-setup.exe>

Comodo (33.5 MB): http://download.comodo.com/cis/download/installs/1000/standalone/cfw_installer_x86.exe

OSSEC Win (632 kb): <http://www.ossec.net/files/ossec-agent-win32-2.5.1.exe>

OSSEC Lin (723 kb): <http://www.ossec.net/files/ossec-hids-2.5.1.tar.gz>

Putty: <http://the.earth.li/~sgtatham/putty/latest/x86/putty.zip>

Sysinternals Suite (12.9 MB): <http://download.sysinternals.com/Files/SysinternalsSuite.zip>

Malwarebytes (7.37 MB): http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html

Service Packs (if needed)

XP sp2 (266 MB): <http://download.microsoft.com/download/1/6/5/165b076b-aaa9-443d-84f0-73cf11fdcdf8/WindowsXP-KB835935-SP2-ENU.exe>

XP sp3 (316 MB): <http://download.microsoft.com/download/d/3/0/d30e32d8-418a-469d-b600-f32ce3edf42d/WindowsXP-KB936929-SP3-x86-ENU.exe>

Server 2k3 SP2 (372 MB): <http://download.microsoft.com/download/5/f/1/5f104409-2736-48ef-82e1-692ec3da020b/WindowsServer2003-KB914961-SP2-x86-ENU.exe>

Windows 7/ Server 2008 SP1: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c3202ce6-4056-4059-8a1b-3a9b77cdfdda&displaylang=en###>

STOPWATCH:

<http://www.online-stopwatch.com/>

DOWNLOAD NOW: UBUNTU 9.10

<http://www.ubuntu.com/getubuntu/download>

CAB FILE:

Step 1: If you do not have the file, download it from <http://go.microsoft.com/fwlink/?LinkId=76054> and save it to C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache\wsusscn2.cab. You may use any folder, but this is where MBSA will store the file after MBSA has downloaded it.

Step 2: Open C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache\wsusscn2.cab using any program able to view an archive file type of *.cab.

Step 3: Open package.cab from the wsusscn2.cab file, and then the package.xml file inside it.

Step 4: View the *OfflineSyncPackage* header element for the *CreationDate*. It should be set to a value such as "2005-06-01T18:42:49Z" (for example). Use the value you find to determine when the file was generated by Microsoft.

TCP VIEW:

<http://download.sysinternals.com/Files/TCPView.zip>

OSSEC Windows:

<http://www.ossec.net/files/ossec-agent-win32-2.3.exe>

OSSEC Linux:

Linux: <http://www.ossec.net/files/ossec-hids-2.3.tar.gz>

Web interface: <http://www.ossec.net/files/ui/ossec-wui-0.3.tar.gz>

PHP5 and Apache2:

Apache2: <http://apache.mirrors.tds.net/httpd/httpd-2.2.15.tar.gz>

PHP5: <http://us3.php.net/get/php-5.3.2.tar.gz/from/this/mirror>

PUTTY:

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

SNORT/BASE: In this order:

Xampp: RAR <http://www.apachefriends.org/download.php?xampp-win32-1.7.3.exe> ZIP

<http://www.apachefriends.org/download.php?xampp-win32-1.7.3.zip>

Snort: <http://dl.snort.org/snort-current/snort-2.8.5.3.tar.gz>

Base: <http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/download>

7ZIP: to unzip snort and base

<http://preview.licenseacquisition.org/48/1056569395.02174/7zip.exe>

tikiwiki download click version 3.5:

<http://sourceforge.net/projects/tikiwiki/files/TikiWiki%203.x%20-Betelgeuse-/Tiki%203.5/tikiwiki-3.5.zip/download>

Nmap Windows

<http://nmap.org/dist/nmap-5.21-setup.exe>

Nmap Linux

<http://nmap.org/dist/nmap-5.21.tar.bz2>

Research

Resources:

- [Open Source Network Security tools](#)
- Sans Top 20 security vulnerabilities - what they are, how to recognize and how to fix them. <http://www.sans.org/top20/2007/#s2>
- NSA Security Configurations for all platforms. http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
- Google (www.google.com) HAHA
- National Vulnerability Database (<http://nvd.nist.gov/>)
- EventID.net (<http://www.eventid.net/>)
- MBSA offline use: <http://support.microsoft.com/kb/926464>
- Download the updated wsusscn2.CAB file from the following new URL:
<http://go.microsoft.com/fwlink/?LinkID=74689> (<http://go.microsoft.com/fwlink/?LinkID=74689>)
- check out Zenoss..
-

- [OSSIM](#) stands for *Open Source Security Information Management*. Its goal is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of his or her networks, hosts, physical access devices, server, etc.

Besides getting the most out of well known open source tools, some of which are briefly described below, OSSIM provides a strong correlation engine, detailed low, medium and high level visualization interfaces, and reporting and incident management tools, based on a set of defined assets such as hosts, networks, groups and services.

All of this information can be restricted by network or sensor in order to provide only the required information to specific users; allowing for a fine grained multi-user security environment. Finally, the ability to perform as an IPS (Intrusion Prevention System), using correlated information from virtually any source, will be a useful addition to any security professional's arsenal.

Components

OSSIM features the following software components:

- Arpwatch – used for MAC anomaly detection.
- P0f – used for passive OS detection and OS change analysis.
- Pads – used for service anomaly detection.
- Nessus – used for vulnerability assessment and for cross correlation (IDS vs Security Scanner).
- Snort – the IDS, also used for cross correlation with nessus.
- Spade – the statistical packet anomaly detection engine. Used to gain knowledge about attacks without signatures.
- Tcptrack – used for session data information which can prove useful for attack correlation.
- Ntop – which builds an impressive network information database from which we can identify aberrant behavior/anomaly detection.
- Nagios – fed from the host asset database, it monitors host and service availability information.
- Osiris – a great HIDS.
- OCS-NG – cross-platform inventory solution.
- OSSEC – integrity, rootkit, registry detection, and more.



State Injects

[Page history](#) last edited by [David B. Pickens](#) 1 year ago

Secondary DNS

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 1:11 PM

Attachments:

From: Management

To: Enterprises Staff
Subject: Secondary DNS

Scenario:

The company owner thinks we need secondary DNS, based on some talk on the golf course. The opinion of highest rank prevails, so we need this set up promptly.

Management Instructions:

Set up secondary DNS on the MS2003 SMTP/POP3 server, external only; synchronize in one hour.

Switch Port Analyzer

[CCDC Judge](#)

You replied on 2/27/2010 3:06 PM.

Sent: Saturday, February 27, 2010 1:23 PM

Attachments:

From: Management
To: Enterprises Staff
Subject: Switch Port Analyzer

Scenario:

It has come to our attention that the border router to our network has a very basic configuration, and doesn't take advantage of more advanced capability. This constitutes a serious security risk to the organization.

Management Instructions:

Improve the security on the router by removing unnecessary services and install appropriate firewall features. Please keep in mind that our services are available to the public, so be sure to maintain open internet access. Include ssh connectivity from the XP workstation to the router.

Please report when this task is completed, including the text of the complete router configuration. This is expected to be completed in 60 minutes.

MD5 Hash Executables

[CCDC Judge](#)

You replied on 2/27/2010 2:34 PM.

Sent: Saturday, February 27, 2010 2:00 PM

Attachments:

From: Management
To: Enterprise Staff
Subject: MD5 Hash Executables

Scenario:

The CEO has been talking with other CIOs and CSOs and has found that one method of compromise detection is to MD5 every executable on the system to ensure tampering does not occur. The CEO is asking that this be done on all company server systems.

Management Instructions:

Create one file per system of the executable files that reside within the operating system of each of the five servers. Keep a copy local and make a backup copy on your XP workstation. Please complete this in 30 minutes.

Please report when you are done.

Top IDS Alarms

[CCDC Judge](#)

You replied on 2/27/2010 3:44 PM.

Sent: Saturday, February 27, 2010 2:27 PM

Attachments:

From: Management
To: Enterprise Staff
Subject: Top IDS Alarms

Scenario:

As an added responsibility Management would like a recurring report of the current top electronic threats being detected within the Enterprise IDS system. This report should be accessible within an hour and updated every two (2) hours, thereafter.

Management Instructions:

In an effort to be more eco-friendly, the CIO has asked that you provide a link where the reports will be stored on a secure portion of the website for review both while at work and while at home. Please provide access instructions to the documentation for the CIO to be able to access.

For the top three (3) threats, please explain the following in each report:

- What threat is posed by this alert
- What countermeasures have/will be implemented to protect the enterprise from this threat
- If the threat detected a breach to the enterprise

Please report when you are done.

Vulnerability Report

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 2:51 PM

Attachments:

From: Management
To: Enterprise Staff
Subject: Vulnerability Report

Scenario:

As part of ongoing security testing there is a need of understanding where the organization stands in terms of threat exposure, patching and configuration lockdown on servers and workstations. You are asked to provide a report based on security scanning both from a network perspective and from within the operating system.

Management Instructions:

Install Nmap and perform network scanning of the server farm, and generate a composite report.

Perform CIS benchmark evaluation for all servers except for the IDS. Record responses to questions asked by the benchmarking process and output of the steps performed.

The deliverable should also include CIS scoring Report for each of the servers. If the CIS scoring tools asks any pre-benchmark survey questions the answers should be recorded in a separate document.

Resources:

Download and install Nmap scanner (<http://nmap.org/download.html>)

Download and install CIS benchmarking tool (<http://cisecurity.org/benchmarks.html>)

Your first report is expected in a 1/2 hour.

RE: Vulnerability Report

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 3:46 PM

To: [CCDC Judge](#)

Attachments:

Please hold on the activity with CIS.

RE: Vulnerability Report

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 3:53 PM

To: [CCDC Judge](#)

Attachments:

Do not use:

"Download and install CIS benchmarking tool (<http://cisecurity.org/benchmarks.html>)"

Instead, please use:

Microsoft Baseline Security Analyzer 2.1 (<http://technet.microsoft.com/en-us/security/cc184923.aspx>)

An additional 1/2 hour is available to complete this task.

