Global Information Assurance Certification Paper

TOO MANY OPERATING SYSTEMS, NOT ENOUGH LAPTOPS

GIAC SECURITY ESSENTIALS CERTIFICATION
PRACTICAL ASSIGNMENT V1.4 (April 8, 2002)

Martin A. Reymer
SANS Tyson's Corner

Submitted August 27, 2002

Summary

How many times have you found a software solution to your problems only to find out that there is no easy installation script or known method to install it on your control PC because it has not been written or developed for your operating system? As the panic begins to rise, many thoughts go racing through your head such as "I'm no programmer, I'm only a system administrator!" and "Now what?" "Hey, what about a laptop with a huge hard drive and a dual-boot operating system?" "I've seen it done before on NT PC's" and "there must be people in the industry that have been successful that can help me!" Then you sit back analyze the situation and realize that you have had various experiences with multiple operating systems, multiple server and workstation disasters and successes and you just might have had enough experiences to get you through this project. After all, what is the worst thing that could happen? The PC Blue Screens to the point that you can no longer operate the PC, you boot it from a restore disk or cd-rom, repartition the hard drive, reformat the hard drive and pick up your wounded pride off the floor and try it again!

After spending considerable time and effort educating myself of the many situations that could exist in the daily life of a system administrator, this project has progressed to the point of becoming a reality. This paper will provide an administrative person with the steps and wherewithal to survey their resources, research processes and procedures mainly from the Internet, and acquire the necessary hardware and software to fully configure a dual-boot laptop for use with the Windows 2000 and the Linux operating systems. This valuable tool can then be used in combination with various software resources to enable the administrative person to monitor, analyze, test and verify information and data contained in their respective network environment.

Research

The first step is to find yourself a good search engine on the Internet such as www.google.com, www.metasearch.com, www.yahoo.com, www.lycos.com and start reading. The purpose of this is to familiarize yourself with various resources available to you concerning your respective hardware and software. This will give you an area to focus your efforts on. You will find a lot of overwhelming information and it will take quite a while to sift through it all. Start your research with your hardware manufacturer and then research your software manufacturers as well. They will take the time and effort to provide as much guidance as possible, because after all, this will promote their hardware and software as business solutions for the computer industry. I started with Compaq laptops, since I have access to several in my business environment. I also

researched the popular versions of Linux and before long I was concentrating on Red Hat Linux. Red Hat's website (www.redhat.com) provided numerous resources and documentation for just about all of their current versions of software. It also provided information related to hardware compatibility (http://hardware.redhat.com/hcl/?pagename=hcl). As it turned out, I also found quite a bit of guidance related to Compaq laptops from Red Hat's website.

Decisions

Since I need to be able to configure a laptop utilizing minimal resources and run both the Windows 2000 and Linux operating systems on it, the following information reflects my particular situation given my available resources and those based on the commitment of my employer to support this effort. Based on research done on the Internet and documentation available for a dual-boot environment utilizing Windows 2000 and Red Hat Linux, I decided to start putting the pieces together for my laptop. My Compaq Evo N600C laptop already came with Windows 2000 preinstalled which made this one less issue I had to worry about. If you are starting with a system that does not already have this you need to obtain an initial copy of the Windows 2000 operating system. Most importantly, my laptop came with a set of restore cd-roms to enable me to be able to recreate the Windows 2000 operating system on my hard drive should something go wrong with the installation process. Next I needed the largest hard drive available for my laptop. This step is optional if your financial resources are limited, however I plan to utilize this laptop for administrative purposes, so a large hard drive is necessary. I found out that Simple Tech has a replacement 40GB hard drive for my laptop, so I purchased one from CDW at $495. I also purchased a copy of Red Hat Linux 7.3 Professional from CDW for $168. This may have seemed unnecessary since Linux software is available for download from the Internet, but by purchasing a copy of the software it allows me to have the necessary resources not only to load the Linux software on my laptop, but to recreate the software if something goes wrong. It also provides me with documentation, both printed and on cd-rom, which will allow me to load the documentation on my Linux partition so I do not have to carry around all the manuals just for reference. This is an additional safeguard in creating my dual-boot laptop. Also, if I have problems due to some hardware incompatibility issue, I can contact Red Hat and obtain assistance because I will have a registered copy of their operating system. Another safeguard in the planning phase of this project. These safeguards are important because I can save time, money and effort in the configuration and support of my system and therefore outweigh the small monetary cost I have incurred in this project.

