GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Creating a Home Test Lab

© SANS Institute 2003, Author retains full rights.

GIAC Security Essentials Certification
Practical Assignment version 1.4b
Option 2 – Cases Study in Information Security
Prepared by: Russell Elliott
February 19, 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

LIST OF TABLES 3
LIST OF FIGURES 4
INTRODUCTION 5
WHY A HOME LAB? 5
DESIGNS OF A HOME LAB 6
SELECTION OF VIRTUAL MACHINE SOFTWARE 8
SETTING UP A HOME LAB WITH VMWARE WORKSTATION 3.2 16
TESTING VIRTUAL NETWORK AND GUEST OSS 22
TESTING THE VIRTUAL NETWORK PERFORMANCE 25
OBSERVATIONS 32
SUMMARY 34
LIST OF REFERENCES 35

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

LIST OF TABLES

Number	Title	Page
1	Alternative Costs	8
2	Host Computer Requirements	10
3	Guest OSs Supported	11
4	Comparable Virtual Machine Specifications	12
5	Differences in Virtual Machine Specifications	13
6	Minimum Virtual Machine Requirements	17
7	Total New Minimum Requirements	23

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

LIST OF FIGURES

Number	Title	Page
1	Custom Networking Configuration	15
2	Initial Virtual Network	21
3	Virtual Network	24
4	VMware Workstation Error	25

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Introduction

"Anyone who works in the field of network security should have a small, personal lab set up at home, where new exploits and tools can be tested without risking repercussions from an employer."[1] This single statement can be used to gauge the dedication and commitment that an individual has towards the field of network security. Being new to the field of network security, the above statement made an impact on my thinking. The biggest concern is how a home lab should be setup. A home lab does not have to be elaborate yet it needs to accomplish its goals while competing for limited space. Looking at the courses System Administration, Networking, and Security (SANS) offers for the Global Information Assurance Certification (GIAC), the home lab will need to provide ways to test firewalls, intrusion detection, Windows and UNIX security. How does one setup a home lab to accomplish these requirements? What options are available? Should multiple computers or one computer with virtual machines be used? This case study discusses: considerations; costs; how a home lab was setup; testing the virtual machines using SANS GIAC Certification: GSEC Security Essentials Toolkit; and finally observations.

Why a Home Lab?

The decision to create a home lab for network security analysis is not an easy decision. There are many advantages and disadvantages of a home lab. A major advantage is that exploits and tools can be tested on an isolated network without the fear of accidentally corrupting or harming production computer systems or networks. In a home lab, you own the machines and network therefore the requirement to receive permission from the targeted machine and network owner is eliminated. Another major advantage of a home lab is no disruptions by users at work. Performing several functions while at work tends minimize the amount of time to spend on new projects. Keeping users functioning and current systems operational are priorities at work. Typically users tend to seek immediate help with old problems, which the user failed to inform you when the problem first occurs and are now just informing you about. The convenience of working any time on the home lab is another advantage. Twenty to thirty minute commutes are reduced to twenty to thirty steps to the home lab. While working in the home lab family members know not to disturb me.

The major disadvantages are the physical space that the lab can occupy and the costs of the lab. The physical space is a practical matter and influences how the lab is designed. This home lab is designed to utilize existing space therefore remodeling, reconfiguring or moving the home office work area were not considered. Another major disadvantage is the cost of the home lab. An extensive cost analysis was not performed. Most costs that are associated with

[1] Cole, p.9.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

this home lab are the out of pocket costs. These costs include the cost of the computer(s), necessary software costs, and necessary peripherals costs. No attempt was made to assign costs to the physical space, depreciation (for both the equipment and home), electric, heating, cooling, etc.

Designs of a Home Lab

The design of this home lab considered the need for exploiting and testing different operating systems (OS). This includes actually seeing the exploit work on different OSs and the reactions of the victim's computer. The range of Microsoft OSs consisting of Windows Me, Windows 2000 Professional, Windows XP Home Edition, and Windows XP Professional are desirable for testing. This range will cover both computers used at work and most home users. Yes, some of our home users still use Windows 95, Windows 98 and a couple even use Linux. Since there are differences between Windows OS and Linux OS, Red Hat Linux version 7.3 will be another operating systems tested. A vast majority of the open source software programs for network security are available for Linux and UNIX. Therefore a minimum of five different OSs is needed for the home lab.

Two different designs or configurations for the home lab were considered. One configuration consists of multiple computers each with a different OS. The second configuration consists of a single computer with virtual machines for each OS. The major disadvantage of the multiple computers would be the physical space that the Central Process Unit (CPU) boxes, keyboard, mouse and monitors will occupy. A single monitor can be used with a keyboard, video, and mouse (KVM) switch and cables, which will eliminate some space requirements and the need for multiple keyboards, mice and monitors. Yet the various computers still will be tied together over a standalone network. This involves creating a network with the necessary cables and hub(s) and/or switch(s).

Let's look at the estimated costs for the multiple computer design choice. Estimated costs are used since several factors impact the cost including: manufacture, source of purchase as sales are always occurring, configuration of the computer, etc. The multiple computer approach would entail the purchase of 5 computers. The cost of these computers will be between $400 and $1,000 each without monitors. Computer vendors are only offering the current support version of the desired OS, such as, Linux 8, Windows XP Home Edition, Windows XP Professional and Windows 2000 Professional. Used computers can be purchased to reduce costs and to obtain the older OS version. Each computer would also need to have a network interface card (NIC). These would either be purchase with a new computer or purchased separately and installed. Costs for NIC range between $10 and $30. Next, will be the cost of the hub and LAN cables. A 5-port hub will cost approximately $75 and the cables cost approximately $7 each. Finally, the approximate cost for a KVM switch for five computers is approximately $100 and the KVM cables, cables that group the mouse, keyboard, and video cables, are $15 each.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The virtual machine alternative costs are different. First, the cost of the host computer will be higher. This is due to the fact that more random access memory (RAM), more disk space, and greater processor speed is desired. The estimated cost for a beefed up system would range between $1,500 and $5,000. Again these costs would depend on the vendor, source of purchase, and configuration. The next significant cost is the cost of the individual guest OS. These can be purchased from vendors or resellers of the virtual machine software in the form of guest OS kits or the OS can be retail packages from the OS manufacturer or reseller. Microsoft requires a separate OS license for each instant of use which includes the guest OS as an instant of use. The guest OS kits include a Microsoft license for the specific OS purchased. The next cost is for the virtual machine software. Two different software manufactures were considered. Virtual PC 5.0 from Connectix Corporation, which costs $229 for either electronic distribution or shipped packaged[2] and VMware Workstation 3.2 from VMware, Inc. which costs from $299 for electronic distribution and $329 for the shipped packaged[3]. Table 1, Alternative Costs, shows the cost comparison between the alternatives.

The cost comparisons of the various alternatives show the cost of each alternative are approximately the same and there is no clear-cut low cost design. The costs associated with a hardware alternative are saved in virtual machine required software costs and the costs associated with the virtual machine alternative are saved in hardware costs, which are offset with virtual machine required software costs. Another consideration is the physical space required for the home lab. If space is not a limiting factor then any of the alternatives can be utilized. On the other hand, if space is limited then the alternative utilizing virtual machines is recommended. Space is a limiting factor in this instance therefore; the virtual machine alternative was selected for the home lab.

