

Designing and implementing an Information Security computer lab
that allows for student hands-on learning

Robert Benson

Lewis University, Romeoville, IL

Information Security Project 68-595-2

Dr. Ray Klump

August 28, 2006

Abstract

Lewis University has a computer lab with a limited amount of space, equipment, and technicians. This makes it impractical to frequently change the configuration of cables, computers, and other peripherals in the computer lab to allow students to experience hands-on learning. Designing and implementing a computer lab using software virtualization will allow instructors to teach courses in a variety of security topics such as ethical hacking, network security monitoring, intrusion detection, computer forensics, firewalls, cryptography, honeypots and server hardening without having to change the physical network topology of the computer lab.

Contents

i.	Abstract	page 2
ii.	Introduction	page 4
	a) Background of the problem	
	b) Problem Statement	
	c) Approach to correct the problem	
iii.	Literature Review	page 6
	a) Summary of relevant literature	
iv.	Procedure	
	a) Installation of VMware Server	page 11
	b) Installation of virtual machines	page 17
	c) Installation of VMWare Workstation 5.5	page 27
	d) "snapshot" feature	page 29
	e) Installation of VMWare PLayer	Page 35
v.	Results	
	a) Virtual appliances	Page 38
	b) Penguin Sleuth - Linux	Page 40
	c) Security Platform appliance	Page 45
	d) Endian Firewall appliance	Page 47
	e) Host requirements	Page 50
vi.	Conclusion	
	a) Recommendations for use	Page 54
vii.	References	Page 58

Introduction

At present, Lewis University offers students limited hands-on experience during computer courses. There is a limited amount of lab space, hardware and technical resources needed to create the necessary lab environments to cover a wide range of computer topics. Students need more hands-on access to a diverse network of different operating systems with a variety of network monitoring, forensic and security tools to learn about Information Security.

VMware provides software virtualization technology that will allow students to gain experience in computer technology and security. VMware Server will be installed on a computer in the lab and VMware Player will be installed on student workstations. Virtual machines will be created as needed for each class or assignment. In addition to virtual machines created in class, many security appliances with forensic, hacking and intrusion detection tools are already available and may be downloaded at no charge from the VMware website.

Another very powerful feature of VMWare Server is called "snapshot" which allows the virtual machine to revert back to a virtual machine's actual state which includes the server's disk and memory at the exact moment of the "snapshot". Only the VMWare Server software provides the 'snapshots' feature. This

feature can be very useful for settings such as a student-centered lab, because individual students can leave a project at the end of a lab period and return to it during the next class.

This paper serves as a blueprint for using VMWare Server in Lewis University's Information Security laboratories. It first describes what virtualization is, how it works, and where and how it is being deployed. It then documents and provides examples of the kinds of appliances that have been created to teach information security and protect existing systems. The paper then documents the installation and deployment process. The paper then returns to the security appliances mentioned earlier in the paper to discuss how they can be used in a lab setting. It is hoped that this paper will motivate the adoption of virtualization in Lewis's computer labs to increase the number of hands-on opportunities for students.

Literature Review

Software companies are experiencing rapid growth in virtualization technologies. The latest version of VMware virtualization software was released in July 2006. Microsoft is now offering its "Virtual Server R2" for free, Debian Linux provides "OpenVZ Virtualization Software" and SUSE Linux now provides "Xen" virtualization. Third-party software developers such as Surgient are marketing commercial virtual training lab management systems that provide students and developers self-service web access to schedule customized lab environments dynamically in collaboration with VMware's commercial ESX virtualization software [22]. Software virtualization provides the ability to create virtual training labs, and learning to apply this technology at Lewis University will greatly enhance the schools ability to provide students with a more hands-on learning environment.

This discussion is about creating a virtual training lab by implementing virtualization software applications, VMware Server and Player. VMware Server is installed on a Windows or Linux host machine and its functionality includes the ability to create new virtual machines or open existing virtual machines

that communicate with the host's physical network or as virtual machines that only communicate within an isolated virtual training lab network, configures the virtual machine settings, monitors performance of the host machine and makes snapshots of a virtual machine's actual state which may be reverted back to using the same utility. VMWare Player is installed on a Windows or Linux workstation. It is designed to run only one virtual machine which may be a downloaded virtual appliance from the VMWare website or a virtual machine created using VMWare Server.

References [1] through [21] provide an excellent introduction to software virtualization technology. VMWare provides an online database of supported VMWare guest operating systems, an administrator guide, documentation on API Programming, and virtual security appliances.

An example of a virtual appliance is the VMware appliance managed by Endian [9] and extensive documentation appears on the site for it. Endian firewall is not just a firewall appliance but a threat management appliance that improves firewall performance by responding to various types of attacks. This appliance is installed by extracting the appliance files to a folder and then opening the virtual machine using VMware Player or Server.

After the files are extracted using VMWare Server, the

following procedure can be followed to deploy the tool. With the VMWare server console open, select File >> Open. Then select the virtual machine using the browse button to locate the virtual machine. See Figure 1.

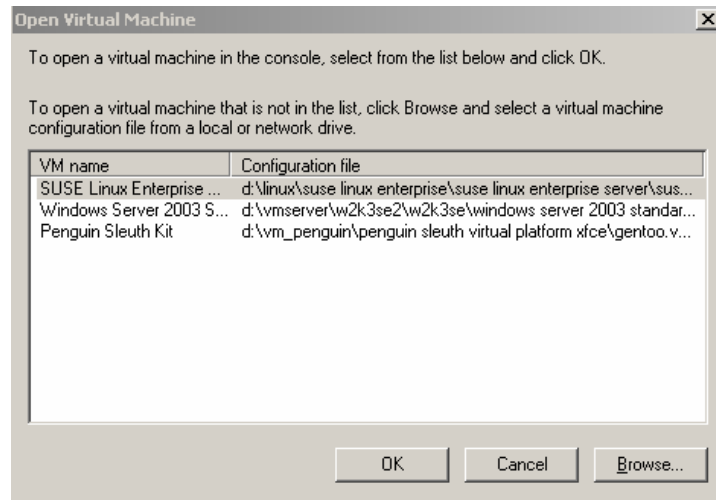


Figure 1: Selecting a virtual machine

After you select the virtual machine located in the folder where the files were extracted, you automatically get the VMWare console again with information about the "EFW_Community_2" appliance with a guest operating system of Red Hat Enterprise Linux 4 and a path to the location of the virtual machine configuration file. Click the green arrow and start the appliance. See Figure 2.

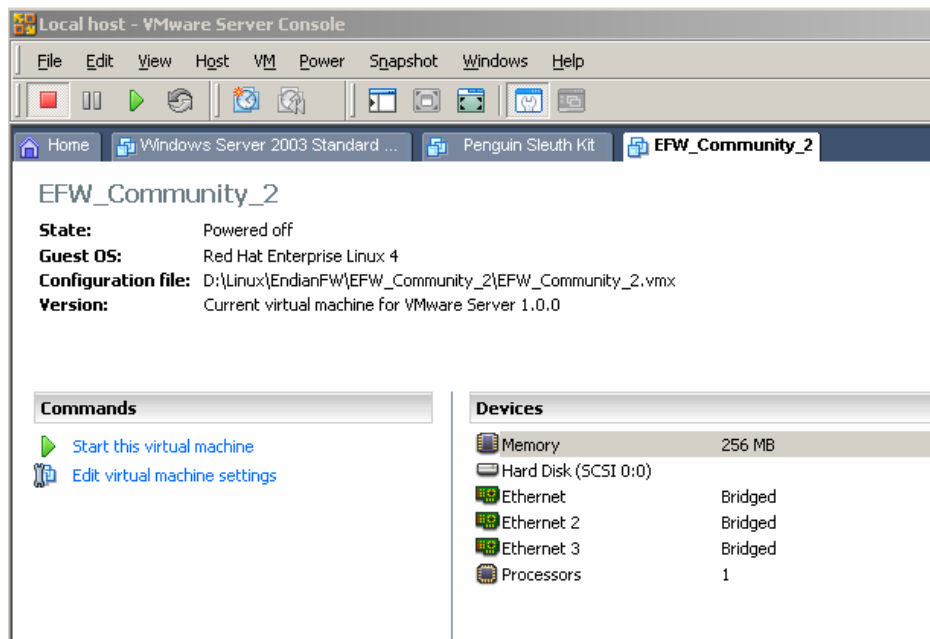


Figure 2: Starting the Endian appliance

Another security appliance program is Sguil, pronounced sgweel. It provides network security monitoring and IDS alert analysis. The Tao security company provides online documentation about their first Sguil virtual machine which is a self-contained Sguil deployment, with sensor, server, database, and client [17].