Hardware

Compaq Evo N600C laptop
256MB Memory
40GB hard drive (Simple Tech replacement – not mandatory or recommended)
Built-in button mouse with touchpad
USB Logitech 3-button mouse (ease of use – not mandatory or recommended)

Software

EZ-Drive V9.11U (hard drive partitioning software that came with the Simple Tech 40GB hard drive)
Windows 2000 Professional Operating System (preinstalled on original laptop)
Red Hat Linux 7.3 Professional (purchase recommended vs. download)

Operating System Installations

Planning your hard drive partitions is the single most important part of this project. This might be a good time to remember a few phrases that might have been mentioned to you in your lifetime such as: "The third time is always the charm!", "If at first you don't succeed, try, try again" and "When in doubt – Read the Manual!". Due to inexperience on my part and being unfamiliar with Linux disk partitioning, it took three times of loading the software on the laptop and reading the documentation for me to realize that the statement at the beginning of this paragraph is truly important. If you get nothing else from this section, pay attention to these two things and it will save you quite a bit of effort and frustration. First, DO NOT utilize any third party disk partitioning software except those specified in the Linux documentation (Fdisk or FIPS) after you have loaded the Linux software partitions. If you utilize the Disk Management software in Windows 2000, it will overwrite the partition table information and render your PC useless. Second, remember to take excellent notes as you are going through this project. If you have to go back and start over from a blank repartitioned hard drive, you will at least have some documentation to recreate your efforts.

Initial Disk Partitions:

I utilized the Simple Tech software to partition the hard drive into three partitions: one large one for Windows 2000 (20GB), a second large one for Linux (15GB) and a third smaller partition (5GB) for a shared partition. The partitioning software places the operating system on each partition for you from a boot diskette. Do not be concerned with this, since when you load Windows 2000 and Red Hat Linux, you will be able to reformat the partitions with the

actual operating system that you are loading. The actual size of the partitions appears smaller due to operating system overhead. This last partition enables you to pass files back and forth between your Windows 2000 and Linux operating systems so that you can utilize your favorite software tools for processing and analysis. This last partition becomes a time saver since you will not have to find alternate software solutions in order to process your information. You can utilize familiar software instead of trying to find additional software for an operating system that you may not be totally comfortable with.

Step-By-Step: EZ-DRIVE:

- Have boot diskette ready with Windows'95 or Windows'98 Operating System
- Boot laptop with EZ-Drive software disk in floppy drive
- Press ENTER to continue with installation
- Remove floppy diskette and replace with boot diskette
- Press ENTER to select Setup Hard Drive
  - If the software located an NTFS partition, it will prompt you to erase it? Type YES and press the ENTER key
- Press ENTER at Yes – use FAT32 partitions
- Use Down Arrow to select Enter New Partition Sizes and press the ENTER key
  - EXAMPLE: Using a 40GB hard drive, partitions are 20000MB, 15000MB and 5000MB selections
- For Enter the Size of Partition 1 on Drive 1: type 20000 and press the ENTER key
- For Enter the Size of Partition 2 on Drive 1: type 15000 and press the ENTER key
- For Enter the Size of Partition 3 on Drive 1: press the ENTER key to use the remaining disk size for the last partition
- Review the listed partition sizes keeping in mind that the first partition with be utilized for Windows 2000, the second for Linux and third for the shared partition
  - If not partitioned correctly, select the Enter New Partition Sizes entry and redo your selections
- Press the ENTER key with Use These Partition Sizes selected
- Press the ENTER key with Continue Setup selected
- The software will now partition your hard drive and place the operating system from the boot diskette on each partition
- Hard Drive Setup Complete! message received on the screen
- Remove your boot diskette from the floppy drive
- Press the ESC key to restart your laptop