[2] Connectix Corporation, Software eStore, http://www.digitalriver.com/dr/v2/ec_MAIN.Entry10?V1=443568&PN=2&SP=10023&xid=3628

[3] VMware, Inc., VMware Store, https://www.vmware.com/vmwarestore/newstore/index.jsp.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 1 - Alternative Costs

	Separate Computers with Monitors	Separate Computers with KVM	Virtual Machine
HARDWARE COSTS			
5 Basic Computers	$3,500 - $5,000	$2,500 - $5,000	
1 VM Computer			$1,500 - $5,000
1 Networking 5 Port Hub and Cables	$100	$100	
KVM Switch with 5 KVM Cables		$400	
TOTAL HARDWARE COSTS	**$3,600 - $5,100**	**$3,000 - $5,500**	**$1,500 - $5,000**
SOFTWARE COSTS			
Operating Systems			
Linux	No cost - $130	No cost - $130	Guest OS: No cost - $130
Windows XP Home Edition	Included	Included	Guest OS: $200
Windows XP Professional	Included	Included	Host OS included, Guest OS: $300
Windows 2000	Included - $200	Included - $200	Guest OS: $200
Windows ME	Included - $180	Included - $180	Guest OS: $180
VM Software			$229 - $329
TOTAL SOFTWARE COSTS	**$0 - $510**	**$0 - $510**	**$1,109 -$1,359**
TOTAL COSTS	**$3,600 -$5,610**	**$3,000 - $6,010**	**$2,609 - $6,339**

Selection of Virtual Machine Software

Two manufactures were considered for the virtual machine software, Virtual PC 5.0 from Connectix Corporation[4] and VMware Workstation 3.2 from VMware, Inc.[5] The comparison for the two consisted of downloading the user's guides from their respective web sites. Connectix makes available the following documents in PDF format; Product Overview – Datasheet, FAQ, Feature FAQ, and Evaluator's Guide[6] and the User Guide[7]. VMware user's manual is available

[4] Connectix Corporation, < http://www.connectix.com >
[5] VMware Inc., < http://www.vmware.com >
[6] Connectix, Evaluator's Guide Virtual PC for Widows August 2002.
< http://www.connectix.com/support/library.html >

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

online in PDF format.[8] The primary areas of concern were the host computer requirements, the guest OS requirements, the virtual machine specifications, and finally, the flexibility of the software for network analysis. It was found that the requirements for the host computer along with the requirements for the guest OS were similar for the requirements as Table 2 – Host Computer Requirements and Table 3 – Guest OS Supported show. The virtual machine specifications have both similarities and differences. It is the differences that aided in the selection of which software to select. Table 4 – Comparable Virtual Machine Specifications show the virtual machine specifications that are similar and would not impact the selection decision. Table 5 – Differences in Virtual Machine Specifications shows where the virtual machine specifications are different and had an impact on the selection.

Let us review Table 5 – Differences in Virtual Machine Specifications. These differences can be categorized into five areas (1) Chip Set, (2) Supported Devices, (3) Supported Ports, (4) Supported Networking, and (5) Remote Connectivity. The differences in each of these categories are discussed.

(1) Chip Set. The chip set differences of the emulated motherboard was not a factor in the selection.

(2) Supported Devices. Virtual PC 5.0 supports up to three IDE drives, no SCSI devices, and one 1.44MB floppy drive whereas, VMware Workstation 3.2 supports up to four IDE devices, up to seven SCSI devices, and up to two 1.44MB floppy drives. The Supported Devices category advantage goes to VMware Workstation 3.2 that provides more flexibility.

(3) Supported Ports. Virtual PC 5.0 supports up to two serial (COM) ports, one bi-directional parallel (LPT) port, and no USB ports whereas, VMware Workstation 3.2 supports up to four serial (COM) ports, up to two bi-directional parallel (LPT) ports, and two USB ports. Again, the advantage goes to VMware Workstation 3.2, which provides more realistic coverage of ports.

(4) Supported Networking. Virtual PC 5.0 supports one Ethernet card and one virtual Ethernet switch for a virtual machine. VMware Workstation 3.2 supports up to three Ethernet cards and nine Ethernet switches. Virtual PC 5.0 supports PPTP VPN networking which VMware Workstation 3.2 does not. The virtual networking protocols are similar except Virtual PC 5.0 supports DLC, IEEE, AppleTalk, SNA, APPC, and APPN, which VMware Workstation 3.2 does not. VMware Workstation 3.2 supports Samba, which Virtual PC 5.0 does not. Virtual PC 5.0 is limited in the Ethernet card and virtual switches areas. VMware Workstation 3.2 is limited in the protocols area in that it does not support all the protocols that Virtual PC 5.0 provides supports for.

---

[7] Connectix, Virtual PC 5.0 for Windows User Guide, < http://www.connectix.com/support/vpcw_online.html >

[8] VMware, VMware Workstation User's Manual, < http://www.vmware.com/support/ws3/doc >

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One of the goals of this home lab is to create a virtual network; therefore VMware Workstation 3.2 has a slight advantage in this category.

(5) Remote Connectivity. Virtual PC 5.0 has the advantage in this category since VMware Workstation 3.2 does not support remote connectivity.

Table 2 - Host Computer Requirements

Requirement	Virtual PC 5.0[9]	VMware Workstation 3.2[10]
PC Hardware		
Processor	Intel: Celeron, Pentium II, III, 4 AMD: Athlon, Duron	Intel: Celeron, Pentium II, III, 4 AMD: K6-2, K6-III, Athlon, Athlon MP, Athlon XP, Duron
Processor Speed	Recommended: 600MHz Minimum: 400MHz	Recommended: 400MHz or faster Minimum: 266MHz
Memory	Minimum: 128MB (Host OS dependent) (Plus memory required for each guest OS)	Recommended: 256MB Minimum: 128MB (Plus memory required for each guest OS)
Display	Minimum: True Color (16-bit) Recommended: 24-bit	Minimum: 256-color (8-bit)
Disk Drives	Minimum for Host: 2GB (Host OS dependent) Guest OS: Dependent upon guest OS	Minimum for installation: 100MB Minimum for guest OS: 1GB plus applications Hard Drives: IDE, SCSI CD-ROM and DVD-ROM
Windows Host OS		Windows .Net Web Server, Standard Server, Enterprise (beta 3)
	Windows XP Professional, Home Edition	Windows XP Professional, Home Edition (Service Pack 1)
	Windows 2000 Professional, Server, Advance Server	Windows 2000 Professional, Server, Advance Server (Service Pack 2, Service Pack 3)
	Windows NT 4.0 Workstation, Server (Service Pack 6 or 6a)	Windows NT 4.0 Workstation, Server (Service Pack 3 or higher)
	Windows ME Windows 98SE	

[9] Connectix, User Guide, p.16.
[10] VMware, User's Manual, pp.14-16.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 3 - Guest OSs Supported

Guest OS	Virtual PC 5.0[11]	VMware Workstation 3.2[12]
Microsoft Windows	Windows .Net Web Server, Standard Server, Enterprise Server Windows XP Professional, Home Edition Windows 2000 Professional, Server, Advance Server Windows NT 4.0 Workstation, Server, Enterprise Windows ME Windows 98, 98SE Windows 95 Windows 3.1	Windows .Net Web Server, Standard Server, Enterprise Server (beta 3) Windows XP Professional, Home Edition (Service Pack 1) Windows 2000 Professional, Server, Advance Server (Service Pack 2, Service Pack 3) Windows NT 4.0 Workstation, Server (Service Pack 3 or higher) Windows ME Windows 98, 98SE Windows 95 (all) Windows for Workgroups Windows 3.1
Microsoft MS-DOS	DOS	MS-DOS 6
Linux	Linux (text and graphic mode)	Mandrake Linux 8.0, 8.1, 8.2 Red Hat Linux 6.2, 7.0, 7.1, 7.2, 7.3 SuSE Linux 7.0, 7.1, 7.2, 7.3, SLES 7, 8 Turbolinux 6.0, 7.0 Caldera OpenLinux 2.x
FreeBSD		FreeBSD 3.x, 4.0, 4.1, 4.2, 4.3, 4.4 and 4.5
OS/2	OS/2 Warp 4	
Novell	Netware 5.x, 6.x	
Solaris	Solaris 8	