Password Strength Audit

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 3:06 PM

Attachments:

From: Management

To: Enterprise Staff

Subject: Password Strength Audit

Scenario:

Management is constantly concerned about the actions of disgruntled IT employees and learned from a 60 minutes piece that it may be trivial for him to crack and discover passwords. They have requested an audit and report on the strength of all passwords.

Management Instructions:

Management has requested a report regarding password strength across all systems and all methods of access. Your team will need to devise a metric to judge the strength of passwords on critical systems. Submit a report of user names and passwords together with any additional access passwords that includes a relative strength rating. In your report abstract give a metric that rates that overall strength of passwords for the network. Along with the detailed list of authentications, a synopsis of the metric devised should be included.

Please submit your report in 90 minutes.

Security Policies

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 3:20 PM

Attachments:

From: Management
To: Enterprises Staff
Subject: Security Policies

Scenario:

Just got a memo from our independent auditors that they'll need to see copies of our IT policies during their next audit – the problem is we don't have any. I need you to take a first cut at a set of IT-related policies.

Management Instructions:

At a minimum we'll need:

- An acceptable use policy that defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.
- An audit vulnerability scanning policy that defines the requirements and provides the authority for the information security team to conduct audits and risk assessments to ensure integrity of information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.
- An email policy that defines standards to prevent tarnishing the public image of the organization.
- An information classification/sensitivity policy that defines the requirements for classifying and securing the organization's information in a manner appropriate to its sensitivity level.
- A server security policy that defines standards for minimal security configuration for servers inside the organization's production network, or used in a production capacity.

I'm sure we need more than that but at least with this set we won't look totally unprepared for the audit. I'm going to need this in 90 minutes.

Password reset

[CCDC Judge](#)

You replied on 2/27/2010 4:32 PM.

Sent: Saturday, February 27, 2010 3:43 PM

Attachments:

From: Management
To: Enterprises Staff
Subject: Password reset

Scenario:

You have analyzed the password strength across all systems. With a goal of constant improvement we can use these results to assure strong passwords are used throughout the enterprise.

Management Instructions:

Establish a password strength metric based on the analysis you have completed. Reset all passwords to conform to the new metric and submit a list to management. This is expected in one hour.

Remember not to modify the following accounts:

- o CyberNEXSAdmin
- o CyberNEXSUser
- o CyberNEXSAdm

Banners

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 3:51 PM

Attachments:

From: Management
To: Staff
Subject: Banners

Scenario:

According to a set a best current practices, banners should not contain system/ version specific information. Banners that contain system information are significantly more likely to be a target of attack.

Management Instructions:

Remove any system or program specific information from the banners of all publicly visible services. Instead, replace this information with something generic. Add warning information that connections are monitored, and that intruders will be prosecuted.

This should be completed in 30 minutes. Submit your report when completed.

configs

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 4:38 PM

Attachments:

Please send us your Router and Switch configuration files.

Setup a User Forum

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 4:51 PM

Attachments:

From: Management

To: Staff

Subject: Setup a User Forum

Scenario:

Our sales group is requesting that we setup an on-line forum for our customer community. This will allow our customers to come together and post messages about our products, provide suggestions for improving customer service, and comment on our product lines, etc.

Management Instructions:

Produce an online forum for our customers and make it reachable at forums.groupX.com (X=team#). Make sure people can sign up for an account. You can house it on any IP address or web server, just make sure the “forums groupX.com” address resolves and takes the customer to the forum. Also make sure our employees can get to the forum from inside the company as we need our customer support staff to be able to read the forums and post replies.

Notify management of completion, and the inside address used for the service.

You have 60 minutes to complete this task.

OpenVAS

[CCDC Judge](#)

You replied on 2/27/2010 7:02 PM.

Sent: Saturday, February 27, 2010 5:00 PM

Attachments:

From: Management
To: Enterprises Staff
Subject: OpenVAS

Scenario:

We have examined vulnerabilities in our network via Nmap, and this has provided significant data to guide our actions towards improving security. The assessment of vulnerabilities and threat exposure is too important to rely on a single tool.

Management Instructions:

Install OpenVAS on the Ubuntu machine. Use OpenVAS to assess vulnerabilities of the network and submit a report on your findings. Highlight any new or different assessments from what is discovered from Nmap.

We will need your report in 90 minutes.

install MRTG

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 5:17 PM

Attachments:

From: Management

To: Staff

Subject: Confirmation of Network Utilization/ Install MRTG

Scenario:

Various sources are concerned about the possible need to acquire more bandwidth for service outside connections. An additional concern is whether our service provider is accurately measuring network utilization.

Management Instructions:

Install MRTG (it's freeware) on the 2003 server so we can establish redundant tracking of our Cisco router interface utilization, and confirm how much traffic is passing through our network. Set it up to track the external interface on one graph and the internal interface on another graph. Put the MRTG data in a password protected area of the website <http:// {webaddress}/mrtg> Let's get this up and running in the next 90 minutes. Have MRTG poll every 5 minutes.

Sugar CRM

[CCDC Judge](#)

You replied on 2/27/2010 7:00 PM.

Sent: Saturday, February 27, 2010 5:25 PM

Attachments:

From: Management

To: Enterprises Staff

Subject: Sugar CRM

Scenario:

Our sales group really needs a customer management tool – something that lets them track clients, contacts, potential sales, etc.. in a web-based collaborative environment.

Management Instructions:

Setup SugarCRM on the Ubuntu server and limit it to internal users only – I don't want external folks to have access to it. In preparation for prime time we need to see a demo of the system. Look for the following option during installation:

Populate database with demo data?

Let's get this running in 90 minutes.

Syslog

[CCDC Judge](#)

You replied on 2/27/2010 6:56 PM.

Sent: Saturday, February 27, 2010 5:30 PM

Attachments:

From: Enterprises Management

To: Enterprises Staff

Subject: Syslog

Scenario:

The Management CSO just returned from a conference where he witnessed a team of hacker's that were hired to show company's how easy it is to get compromised. He is concerned that we may have a backdoor already on our network and he would like to make sure we track everything.

Management Instructions:

To keep cost down, research an open source Syslog solution that will run on Ubuntu. Next set this as the central logging system for all other system on our network. This way, all computers will immediately send any system-related events to the syslog server, ensuring that your logs will be completely accurate and un-tampered with at all times.

Once you get it implemented I'll need a quick summary report outlining what solution you've chosen, why you chose it, and how you've implemented it in our environment. We will also need a printout of any log file reflecting any intruders.

Let's get this up and running in the next 60 minutes.

User Account Audit

[CCDC Judge](#)

Sent: Saturday, February 27, 2010 5:49 PM

Attachments:

From: Enterprises Management

To: Enterprises Staff

Subject: User Account Audit

Scenario:

The Annual Audit Committee has requested that our IT Department provide a user account audit report of all management systems.

Instructions from Management:

Perform a user account audit management computer systems. Provide us a list of the following items:

1. All user accounts along with their security privileges
2. A list of events showing users account created / deleted
3. A list of events showing the frequency of password changes
4. List of events with details related to security enabled local group changes
5. List of events with details related to security enabled global group changes

Let's get this completed in the next 60 minutes.

Inject notes for CCDC

Checklist:

1. Figure out what we have to do
2. Check for vulnerabilities in the suggested software
3. Know what machines we need
4. Questions on the injects
5. Let management know what changes are being made
6. Implement the injects

Find impacts of each inject on the systems and overall security

Only do one change at a time, announce changes

Interpret injects and get team consensus

Page Tools

Insert links

Insert links to other pages or uploaded files.

Pages Images and files

[Insert a link to a new page](#)[Insert image from URL](#)**Tip:** To turn text into a link, highlight the text, then click on a page or file from the list above.

01 IT Progress Memo

Method:

Time:

Summary:

Please provide me with an IT Progress Memo at 11:00, 15:00 and 19:00 each day. It can include the following:

- Summary of all downtime with an explanation of the cause
- Summary of all tasks and activities undertaken, including the requests coming from me.
- Summary of significant configuration changes that you have made since the previous report.
- Any completed incident reports you have not yet submitted.

You may, of course, include more information as you find relevant or appropriate.

I've also provided you with an incident reporting form from our CPA firm. Please

use it to document any and all suspicious activity. This documentation could become crucial in the future, should one of your predecessors have a breach of ethics. Please complete these as you identify and resolve any activity you might discover.

02 Source Code Repository

Method:

Time:

Summary:

Last night our internal source code repository became inadvertently exposed to the internet. This was due to improper permissions set on the directory during our regular maintenance window. The decision has been made to further restrict access to source code URLs with help of the web-server authentication mechanisms. We are working toward purchasing a full-featured source control system but we need a quick fix for the next few months. Please evaluate different methods of authentication and present proof-of-concepts to the executive committee in an hour.

You will need to create two URLs containing several files and protected by one of the two methods of authentication: HTTP Basic Auth using Apache on *ohm*, and HTTP Digest using IIS on *voltaire*. Select the test users yourself, but use the user's same password for simplicity.

For Basic Authentication

Create a subdirectory and populate the directory with files of your choosing.

Configure HTTP-Auth authentication for two users and make it available for anyone from the outside.