Windows Operating System:

Due to the fact that the partitioning software deleted everything on the hard drive, it was necessary to utilize the restore cd-roms that came with my laptop to reload the Windows 2000 operating system onto the first partition of the hard drive. This not only provided the operating system but the utilities that came with the laptop and some miscellaneous software applications as well. For the most part you can load Windows 2000 with defaults, adjusting some of the settings for your environment.

Step-By-Step: WINDOWS 2000

NOTE: Since the use of Compaq laptops may not be your actual environment, this procedure will detail the Windows 2000 installation from an original Windows 2000 cd-rom instead of the Compaq Restore cd-rom set of discs.

- Insert Windows 2000 cd-rom into the drive and reboot laptop
- Press ENTER to install Windows 2000
- Read Licensing Agreement, Page Down to the bottom of the document and press F8=I agree to continue with installation
- Next you will see the three partitions listed as C: FAT32, D: FAT32 and E: FAT32, with C: FAT32 highlighted, press the ENTER key to install Windows 2000 on that partition
- Up Arrow to highlight the Format the partition using the NTFS file system and press the ENTER key
- Press the F key to format the partition
- After the software has formatted the partition and copied the files to the hard drive, remove the cd-rom when prompted and the laptop will reboot to continue the software installation
- If you need to change system or user locale settings or keyboard layout, click on Customize and change accordingly.
- When finished with adjustments, click on Next
- Enter Name and Organization and click on Next
- Enter your Product Key information that came with your Windows 2000 distribution
- Enter a Computer Name according to your standards and type an Administrator password twice, then click on Next
- Enter Modem Dialing Information if your laptop contains a modem and click on Next
- Select Date, Time and Time Zone information appropriately and click on Next

- The wizard will install the networking software for your system
- Click Custom Settings and then click on Next
- In the Networking Components screen, double-click the Internet Protocol (TCP/IP)
- Enter the appropriate IP settings for your network.
- The wizard performs Final Tasks
- Click Finish to reboot your laptop
- Click Next to run the Network Identification Wizard
- Click the Users must enter a name and password to use this computer radio button and then click Next
- Click Finish
- Log onto the computer with the Administrator userid and password to verify that the Windows 2000 operating system is installed and operational

Linux Operating System:

Next I followed several sets of documentation that I found on the Internet for installing Linux on a system that already contained a Windows 2000 operating system on its primary partition. Remember that I told you that it took me three times to correctly partition and load the Red Hat Linux 7.3 software on my laptop. I had to combine these sets of instructions to be able to successfully load the Red Hat Linux operating system software along with provided system utilities to provide a graphics environment on the second hard drive partition. With the excellent documentation from the GSEC Security Essentials Toolkit written by Eric Cole, Mathew Newfield, and John M. Millican[1], I was able to load the Red Hat Linux software utilizing the GRUB loader to dual-boot the operating systems instead of utilizing LILO (Linux Loader). By having the Red Hat Linux installation place the GRUB loader in the MBR (Master Boot Record), the menu appears when the laptop is powered on and I have the selection of whether to boot to Windows 2000 or Red Hat Linux 7.3. The GRUB loader is very simplified compared to the configuration and use of LILO (utilized in previous versions of Red Hat Linux software). In hind sight, I wanted to utilize LILO according to the documentation I found in my research on the Internet and even attempted several times to configure the Windows 2000 loader to control the dual-boot process. I found out that utilizing the GRUB loader was far more simplified and configured my laptop accordingly.

Step-By-Step: LINUX

NOTE: The Red Hat Linux 7.3 Professional software allows you to load the

[1] Cole, Eric, Mathew Newfield, John M. Millican, GSEC Security Essentials Toolkit, Indiana: Que Publishing, 2002. p 9-29.

software with tools and utilities as if you were a workstation, server, laptop or with custom install options. For the purpose of documenting this procedure, I will install Linux using the laptop installation option.