The VMWare website lists and provides documentation on a virtual machine called the Penguin Sleuth Kit Virtual Computer Forensics and Security Platform [18]. This virtual appliance has many forensic applications installed and is designed for professionals and students wanting to learn computer forensics.

Another security-related virtual machine appliance is

available on the VMWare website for hacking and networking security usage and training [19]. The hacking and networking security virtual machine includes many hacking and network tools and some of the tools have been installed but require configuration. This virtual machine comes with a collection of tools to help students with studying and refining their ethical hacking techniques.

The VMWare website includes an open source Ubuntu Linux distribution designed to provide secure Internet browsing that uses a Firefox web browser. It prevents most adware, spyware and malware by leveraging the virtual machine's isolation capabilities to prevent downloaded malware from propagating to the host computer, and the appliance is configured to reset after each use so no personal information is stored on the appliance. All the necessary documentation for this appliance is located online [20].

There are many security related appliances that may be run as a virtual guest machine using the VMWare Player or Server software. There are appliances in the security category that may be downloaded from the VWware website [7].

Deploying VMWare Server

The VMWare server software may be downloaded from the VMware web site after registering for a free license [2]. The vendor provides online documentation for this software [4]. This software installs on either a Linux or Windows operating systems. VMWare Server version 1.0 released 7/10/06 with a build number of 28343, was used for this research and testing. The open-source software included 100 Windows hosts and 100 Linux hosts licenses. Most of this research has been performed on the Windows version of VMWare Server, and so the paper will focus on this version of the product.

Installing VMWare Server is a simple process. The process begins with the dialog shown in Figure 3. Click the next button to begin the install process on any supported host operating system. The supported host operating systems are Windows 2000 Server and Advance Server SP3 and SP4, Windows 2003 versions of Standard Edition, Enterprise Edition and Web Editions Service Pack 1. A complete list of Windows Server 32-bit and 64-bit host operating systems is listed online [4]. A wide range of processors are supported. Compatible processors include Intel Pentium, Pentium II, Pentium III, Pentium 4, Pentium M Xeon, BM64T, AMD Athlon, Athlon MP, Athlon XP, AMD Opteron, AMD Athlon 64, Turion 64. Dual-core processors are also supported [4].



Figure 3: Introductory dialog during installation

The minimum hardware requirements for the host should be based on the anticipated usage of the server. The maximum memory that may be used concurrently by virtual machines is 4 GB if the operating system is using Windows without Physical Address Extensions (PAE) enabled [21]. The amount of memory supported on Windows hosts with PAE enabled is 64 GB [4]. The recommended memory for a virtual machine server is 384 MB. You may change the assigned amount of memory, but be warned that if you assign a lower amount than needed, the virtual machine will start using virtual memory swapping, which will slow performance considerably. Additional disk space is required for each virtual machine. The additional physical disk space for each virtual machine should equal the actual amount that would be used if it were a separate physical server. Any network interface card that

is supported by the virtual host can be used, and a static IP address is preferred [4].

The next dialog that appears during the setup is the end-user license agreement, which is shown in Figure 4. Read and accept licensing agreement and click the next button.



Figure 4: End-user license agreement during installation

It is recommended that the physical disk or logical raid volume of the computer be partitioned before the software install. There should be a C partition for the default VMWare software install and at least two additional primary partitions. The additional partitions may have drive letters D and E and should have volume labels that reference the type of virtual machines that will be created and stored on this disk space. Select custom install and verify the components that get installed on the host. The physical disk space needed for a

Windows host server is 250 MB for VMware Server, VMware Management Interface, VmPerl API, VmCOM API, Programming API, and VMware Server Console installation [5]. Figure 5 shows a list of the modules which can be included. Click the next button and the software is ready to be installed.

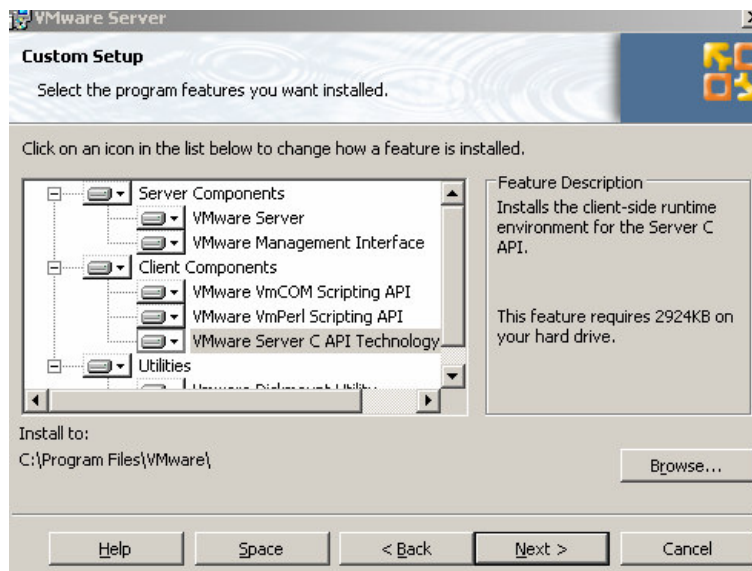


Figure 5: Selecting program features

Figures 6 through 9 illustrate the remainder of the installation process. As you can see, installing VMware Server on a Windows machine is a rather straightforward process.