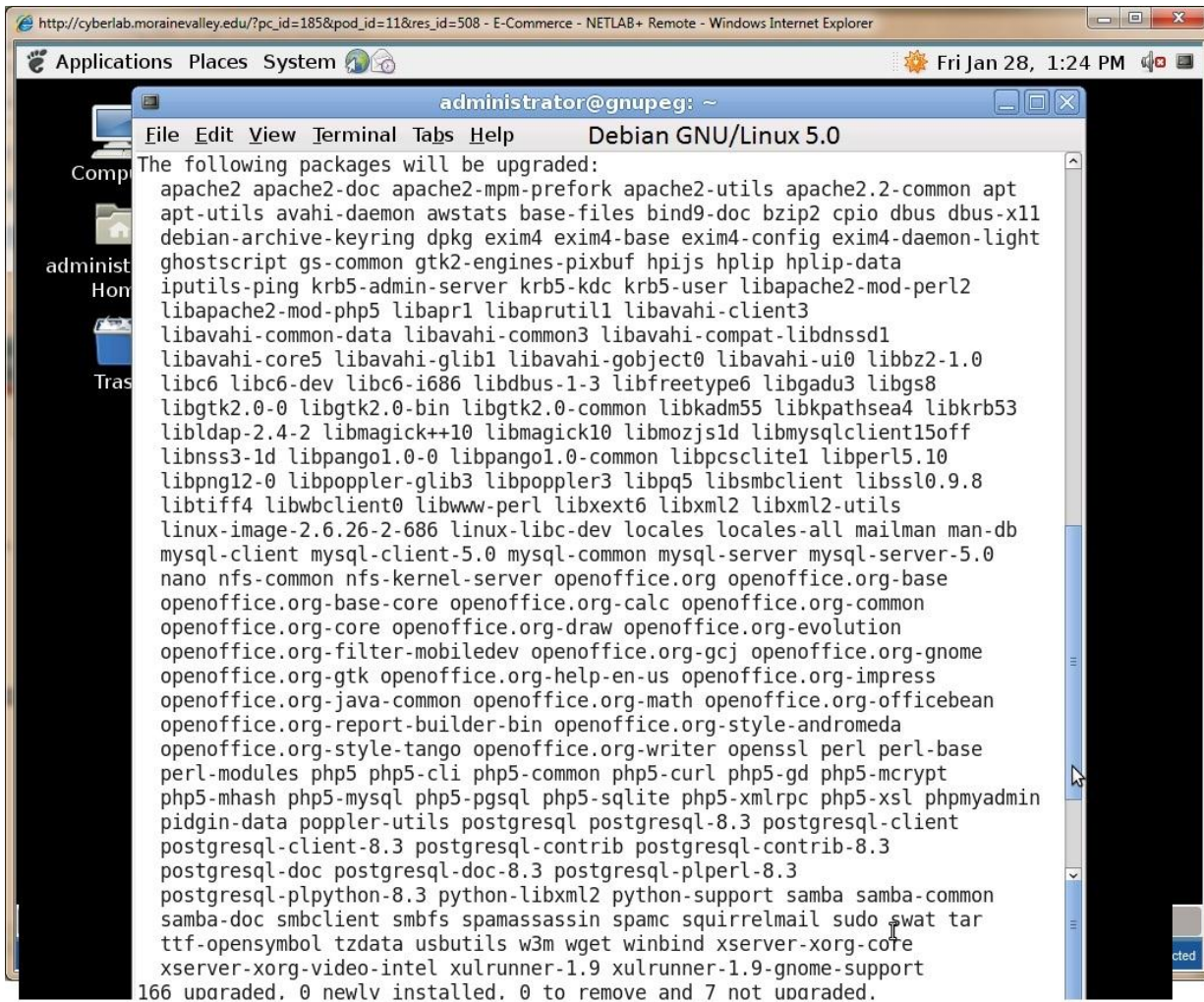
For Digest Authentication

Create a subdirectory and populate the directory with files of your choosing.

Configure two users to use HTTP Digest authentication and make authentication available to the outside.

HTTP Digest using IIS on
users' same password for simplicity.

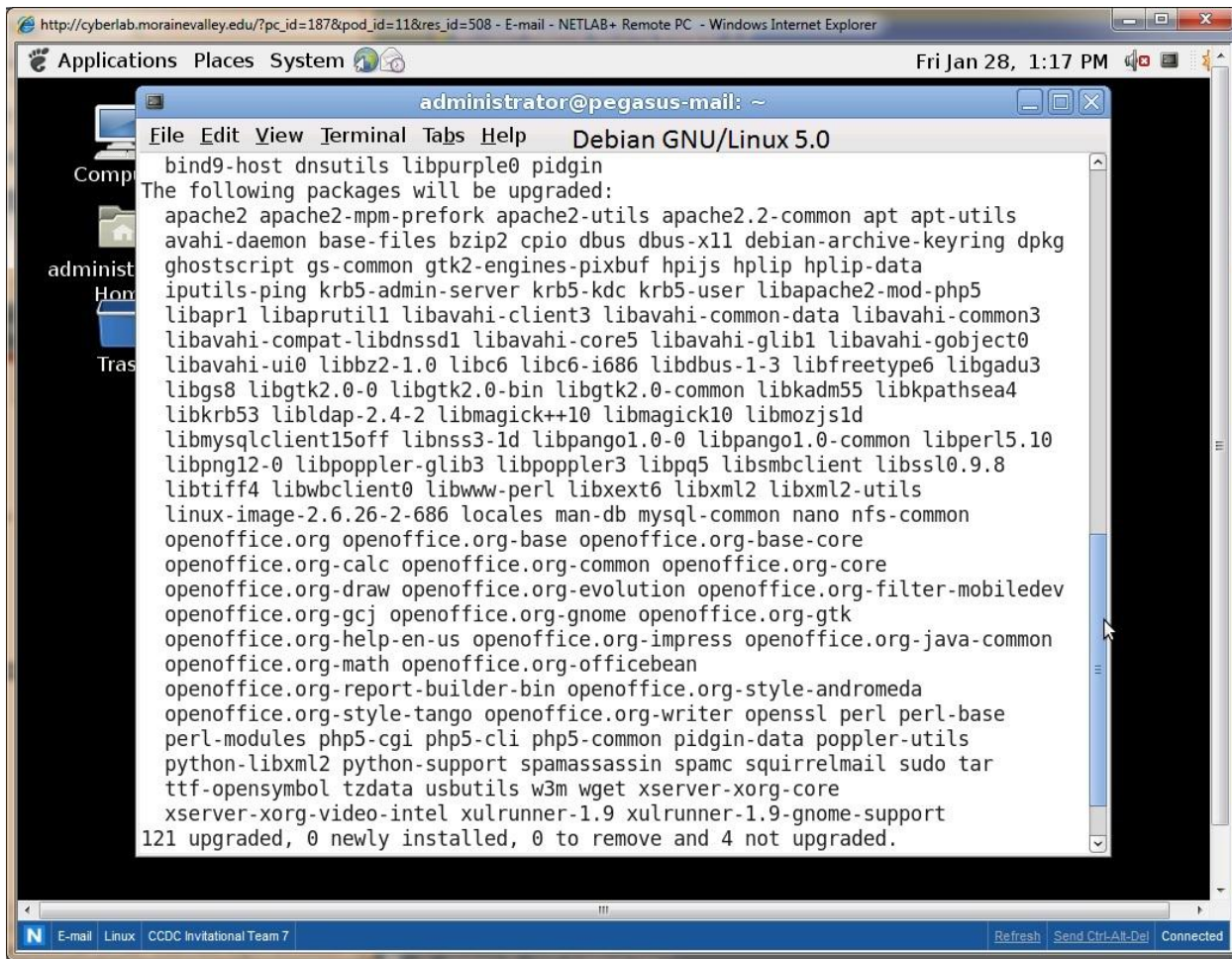
E-Commerce recon



The screenshot shows a terminal window titled "administrator@gnupeg: ~" with a menu bar containing "File Edit View Terminal Tabs Help". The terminal output lists packages to be upgraded, including various system utilities, libraries, and application components. At the bottom, it states "166 upgraded, 0 newly installed, 0 to remove and 7 not upgraded."

```
http://cyberlab.morainevalley.edu/?pc_id=185&pod_id=11&res_id=508 - E-Commerce - NETLAB+ Remote - Windows Internet Explorer
Applications Places System Fri Jan 28, 1:24 PM
administrator@gnupeg: ~
File Edit View Terminal Tabs Help Debian GNU/Linux 5.0
The following packages will be upgraded:
apache2 apache2-doc apache2-mpm-prefork apache2-utils apache2.2-common apt
apt-utils avahi-daemon awstats base-files bind9-doc bzip2 cpio dbus dbus-x11
debian-archive-keyring dpkg exim4 exim4-base exim4-config exim4-daemon-light
ghostscript gs-common gtk2-engines-pixbuf hpijs hplip hplip-data
iputils-ping krb5-admin-server krb5-kdc krb5-user libapache2-mod-perl2
libapache2-mod-php5 libapr1 libaprutil1 libavahi-client3
libavahi-common-data libavahi-common3 libavahi-compat-libdnssd1
libavahi-core5 libavahi-glib1 libavahi-gobject0 libavahi-ui0 libbz2-1.0
libc6 libc6-dev libc6-i686 libdbus-1-3 libfontconfig1 libgadu3 libgs8
libgtk2.0-0 libgtk2.0-bin libgtk2.0-common libkadm5 libkpathsea4 libkrb53
libldap2.4-2 libmagick++10 libmagick10 libmozjs1d libmysqlclient15off
libnss3-1d libpango1.0-0 libpango1.0-common libpcsc-lite libperl5.10
libpng12-0 libpoppler-glib3 libpoppler3 libpq5 libsmbclient libssl0.9.8
libtiff4 libwbclient0 libwww-perl libxext6 libxml2 libxml2-utils
linux-image-2.6.26-2-686 linux-libc-dev locales locales-all mailman man-db
mysql-client mysql-client-5.0 mysql-common mysql-server mysql-server-5.0
nano nfs-common nfs-kernel-server openoffice.org openoffice.org-base
openoffice.org-base-core openoffice.org-calc openoffice.org-common
openoffice.org-core openoffice.org-draw openoffice.org-evolution
openoffice.org-filter-mobiledev openoffice.org-gcj openoffice.org-gnome
openoffice.org-gtk openoffice.org-help-en-us openoffice.org-impress
openoffice.org-java-common openoffice.org-math openoffice.org-officebean
openoffice.org-report-builder-bin openoffice.org-style-andromeda
openoffice.org-style-tango openoffice.org-writer openssl perl perl-base
perl-modules php5 php5-cli php5-common php5-curl php5-gd php5-mcrypt
php5-mhash php5-mysql php5-pgsql php5-sqlite php5-xmllrpc php5-xsl phpmyadmin
pidgin-data poppler-utils postgresql postgresql-8.3 postgresql-client
postgresql-client-8.3 postgresql-contrib postgresql-contrib-8.3
postgresql-doc postgresql-doc-8.3 postgresql-plperl-8.3
postgresql-plpython-8.3 python-libxml2 python-support samba samba-common
samba-doc smbclient smbfs spamassassin spamc squirrelmail sudo swat tar
ttf-opensymbol tzdata usbutils w3m wget winbind xserver-xorg-core
xserver-xorg-video-intel xulrunner-1.9 xulrunner-1.9-gnome-support
166 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
```