[11] Connectix, User Guide, p.22.
[12] VMware, User's Manual, pp.20-21.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 4 - Comparable Virtual Machine Specifications

Virtual Machine Specifications	Virtual PC 5.0[13]	VMware Workstation 3.2[14]
Processor	Intel Pentium II or later AMD Athlon or later (Dependent on host processor)	Intel Pentium II or later (Dependent on host processor) Intel MMX if supported by host processor
BIOS	AMIBIOS core 8.0 based BIOS ACPI compliant	PhoenixBIOS 4.0 Release 6
Memory	Up to 1GB (dependent on host memory) Maximum: 1.6 – 2 GB available for all virtual machines	Up to 1GB (dependent on host memory) Maximum: 1GB available for all virtual machines
Graphics	VGA, SVGA	VGA, SVGA
Keyboard	104-key Windows enhanced	104-key Windows 95/98 enhanced
Mouse and Drawing Tablets	PS/2 mouse Serial tablets	PS/2 mouse Serial tablets
Sound	Output and input Creative Labs Sound Blaster 16 ISA 16-bit, 44kHz input	Output and input Creative Labs Sound Blaster 16, PCM sound compatible (MIDI sound, game controllers and joysticks not supported)

[13] Connectix, User Guide, pp.79-82.
[14] VMware, User's Manual, pp.18-19.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 5 – Differences in Virtual Machine Specifications

Virtual Machine Specifications	Virtual PC 5.0[15]	VMware Workstation 3.2[16]
Chip Set		Motherboard: Intel 440BX NS338 SIO Chip
IDE Drives	Up to three hard drives	Up to four devices
SCSI Devices		Up to seven
Floppy Drives	One 1.44MB, physical or image file	Up to two 1.44MB, physical or image file
Serial (COM) Ports	Up to two serial Output to serial ports or host files	Up to 4 serial Output to serial ports, Windows or Linux files, or named pipes
Parallel (LPT) Ports	One bi-directional port	Up to two bi-directional
USB Ports		Two-port USB 1.1 controller Supported devices include: USB printers, scanners, PDAs, hard disk drives, memory card readers, and still digital cameras
Ethernet Card	DEC/Intel 21140-A PCI Ethernet Controller 10/100BASE-TX Full-Duplex	Up to three virtual Ethernet cards AMD PCnet-PC II compatible
Virtual Networking and File Sharing	One virtual Ethernet switch Local only Local and host Local, host and external External only NAT networking – using client TCP/IP, FTP, DNS, HTTP, Telnet, PPTP VPN Virtual Ethernet – TCP/IP, NetBEUI, Microsoft Networking, DLC, IEEE, AppleTalk, IPX/SPX, SNA, APPC, APPN, Network File System	Nine virtual Ethernet switches Bridge networking Host-only networking NAT networking – using client TCP/IP, FTP, DNS, HTTP, Telnet Virtual Ethernet – TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell NetWare, Network File System

[15] Connectix, User Guide, pp.79-82.
[16] VMware, User's Manual, pp.18-19.

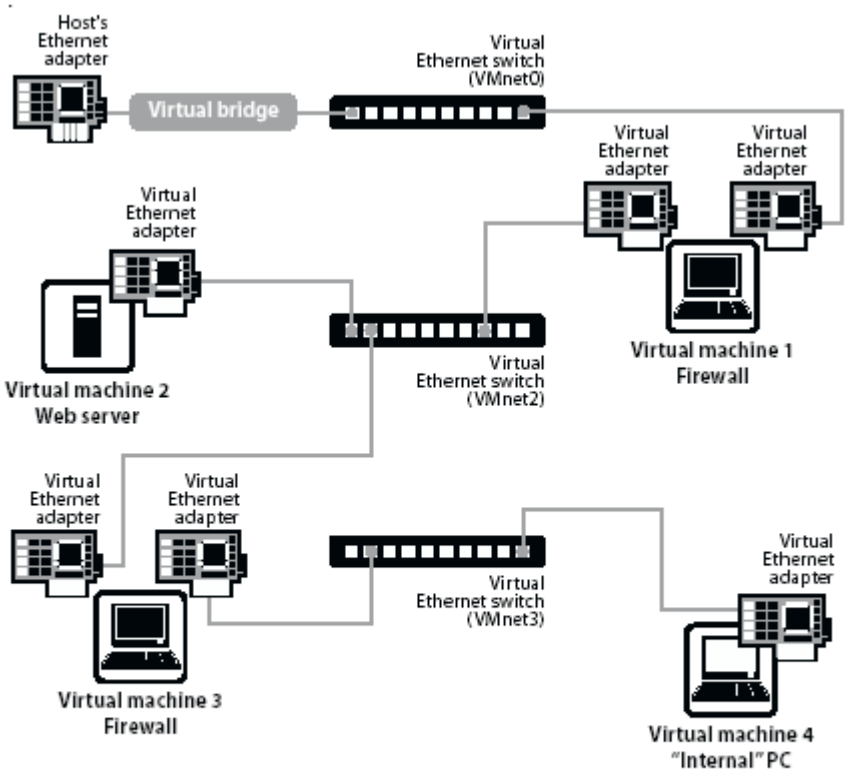
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Virtual Machine Specifications	Virtual PC 5.0[15]	VMware Workstation 3.2[16]
Remote Connectivity Server	VNC (Virtual Networking Computing) Server Supports most VNC clients, Java 8-bit clients 8-bit direct-mapped and CLUT (color lookup table) based encoding 16-bit and 32-bit pixel encoding	

While researching the two different virtual machine software packages, the VMware Workstation User's Manual provided better explanations of the various networking options available. The VMware Workstation User's Manual also provided an explanation on how to setup a custom virtual network as illustrated in Figure 1 – Custom Networking Configuration. A virtual bridge is used to connect between the virtual network and an external network utilizing the host machine. Two virtual machines are used as firewalls on the virtual network to create a DMZ. Another virtual machine is created and used as a web server located in the DMZ. Finally, another virtual machine is created on the internal virtual network. With this virtual network, the internal PC can administer the web server. The external network should not be able to see the internal PC. This virtual network can be used to test both the external and internal firewall rules.[17]

[17] VMware, User's Manual, pp 292-294.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



In this custom configuration, a Web server connects through a firewall to an external network. An administrator's computer can connect to the Web server through a second firewall.

Figure 1 - Custom Networking Configuration, VMware Workstation User's Manual, (Palo Alto, 2002) 292.

Remember, one goal of the home lab is to provide ways to test firewalls, intrusion detection, and security. SANS subject areas include; Firewalls, Perimeter Protection, and VPNs; Intrusion Detection in Depth; Hacker Techniques, Exploits, and Incident Handling; Securing Windows; Securing UNIX; and Auditing Networks, Perimeters, and Systems.[18] These subject areas imply the need to use networks to study various network security issues. The home lab can be an insolated network where you can test all you want without the fear of accidentally corrupting or harming other computer systems or networks. The selected virtual software must be able to meet these criteria.

Basically, Virtual PC 5.0 and VMware Workstation 3.2 are similar software packages providing emulation of various OSs on a single host computer. Each package has its strong points and each package stands out in specific areas. VMware Workstation 3.2 has better support for types of devices and ports than Virtual PC 5.0 and provides better overall virtual networking support but lacks in some networking protocols, namely DLC, IEEE, AppleTalk, SNA, APPC, and

[18] SANS Institute, GIAC Certification – What It Is and How It Works, (2002) p 10.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPN and lacks in remote connectivity support. The better support for devices, ports, and virtual networking capability of VMware Workstation 3.2 has led to the selection of VMware Workstation 3.2.