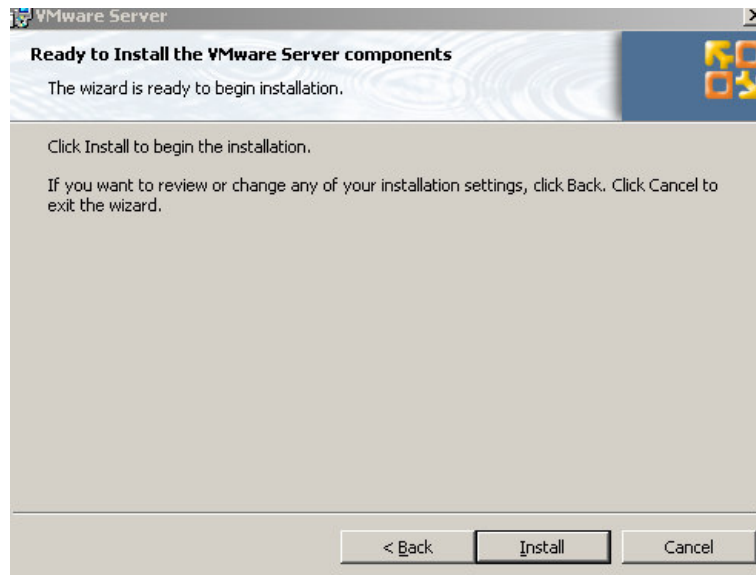


Figure 6: Final screen before installation

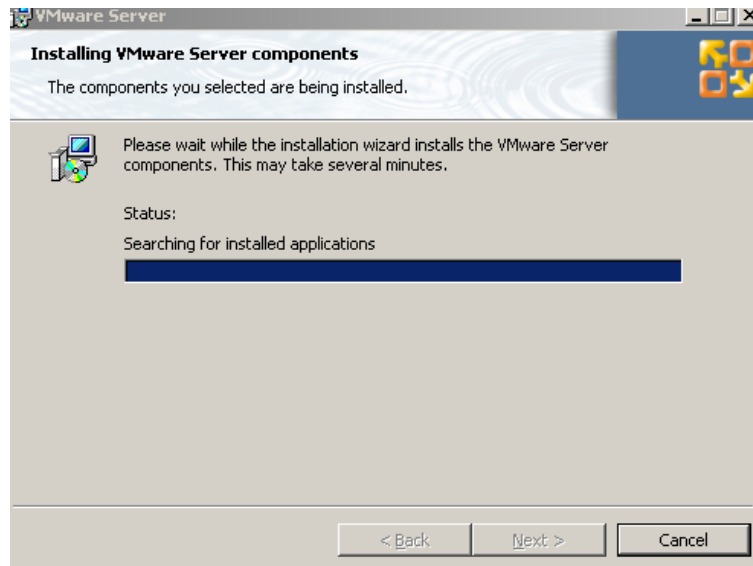
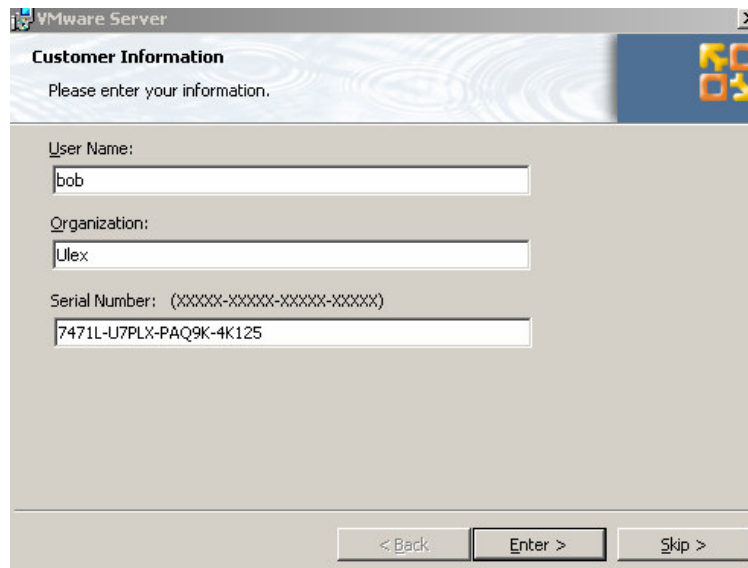


Figure 7: Installation progress



The screenshot shows a window titled "VMware Server" with a "Customer Information" header. Below the header, it says "Please enter your information." There are three input fields: "User Name:" with the text "bob", "Organization:" with the text "Ulex", and "Serial Number: (XXXXX-XXXXX-XXXXX-XXXXX)" with the text "7471L-U7PLX-PAQ9K-4K125". At the bottom, there are three buttons: "< Back", "Enter >", and "Skip >".

Figure 8: Providing registration information



Figure 9: Finishing installation

After installing the VMware Server software, a virtual machine may be created as new virtual machine or opened as an existing virtual one. A virtual machine is a guest of the host operating system. VMware supports both 32-bit and 64-bit guests. The guest operating systems supported are listed online and

include Linux, Windows, FreeBSD, Sun Solaris, and Novell [4]. The virtual machines always have the same hardware drivers as shown online and they do not require any configuration [4].

The process of creating a new virtual machine starts within the VMWare Server Console. Figure 10 is a screen shot of the opened console showing the option to create a “New Virtual Machine” or “Open Existing Virtual Machine”.

VMware Server Console

Connected to Local host running VMware Server 1.0.0

The VMware Server Console lets you connect to virtual machines that run on VMware Server systems. Each virtual machine is equivalent to a physical server with storage, networking, memory and devices. The VMware Server Console gives you full control over virtual machines, including keyboard, video and mouse interactivity.

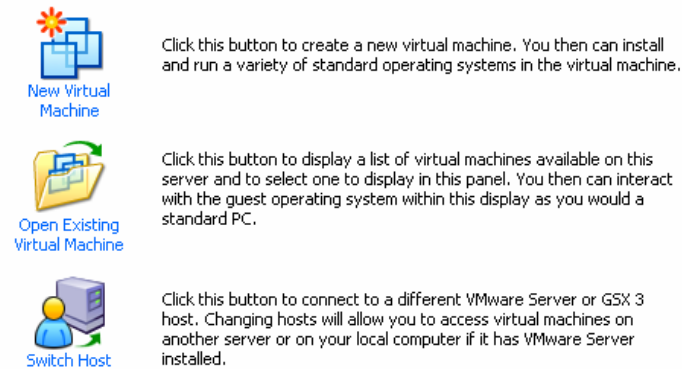


Figure 10: Opening a virtual machine

The next dialog box, which is shown in Figure 11, will request if this is a typical virtual machine configuration or custom configuration. The typical machine configuration setting was used for this research and testing.

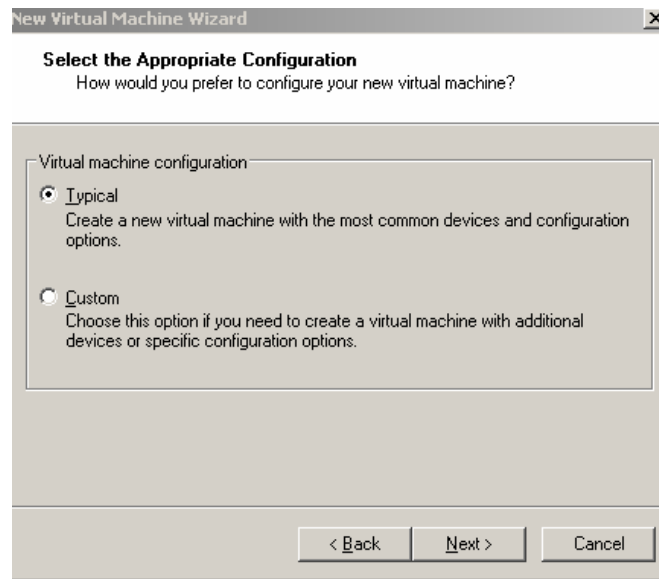


Figure 11: Selecting a configuration

The next screen shot is of the dialog box requesting input on what type of guest operating system and version will be installed on the virtual machine. The guest Windows and Linux machines that are supported are listed by VMware online documentation [13]. Most Windows 32-bit and 64-bit workstations and servers may be virtual machine guests. However, only certain service pack levels are supported. VMware Player and Server also support non-Windows virtual machines with operating systems including 32-bit Novell Netware, 32-bit and 64-bit Linux systems, 32-bit and 64-bit FreeBSD systems and 32-bit and 64-bit Sun Solaris systems. The dialog shown in Figure 12 illustrates selecting the guest operating system.

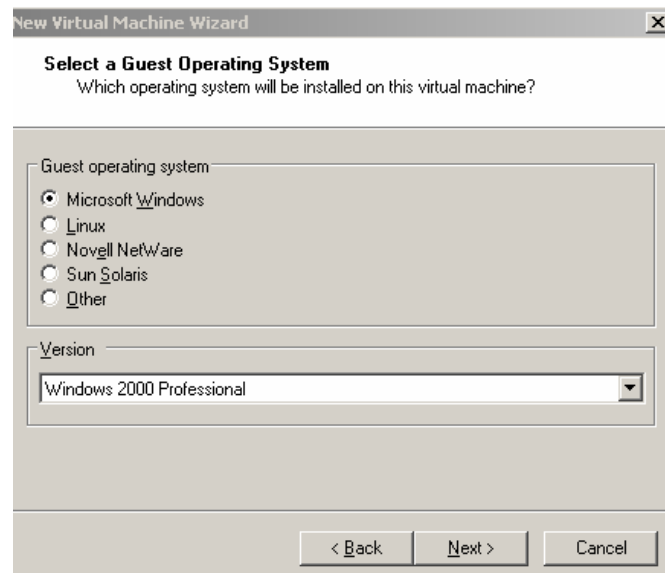


Figure 12: Selecting the guest operating system

The next dialog, which is shown in Figure 13, requests the location where the virtual machine will be created. The actual virtual machine is stored as a set of files [5]. These files are not encrypted and file access controls should be implemented to protect file integrity and confidentiality. The Lewis University governance board should make decisions on the availability of the repository data to students and faculty. The role each unit of the Information Technology Service Organization will have in maintaining the file system needs to be documented and adopted into a policy. If students need access to the files remotely for on-line courses then security safeguards in authentication, authorization, auditing controls and procedures need to be implemented. University policy should outline the design and implementation of a hierarchical file structure which will allow

for the delegation of administration duties by units of the Information Technology Service Organization at Lewis University. The file structure should also be designed to allow for role-based access controls by granting file access permissions to groups and then adding and removing individuals from the groups as their job responsibilities change. Students may be added to groups that have access to network shares for a particular course. Group memberships should be regularly updated to remove unauthorized accounts. Applying auditing controls to monitor the files and folders that users successfully and unsuccessfully access and reviewing the log files by the system administrators would be highly recommended.