E-mail recon



FTP recon

root@pegasus-ftp:~

File Edit View Terminal Tabs Help

Package	Arch	Version	Repository	Size
Installing:				
kernel	x86_64	2.6.18-194.32.1.el5	updates	19 M
Updating:				
ImageMagick	i386	6.2.8.0-4.el5_5.3	updates	3.3 M
ImageMagick	x86_64	6.2.8.0-4.el5_5.3	updates	3.3 M
NetworkManager	i386	1:0.7.0-10.el5_5.2	updates	1.0 M
NetworkManager	x86_64	1:0.7.0-10.el5_5.2	updates	1.1 M
NetworkManager-glib	i386	1:0.7.0-10.el5_5.2	updates	82 k
NetworkManager-glib	x86_64	1:0.7.0-10.el5_5.2	updates	84 k
NetworkManager-gnome	x86_64	1:0.7.0-10.el5_5.2	updates	330 k
apr	x86_64	1.2.7-11.el5_5.3	updates	118 k
apr-util	x86_64	1.2.7-11.el5_5.2	updates	79 k
autofs	x86_64	1:5.0.1-0.rc2.143.el5_5.6	updates	910 k
avahi	i386	0.6.16-9.el5_5	updates	251 k
avahi	x86_64	0.6.16-9.el5_5	updates	257 k
avahi-compat-libdns_sd	x86_64	0.6.16-9.el5_5	updates	24 k
avahi-glib	i386	0.6.16-9.el5_5	updates	15 k
avahi-glib	x86_64	0.6.16-9.el5_5	updates	15 k
bind	x86_64	30:9.3.6-4.P1.el5_5.3	updates	986 k
bind-chroot	x86_64	30:9.3.6-4.P1.el5_5.3	updates	44 k
bind-libs	x86_64	30:9.3.6-4.P1.el5_5.3	updates	891 k
bind-utils	x86_64	30:9.3.6-4.P1.el5_5.3	updates	176 k
bzip2	x86_64	1.0.3-6.el5_5	updates	50 k
bzip2-libs	i386	1.0.3-6.el5_5	updates	37 k
bzip2-libs	x86_64	1.0.3-6.el5_5	updates	35 k
crash	x86_64	4.1.2-4.el5.centos.1	updates	1.7 M
cups	x86_64	1:1.3.7-18.el5_5.8	updates	3.1 M
cups-libs	i386	1:1.3.7-18.el5_5.8	updates	199 k
cups-libs	x86_64	1:1.3.7-18.el5_5.8	updates	195 k
db4	i386	4.3.29-10.el5_5.2	updates	910 k
db4	x86_64	4.3.29-10.el5_5.2	updates	899 k
dbus-glib	i386	0.73-10.el5_5	updates	161 k
dbus-glib	x86_64	0.73-10.el5_5	updates	163 k

Centos

provided to t
ndors redis
a vendor br

the core dev
, enterpris

unity, quick
and respon
[Mail Lists, Fo](#)

root@pegasus-ftp:~

File Edit View Terminal Tabs Help

device-mapper	x86_64	1.02.39-1.el5_5.2	updates	758 k
device-mapper-event	x86_64	1.02.39-1.el5_5.2	updates	21 k
device-mapper-multipath	x86_64	0.4.7-34.el5_5.6	updates	3.0 M
dhclient	x86_64	12:3.0.5-23.el5_5.2	updates	282 k
e2fsprogs	x86_64	1.39-23.el5_5.1	updates	995 k
e2fsprogs-libs	i386	1.39-23.el5_5.1	updates	118 k
e2fsprogs-libs	x86_64	1.39-23.el5_5.1	updates	118 k
esc	x86_64	1.1.0-12.el5	updates	547 k
expat	i386	1.95.8-8.3.el5_5.3	updates	77 k
expat	x86_64	1.95.8-8.3.el5_5.3	updates	76 k
firefox	i386	3.6.13-2.el5.centos	updates	14 M
firefox	x86_64	3.6.13-2.el5.centos	updates	14 M
freetype	i386	2.2.1-28.el5_5.1	updates	312 k
freetype	x86_64	2.2.1-28.el5_5.1	updates	311 k
ghostscript	i386	8.15.2-9.12.el5_5	updates	5.9 M
ghostscript	x86_64	8.15.2-9.12.el5_5	updates	5.9 M
glibc	i686	2.5-49.el5_5.7	updates	5.3 M
glibc	x86_64	2.5-49.el5_5.7	updates	4.8 M
glibc-common	x86_64	2.5-49.el5_5.7	updates	16 M
gnome-python2-extras	x86_64	2.14.2-7.el5	updates	24 k
gnome-python2-libegg	x86_64	2.14.2-7.el5	updates	55 k
gnome-screensaver	x86_64	2.16.1-8.el5_5.2	updates	1.8 M
gnome-vfs2	i386	2.16.2-6.el5_5.1	updates	1.2 M
gnome-vfs2	x86_64	2.16.2-6.el5_5.1	updates	1.3 M
gnome-vfs2-smb	x86_64	2.16.2-6.el5_5.1	updates	37 k
gnupg	x86_64	1.4.5-14.el5_5.1	updates	1.8 M
gnutls	i386	1.4.1-3.el5_4.8	updates	351 k
gnutls	x86_64	1.4.1-3.el5_4.8	updates	364 k
gtk2	i386	2.10.4-21.el5_5.6	updates	6.5 M
gtk2	x86_64	2.10.4-21.el5_5.6	updates	6.6 M
httpd	x86_64	2.2.3-43.el5.centos.3	updates	1.2 M
httpd-manual	x86_64	2.2.3-43.el5.centos.3	updates	814 k
initscripts	x86_64	8.45.30-3.el5.centos	updates	1.6 M
ipsec-tools	x86_64	0.6.5-14.el5_5.5	updates	398 k
java-1.6.0-openjdk	x86_64	1:1.6.0.0-1.16.b17.el5	updates	35 M
kpartx	x86_64	0.4.7-34.el5_5.6	updates	434 k

provided to t
ndors redis
a vendor br

the core dev
, enterpris

unity, quick
and respon
[Mail Lists, Fo](#)

root@pegasus-ftp:~

File Edit View Terminal Tabs Help

krb5-libs	i386	1.6.1-36.el5_5.6	updates	663 k
krb5-libs	x86_64	1.6.1-36.el5_5.6	updates	675 k
krb5-workstation	x86_64	1.6.1-36.el5_5.6	updates	912 k
ksh	x86_64	20100202-1.el5_5.1	updates	1.2 M
lftp	x86_64	3.7.11-4.el5_5.3	updates	957 k
libbonobo	i386	2.16.0-1.1.el5_5.1	updates	502 k
libbonobo	x86_64	2.16.0-1.1.el5_5.1	updates	524 k
libpng	i386	2:1.2.10-7.1.el5_5.3	updates	241 k
libpng	x86_64	2:1.2.10-7.1.el5_5.3	updates	234 k
libpurple	x86_64	2.6.6-5.el5_5	updates	8.4 M
libsmbclient	x86_64	3.0.33-3.29.el5_5.1	updates	916 k
libtiff	i386	3.8.2-7.el5_5.5	updates	308 k
libtiff	x86_64	3.8.2-7.el5_5.5	updates	313 k
libvolume_id	i386	095-14.21.el5_5.1	updates	40 k
libvolume_id	x86_64	095-14.21.el5_5.1	updates	39 k
libxml2	i386	2.6.26-2.1.2.8.el5_5.1	updates	795 k
libxml2	x86_64	2.6.26-2.1.2.8.el5_5.1	updates	807 k
libxml2-python	x86_64	2.6.26-2.1.2.8.el5_5.1	updates	713 k
logrotate	x86_64	3.7.4-9.el5_5.2	updates	41 k
lvm2	x86_64	2.02.56-8.el5_5.6	updates	2.7 M
mkinitrd	i386	5.1.19.6-61.el5_5.2	updates	467 k
mkinitrd	x86_64	5.1.19.6-61.el5_5.2	updates	454 k
mod_ssl	x86_64	1:2.2.3-43.el5.centos.3	updates	92 k
module-init-tools	x86_64	3.3-0.pre3.1.60.el5_5.1	updates	443 k
mysql	x86_64	5.0.77-4.el5_5.4	updates	4.8 M
mysql-server	x86_64	5.0.77-4.el5_5.4	updates	9.8 M
nash	x86_64	5.1.19.6-61.el5_5.2	updates	1.1 M
net-snmp-libs	x86_64	1:5.3.2.2-9.el5_5.1	updates	1.3 M
nfs-utils	x86_64	1:1.0.9-47.el5_5	updates	390 k
nscd	x86_64	2.5-49.el5_5.7	updates	166 k
nspluginwrapper	i386	1.3.0-9.el5	updates	199 k
nspluginwrapper	x86_64	1.3.0-9.el5	updates	185 k
nspr	i386	4.8.6-1.el5_5	updates	120 k
nspr	x86_64	4.8.6-1.el5_5	updates	119 k
nss	i386	3.12.8-1.el5.centos	updates	1.1 M
nss	x86_64	3.12.8-1.el5.centos	updates	1.1 M

provided to t
ndors redis
a vendor br

the core dev
, enterpris

unity, quick
and respon
[Mail Lists, Fo](#)