- Place the Red Hat Linux 7.3 Operating System CD 1 in the drive and power on the laptop
- Press the ENTER key to start the installation program
- Click on Next when the Welcome to Red Hat Linux screen appears
- With English (default), your installation language highlighted, click on Next
- Keyboard Configuration – take defaults – click on Next
- Mouse Configuration – click on Emulate 3 Buttons and then click Next
- Installation Type – with Laptop highlighted click Next
- Disk Partitioning Setup – click the radio button next to Manually partition with Disk Druid and then click Next
    - You will get a message regarding the inconsistency of the disk partition, click Ignore
    - **PAY ATTENTION - Here is where it starts to get a little tricky.**
    - NOTE: Linux keeps partition sizes in cylinders
    - Take advantage of the Online Help on the left side of the screen
    - Make particular note of the drive names that correspond to your three partitions (I.E. first = hda1, second = hda5 and third = hda6)
    - **STAY AWAY FROM hda1** – that is your Windows 2000 installation!
    - **Hda5** is your Linux partition
    - **Hda6** is your shared partition – DO NOT FORMAT – leave it vfat
    - You need three mount points specified; /(root), /boot and <swap>
    - A fourth mount point is recommended (/home) so that you can have a separate workspace for backup files, settings, etc. (just in case you need to reload the operating system, you won't have to recreate everything from your notes!)
    - And lastly, we need to name the third partition so that it can be referenced from within the Linux environment (I.E. /w2k)
- Disk Setup – at the top of the screen will appear a display of your three disk partitions. At the bottom of the display is a graphical representation of the same three partitions.
- Highlight /dev/hda5 on the graphical portion of the screen and click Delete and then click Yes to response – NOTE: device names just changed!
- Highlight Free space after hda2 entry and click on New
- Filesystem Type – use down arrow to select swap, Size(MB) set to size of your laptops' memory X 2 (I.E. 128 X 2 = 256 MB) then click OK to continue
- Highlight Free space after /dev/hda6 entry and click on New
- Mount Point – use down arrow to select /boot, Size highlight and type 50 then click on OK to continue

- **PAY ATTENTION TO YOUR GRAPHICAL DISPLAY** – changing Device name – always look for the Free space underneath you last addition with the largest Size (MB)
- Highlight Free space after /dev/hda7 entry and click on New
- Mount Point – use down arrow to select /home, Size highlight and type 2000 and then click on OK to continue
- Highlight Free space after /dev/hda8 entry and click on New
- Mount Point – use down arrow to select the root directory /, click the radio button next to Fill to maximum allowable size and then click OK
- Find the last Device entry that matches the top right-most partition on the graphical partition map (hda5) and then go to that entry on the bottom half of the disk setup screen, highlight that entry (i.e. /dev/hda5), click on the Edit key, for the Mount Point name type /w2k and click OK
- **NOW REVIEW SETTINGS BEFORE GOING FURTHER:**
  - /dev/hda1 – NTFS partition – Format **No**
  - /dev/hda6 – 52MB - /boot – Format Yes
  - /dev/hda7 – 258MB - <swap> - Format Yes
  - /dev/hda8 – 1997MB - /home – Format Yes
  - /dev/hda9 – remaining space - /(root) - Format Yes
  - /dev/hda5 – 4997MB - /w2k – Format **No**
- Click Next button at bottom of screen to continue
- Boot Loader Configuration – Click box next to Force use of LBA32 (not normally required) then select the NTFS partition from the table at the bottom part of the screen and type Windows 2000 for the Boot label: and check the Default boot image selection.
  - By selecting these choices you enable the GRUB Loader to serve as the loader software instead of the Windows 2000 loader software. The other selections enable the configuration to reflect that if nothing is done when the laptop is powered on, Windows 2000 is the operating system of choice.
- Click Next to continue installation
- Click Yes to continue and force LBA32 mode
- Click Next to skip the Boot loader password configuration
- Network Configuration – Uncheck the Configure Using DHCP check box and fill in the appropriate network addresses for your laptop
- Firewall Configuration – select Medium selection, check the Trusted Devices: Eth0 box and select the Allow Incoming: boxes for the appropriate services that you need on your laptop (i.e. SSH, Telnet, WWW (HTTP), Mail (SMTP)) and then click Next
- Additional Language Support – click Next
- Time Zone Selection – select appropriate zone and click Next
- Account Configuration – type root password twice for verification (MAKE IT