The vmx file stores configuration information about the hard disks, networking, printing, available devices etc. The vmdk files store all the data and system files that are within your virtual machine. The nvram file performs the same function as the BIOS on a physical computer. The entire virtual machine is stored in these files. This allows you to move a virtual machine from one location to another. Usually the files are zipped up together and unpacked when needed. Virtual machines should be located on a separate partition or disk drive in a hierarchical directory structure which is necessary to keep the virtual machines organized for file and disk maintenance. This

is important because you often need to determine where the files are stored for a particular virtual machine. When creating a virtual machine you need to specify the guest operating system and version, virtual machine name and location where the files will be stored.

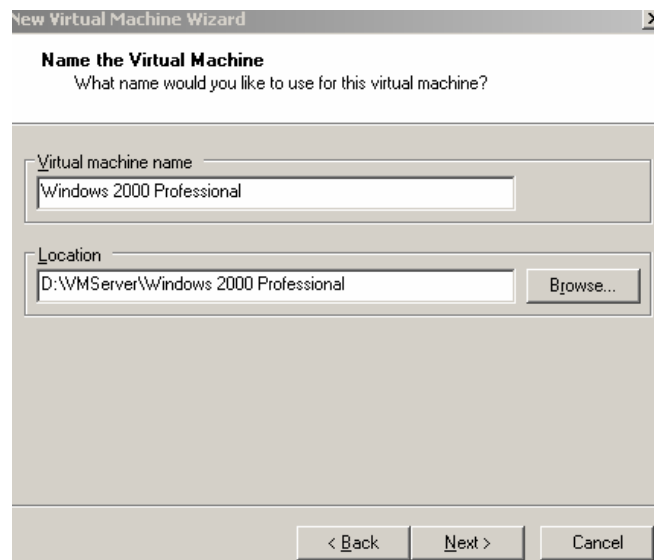


Figure 13: Identifying and locating the virtual machine

VMware Server has a utility "Manage Virtual networks" within the programs/vmware/vmware servers group. This utility allows the user to change the VMWare network configuration from the default settings. This functionality enables customized configuration that may allow the software to create multiple local-host and bridged networks that may be routable like a physical local area network. VMWare of Palo Alto, California, has identified and corrected vulnerabilities in their software that allow guest virtual machines to attack local host machines

and has recommended applying software patches as needed. One such vulnerability involved the NAT feature which allowed the guest machine to execute unwanted code on the host machine [23]. Host operating systems with routing and firewall software may also be implemented as virtual machines with multiple bridged and host-only network adapters. Figure 14 provides a screen shot of the Virtual Network Editor.

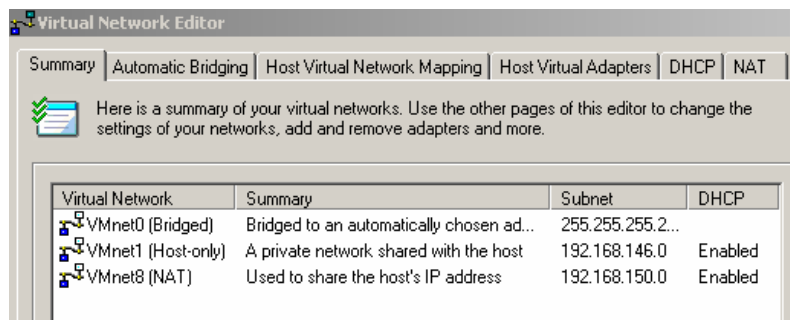


Figure 14: The Virtual Network Editor

The subsequent dialog, shown in Figure 15, requests the type of network connection the virtual machine should use. To set the VMWare network configuration, you need to understand the meaning of a number of terms [11]. The bridged network adapter describes the mechanism through which a virtual machine's IP address is bridged to the host's physical network adapter on the same Ethernet network. The host-only adapter setting may be categorized as the host-only adapter labeled VMnet1 by default. Host-only adapters do not have access to the physical network of the host. They show up in the Ethernet configuration settings of

the virtual machine as a “private network shared with the host” which means the virtual machine can only communicate with other virtual machines using the same default VMnet1 virtual network. The VMnet1 host-only network is an isolated virtual network that uses the TCP/IP protocol and an internal dynamic host configuration protocol (DHCP) service to assign IP addresses to each virtual machine. Finally, the host-only adapter VMnet8 settings allow access to the physical network indirectly using network address translation, NAT and enable the virtual machine to share the host’s IP address. This is primarily used when the virtual machines require access to the Internet or external network using the host’s IP address.

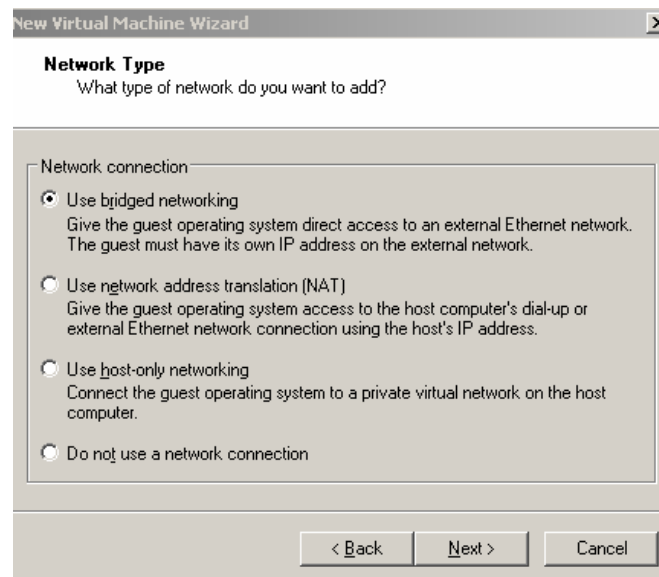


Figure 15: Selecting the type of network

The next setting controls the disk capacity the virtual machine will use. Figure 16 shows how to set this parameter.

When a virtual machine is created, there are options to specify disk space as either a fixed pre-allocated amount or a dynamic disk size that grows until a specified size limit. The fixed pre-allocated disk size may improve performance due to less disk fragmentation. The virtual dynamic disk space may be selected which allows the virtual disk space to grow as needed. You can also check the box to split the virtual disk into 2 GB files. It is recommended to use the virtual disk with dynamic growth which is the default setting [10]. It does not take up as much disk space and performance is acceptable. Choosing to split the disk into 2 GB files makes the files easier to manage due to the fact the file sizes are smaller. After the virtual machine is created, the operating system will be installed as if it were an installation on a physical computer. The dialog in Figure 16 confirms the allocation of the specified disk space to the new virtual machine. Various properties of the configuration may be changed by clicking the "Edit virtual machine settings" link as shown in figure 17.

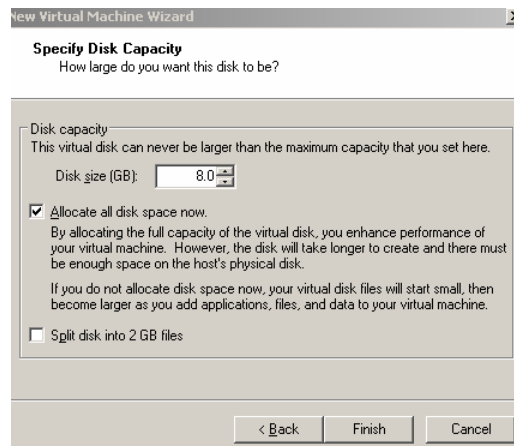


Figure 16: Setting disk capacity

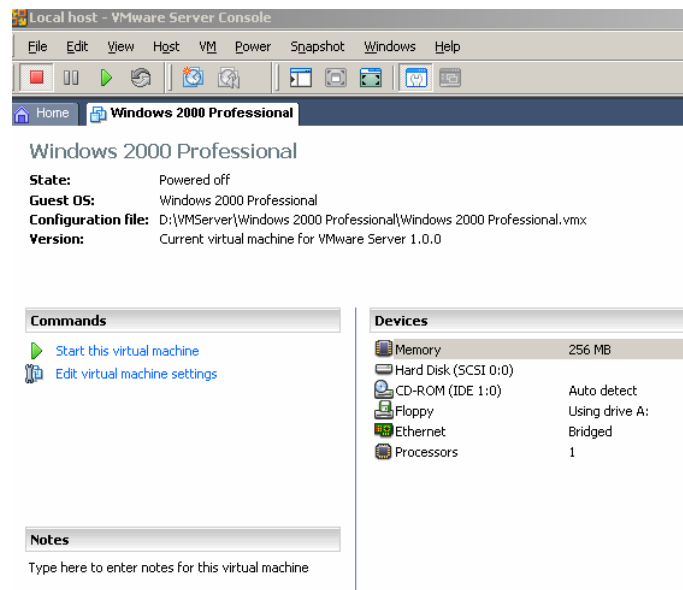


Figure 17: Edit virtual machine settings

The Virtual machine is now ready to be installed. The CD-ROM needs to be connected to the virtual machine to enable it to install the operating system from a CD or an ISO file. Figure 18 shows the properties that may be changed. If this is an ISO install, copy the ISO file to the drive of the host machine and select "Use ISO Image" and then browse to the location of the

file. When a virtual machine is not using a CD-ROM drive it should be disconnected to improve the performance of the virtual machine.