root@pegasus-ftp:~

File Edit View Terminal Tabs Help

nss-tools	x86_64	3.12.8-1.el5.centos	updates	1.2 M
nss_db	i386	2.2-35.4.el5_5	updates	763 k
nss_db	x86_64	2.2-35.4.el5_5	updates	747 k
openldap	i386	2.3.43-12.el5_5.3	updates	295 k
openldap	x86_64	2.3.43-12.el5_5.3	updates	303 k
openoffice.org-calc	x86_64	1:3.1.1-19.5.el5_5.1	updates	9.3 M
openoffice.org-core	x86_64	1:3.1.1-19.5.el5_5.1	updates	110 M
openoffice.org-draw	x86_64	1:3.1.1-19.5.el5_5.1	updates	1.0 M
openoffice.org-graphicfilter	x86_64	1:3.1.1-19.5.el5_5.1	updates	317 k
openoffice.org-impress	x86_64	1:3.1.1-19.5.el5_5.1	updates	1.4 M
openoffice.org-math	x86_64	1:3.1.1-19.5.el5_5.1	updates	1.5 M
openoffice.org-ure	x86_64	1:3.1.1-19.5.el5_5.1	updates	3.0 M
openoffice.org-writer	x86_64	1:3.1.1-19.5.el5_5.1	updates	6.5 M
openoffice.org-xsltfilter	x86_64	1:3.1.1-19.5.el5_5.1	updates	313 k
openssh	x86_64	4.3p2-41.el5_5.1	updates	287 k
openssh-askpass	x86_64	4.3p2-41.el5_5.1	updates	41 k
openssh-clients	x86_64	4.3p2-41.el5_5.1	updates	450 k
openssh-server	x86_64	4.3p2-41.el5_5.1	updates	274 k
openssl	i686	0.9.8e-12.el5_5.7	updates	1.4 M
openssl	x86_64	0.9.8e-12.el5_5.7	updates	1.4 M
pam	i386	0.99.6.2-6.el5_5.2	updates	980 k
pam	x86_64	0.99.6.2-6.el5_5.2	updates	978 k
pango	i386	1.14.9-8.el5.centos	updates	335 k
pango	x86_64	1.14.9-8.el5.centos	updates	339 k
pcsc-lite	x86_64	1.4.4-4.el5_5	updates	125 k
pcsc-lite-libs	x86_64	1.4.4-4.el5_5	updates	24 k
perl	x86_64	4:5.8.8-32.el5_5.2	updates	12 M
perl-Archive-Tar	noarch	1:1.39.1-1.el5_5.2	updates	53 k
php	x86_64	5.1.6-27.el5_5.3	updates	2.3 M
php-cli	x86_64	5.1.6-27.el5_5.3	updates	2.2 M
php-common	x86_64	5.1.6-27.el5_5.3	updates	153 k
php-ldap	x86_64	5.1.6-27.el5_5.3	updates	38 k
poppler	x86_64	0.5.4-4.4.el5_5.14	updates	3.0 M
poppler-utils	x86_64	0.5.4-4.4.el5_5.14	updates	76 k
popt	i386	1.10.2.3-20.el5_5.1	updates	74 k
popt	x86_64	1.10.2.3-20.el5_5.1	updates	77 k

root@pegasus-ftp:~

File Edit View Terminal Tabs Help

postgresql-libs	x86_64 8.1.22-1.el5_5.1	updates 196 k
python	x86_64 2.4.3-27.el5_5.3	updates 6.0 M
rpm	x86_64 4.4.2.3-20.el5_5.1	updates 1.2 M
rpm-libs	x86_64 4.4.2.3-20.el5_5.1	updates 923 k
rpm-python	x86_64 4.4.2.3-20.el5_5.1	updates 63 k
samba	x86_64 3.0.33-3.29.el5_5.1	updates 16 M
samba-client	x86_64 3.0.33-3.29.el5_5.1	updates 5.7 M
samba-common	x86_64 3.0.33-3.29.el5_5.1	updates 6.8 M
selinux-policy	noarch 2.4.6-279.el5_5.2	updates 406 k
selinux-policy-targeted	noarch 2.4.6-279.el5_5.2	updates 1.2 M
sox	x86_64 12.18.1-1.el5_5.1	updates 321 k
sudo	x86_64 1.7.2p1-9.el5_5	updates 236 k
tcsh	x86_64 6.14-17.el5_5.2	updates 476 k
tomcat5-jsp-2.0-api	x86_64 5.5.23-0jpp.11.el5_5	updates 103 k
tomcat5-servlet-2.4-api	x86_64 5.5.23-0jpp.11.el5_5	updates 162 k
totem	i386 2.16.7-7.el5	updates 1.9 M
totem	x86_64 2.16.7-7.el5	updates 1.9 M
tzdata	x86_64 2010l-1.el5	updates 796 k
udev	x86_64 095-14.21.el5_5.1	updates 2.4 M
vnc-server	x86_64 4.1.2-14.el5_5.4	updates 2.0 M
xorg-x11-drv-ati	x86_64 6.6.3-3.27.el5_5.1	updates 567 k
xorg-x11-server-Xnest	x86_64 1.1.1-48.76.el5_5.2	updates 1.4 M
xorg-x11-server-Xorg	x86_64 1.1.1-48.76.el5_5.2	updates 3.4 M
xulrunner	i386 1.9.2.13-3.el5	updates 12 M
xulrunner	x86_64 1.9.2.13-3.el5	updates 11 M
yelp	x86_64 2.16.0-26.el5	updates 583 k
Installing for dependencies:		
tzdata-java	x86_64 2010l-1.el5	updates 177 k

Transaction Summary

```

=====
Install      2 Package(s)
Upgrade     165 Package(s)
    
```

Total download size: 457 M

Is this ok [y/N]:

NMAP Quick Scan Results

[Page history](#) last edited by [cameron murad](#) 1 month ago

Starting Nmap 5.50 (<http://nmap.org>) at 2011-01-28 19:27 Pacific Standard Time

Nmap scan report for 172.20.241.1

Host is up (0.00s latency).

Not shown: 96 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	Cisco SSH 1.25 (protocol 1.99)
--------	------	-----	--------------------------------

23/tcp	open	telnet	Cisco IOS telnetd
--------	------	--------	-------------------

80/tcp	open	http	Cisco IOS http config
--------	------	------	-----------------------

443/tcp	open	ssl/http	Cisco IOS http config
---------	------	----------	-----------------------

MAC Address: 00:15:FA:20:34:40 (Cisco Systems)

Device type: router

Running: Cisco IOS 12.X

OS details: Cisco 836, 890, 1751, 1841, or 2800 router (IOS 12.4 - 15.0)

Network Distance: 1 hop

Service Info: OS: IOS; Device: switch

Nmap scan report for pegasus-ad.pegasus.com (172.20.241.5)

Host is up (0.00s latency).

Not shown: 91 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

53/tcp	open	domain	Microsoft DNS
--------	------	--------	---------------

88/tcp	open	tcpwrapped	
--------	------	------------	--

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	
---------	------	-------------	--

389/tcp	open	ldap	
---------	------	------	--

445/tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
---------	------	--------------	---

1025/tcp	open	msrpc	Microsoft Windows RPC
----------	------	-------	-----------------------

1027/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
----------	------	------------	-------------------------------------

3389/tcp	open	microsoft-rdp	Microsoft Terminal Service
----------	------	---------------	----------------------------

MAC Address: 00:0C:29:E9:E6:CA (VMware)

Device type: general purpose

Running: Microsoft Windows 2003

OS details: Microsoft Windows Server 2003 SP1 or SP2

Network Distance: 1 hop

Service Info: OS: Windows

Nmap scan report for gnupeg.pegasus.com (172.20.241.14)

Host is up (0.00s latency).

Not shown: 87 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	ProFTPD 1.3.1
--------	------	-----	---------------

22/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (protocol 2.0)
--------	------	-----	---------------------------------------

53/tcp	open	domain	ISC BIND 9.5.1-P3
--------	------	--------	-------------------

80/tcp	open	http	Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g mod_perl/2.0.4 Perl/v5.10.0)
--------	------	------	--

110/tcp	open	pop3	Courier pop3d
---------	------	------	---------------

111/tcp	open	rpcbind	2 (rpc #100000)
---------	------	---------	-----------------

139/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: COM)
---------	------	-------------	---------------------------------

143/tcp	open	imap	Courier Imapd (released 2008)
---------	------	------	-------------------------------

443/tcp	open	http	Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g mod_perl/2.0.4 Perl/v5.10.0)
---------	------	------	--

445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: COM)
---------	------	-------------	---------------------------------

993/tcp	open	ssl/imap	Courier Imapd (released 2008)
---------	------	----------	-------------------------------

995/tcp	open	pop3s?	
---------	------	--------	--

2049/tcp	open	nfs	2-4 (rpc #100003)
----------	------	-----	-------------------

MAC Address: 00:0C:29:93:3E:91 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.13 - 2.6.31

Network Distance: 1 hop

Service Info: OSs: Unix, Linux

Nmap scan report for sharepeg.pegasus.com (172.20.241.19)

Host is up (0.00s latency).

Not shown: 91 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	http	Microsoft IIS httpd 6.0
--------	------	------	-------------------------

88/tcp	open	tcpwrapped	
--------	------	------------	--

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	
---------	------	-------------	--

389/tcp	open	ldap	
---------	------	------	--

445/tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
---------	------	--------------	---

1025/tcp	open	msrpc	Microsoft Windows RPC
----------	------	-------	-----------------------

1027/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
----------	------	------------	-------------------------------------

3389/tcp	open	microsoft-rdp	Microsoft Terminal Service
----------	------	---------------	----------------------------

MAC Address: 00:0C:29:44:AD:9D (VMware)

Device type: general purpose

Running: Microsoft Windows 2003

OS details: Microsoft Windows Server 2003 SP1 or SP2

Network Distance: 1 hop

Service Info: OS: Windows

Nmap scan report for mailpeg.pegasus.com (172.20.241.28)

Host is up (0.00s latency).

Not shown: 94 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (protocol 2.0)
--------	------	-----	---------------------------------------

25/tcp	open	smtp	Postfix smtpd
--------	------	------	---------------

80/tcp	open	http	Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch)
--------	------	------	---

110/tcp	open	pop3	Dovecot pop3d
---------	------	------	---------------

111/tcp	open	rpcbind	
---------	------	---------	--

143/tcp	open	imap	Dovecot imapd
---------	------	------	---------------

MAC Address: 00:0C:29:03:30:62 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.13 - 2.6.31

Network Distance: 1 hop

Service Info: Host: pegasus.pegasus.com; OS: Linux

Nmap scan report for 172.20.241.80

Host is up (0.00s latency).