Setting up a Home Lab with VMware Workstation 3.2

How does one set up a home lab with VMware Workstation 3.2? What steps does one follow to accomplish this? These questions along with setup tips will now be discussed. It should be noted that these steps can also be applicable to business test labs and not limited to just home labs. The first step is to configure or prepare the host computer to meet the at least the minimum specifications for the home lab. First, let's review the desired configuration for this home lab. There are five OSs that consist of Windows ME, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, and Red Hat Linux version 7.3. Given these guest OSs and the host OS, (Windows XP Professional) the minimum amount of RAM and hard disk space are calculated. Table 6 – Minimum Virtual Machine Requirements list these requirements. Thus, the virtual machine will require at least 672 MB of RAM and at least 12 GB of hard disk space. The workstation that was used has the following configuration: Intel Xeon 2.0 GHz processor; 1 GB RAM; and 100 GB hard disk space. This configuration more than meets the minimum requirements. Two additional preparations were made on the workstation. First, an 18 GB partition was created for installing the guest OSs in. The second preparation entailed creating a partition for Red Hat Linux 7.3, installing Red Hat Linux 7.3, and making the machine a dual boot between Windows XP Professional and Red Hat Linux 7.3. This was done for network performance and OSs performance comparisons between the virtual network and the home network.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 6 – Minimum Virtual Machine Requirements

Operating System	Minimum Amount of RAM	Minimum Disk Space
Windows XP Professional (Host OS)	128 MB	2 GB
Windows ME (Guest OS)	96 MB	2 GB
Windows 2000 Professional (Guest OS)	128 MB	2 GB
Windows XP Home Edition (Guest OS)	128 MB	2 GB
Windows XP Professional (Guest OS)	128 MB	2 GB
Red Hat Linux version 7.3 (Guest OS)	64 MB	2 GB
TOTAL MINIMUM REQUIREMENTS	**672 MB**	**12 GB**

The next step is to install VMware Workstation 3.2 software onto the host computer. The installation procedure was followed in the VMware Workstation User's Manual under the Windows Host section. The installation ran smoothly and was typical of most Windows software installation. The following steps were taken:

1. You must be logged on as an Administrator or as a user who is a member of the Administration Group.
2. You must agree to the End Users License Agreement.
3. Choose the directory to install VMware Workstation 3.2.
4. VMware strongly encourages that the autorun feature of the CD-ROM drive be disabled. This is to prevent undesirable interactions between your OS and the virtual machines. This will be checked during the installation and if the autorun feature is enabled a message will ask if you want this feature to be disabled.
5. After the installation, you will be prompted to reboot your computer. [19]

The first time you run VMware, you must enter the serial number. This completes the installation procedures.

Once the software is installed, virtual machines need to be installed. The installation of virtual machines requires that you first create a virtual machine on the host computer. This entails using the "New Virtual Machine Wizard".[20] You

[19] VMware, User's Manual, pp. 29-33.
[20] VMware, User's Manual, p 60.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

will be given the option of selecting a method for configuring the new virtual machine. The options are:

Typical – You will be given the choice of selecting defaults or specifying the follow: guest OS, virtual machine name, location of the virtual machine files, and network connections type.

Custom – Allows you to specify how the virtual machine disks are configured. This option is used to make disks a size different than the default of 4 GB. Location of the virtual machine files. Use a different type, IDE or SCSI, disk other than the default. Use physical disk rather than virtual disks.

VMware Guest OS Kit – Allow you to install a VMware Guest OS Kit.[21]

Pay close attention to tips provided in the VMware Workstation User's Guide when configuring a new virtual machine. Such tips include:

- "The virtual disk should be large enough to hold the guest operating system and all the software that you intend to install, with room for data and growth.
- You cannot change the virtual disk's maximum capacity later.
- You can install additional virtual disks using the Configuration Editor.
- For example, you need about 500MB of actual free space on the file system containing the virtual disk to install Windows ME and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up – installing the operating system on the first virtual disk and using a second virtual disk for applications or data files."[22]

Once the new virtual machine is configured you power on the virtual machine. Since there is no operating system yet for the virtual machine, the virtual machine will boot from the CD-ROM drive or the floppy disk drive. Be sure to have the OS installation disc in the either the CD-ROM or the floppy disk drive. The OS is installed as if the virtual machine was an actual physical machine. VMware Guest OS Kits were not purchased as the retail packages of the various OSs were purchased. At the time VMware Workstation 3.2 was purchased the various guest OS were not available. Therefore, installation of a VMware Guest OS Kit will not be addressed.

There are several installed networking options that can be used. A bridge network allows the guest OS access an external network. A host-only network

[21] VMware, User's Manual, p 61.
[22] VMware, User's Manual, p 65.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

where the guest OS only has access to the host computer resources. And, NAT networking allows the guest OS to use the host computer IP address to access the external network. A Dynamic Host Configuration Protocol (DHCP) server is automatically installed when the VMware software is installed. This allows for the functionality of the host-only and NAT networking options.

A unique feature of Windows XP is the activation requirement. When activation is required configure a bridge network so that the guest OS can register via the Internet. The following issues are unique to Windows XP guest OS installation due to the activation requirement.

> "The Microsoft Windows XP product activation feature creates a numerical key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine may require you to reactive the operating system. These are some steps you can take to minimize the number of significant changes.
>
> - Set the final memory size for your virtual machine before you activate Windows XP. When you cross certain thresholds – approximately 32MB, 64MB, 128MB, 256MB, 512MB, and 1GB – the product activation feature sees the changes as significant. …
> - Install VMware Tools before you activate Windows XP. When the SVGA driver in the VMware Tools package is installed, it activates features in the virtual graphics adapter that make it appear to Windows XP as a new graphics adapter.
> - If you want to experiment with any other aspects of the virtual machine configuration, do so before activating Windows XP. Keep in mind that you have 30 days for experimentation before you have to activate the operating system.
> - In order to install and run a checked (debug) build of Windows XP in a virtual machine, you must first edit the virtual machine configuration (.vmx or .cfg) file. Add the following line: uchi.forecHlatBit = True."[23]

All five guest OSs were installed without any problems. Installing a retail version of an OS is more time consuming than using a VMware Guest OS Kit. These kits already have the guest OS pre-configured and you can specify where to place the guest OS files. When installing the Windows XP OSs, a bridge network was utilized for Internet activation. Once the Windows XP systems were configured the system was activated. After activation, the bridge was removed form the Windows XP Home Edition OS. A bridge still exists for the Windows XP Professional OS to aid in downloading files and programs from the Internet for the virtual network. The bridge can be enabled, disabled, added, or removed

[23] VMware, User's Manual, p 141.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

depending on the current work requirements. Microsoft considers increases in RAM and hard disk space as changes in the system and therefore requires reactivation.