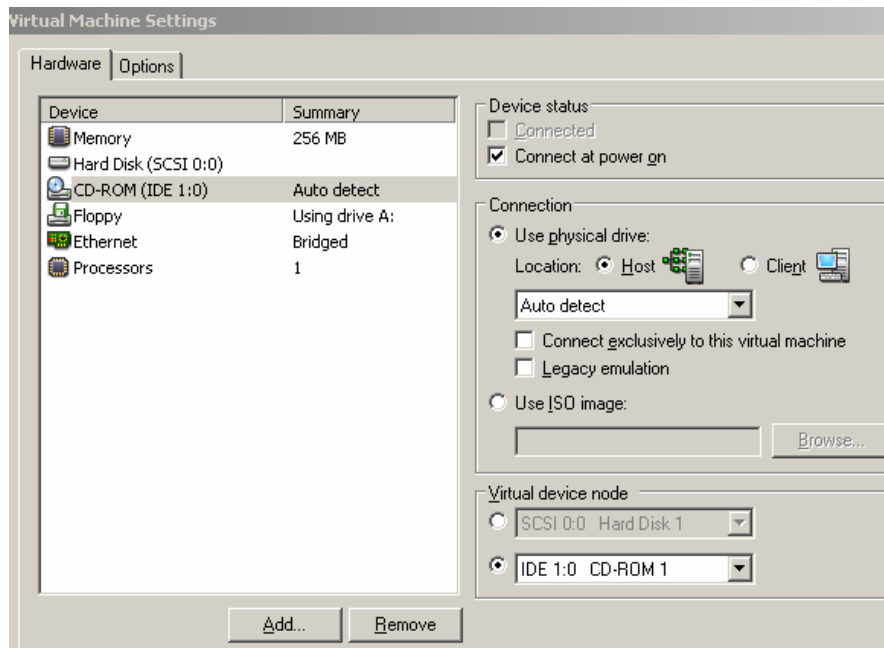


Figure 18: Identifying the OS source

When the green start arrow is pressed, as shown on figure 17, the system will start the install from an ISO file. Figure 19 shows a Fedora operating system being installed on a virtual machine from a standard Fedora ISO file.

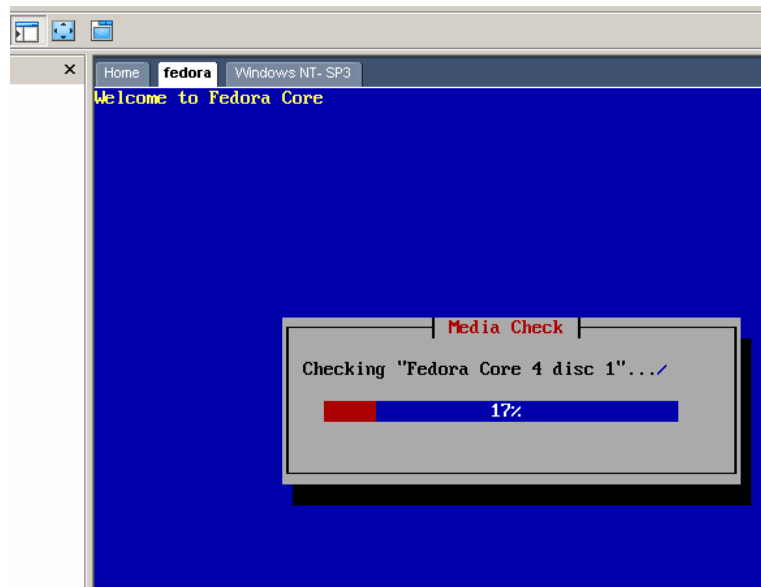


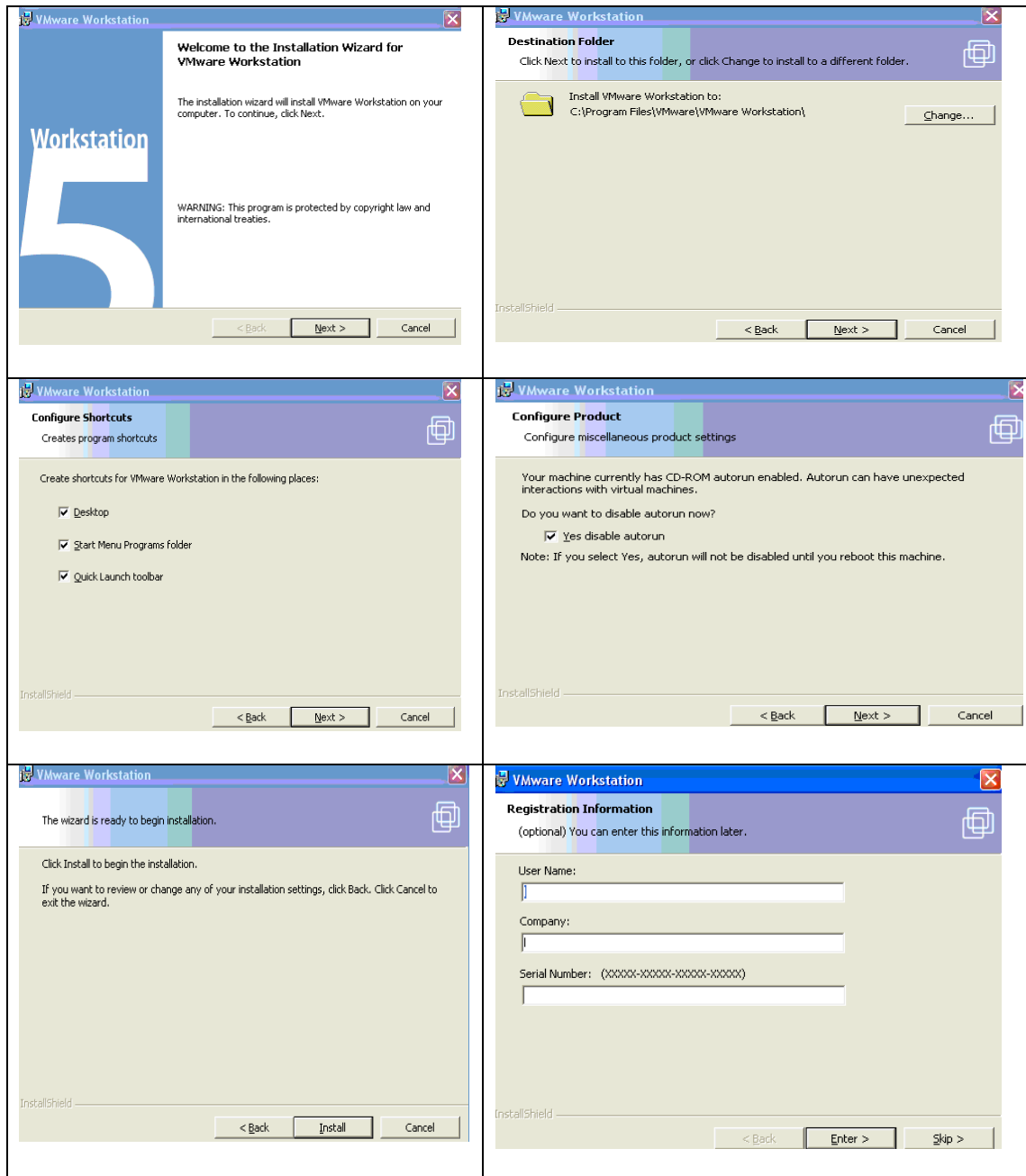
Figure 19: Installation of Fedora OS

Installing VMWare Workstation 5.5

VMWare Workstation 5.5 is a commercial product that installs on both a Linux or Windows operating systems. It installs on both Windows client and server host systems. This software runs guest operating systems of both Windows client and server editions, downloadable appliances and Linux guest operating systems. This software also creates virtual machines using the same steps demonstrated using VMWare Server. VMWare Workstation 5.5 includes the Snapshot Manager which will be demonstrated after a review of the installation procedure. VMware offers a 30 day evaluation copy of this software and provides online documentation at their website [24].