All 100 scanned ports on 172.20.241.80 are closed

MAC Address: 00:0C:29:33:28:01 (VMware)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Skipping SYN Stealth Scan against pegasus-xp-work.pegasus.com (172.20.241.82) because Windows does not support scanning your own machine (localhost) this way.

Skipping OS Scan against pegasus-xp-work.pegasus.com (172.20.241.82) because it doesn't work against your own machine (localhost)

Nmap scan report for pegasus-xp-work.pegasus.com (172.20.241.82)

Host is up.

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

7/tcp	unknown	echo	
-------	---------	------	--

9/tcp	unknown	discard	
-------	---------	---------	--

13/tcp	unknown	daytime	
--------	---------	---------	--

21/tcp	unknown ftp
22/tcp	unknown ssh
23/tcp	unknown telnet
25/tcp	unknown smtp
26/tcp	unknown rsftp
37/tcp	unknown time
53/tcp	unknown domain
79/tcp	unknown finger
80/tcp	unknown http
81/tcp	unknown hosts2-ns
88/tcp	unknown kerberos-sec
106/tcp	unknown pop3pw
110/tcp	unknown pop3
111/tcp	unknown rpcbind
113/tcp	unknown auth
119/tcp	unknown nntp
135/tcp	unknown msrpc
139/tcp	unknown netbios-ssn
143/tcp	unknown imap
144/tcp	unknown news
179/tcp	unknown bgp
199/tcp	unknown smux
389/tcp	unknown ldap
427/tcp	unknown svrloc
443/tcp	unknown https
444/tcp	unknown snpp
445/tcp	unknown microsoft-ds
465/tcp	unknown smtps
513/tcp	unknown login
514/tcp	unknown shell
515/tcp	unknown printer
543/tcp	unknown klogin
544/tcp	unknown kshell
548/tcp	unknown afp
554/tcp	unknown rtsp
587/tcp	unknown submission
631/tcp	unknown ipp
646/tcp	unknown ldap
873/tcp	unknown rsync
990/tcp	unknown ftps

993/tcp unknown imaps
995/tcp unknown pop3s
1025/tcp unknown NFS-or-IIS
1026/tcp unknown LSA-or-nterm
1027/tcp unknown IIS
1028/tcp unknown unknown
1029/tcp unknown ms-lsa
1110/tcp unknown nfsd-status
1433/tcp unknown ms-sql-s
1720/tcp unknown H.323/Q.931
1723/tcp unknown pptp
1755/tcp unknown wms
1900/tcp unknown upnp
2000/tcp unknown cisco-sccp
2001/tcp unknown dc
2049/tcp unknown nfs
2121/tcp unknown ccproxy-ftp
2717/tcp unknown pn-requester
3000/tcp unknown ppp
3128/tcp unknown squid-http
3306/tcp unknown mysql
3389/tcp unknown ms-term-serv
3986/tcp unknown mapper-ws_ethd
4899/tcp unknown radmin
5000/tcp unknown upnp
5009/tcp unknown airport-admin
5051/tcp unknown ida-agent
5060/tcp unknown sip
5101/tcp unknown admdog
5190/tcp unknown aol
5357/tcp unknown wsapi
5432/tcp unknown postgresql
5631/tcp unknown pcanywheredata
5666/tcp unknown nrpe
5800/tcp unknown vnc-http
5900/tcp unknown vnc
6000/tcp unknown X11
6001/tcp unknown X11:1
6646/tcp unknown unknown
7070/tcp unknown realserver

8000/tcp unknown http-alt
8008/tcp unknown http
8009/tcp unknown ajp13
8080/tcp unknown http-proxy
8081/tcp unknown blackice-icecap
8443/tcp unknown https-alt
8888/tcp unknown sun-answerbook
9100/tcp unknown jetdirect
9999/tcp unknown abyss
10000/tcp unknown snet-sensor-mgmt
32768/tcp unknown filenet-tms
49152/tcp unknown unknown
49153/tcp unknown unknown
49154/tcp unknown unknown
49155/tcp unknown unknown
49156/tcp unknown unknown
49157/tcp unknown unknown

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/> .

Nmap done: 256 IP addresses (7 hosts up) scanned in 39.56 seconds

Starting Nmap 5.50 (<http://nmap.org>) at 2011-01-28 16:28 Pacific Standard Time

NSE: Loaded 57 scripts for scanning.

NSE: Script Pre-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 16:28

Completed NSE at 16:28, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating ARP Ping Scan at 16:28

Scanning 82 hosts [1 port/host]

Completed ARP Ping Scan at 16:28, 1.33s elapsed (82 total hosts)

Initiating Parallel DNS resolution of 1 host. at 16:28

Completed Parallel DNS resolution of 1 host. at 16:28, 0.00s elapsed

Initiating SYN Stealth Scan at 16:28

Scanning 8 hosts [1000 ports/host]

Discovered open port 993/tcp on 172.20.241.14

Discovered open port 22/tcp on 172.20.241.14

Discovered open port 22/tcp on 172.20.241.36

Discovered open port 22/tcp on 172.20.241.1

Discovered open port 22/tcp on 172.20.241.28

Discovered open port 135/tcp on 172.20.241.81
Discovered open port 135/tcp on 172.20.241.5
Discovered open port 135/tcp on 172.20.241.19
Discovered open port 143/tcp on 172.20.241.14
Discovered open port 143/tcp on 172.20.241.28
Discovered open port 554/tcp on 172.20.241.81
Discovered open port 80/tcp on 172.20.241.14
Discovered open port 80/tcp on 172.20.241.19
Discovered open port 80/tcp on 172.20.241.28
Discovered open port 1025/tcp on 172.20.241.5
Discovered open port 80/tcp on 172.20.241.1
Discovered open port 445/tcp on 172.20.241.81
Discovered open port 445/tcp on 172.20.241.5
Discovered open port 445/tcp on 172.20.241.14
Discovered open port 1025/tcp on 172.20.241.19
Discovered open port 110/tcp on 172.20.241.14
Discovered open port 445/tcp on 172.20.241.19
Discovered open port 110/tcp on 172.20.241.28
Discovered open port 139/tcp on 172.20.241.81
Discovered open port 139/tcp on 172.20.241.5
Discovered open port 139/tcp on 172.20.241.14
Discovered open port 23/tcp on 172.20.241.1
Discovered open port 3389/tcp on 172.20.241.5
Discovered open port 139/tcp on 172.20.241.19
Discovered open port 3389/tcp on 172.20.241.81
Discovered open port 3389/tcp on 172.20.241.19
Discovered open port 111/tcp on 172.20.241.36
Discovered open port 111/tcp on 172.20.241.14
Discovered open port 21/tcp on 172.20.241.36
Discovered open port 21/tcp on 172.20.241.14
Discovered open port 111/tcp on 172.20.241.28
Discovered open port 25/tcp on 172.20.241.28
Discovered open port 995/tcp on 172.20.241.14
Discovered open port 443/tcp on 172.20.241.14
Discovered open port 53/tcp on 172.20.241.36
Discovered open port 53/tcp on 172.20.241.5
Discovered open port 53/tcp on 172.20.241.14
Discovered open port 443/tcp on 172.20.241.1
Discovered open port 3269/tcp on 172.20.241.5
Discovered open port 49155/tcp on 172.20.241.81

Discovered open port 10243/tcp on 172.20.241.81
Discovered open port 2049/tcp on 172.20.241.14
Discovered open port 8093/tcp on 172.20.241.19
Discovered open port 464/tcp on 172.20.241.5
Discovered open port 464/tcp on 172.20.241.19
Discovered open port 901/tcp on 172.20.241.14
Discovered open port 1060/tcp on 172.20.241.5
Discovered open port 56738/tcp on 172.20.241.19
Discovered open port 2869/tcp on 172.20.241.81
Discovered open port 88/tcp on 172.20.241.5
Discovered open port 49153/tcp on 172.20.241.81
Discovered open port 49154/tcp on 172.20.241.81
Discovered open port 88/tcp on 172.20.241.19
Discovered open port 593/tcp on 172.20.241.5
Discovered open port 1111/tcp on 172.20.241.5
Discovered open port 1027/tcp on 172.20.241.5
Discovered open port 3268/tcp on 172.20.241.5
Discovered open port 49156/tcp on 172.20.241.81
Discovered open port 593/tcp on 172.20.241.19
Discovered open port 1027/tcp on 172.20.241.19
Discovered open port 1039/tcp on 172.20.241.5
Discovered open port 636/tcp on 172.20.241.5
Discovered open port 1039/tcp on 172.20.241.19
Discovered open port 389/tcp on 172.20.241.5
Discovered open port 636/tcp on 172.20.241.19
Discovered open port 389/tcp on 172.20.241.19
Discovered open port 5357/tcp on 172.20.241.81
Discovered open port 56737/tcp on 172.20.241.19
Completed SYN Stealth Scan against 172.20.241.5 in 1.75s (7 hosts left)
Completed SYN Stealth Scan against 172.20.241.14 in 1.75s (6 hosts left)
Completed SYN Stealth Scan against 172.20.241.36 in 1.75s (5 hosts left)
Completed SYN Stealth Scan against 172.20.241.80 in 1.75s (4 hosts left)
Discovered open port 8082/tcp on 172.20.241.19
Discovered open port 49152/tcp on 172.20.241.81
Discovered open port 9618/tcp on 172.20.241.19
Completed SYN Stealth Scan against 172.20.241.19 in 1.86s (3 hosts left)
Completed SYN Stealth Scan against 172.20.241.28 in 1.86s (2 hosts left)
Completed SYN Stealth Scan against 172.20.241.81 in 1.86s (1 host left)
Completed SYN Stealth Scan at 16:28, 4.00s elapsed (8000 total ports)
Initiating Service scan at 16:28