The initial attempts to setup the virtual network were unsuccessful. This was caused primarily by headspace error. Once the virtual network was drawn out with the guest OS, virtual machine names and assigned IP addresses, the virtual network became functional. Drawing the virtual network before hand will greatly assist in the creation of the virtual network. A custom network switch is used for the internal virtual network, a host-only switch for communications between the host OS and the Windows XP Professional guest OS, and a bridge for communications between the Windows XP Professional guest OS and the Internet. Figure 2 – Initial Virtual Network, illustrates how the virtual network relates to a home network and the Internet. Initial testing of the virtual network consisted of pinging the various guest machines by both IP address and name. The attempts to ping the host OS failed due to the subnet masks and the use of a custom switch. This was a desirable result as the only virtual machine to communicate with the host OS is the Windows XP Professional guest.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

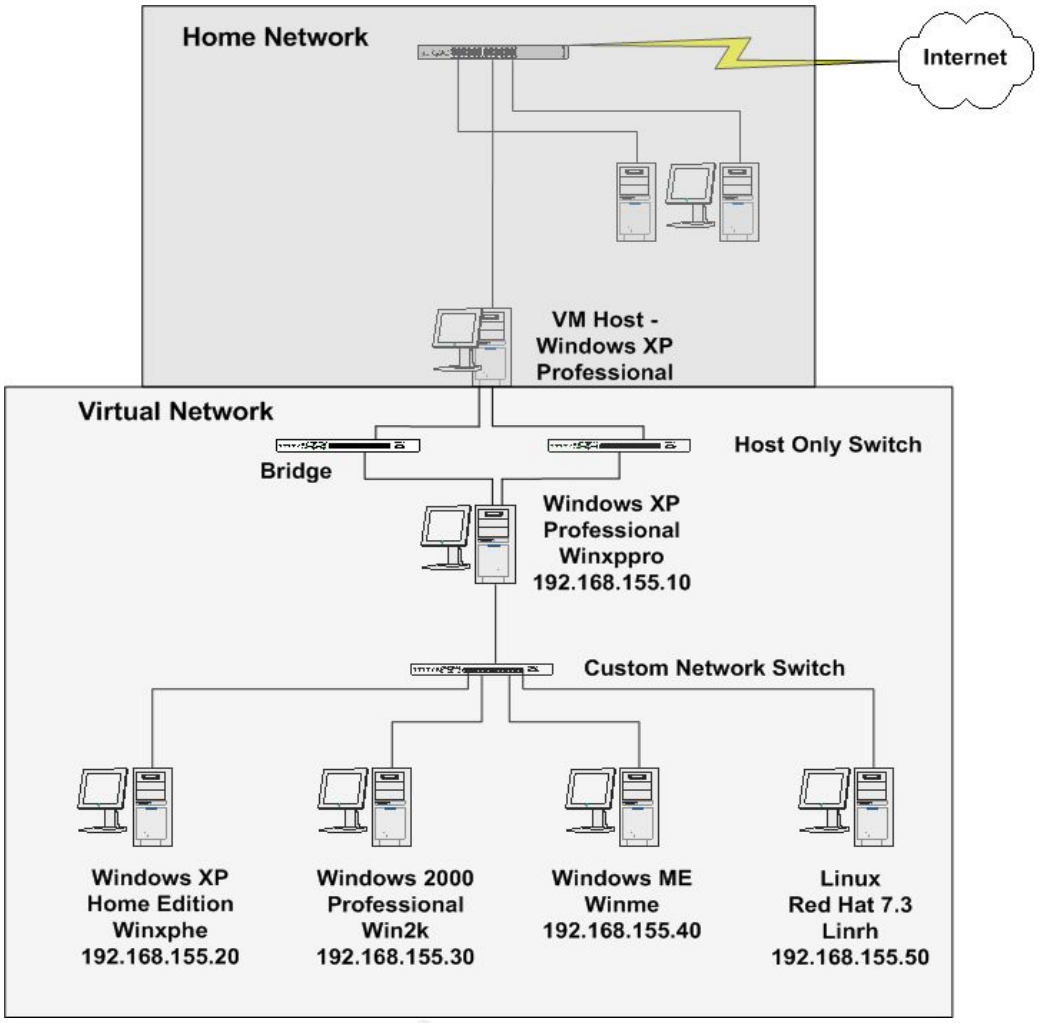


Figure 2 – Initial Virtual Network

The discussion thus far has been dealing with the reasoning behind a home lab, the estimated costs of three home lab configuration options, the comparison and the selection between two virtual machine software packages, and the installation and setup of a virtual network using VMware Workstation 3.2. The virtual machines can ping each other indicates that the virtual network works. The next step is to test the virtual network. This will be accomplished by using the exercises contained in SANS GIAC Certification: GSEC Security Essentials Toolkit as guidelines. The use of these exercises and tools will test the operation of the virtual network and guest OSs with an expectation of the virtual behaving similar to an actual network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Testing Virtual Network and Guest OSs

The SANS GIAC Certification: GSEC Security Essentials Toolkit covers the following areas, host-based intrusion detection, network-based intrusion detection, firewalls, scanning, exploits, denial of service and deception attacks, web security, and network security. These areas are important security concerns and are covered in depth in other SANS courses. The main reasons for testing the virtual network are to illustrate the use of virtual networks, to gather information on the characteristics of virtual networks, and to perform a limited comparison between a virtual network and an actual network. The initial virtual network shown in Figure 2 is simplistic in design. The network can be used to perform several areas of security testing. These areas include host-based intrusion detection, scanning, exploits, denial of service and deception attacks.

Once the initial virtual network was setup and operational, an observation was made that it lacked the desirability to emulate a real network connected to the Internet. The virtual network was then redesigned to include home users connected to the Internet and a defense in layer approach for a corporate network. The addition of the router and corporate firewall presents a slight problem. The host workstation does not have enough resources to run all the virtual machines at the same time. The constraining requirement is the required minimum amount of RAM. It is a personal preference to maintain at least 256 MB of RAM for the host OS. Table 7 – Total New Minimum Requirements, illustrates the new amount of resources needed for the complete network to operate is 1088 MB. Given the current configuration of the host workstation, the complete network cannot operate at one time. Solutions to the resource problem include only run portions of the networks at any given time, eliminate a guest OS, or reducing the RAM for each guest OS. The 64 MB of RAM for Linux operating systems is for text mode whereas a minimum of 128 MB of RAM is needed for Linux to operate in graphical mode which the Linux guest OSs are running. The Linux guest OS was eliminated from the primary redesign. When the Linux guest OS needs to be outside the firewall acting as a home user, then a home user guest OS or corporate guest OS can be turned off and the Linux guest OS turned on. Or, when the Linux guest OS need to be inside the firewall, then either a corporate guest OS or a home user guest OS can be turned off.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TABLE 7 – Total New Minimum Requirements

Operating System	Minimum Amount of RAM (Actual Amount)	Minimum Disk Space (Actual Space)
Windows XP Professional (Host OS)	128 MB (256 MB)	2 GB (4 GB)
Windows ME (Guest OS)	96 MB (96 MB)	2 GB (4 GB)
Windows 2000 Professional (Guest OS)	128 MB (128 MB)	2 GB (6 GB)
Windows XP Home Edition (Guest OS)	128 MB (128 MB)	2 GB (6 GB)
Windows XP Professional (Guest OS)	128 MB (128 MB)	2 GB (6 GB)
Red Hat Linux version 7.3 (Guest OS)	64 MB (128 MB)	2 GB (4 GB)
ORIGINAL TOTAL MINIMUM REQUIREMENTS	**672 MB (864 MB)**	**12 GB (30 GB)**
Red Hat Linux version 7.3 (Guest OS – Firewall)	64 MB (128 MB)	2 GB (2 GB)
Red Hat Linux version 7.3 (Guest OS – Router)	64 MB (96 MB)	2 GB (2 GB)
TOTAL REVISED MINIMUM REQUIREMENTS	**800 MB (1088 MB)**	**16 GB (34 GB)**

This redesign includes an office network with Windows XP Professional and Windows 2000 Professional client machines behind a corporate firewall and a home user network with Windows XP Home Edition and Windows ME. The two networks are connected to a router that emulates an Internet Service Provider (ISP). The router is configured to pass all network traffic with no filtering or blocking. As an afterthought, a bridge is used to connect the virtual router to the home network. This will assist in copying files between the home network and the guest OSs. Finally, a firewall is placed between the router and the office network. This configuration provides a more realistic scenario for analysis as Figure 3 – Virtual Network illustrates. The operating system, client name, IP address, and gateway(s) (GW) are shown for each virtual machine. The network interface card (NIC) names, eth0 and eth1 for the firewall and, eth0, eth1, and eth2 for the router are provided. The gateways and NIC are used to establish the routing tables used on the router, firewall, and client machines.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