The following is a brief overview of the install process of VMWare Workstation 5.5 which is very similar to installing

VMWare Server. Creating virtual machines and opening downloaded appliances is also accomplished using the same steps used by VMWare Server. The following Figure 20 provides an overview of the install steps. Accept the default settings for installing the software.



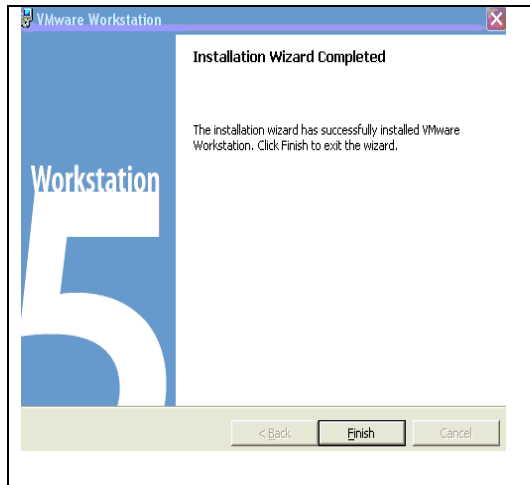


Figure 20: Installing VMWare Workstation 5.5

SNAPSHOT AND SNAPSHOT MANAGER

Figure 21 and 22 demonstrate the configuration of the snapshot feature using VMWare Server. The snapshot feature may be implemented with the automatic settings shown or manually using the Virtual Machine Console. A manual snapshot may be created of a virtual machine. The snapshot feature is located on the Virtual Machine Console as shown in Figure 22.

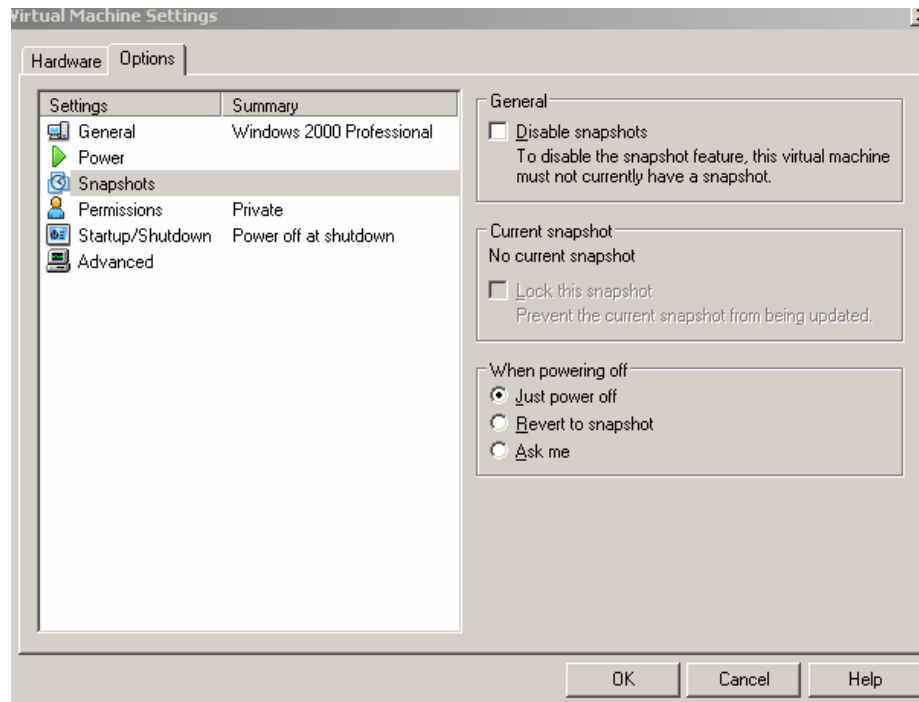


Figure 21: Setting up the Snapshot feature

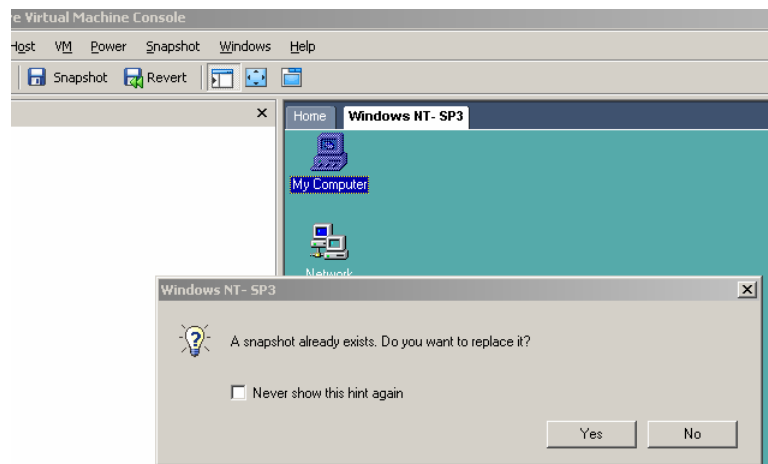


Figure 22: Snapshot feature on the Virtual Machine Console

Snapshots are an interesting and valuable concept. Virtual machines may be reverted back to a virtual machine's actual state which includes the virtual machine's disk and memory at the exact time when the snapshot was created. A screen shot of a

reverted snapshot is shown by figure 23.