Scanning 76 services on 8 hosts

1. Rootkit and Bot detection demonstration

- i. Sysinternals suite - rootkit revealer
 - a. Console error - <http://support.microsoft.com/kb/278845>
 - b. `mstsc -v:servername /F -console`
 - c. <http://technet.microsoft.com/en-us/sysinternals/bb897445>
- ii. Sophos Free tool - <http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html>
- iii. Detecting rootkits on linux - <http://linuxhelp.blogspot.com/2006/12/various-ways-of-detecting-rootkits-in.html>
 - a. `chkrootkit`
 - a. http://www.sans.org/reading_room/whitepapers/linux/linux-rootkits-beginners-prevention-removal_901
 - b. `rkhunter -c`
 - a. http://www.rootkit.nl/projects/rootkit_hunter.html
- iv. Bot Hunter
 - a. <http://www.bothunter.net>
 - b. User Guide - <http://www.bothunter.net/OnlinePDF.html>

2. IPv6 protection - Disable on all hosts

- i. <http://www.cyberciti.biz/tips/linux-how-to-disable-the-ipv6-protocol.html>
- ii. Windows - uncheck IPv6 in Network properties

First Half-Hour

[Page history](#) last edited by [Chris](#) 1 month, 3 weeks ago

JOBS IN A NUMERICAL LIST AND CORRESPONDING RESPONSIBILITIES

- 0: get a feel for it
- 1: harden systems- general stuff firewalls rouge apps and junk like that
- 2: cisco- wire check (interface check)
- 3: install ossec
- 4: wireshark/nmap
- 5: monitor/make changes to the topology as needed

JOBS THAT NEED TO BE PERFORMED BY GROUPS AND MANAGED BY THEIR LEADERS

<u>Outside Facing Services</u>	<u>Monitoring</u>	<u>Network</u>	<u>Injects</u>
0	0	0	0
1	1	1	1
3	3	2	
5	5	4	

1. Change admin passwords
2. Change admin names
3. Router and Switch configs
4. Remove other non-worker accounts off the active directory
5. Make sure DNS is up and running correctly

Step 1: WireShark

Download and run WireShark. When you first enter the room, there should be no activity on the network besides the computers communicating with each other. Disconnect the line out, if you want, to ensure that nothing is escaping your network that you do not want. With WireShark, you will be able to check for any programs that are attempting to phone home and trace back to where they are coming from. This will be a good start for finding out which boxes already have back doors.

Step 2: Nmap/Netstat

Before making any significant changes to the network, try to run an nmap scan. This will also help to find any boxes that might have backdoors. If the MySQL server has port 80 open, there is most likely something using that port. This is a good start for knowing what needs to be shut down (although there is no reason anything but the ports that the specific services running use). Also running netstat on each machine will display everything that the machine is connected to and if there is a possible back door.

Step 3: Processes

Once you have an idea of how your network actually looks, along with how the network is supposed to look, you will be able to start shutting down services and processes on all the machines. Check top on the *nix boxes and task manager on windows. Take snapshots and kill any process you are unsure about.

Step 4: Lock down

At this point you can begin to start locking down the boxes. Set up firewalls. Some tips: only allow OSCommerce to communicate with the MySQL box. Check for other users on the boxes. On unix boxes, check inside /etc/passwd and /etc/group.

Windows Hardening

Backup, Change, Report.

First 15 Minutes:

Team member 1	Team member 2
Anti-Malware: Malwarebytes'	Close Unneccesary Ports
Turn on Automatic Updates	Create Limited Account for Internet Use
Firewall: ZoneAlarm	Set Minnimum Password Length
Anti-Virus: Microsoft Security Essentials	Enable Password Complexity
	Change Admin Password
	Turn Off Guest Account(s)
	Audit Admin Account
Submit Report to Captain	Submit Report to Captain

First Half-Hour

JOBS IN A NUMERICAL LIST AND CORRESPONDING RESPONSIBILITIES

- 0: get a feel for it
- 1:harden systems- general stuff firewalls rouge apps and junk like that
- 2:cisco- wire check (interface check)
- 3:install ossec
- 4:wireshark/nmap
- 5:monitor/make changes to the topology as needed

JOBS THAT NEED TO BE PERFORMED BY GROUPS AND MANAGED BY THEIR LEADERS

Outside Facing Services	Monitoring	Network	Injects
0	0	0	0
1	1	1	1
3	3	2	
5	5	4	

- 1. Change admin passwords
- 2. Change admin names
- 3. Router and Switch configs
- 4. Remove other non-worker accounts off the active directory

5. Make sure DNS is up and running correctly

Step 1: WireShark

Download and run WireShark. When you first enter the room, there should be no activity on the network besides the computers communicating with each other. Disconnect the line out, if you want, to ensure that nothing is escaping your network that you do not want. With WireShark, you will be able to check for any programs that are attempting to phone home and trace back to where they are coming from. This will be a good start for finding out which boxes already have back doors.

Step 2: Nmap/Netstat

Before making any significant changes to the network, try to run an nmap scan. This will also help to find any boxes that might have backdoors. If the MySQL server has port 80 open, there is most likely something using that port. This is a good start for knowing what needs to be shut down (although there is no reason anything but the ports that the specific services running use). Also running netstat on each machine will display everything that the machine is connected to and if there is a possible back door.

Step 3: Processes

Once you have an idea of how your network actually looks, along with how the network is supposed to look, you will be able to start shutting down services and processes on all the machines. Check top on the *nix boxes and task manager on windows. Take snapshots and kill any process you are unsure about.

Step 4: Lock down

At this point you can begin to start locking down the boxes. Set up firewalls. Some tips: only allow OSCommerce to communicate with the MySQL box. Check for other users on the boxes. On unix boxes, check inside /etc/passwd and /etc/group.

Linux First 15 Minutes

[Page history](#) last edited by [rhema_junior@...](#) 1 month, 3 weeks ago

Number 1 - Ohm

Limit user root access, set sudo values. Change system admin passwords.

Disable unnecessary services. Do not enable telnet.

Change File and folder permissions through chmod.

Internet Connection Required:

Run Update Manager (yum or pm) update icon is in top right corner. Can trigger manual update through term.

Start configure of Bastille system. Check for malicious files.

Specialized rootkit and virus programs if necessary

Number 2

Download anything needed

Researching linux security

Assisting with technical problems.

Things To Practice

We must become proficient in the following:

1. FreeBSD
2. Linux
3. Anti-virus software must be used!
4. Host based firewalls
5. Man-in-the-middle DNS attacks
6. MySQL
7. PHP
8. IPS & IDS - SNORT - BASE - OSSEC
9. Web Application Security
10. VLAN routing - secure branch office
11. Cisco Security - turn off SNMP!
12. IPSEC - encrypt all traffic
13. Static Arp entries
14. REPORTING
15. DOCUMENTATION
16. Communication - Clarify, ask questions, make sure everyone is comfortable talking!
17. Practice, Practice, Practice, Practice, Practice'
18. Don't procrastinate start practicing NOW
19. Stateful Routing!
20. Backup - on VMWare - pause, copy .vmdk (virtual hard drive) to backup location, resume
21. Build new systems & transfer databases, users, and all services to new systems - build these in parallel to current running systems, simultaneously turn off old system and turn on new system, check services
22. Hang around after the competition and take advantage of winning teams pride to ask them important questions about how they succeeded!
23. Build topology to include scoring engine and red team access
24. Use RunAS
25. Encrypt all traffic - IPSEC
26. Use Static ARP entries
27. Turn off SNMP on router
28. Disable CDP

List from State competition

1. Install and configure Syslog to work correctly - ossec with MySql.
2. Team wiki
3. Ossec on Cisco equipment
4. Learn what the Ossec errors are
5. How to build a forums page
6. Secondary DNS (just review it again)
7. Single Sign-on

8. Raidus server
9. Vlans
10. SSL for both Ossec and the team site
11. MySQL database backup so we can move the database to a new server
12. Adding and changing MySQL users for databases
13. Learn more of the Mysql commads like password recovery/reset and those types of things
14. Ossec logs with mysql how to set that up
15. How to kill and block services/ips from command line or with diffrent tools
16. Free buisness firewalls
17. How to set up the Linux (and Windows) firewalls
18. Patching Linux and Windows **WITHOUT** the internet
19. Installing things on Linux **WITHOUT** the internet
20. Changing users, groups, and permissions in Linux
21. How to export the Active Directory user list to a text document
22. **Documentation!!!!!!**
23. OpenVAS
24. Sugar CRM
25. MRTG
26. see the full list of state injects here http://docs.google.com/View?id=dgf43qmk_30phzx5ccs

Unix hardening

Password protect boot loader.

Know /etc/shadow <http://www.cyberciti.biz/faq/understanding-etcshadow-file/>

Monitoring Linux <http://www.cyberciti.biz/tips/top-linux-monitoring-tools.html>

20 Linux server hardening tips <http://www.cyberciti.biz/tips/linux-security.html>

Find out about permissions on files, groups and owners and how to assign/change.

Use PAM to limit root access

Find out about /init.d and runlevels of daemons

Find out about vulnerable daemons to disable.

netstat -a to find out what ports and services are being used.

Secure SSH

Know how to patch each UNIX version.

Learn about Syslog and store on a separate machine.

Edited by DD

A good FreeBSD security tutorial. http://onlamp.com/pub/a/bsd/2002/08/08/FreeBSD_Basics.html?page=1 . You will need to know some basics on editing files in UNIX. I also noticed some options requiring kernel compiles. I will do a little more research to see if this is viable.

Red Hat Hardening checklist - <http://security.utexas.edu/admin/redhat-linux.html>

SANs institute Linux Hardening - <http://www.sans.org/score/checklists/linuxchecklist.pdf>

Bastille Linux

A hardening program for RedHat, SUSE, Debian, Gentoo, and Mandrake distributions, Bastille Linux attempts to lock down a Linux server. It walks the user through a series of questions and builds a policy based on the answers.

http://bastille-linux.sourceforge.net/running_bastille_on.htm

****On Ubuntu or debian you can install it using "sudo apt-get install bastille". You can find help on Bastille by using the man page "man bastille". In order to harden your system "bastille". Follow the prompts and answer the questions. Your system is now hardened.**

Harden package

The harden package tries to make it more easy to install and administer hosts that need good security. This package should be used by people that want some quick help to enhance the security of the system. It automatically installs some tools that should enhance security in some way: intrusion detection tools, security analysis tools, etc. Harden installs the following *virtual* packages (i.e. no contents, just dependencies or recommendations on others):

- `harden-tools`: tools to enhance system security (integrity checkers, intrusion detection, kernel patches...)
- `harden-environment`: helps configure a hardened environment (currently empty).
- `harden-servers`: removes servers considered insecure for some reason.
- `harden-clients`: removes clients considered insecure for some reason.
- `harden-remoteaudit`: tools to remotely audit a system.
- `harden-nids`: helps to install a network intrusion detection system.
- `harden-surveillance`: helps to install tools for monitoring of networks and services.