GOOD!) and then click on Add button to add one additional account to the Linux installation. Type User Name, Full Name, Password and Confirm (second time) and then click on OK button. Click Next button to continue

- Package Group Selection – click Next
- Graphical Interface (X) Configuration – software should select correct graphics adapter – click Next
- Click Next to begin installation of Red Hat Linux
- The Installation Software will Format the Filesystems, Transfer install image to the hard drive, Setup Rpm process and then install the various software packages – a great opportunity to read one of those manuals here or just enjoy the trivia screens as part of the Linux installation
- When prompted, remove the CD 1 and replace with CD 2
- Boot Disk Creation – check Skip boot disk creation and click Next
- Monitor Configuration – Select Generic, then highlight Generic Laptop Display panel 1024x768 and click Next
- Customize Graphics Configuration - Color Depth: High Color (16 bit), Screen Resolution: 1024x768, click Test Setting button, when screen appears, click Yes, Desktop environment is: Gnome, Login type: Graphical and then click Next
- Click Exit button to reboot laptop – the CD 2 will be ejected as part of the shutdown procedure

Hardening the Operating Systems

Webster's defines the word harden as "3 a: Inure, toughen b: to inure to unfavorable environmental conditions"[2]. As it applies to operating system software, we can utilize this definition to strengthen, supplement, and refine the existing environment to make it better. Many operating systems are believed to be secure out-of-the-box. The fact is, that if the manufacturer did not release the product as a secure product, it can not be considered secure and there is still a lot of work to do to ensure that operating system is truly secure. Hardening an operating systems can be thought of as taking the extra time and effort to make sure that the only thing running on your operating system is that which is absolutely necessary and vital to the operation of the software applications running on that PC. By applying a structured approach to the review of your operating systems, you can minimize the impact of outside influences from negatively impacting your environment.

Due to the involved nature of "hardening" an operating system, this paper will provide a general guidance and additional sources to authors that have taken the necessary time to provide detailed information on this subject. Listed

[2] Merriam Webster's Deluxe Dictionary, Tenth Collegiate Edition, New York: The Reader's Digest Association, Inc., 1998, p.835.

below are a few of the specific resources available on the Internet to harden both Windows 2000 and Linux operating systems.

Typical steps that are taken during the system hardening include:

1. Minimizing installed software
2. Patching the system
3. Securing filesystem permissions and S*ID binaries
4. Improving login and user security
5. Setting some physical and boot security controls
6. Securing the daemons via network access controls
7. Increasing logging and audit information
8. Configuring vendor supplied security software (IDS, host firewall) [3]

Windows 2000 Resources:

www.ntbugtraq.com – mailing list for the discussion of security exploits and security bugs in Windows NT, Windows 2000, and Windows XP plus related applications

http://ntsecurity.ntadvice.com – web archive dedicated, currently, to discussing the issues surrounding vulnerability disclosures, publications, exploit samples

www.ntsecurity.net – secure NT system

www.ntobjectives.com – excellent security and admin NT utilities

www.atstake.com/index.html - focus on hacking your NT system

http://www.microsoft.com/windows2000/professional/default.asp – Windows 2000 Professional support page

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp – Windows 2000 security information

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2kprocl.asp - Windows 2000 Professional Baseline Security Checklist

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/lockguide.asp - New Lockdown Guidelines for Windows 2000 Professional Workstations - *** **MUST READ** ***