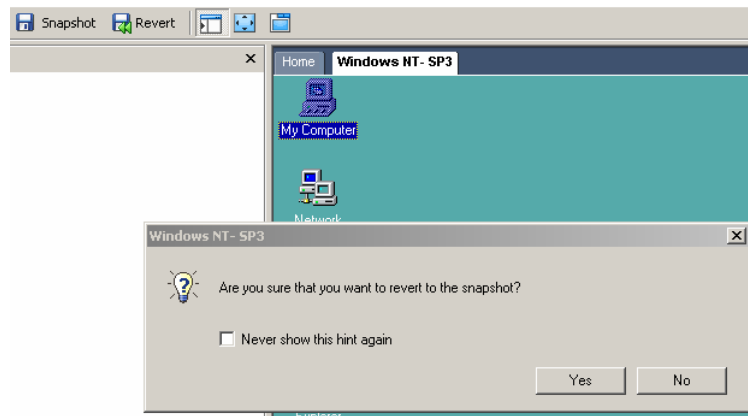
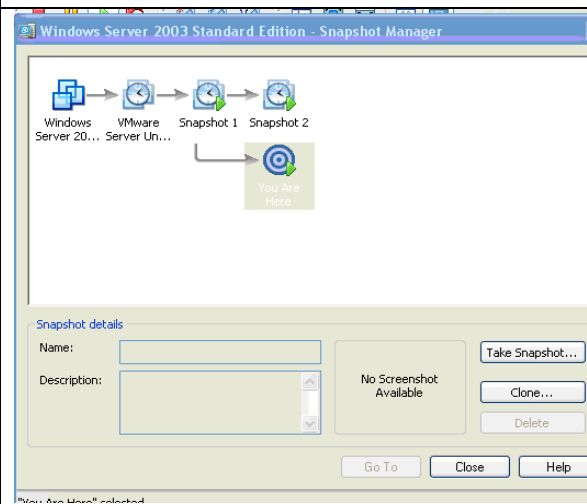
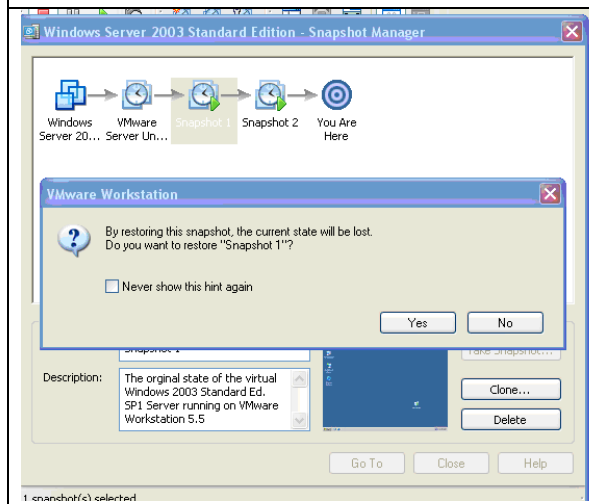
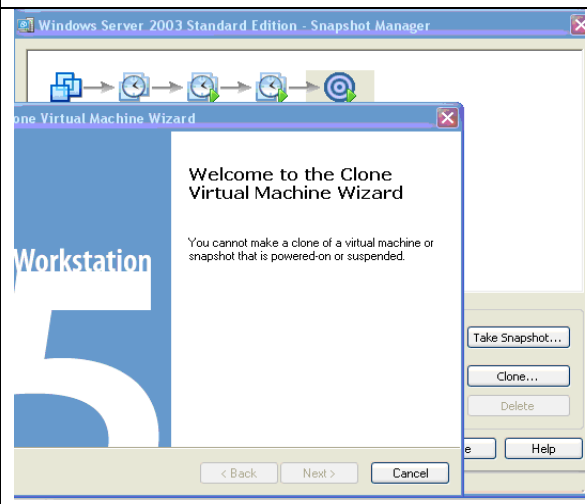
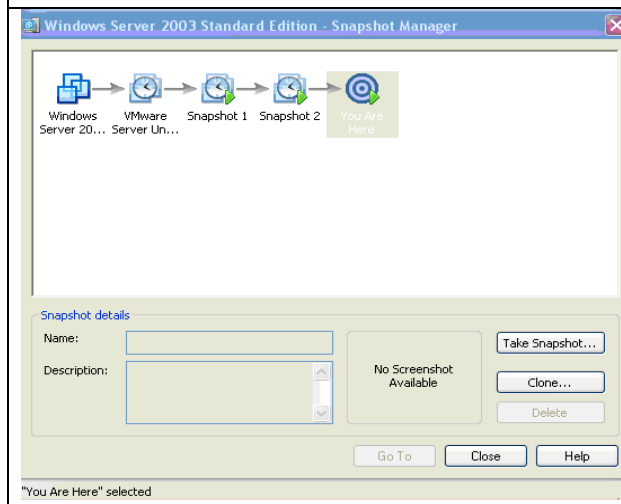
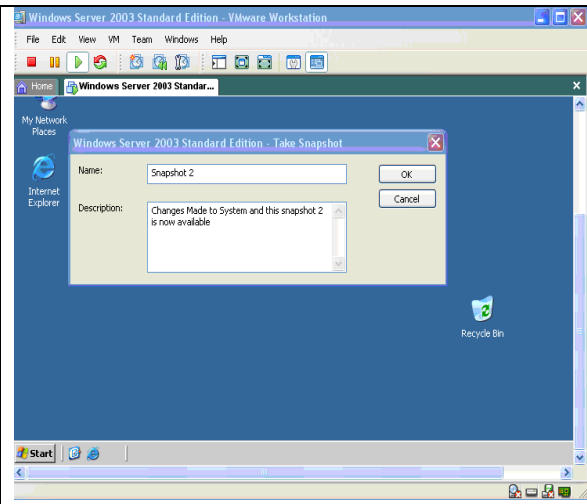
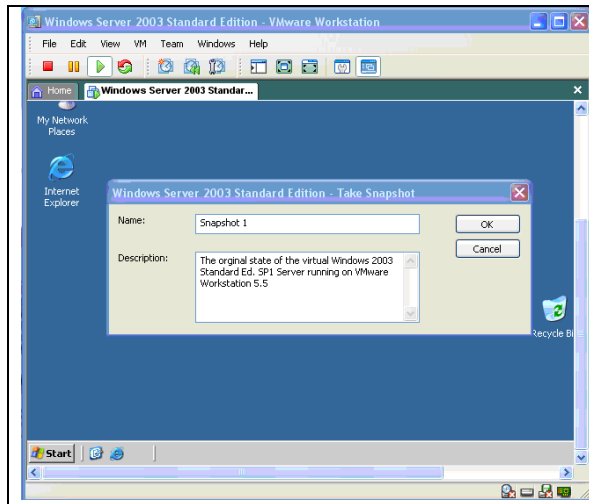
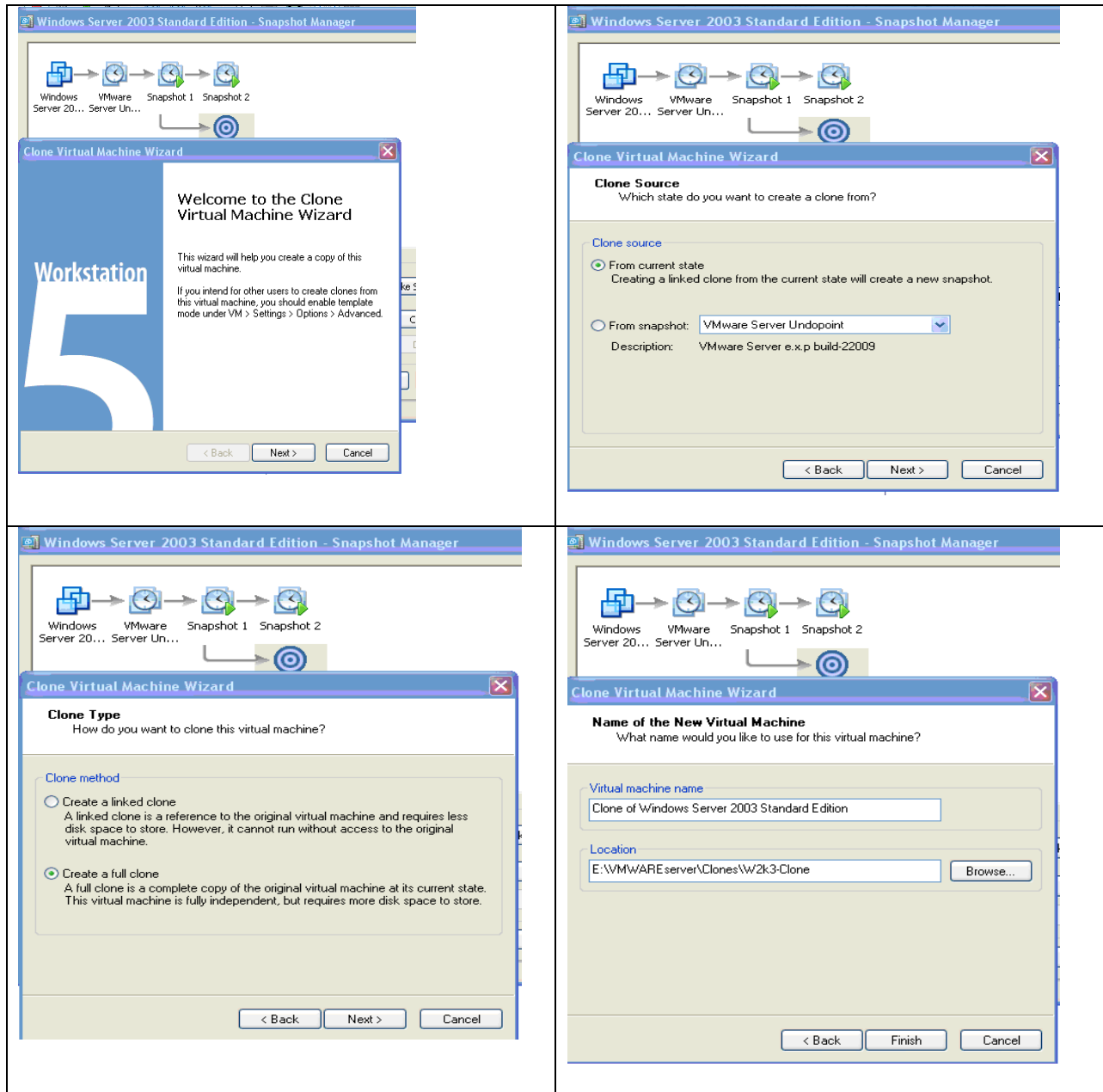


Figure 23: Reverting to a snapshot

The commercial version of VMWare Workstation 5.5 includes a “snapshot manager” feature that tracks the snapshots and shows what snapshot is in use and has the capability of navigating back several versions of a virtual machine. Workstation 5.5, would be able to snapshot a virtual machine at each lesson and clone a virtual machine for future use [24].