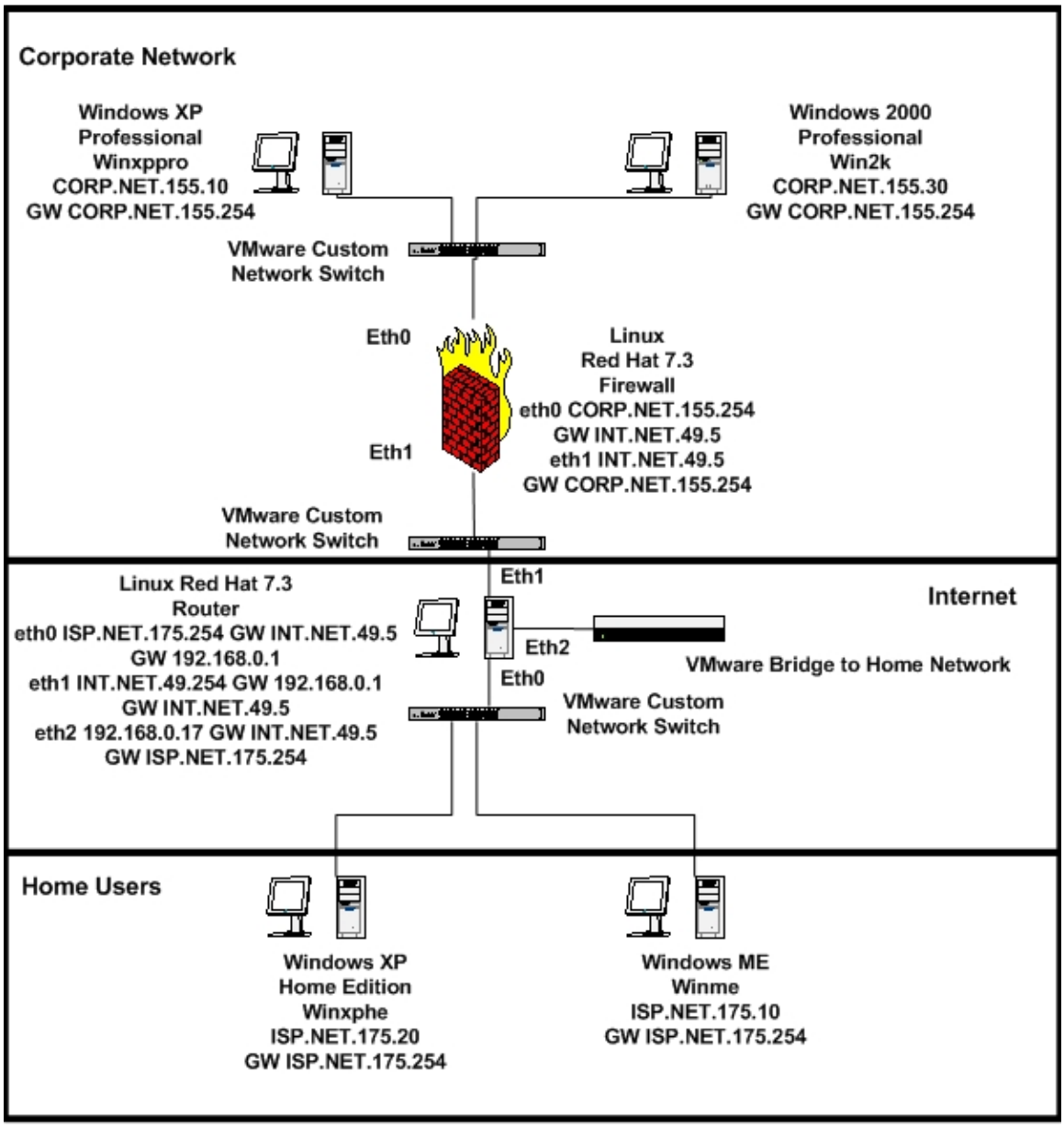


Figure 3 – Virtual Network

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After the redesigned network was created and verified that all machines on both the virtual network and the home network could communicate, a test was done to see what would happen if the original Linux guest OS was turned on. As expected, VMware gave an error message. This was one of the more memorable error messages received while testing the virtual network. Figure 4 – VMware Workstation Error, is nostalgic in that it states "… use the configuration editor to decrease the memory size of this virtual machine to 16 megabytes, …" When was the last time a PC could operate on only 16 MB of memory? PocketPC requires at least 32 MB of memory. Not to give away my age, but do you remember when 16 MB of memory was a lot of memory? Knowing that the virtual OSs are working, the virtual network is working, and all computers on both the home network and the virtual network are communicating with each other, the testing begins.

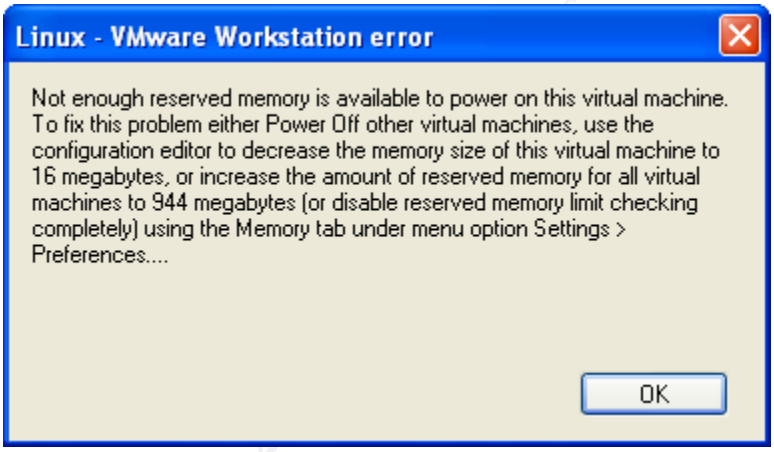


Figure 4 – VMware Workstation Error

Testing the Virtual Network Performance

The testing can be the most fun and yet the most frustrating. The fun part is trying different techniques and seeing the actual responses from the guest OSs. The frustration comes into play when a software package is loaded to implement a technique and finding out you need additional software packages installed in order for the software to either load or to work. Many of the techniques were originally written for Linux and/or Unix and are ported over to Windows that requires additional software packages to recompile and install. These obstacles can be overcome by installing the required software packages under Windows, by looking for and utilizing precompiled Windows distributions, or by switching to a Linux machine. The way this obstacle was overcome was to search for precompiled Windows distributions. There are a couple of reasons for taking this approach. First, my background and knowledge is in Windows OSs, thus I am

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

more comfortable using Windows based graphical interface including point and click. Yes, I may be a little lazy. Second, I do not have a complete and full grasp of the Linux OS. I am learning Linux, as evident with using a Linux firewall and router, and I do want to learn more about Linux. The Linux text mode is its strength and requires the knowledge and understanding that I have not yet grasped.

The initial tools used were Windows commands, ping, ipconfig, and tracert, and Linux commands, ping, ifconfig, and traceroute. These were essential in configuring the network interface cards of the virtual machines. Ipconfig and the Linux equivalent, ifconfig, provide the configuration information of the NIC. Without this information, it would be difficult in determining how the client was communicating with the network. Ping and tracert, and the Linux equivalent, ping and traceroute, were needed to determine if the virtual network was operational. When a machine could not be pinged, then tracert or traceroute was used to determine where the packets were being blocked. Several evening were occupied trying to get the ISP.NET.175.0 network to communicate with the INT.NET.49.0 network. The ISP.NET.175.0 and INT.NET.49.0 networks could ping the router but they could not ping the other network and router could ping both networks. Ping indicated that the INT.NET.49.0 network was unreachable from the ISP.NET.175.0 network. Tracert showed that the packets were reaching the router but the router could not reach the INT.NET.49.0 network. Therefore the problem was related to the router. After some additional research, it was found the IP forwarding is disabled by default and that it needs to be enabled at either a command prompt or in the system configuration file.