Useful packages which are not a dependence:

- `harden-doc`: provides this same manual and other security-related documentation packages.
- `harden-development`: development tools for creating more secure programs.

Be careful because if you have software you need (and which you do not wish to uninstall for some reason) and it conflicts with some of the packages above you might not be able to fully use `harden`. The `harden` packages do not (directly) do a thing. They do have, however, intentional package conflicts with known non-secure packages. This way, the Debian packaging system will not approve the installation of these packages. For example, when you try to install a telnet daemon with `harden-servers`, `apt` will say:

```
# apt-get install telnetd
The following packages will be REMOVED:
  harden-servers
The following NEW packages will be installed:
  telnetd
Do you want to continue? [Y/n]
```

This should set off some warnings in the administrator head, who should reconsider his actions.

Team Checklist

Page history last edited by tonyborgert@gmail.com 6 days, 10 hours ago

General rule - Backup, Change, report!

Monitoring	Router	Pix	Switch	AD-Server	E- Comm	SharePoint	E-Mail	FTP	Win XP	Win 7	Splunk
	2811	515/515E	2950T-24	WS 2003	Debian Linux	WS 2003	Debian Linux	CentOS Linux	Win Xp	Win7	Ubuntu 10.10 Server
OpenVAS									Download to		
OSSEC									Share File,		
NAGIOS									MBSA		
SNORT+BASE									7zip		
									Comodo		
									OSSEC Win		
MBSA									OSSEC		
NMAP									Linux		
									Sysinternals		
									Malwarebytes		
									Recon	Recon	OpenVAS
									network	network	OSSEC
				MBSA		MBSA			MBSA	MBSA	Nagios
									NMAP	NMAP	SNORT+BASE
	Backup config	Backup Config	Backup Config	Service Pack / Updates	APT/RPM update	Service Pack / Updates	APT/RPM update	APT/RPM update	Service Pack / Updates	Service Pack / Updates	APT/RPM update
				Remove	Remove	Remove	Remove	Remove	Remove	Remove	Remove
				Unneeded	Unneeded	Unneeded	Unneeded	Unneeded	Unneeded	Unneeded	Unneeded
				Users	Users	Users	Users	Users	Users	Users	Users
	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password	Change Password
	Port/Device for ACLS		Port/ Mac Security	ID needed ports	ID needed ports	ID needed ports	ID needed ports	ID needed ports	ID needed ports	ID needed ports	ID needed ports
				Block all other ports	Block all other ports	Block all other	Block all other ports	Block all other ports	Block all other ports	Block all other ports	Block all other ports

			ports							
Install										
ACLs	Setup	Port	Setup	Setup	Setup	Setup	Setup	Setup	Setup	Setup
After first	Firewall	security	Firewall	Firewall	Firewall	Firewall	Firewall	Firewall	Firewall	Firewall
45 minutes			Comodo	Fire Starter	Comodo	Comodo	Fire Starter	Comodo	Cmodo	Fire Starter
			Install	Install	Install	Install	Install	Install	Install	Install
			Monitoring	Monitoring	Monitoring	Monitoring	Monitoring	Monitoring	Monitoring	Monitoring
			Services	Services	Services	Services	Services	Services	Services	Services
			OSSEC	OSSEC	OSSEC	OSSEC	OSSEC	OSSEC	OSSEC	OSSEC
			Client	Client	Client	Client	Client	Client	Client	Client

Reporting

Template

Change

Managment

SSL in Ubuntu

[Page history](#) last edited by [Rocketcandy](#) 12 months ago

Setting up ssl certificates

<http://beginlinux.com/blog/2009/01/ssl-on-ubuntu-810-apache2/>

<http://www.howtoforge.com/how-to-set-up-an-ssl-vhost-under-apache2-on-ubuntu-9.10-debian-lenny>

<http://www.tc.umn.edu/~brams006/selfsign.html>

Enabling ssl for oscommerce

http://forums.oscommerce.com/topic/233458-how-to-install-ssl-on-osc-a-simple-1-2-3-instruction/page_hl_ssl%2030

Linux

[Page history](#) last edited by [David B. Pickens](#) 12 months ago

How to set a default route

```
sudo route add default gw X.X.X.X
```

Changing to Static Ip

<http://www.howtogeek.com/howto/ubuntu/change-ubuntu-server-from-dhcp-to-a-static-ip-address/>

Updating Linux with internet

sudo apt-get update

sudo apt-get upgrade

Some Usefull Linux Commands:

sudo netstat -lnp --> shows everything that is listening on your computer

How to do a password Reset:

1. interrupt grub (hit escape while unix is booting)
2. press "e" to edit Kernal
3. change to "rw init=/bin/bash"
4. hit "b" to boot
5. brings you to the root shell
6. passwd accountname
7. shutdown -

Change Root Password and never log into root after that!

Usefull commands

ifconfig = lists anything that is running

-a = shows all the connections the computer has

nameofdevise down = shuts it down

nameofdevise up = turns it back on

ps aux = lists all the proccess running on the machine

ps aux | grep proccessname = searches the outputs for the praccess

kill proccessnumber = kills the proccess

killall something = kills everything that has something in it

kill -9 name = kills name no matter what stage of proccessing it is in

ufw = configures the server firewall

man appname = brings up the man page for the app

How to Secure it

<http://www.chkrootkit.org/>

Page Tools

Insert links

Insert links to other pages or uploaded files.

Pages Images and files

Insert a link to a new pageInsert image from URL**Tip:** To turn text into a link, highlight the text, then click on a page or file from the list above.

Downloads

MBSA (1.54 MB): <http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c>

7zip (1.05 MB): <http://sourceforge.net/projects/sevenzzip/files/7-Zip/9.20/7z920.exe/download>

Nmap (18.9 MB): <http://nmap.org/dist/nmap-5.51-setup.exe>

Comodo (33.5 MB): http://download.comodo.com/cis/download/installs/1000/standalone/cfw_installer_x86.exe

OSSEC Win (632 kb): <http://www.ossec.net/files/ossec-agent-win32-2.5.1.exe>

OSSEC Lin (723 kb): <http://www.ossec.net/files/ossec-hids-2.5.1.tar.gz>

Putty: <http://the.earth.li/~sgtatham/putty/latest/x86/putty.zip>

Sysinternals Suite (12.9 MB): <http://download.sysinternals.com/Files/SysinternalsSuite.zip>

Malwarebytes (7.37 MB): http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html

Service Packs (if needed)

XP sp2 (266 MB): <http://download.microsoft.com/download/1/6/5/165b076b-aaa9-443d-84f0-73cf11fdcdf8/WindowsXP-KB835935-SP2-ENU.exe>

XP sp3 (316 MB): <http://download.microsoft.com/download/d/3/0/d30e32d8-418a-469d-b600-f32ce3edf42d/WindowsXP-KB936929-SP3-x86-ENU.exe>

Server 2k3 SP2 (372 MB): <http://download.microsoft.com/download/5/f/1/5f104409-2736-48ef-82e1-692ec3da020b/WindowsServer2003-KB914961-SP2-x86-ENU.exe>

Windows 7/ Server 2008 SP1: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c3202ce6-4056-4059-8a1b-3a9b77cdfdda&displaylang=en###>

STOPWATCH:

<http://www.online-stopwatch.com/>

DOWNLOAD NOW: UBUNTU 9.10

<http://www.ubuntu.com/getubuntu/download>

CAB FILE:

Step 1: If you do not have the file, download it from <http://go.microsoft.com/fwlink/?LinkId=76054> and save it to C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache\wsusscn2.cab. You may use any folder, but this is where MBSA will store the file after MBSA has downloaded it.

Step 2: Open C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache\wsusscn2.cab using any program able to view an archive file type of *.cab.

Step 3: Open package.cab from the wsusscn2.cab file, and then the package.xml file inside it.

Step 4: View the *OfflineSyncPackage* header element for the *CreationDate*. It should be set to a value such as "2005-06-01T18:42:49Z" (for example). Use the value you find to determine when the file was generated by Microsoft.

TCP VIEW:

<http://download.sysinternals.com/Files/TCPView.zip>

OSSEC Windows:

<http://www.ossec.net/files/ossec-agent-win32-2.3.exe>

OSSEC Linux:

Linux: <http://www.ossec.net/files/ossec-hids-2.3.tar.gz>

Web interface: <http://www.ossec.net/files/ui/ossec-wui-0.3.tar.gz>

PHP5 and Apache2:

Apache2: <http://apache.mirrors.tds.net/httpd/httpd-2.2.15.tar.gz>

PHP5: <http://us3.php.net/get/php-5.3.2.tar.gz/from/this/mirror>

PUTTY:

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

SNORT/BASE: In this order:

Xampp: RAR <http://www.apachefriends.org/download.php?xampp-win32-1.7.3.exe> ZIP

<http://www.apachefriends.org/download.php?xampp-win32-1.7.3.zip>

Snort: <http://dl.snort.org/snort-current/snort-2.8.5.3.tar.gz>

Base: <http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/download>

7ZIP: to unzip snort and base

<http://preview.licenseacquisition.org/48/1056569395.02174/7zip.exe>

tikiwiki download click version 3.5:

<http://sourceforge.net/projects/tikiwiki/files/TikiWiki%203.x%20-Betelgeuse-/Tiki%203.5/tikiwiki-3.5.zip/download>

Nmap Windows

<http://nmap.org/dist/nmap-5.21-setup.exe>

Nmap Linux

<http://nmap.org/dist/nmap-5.21.tar.bz2>