[3] Chuvakin, Anton, Ph.D. “Linux Kernel Hardening”. Last updated January 23, 2002 . URL: http://online.securityfocus.com/infocus/1539 (18 August 2002)

http://csrc.nist.gov/itsec/guidance_W2Kpro.html - NIST System Administration Guidance for Windows 2000 Professional

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp – Microsoft HotFix & Security Bulletin Service

http://support.microsoft.com/default.aspx?scid=FH;[LN];sp& - Microsoft Service Packs

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/default.asp – Microsoft Security Best Practices

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp – Microsoft Best Practices for Applying Service Packs, Hotfixes and Security Patches

http://www.microsoft.com/security/default.asp – Microsoft Security homepage

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp – Microsoft TechNet Security homepage

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/lockdown.asp – Microsoft – How to Lockdown

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313203&sd=tech#toc - HOW TO: Analyze System Security in Windows 2000

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309689&sd=tech - HOW TO: Apply Predefined Security Templates in Windows 2000

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313434&sd=tech - HOW TO: Define Security Templates in the Security Templates Snap-in in Windows 2000

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300958&sd=tech - HOW TO: Monitor for Unauthorized User Access in Windows 2000

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/howto/SECHOW.ASP - Don't be a Victim! Make Sure You're Protected Against Commonly-Exploited Vulnerabilities!

http://www.microsoft.com/ntserver/techresources/security/Secure_NTInstall.asp -

Securing Microsoft Windows NT Installation

http://www.cert.org/tech_tips/win-resources.html - CERT® Coordination Center - Windows NT Security and Configuration Resources

http://www.auscert.org.au/Information/Auscert_info/Papers/win_configuration_guidelines.html - Australian Computer Emergency Response Team - Windows NT Configuration Guidelines - *** **MUST READ** ***

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secopsb.asp – Default Windows 2000 Services - *** **MUST READ** ***

http://secinf.net/info/nt/hard/hard.html - Hardening Windows NT Against Attack

Linux Resources:

http://hardware.redhat.com/hcl/?pagename=hcl – Red Hat Hardware Compatibility List

http://www.redhat.com/docs/manuals/linux/ - Red Hat Linux Manuals

http://www.redhat.com/mirrors/LDP/ - The Linux Documentation Project

http://www.redhat.com/docs/manuals/ - Red Hat Manuals

http://www.cert.org/tech_tips/usc20_full.html - CERT® Coordination Center - UNIX Security Checklist v2.0 – *** **MUST READ** ***

http://www.auscert.org.au/Information/Auscert_info/Papers/usc20.html - Australian Computer Emergency Response Team - UNIX Security Checklist v2.0

http://www.auscert.org.au/Information/Auscert_info/Papers/usc20_essentials.html - Australian Computer Emergency Response Team - UNIX Security Checklist v2.0 - The Essentials

http://www.enteract.com/~lspitz/linux.html – Armoring Linux - Preparing your Linux box for the Internet

http://www.enteract.com/~lspitz/swatch.html – Watching You Logs – How to automate your log filtering

http://www.enteract.com/~lspitz/ids.html – Intrusion Detection – Knowing when someone is knocking on your door.

http://www.linux-sec.net/Harden/harden.gwif.html – Hardening and Tightening Security on Your Server/Network

http://www.linux-sec.net/services.gwif.html - Services Hardening

http://www.linux-sec.net/server.gwif.html - Dedicated Function Server Hardening

http://www.linux-sec.net/audit_tools.gwif.html - Check Your Vulnerabilities

http://www.linux-sec.net/exploits.gwif.html - Vulnerabilities and Exploits

http://www.linux-sec.net/server_monitoring.gwif.html - Server Monitoring Systems

http://www.linux-sec.net/eth.gwif.html - Ethernet Monitoring

http://www.linux-sec.net/ids_tools.gwif.html - Intrusion Detection Systems

http://www.linux-sec.net/logging.gwif.html - Logging File Analysis

http://www.linux-sec.net/tracking.gwif.html - Tracking, Tracing, Cleanup

http://www.linux-sec.net/Harden/howto.gwif.html - Hardening HowTos

http://www.linux-sec.net/policy.gwif.html - Security and Network Policy

http://www.linux-sec.net/patches.gwif.html - Security Patches & Updates

http://www.linux-sec.net/distro.gwif.html - Linux Distributions

http://online.securityfocus.com/infocus/1539 - Linux Kernel Hardening

Windows 2000 Software Tools:

http://www.ipswitch.com/Products/WS_Ping/ - WS_Ping ProPack provides all the tools you need to help diagnose network problems and get information about users, hosts, and networks on the Internet or on your Intranet.

http://grc.com/pw/patchwork.htm - Patchwork - Internet Anti-Intrusion Patch Verification and Intrusion Evidence Scanner for Microsoft Windows NT

http://packetstorm.decepticons.org/Win2k – Packet Storm Project

http://www.foundstone.com/rdlabs/termsofuse.php?filename=FportNG.zip - Fport – Reports all open TCP and UDP ports and maps them to the running application.

http://prdownloads.sourceforge.net/ethereal/ethereal-setup-0.9.5.exe - Ethereal – Network sniffing and packet analysis tool.

http://windump.polito.it - Windump – A packet sniffer for Windows.

http://www.somarsoft.com/somarsoft_main.htm - Dumpsec – Windows security auditing program.

http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp - Dumpel – Dumps the contents of the Windows NT and Windows 2000 event logs.

http://www.microsoft.com/downloads/release.asp?releaseid=31154 - HFNETCHCK – A tool developed by Microsoft to help administrators stay current with system patches.

http://www.grc.com/lt/leaktest.htm - LeakTest – Tests personal firewalls to determine if they warn when outbound connections are made.

http://www.nmrc.org/files/snt - Legion – A Windows-based share scanner.

http://www.nmrc.org/files/snt/#menu – Nomad Mobile Research Centre – NT Files

http://www.atstake.com/research/lc3 - L0pht Crack 3.0 – a password cracker.

http://www.atstake.com/research/tools/index.html - @Stake Research Labs - Tools

http://www.zonealarm.com/store/content/company/zap_za_grid.jsp - ZoneAlarm Personal Firewall – Personal firewall for Windows-based systems.

Linux Software Tools:

http://packetstorm.decepticons.org/defense.html – Packet Storm Defenses

http://packetstorm.decepticons.org/linux/security – Packet Storm Linux Security

http://www.nessus.org/index2.html - Nessus is a free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems. It is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 910 remote security checks. It has powerful reporting capabilities (HTML, LaTeX, and ASCII text) and not only points out problems, but also suggests a solution for each of them.

http://www.insecure.org/nmap. - Nmap is a utility for port scanning large networks, although it works fine for single hosts. Sometimes you need speed, other times you may need stealth. In some cases, bypassing firewalls may be required. Not to mention the fact that you may want to scan different protocols (UDP, TCP, ICMP, etc.). Nmap supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, SYN/FIN scanning using IP fragments to bypass firewalls, TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, uptime calculation, and Reverse-ident scanning. Most UNIX and Windows platforms are supported in both GUI and command-line modes, along with several popular handheld devices.

http://www.snort.org. - Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Includes real time alerting, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages via smbclient.

http://www.ethereal.com. - Ethereal is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Ethereal features that are missing from closed-source sniffers.

http://michael.toren.net/code/tcptraceroute. - Tcptraceroute is an implementation of traceroute, which uses TCP SYN packets, instead of the more traditional UDP or ICMP ECHO packets. In doing so, it is able to trace through many common firewall filters. Changes: Now functions properly on Linux PPP interfaces. Improved command line handling, properly aligning packet data for architectures that don't allow non-aligned memory access, the ability to traceroute to a local IP address, the ability to probe with TCP ACK packets, making it possible to

traceroute through stateless firewalls that permit hosts sitting behind the firewall to establish outbound connections, and the ability to track probes by source port numbers instead of IP IDs.