The first series of test performed was to test the working of the firewall under various configurations by performing trace routes and scanning the virtual networks. Several trace routes where performed to see how different configurations in the firewall would impact the communications from the home users network to the corporate network. The first trace route had the firewall open, the second has the firewall blocking ICMP traffic, and the third had all outside traffic blocked at the firewall. Output 1 – Trace Routes, illustrates the different responses under the three different firewall configurations. When the firewall is open, trace route will show each hop to the destination machine and will give the name of the machine. With ICMP packets blocked, the destination machine name is shown, the first hop is identified, and all other hop attempted timed out. Finally, will all outside traffic blocked, only the first hop is identified and all other attempted hops timed out.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Output 1 – Trace Routes

Tracing with firewall open.

```
Tracing route to WINXPPRO [CORP.NET.155.10] over a maximum of 30 hops:
  1     7 ms     4 ms     2 ms  ISP.NET.175.254
  2     1 ms     5 ms     3 ms  INT.NET.49.5
  3     2 ms     3 ms     5 ms  WINXPPRO [CORP.NET.155.10]

Trace complete.
```

Tracing with ICMP packets blocked at firewall.

```
Tracing route to WINXPPRO [CORP.NET.155.10] over a maximum of 30 hops
  1     1 ms     1 ms    <1 ms  ISP.NET.175.254
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  .     .        .        .        .      .     .
  .     .        .        .        .      .     .
  .     .        .        .        .      .     .
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Tracing with firewall blocking outside sources.

```
Tracing route to CORP.NET.155.10 over a maximum of 30 hops
  1     1 ms     1 ms    <1 ms  ISP.NET.175.254
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  .     .        .        .        .      .     .
  .     .        .        .        .      .     .
  .     .        .        .        .      .     .
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Two virtual network scans were preformed to test the firewall and the virtual network. There are many tools available that will automatically scan networks and identify whether a machine is on or reachable, identify which ports are open, and identify the operating system. The tool used was nmap. Nmap was used to scan the entire virtual network under two scenarios, no firewall blocking on the corporate network and firewall blocking of incoming traffic. The command entered for the two scans, -v –sS –oN scanXX –O CORP.NET.155.0/24 INT.NET.49.0/24 ISP.NET.175.0/24, are identical except for the –oN scanXX. The –oN command will print the results of the scan into a text file named scanXX. ScanXX is a user generated name. The XX is incremented with each scan in order to identify the scan. The other commands used were –v verbose mode gives more information about what is going on with the scan, -sS perform a TCP SYN scan by sending a SYN packet and wait for a response as if you are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

attempting a real connection, -oN print output to a file, –O performs fingerprinting of the targeted machine and finally the networks to scan[24]. Comments provided in the outputs are in bold and enclosed in **{ }**. Output 2 – No Firewall Blocking Scan is analyzed first and then Output 3 – Firewall Blocking Scan.

Some interesting results appear in the scans. First, it should be mentioned that the Microsoft Windows machines used the default install settings. No changes were made to the system configurations nor were the systems patched. This was done to see how the systems operate right out of the box. The corporate network machines have numerous ports opened that can be utilized for exploits from either inside or outside the firewall. Second, the version of the operating system is not identified. The vendor of the operating system is identified which is helpful information. If the version is necessary, then another tool can be used. Third, note that one of the home users machine is missing in the scans. The scans were performed from Windows XP Home Edition, with the IP address of ISP.NET.175.20. This makes sense as you are looking for information about other machines. There are other tools available to scan ports on the host machine. Finally, the Linux systems have a higher difficulty rating with the good luck message whereas the Windows systems have a lower difficulty rating with the message worthy challenge.

The second scan, Output 3 – Firewall Blocking Scan, is similar to the first scan. The major difference is the absence of the corporate network users along with the firewall interface to the internal corporate network. One interesting observation is that the difficulty ratings vary when like machines are compared between the two scans. The difficulty ratings message remains the same.

[24] Fyodor. Nmap network security scanner man page.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Output 2 – No Firewall Blocking Scan

```
# nmap (V. 3.00) scan initiated Mon Feb 03 22:59:26 2003 as: nmap -v -
sS -oN scan5 -O CORP.NET.155.0/24 INT.NET.49.0/24 ISP.NET.175.0/24
{  CORP.NET.155.0/24 – Corporate Network
   INT.NET.49.0/24 – Internet
   ISP.NET.175.0/24 – Home Users  }
 Interesting ports on WINXPPRO (CORP.NET.155.10): {Corporate Network}
(The 1587 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
17/tcp     open        qotd
19/tcp     open        chargen
25/tcp     open        smtp
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
1027/tcp   open        IIS
5000/tcp   open        UPnP
Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP  {Operating system in Windows XP Professional}

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=9291 (Worthy challenge)
IPID Sequence Generation: Incremental

Interesting ports on WIN2K (CORP.NET.155.30):  {Corporate Network}
(The 1592 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
1026/tcp   open        LSA-or-nterm
Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP  {Operating system is Windows 2000 Professional}
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=18887 (Worthy challenge)
IPID Sequence Generation: Incremental

Interesting ports on  (CORP.NET.155.254):  {Internal firewall
connection}
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
111/tcp    open        sunrpc
1024/tcp   open        kdm
6000/tcp   open        X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
Uptime 0.634 days (since Mon Feb 03 07:46:31 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4621174 (Good luck!)
IPID Sequence Generation: All zeros

Host   (INT.NET.49.0) seems to be a subnet broadcast address (returned
1 extra pings). Skipping host.
Interesting ports on  (INT.NET.49.5):  {External firewall connections}
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
1024/tcp   open        kdm
6000/tcp   open        X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
Uptime 0.634 days (since Mon Feb 03 07:46:31 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3329253 (Good luck!)
IPID Sequence Generation: All zeros

Interesting ports on  (INT.NET.49.254):  {Router connection going to
firewall}
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
1024/tcp   open        kdm
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
Uptime 0.635 days (since Mon Feb 03 07:46:09 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=2891165 (Good luck!)
IPID Sequence Generation: All zeros

Host   (INT.NET.49.255) seems to be a subnet broadcast address
(returned 1 extra pings). Skipping host.
Interesting ports on WINME (ISP.NET.175.10):  {Home user}
(The 1600 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn
Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP  {Operating system is Windows ME}
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=8352 (Worthy challenge)
IPID Sequence Generation: Incremental

Interesting ports on  (ISP.NET.175.254):  {Router connection going to
home users}
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
111/tcp    open        sunrpc
1024/tcp   open        kdm
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1332029 (Good luck!)
IPID Sequence Generation: All zeros

Host   (ISP.NET.175.255) seems to be a subnet broadcast address
(returned 1 extra pings). Skipping host.
# Nmap run completed at Mon Feb 03 23:00:31 2003 -- 768 IP addresses (7
hosts up) scanned in 65 seconds
```

Output 3 – Firewall Blocking Scan

```
 # nmap (V. 3.00) scan initiated Mon Feb 03 23:03:19 2003 as: nmap -v -
sS -oN scan6 -O CORP.NET.155.0/24 INT.NET.49.0/24 ISP.NET.175.0/24
{  CORP.NET.155.0/24 – Corporate Network
   INT.NET.49.0/24 – Internet
   ISP.NET.175.0/24 – Home Users  }
Host   (INT.NET.49.0) seems to be a subnet broadcast address (returned
1 extra pings). Skipping host.
Interesting ports on  (INT.NET.49.5):  {External firewall connections}
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
1024/tcp   open        kdm
6000/tcp   open        X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
Uptime 0.637 days (since Mon Feb 03 07:46:32 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3210259 (Good luck!)
IPID Sequence Generation: All zeros

Interesting ports on  (INT.NET.49.254):  {Router connection going to
firewall}
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
1024/tcp   open        kdm
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=2158057 (Good luck!)
IPID Sequence Generation: All zeros

Host   (INT.NET.49.255) seems to be a subnet broadcast address
(returned 1 extra pings). Skipping host.
Interesting ports on WINME (ISP.NET.175.10):  {Home user}
(The 1600 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP  {Operating system is Windows ME}
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=10883 (Worthy challenge)
IPID Sequence Generation: Incremental

Interesting ports on  (ISP.NET.175.254):  {Router connection going to
home users}
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
1024/tcp   open        kdm
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  {Operating
system is Linux Red Hat 7.3}
Uptime 0.637 days (since Mon Feb 03 07:46:09 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3445113 (Good luck!)
IPID Sequence Generation: All zeros

Host   (ISP.NET.175.255) seems to be a subnet broadcast address
(returned 1 extra pings). Skipping host.
# Nmap run completed at Mon Feb 03 23:04:07 2003 -- 768 IP addresses (4
hosts up) scanned in 48 seconds
```

Satisfied with the operations of the firewall, the next step was to determine the functionality of the virtual network. The statistics provided by nmap at the completion of the first scan shows that 768 IP addresses were scanned with 7 hosts up and identified in 65 seconds. The seven hosts identified are actual IP addresses grouped as follows; corporate users - CORP.NET.155.10 and CORP.NET.155.30; firewall - CORP.NET.155.254 and INT.NET.49.5; router INT.NET.49.254 and ISP.NET.175.245; and home user - ISP.NET.175.10. The number of TCP port scans on each IP address was 1,601 for a total of 11,207 ports. This indicates a minimum of 11,975 packets was transmitted over the virtual network in 65 seconds. The 11,975 packets consist of 768 packets sent to identify hosts that are up plus an additional 11,207 packets sent to identify open ports. Additional traffic analysis was done on the corporate network with ethereal. Ethereal captured the IP packets and summary statistics were generated. These statistics show that over an 94 second period, 4,071 packets were transmitted, consisting of 258,595 bytes of traffic. The average bytes per second were 2,748.99 or 0.022 MB per second and an average of 43.27 packets per second. This doesn't compare with actual 100 MB LAN connects in the real world. Yet, the response time was not expected to match the real world since this is in a virtual environment.

Observations

A lot of knowledge was obtained while creating this home lab. This knowledge includes: a better understand and appreciation for Linux; an understanding of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP/IP routing; an understanding of firewalls; and a better awareness of the types of tools, availability of tools, and the potential dangers of the tools used for exploiting systems. The lab is functional and useable as shown in the tests performed. There are a number of observations, both subtle and obvious, that are discussed next.

The major observation and tip is to read the manuals and research the areas that are being tested and/or incorporated in the virtual lab. An example of this was setting up the router between the home user group and the corporation network. Several evening were occupied trying to get the ISP.NET.175.0 network to communicate with the INT.NET.49.0 network. The ISP.NET.175.0 and INT.NET.49.0 networks could ping the router but they could not ping the other network and router could ping both networks. After researching the problem, it was found that the router IP forwarding had to be turned on either at a command prompt or in the system configuration file. Once IP forwarding was enabled, the two networks could communicate with each other.

Care must be taken when creating the VMware virtual network. When creating the virtual machine with multiple network cards, do not install all the network cards at one time. It is easier to install one network card and configure the card before adding additional cards. A problem occurred when two network cards where installed during the initial virtual guest operating system. It was difficult to determine the network connection for each card. Windows systems tend not to have this problem as the command ipconfig /all will indicate the virtual network switch. Linux system's ifconfig command will not indicate the virtual network switch. Several attempts to add multiple network cards resulted in the wrong configuration of the card. Since the original network was redesigned, it was found that with the Windows systems that were moved from one network to another the registry had to be edited to completely remove the network card from the pervious network.

The concept of virtual machines and virtual networks works. Actual OSs were installed on various guest machines and behaved as expected. The virtual network has most of the components of an actual network and has similar behavior as actual networks. The performance of the guest OSs and virtual network is dependent on the resources available on the host OS. The most critical resource needed for the virtual machines and virtual network is RAM memory. Each virtual machine reserves RAM memory located on the host machine and each OS needs a minimum amount of RAM memory to function. Any additional services that VMware Workstation 3.2 installs and enables that are not needed should be disabled to conserve resources. These services include a Dynamic Host Configuration Protocol DHCP server and a Network Address Translation (NAT) server.

The virtual network has limitations. All the virtual guest OSs and virtual network switches share the host's computer CPU and of course RAM memory. The

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

limitation was most evident when a denial of service (DOS) attack was performed on the home network. The targeted OS was Windows 98. During the attack, the system became very sluggish with CPU utilization at 100% and memory utilization level at 80%. A similar DOS attack was performed on the virtual network with the targeted guest OS being Windows ME. The guest OS become slow but not sluggish with the guest OS CPU utilization level at 78%, and memory utilization level at 50%. The virtual network test with ethereal also illustrated this with the low transfer rate of 0.022 MB per second.

Summary

Being new to the field of computer and network security, the thought and reasoning for having a home lab was intriguing. How a home lab should be designed was unknown. Therefore, the considerations, costs, and design of the home lab were explored. The actual space required for the home lab was a major factor in the design process. Realizing that, virtual machines software was investigated. Two software packages were considered, Virtual PC 5.0 and VMware Workstation 3.2. VMware Workstation 3.2 was selected based on the flexibility in creating a virtual network. The final virtual network consisted of a corporate user network separated from a virtual internet by a firewall and a home user network. The corporate users consisted of Windows XP Professional and Windows 2000 Professional virtual machines and the home users consisted of Windows ME and Windows XP Home Edition virtual machines. The corporate firewall and the router consisted of Linux Red Hat OS. A lot of knowledge was gained in routing, firewalls, and Linux. Tests of the virtual network shows that the virtual network is functional and performs as desired. The only lack of performance is due to the inherent limitations and limited resources, CPU and RAM memory, that are available for the virtual network. Everything has a trade off. Security has a trade off with risk. The virtual network has a trade off with physical space. Overall, the design and implementation of the home lab was successful.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

List of References

Ball, Bill, Pitts, David, et al. Red Hat Linux 7 Unleashed. Indianapolis: Sams, 2001.

Cole, Eric, Newfield, Mathew, and Millican, John M. SANS GIAC Certification: GSEC Security Essentials Toolkit. Indianapolis: Que Publishing, March 2002.

Fyodor. Nmap network security scanner man page. Insecure.Com LLC, 2002.

Miller, Michael Joseph. Linux for Windows Addicts: A 12-Step Program for Habitual Windows Users. New York: Osborne/McGraw-Hill, 2001.

Negus, Christopher. Red Hat Linux 8 Bible. Indianapolis: Wiley, 2002.

Nemeth, Evi, Snyder, Garth, and Hein, Trent R. with Boggs, Adam, Crosby, Matt, and McClain, Ned. Linux Administration Handbook. Upper Saddle River: Prentice Hall PTR, 2002.

SANS Institute. GIAC Certification – What It Is and How It Works. 2002.

Stevens, Richard W. TCP/IP Illustrated, Volume 1 The Protocols. New YorK: Addison Wesley, 1994.

User's Manual VMware Workstation Version 3.2. Plato Alto: VMware, Inc., 2002.

Virtual PC for Windows, Version 5.0, Users Guide. San Mateo: Connectix Corporation, July 2002.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.