A quick word about obtaining software from Internet sources. Contrary to popular belief, not everyone on the Internet wants to be helpful. Some can be misleading, sneaky, and downright nasty by altering source code and even planting vicious surprises into seemingly harmless programs. How are you going to know the reliability of your downloaded programs? You're not, unless you do some basic checking. Locate your downloaded source code, binaries, and executables from known security sources or organizations. When in doubt, research the program or utility by organization or author and try to obtain an original source. Programs are sometimes published with checksums (MD5 or PGP). Checksums are very basic methods to help you identify that nothing has happened to the software program between the time the file was created and the time that it actually reaches your PC by downloading the file from the Internet. When you have questions or problems with a program, ask your co-workers, associates, or mentors. Chances are good that even if they have not experienced and resolved the situation you are going through, they might be able to give you some ideas or suggestions as to how to proceed with your problem or situation.

Solution

By now, you have come to realize that this project is by no means a quick and simple fix to a serious network issue: that of providing the correct tools for a system administrator to be able to deal with daily issues. Because the industry changes at such a rapid pace, it is easy to not pay attention to the details and find yourself in a situation where you are trying to constantly catch up and unable to meet your business' needs. If you take the time to work through all the steps of; research, read a myriad of documentation, acquire the necessary hardware and software, properly install and configure both the Windows 2000 and Linux operating systems, harden both operating systems, obtain the necessary software tools, and test the use of those tools on a non-production network after getting appropriate permission to do so, you will have an extremely valuable asset. You not only learn the use of those tools by testing them out in a non-production environment, but you have learned the details of networking. The added advantage you now posses will be a usable laptop with dual-boot capabilities to assist you and your staff with your daily responsibilities.

References

Computer Discount Warehouse
URL: http://www.cdw.com (18 August 2002)

Cole, Eric, Mathew Newfield, John M. Millican, GSEC Security Essentials Toolkit, Indiana: Que Publishing, 2002. pg. 9-29.

"Benchtest.com - Linux/Win2k dual boot".
URL: http://www.benchtest.com/linux_win2k.html (18 August 2002).

"Dual Boot - NT4 and redhat 7".
URL: http://www.benchtest.com/dual_nt_linux.html (18 August 2002).

Blackshaw, Bruce P. "Dual booting Linux and Windows 2000/XP on large hard disks". URL:
http://windows.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.enterprisedt.com%2Fpublications%2Fdual_boot.html (18 August 2002)

Selvadurai, Naveen. "Dual-booting Linux and Windows 2000/XP ". URL:
http://windows.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.wpi.edu%2F%7Enaveen%2Fprojects%2Fcontent%2Fd%2Fdualbootlin2000.html
(18 August 2002)

"HD configs, Windows, and other musings". URL: http://www.faqs.org/faqs/pc-hardware-faq/laptops/compaq-aero/section-184.html (18 August 2002)

Merriam Webster's Deluxe Dictionary, Tenth Collegiate Edition, New York: The Reader's Digest Association, Inc., 1998, pg. 835.

Chuvakin, Anton, Ph.D. "Linux Kernel Hardening". Last updated January 23, 2002 . URL: http://online.securityfocus.com/infocus/1539 (18 August 2002)

Additional References

Compaq EVO N600C Laptop.
URL: http://www.compaq.com/products/notebooks/ (18 August 2002)

Red Hat Linux 7.3 Professional
URL: http://www.redhat.com (18 August 2002)

SANS Reading Room Documents.
URL: http://rr.sans.org/index.php (18 August 2002)

Hatch, Brian, James Lee, George Kurtz, Hacking Linux Exposed: Linux Security Secrets and Solutions, Osborne/McGraw-Hill, 2001.

CERT® Security Improvement Modules
URL: http://www.cert.org/security-improvement/index.html (18 August 2002)

Linux Security
URL: http://www.linuxsecurity.com (25 August 2002)

Last Updated: October 24th, 2017

Upcoming Training

San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event