Figure 24 illustrates how the snapshot manager allows easy navigation between snapshots and creating clones that may be later opened using VMWare Workstation 5.5.





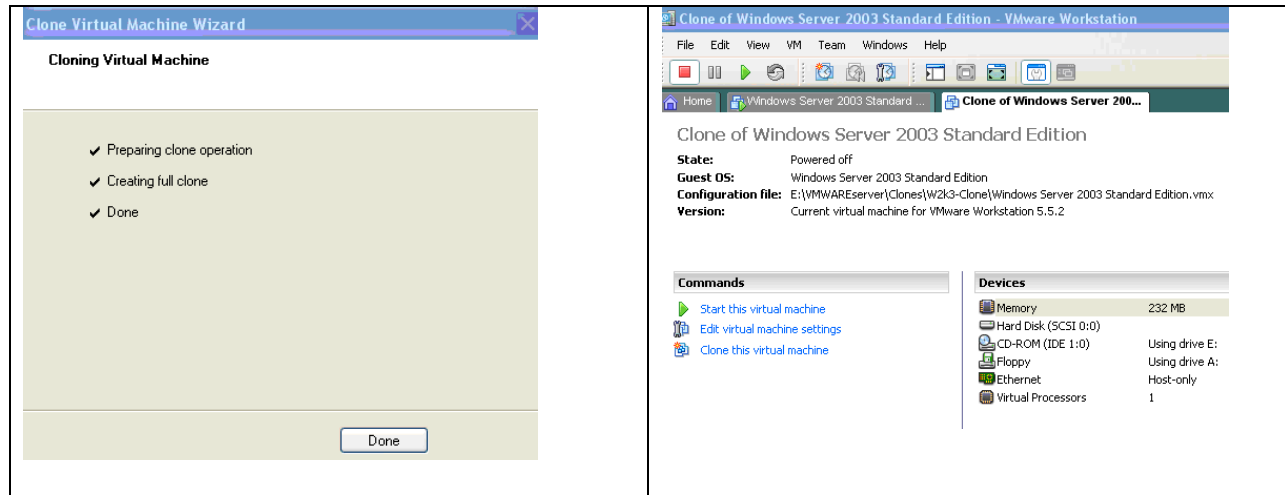


Figure 24: Illustrating the use of the Snapshot Manager

Installation of VMWare Player

VMWare Player 1.0.2 released on 8/10/2006 with Build 29634 was installed for this research and testing. VMWare provides online documentation for the product [13]. The software was installed on a Windows XP professional SP2 computer with 768 MB of RAM. The following are screen shots of the install.

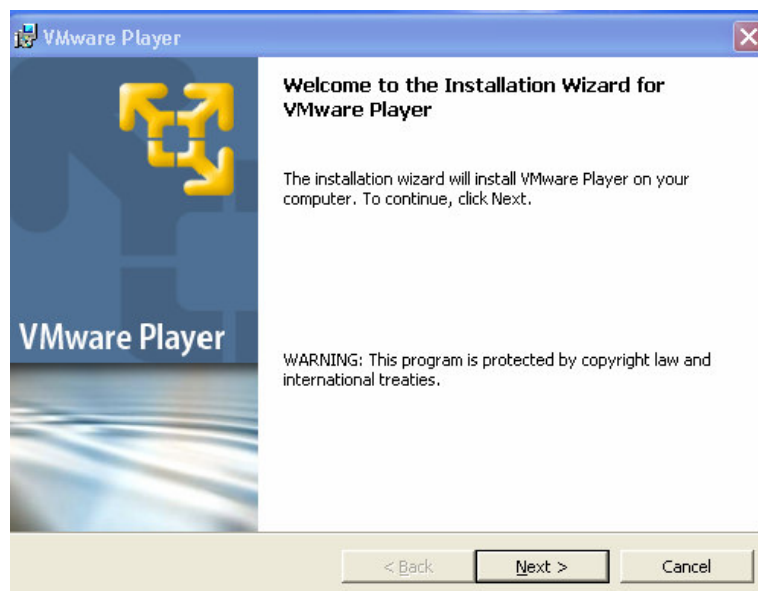


Figure 25: Start of VMWare Player installation

This application may be installed on both Windows workstations and servers. Supported workstations are 32-bit and 64-bit system Windows 2000 professional SP3 and SP4, Windows XP Home Edition SP1 and SP2, Windows XP Professional SP1 and SP2. Internet Explorer version 4.0 or higher must also be installed. The vendor recommends a minimum amount of 128 MB of memory and a recommended amount of 256 MB [13]. Performance was very slow when the test computer for this research was equipped with 512

MB of RAM. Click next as shown on Figure 25 to continue the install.

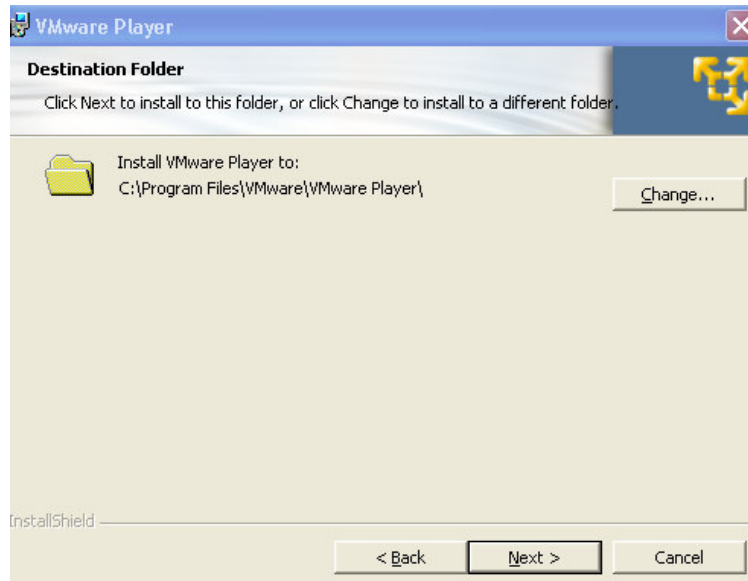


Figure 25: Locating the VMWare Player

The hard disk must have a minimum of 1 GB of free space for each guest operating system. The VMWare Player software requires approximately 150 MB of disk space. Accept the default software install location. Virtual machines should be created and stored on a separate disk partition. The virtual machine files should be located in folders referencing the name of the actual virtual machine to make it easier to maintain the file system and repair a virtual machine if necessary. Click the next button as shown in Figures 25 and 26 to continue the install.

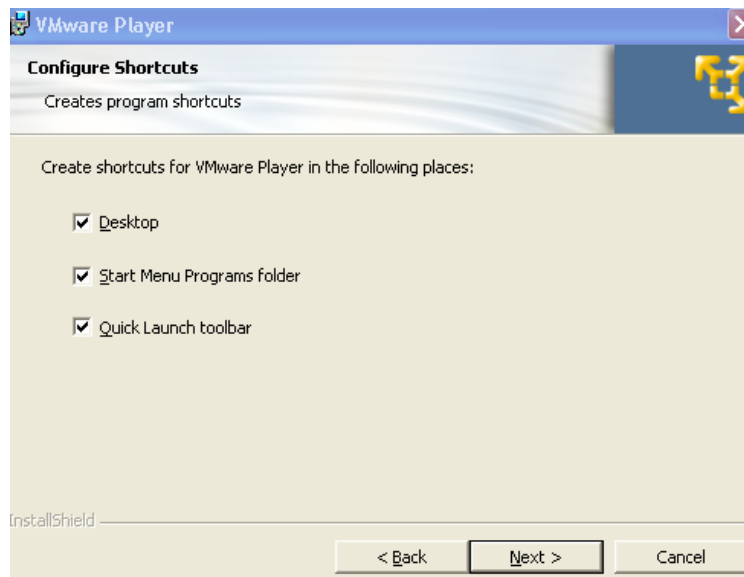


Figure 26: Configure shortcuts VMWare Player

Click next as shown on figure 27 to continue the install.

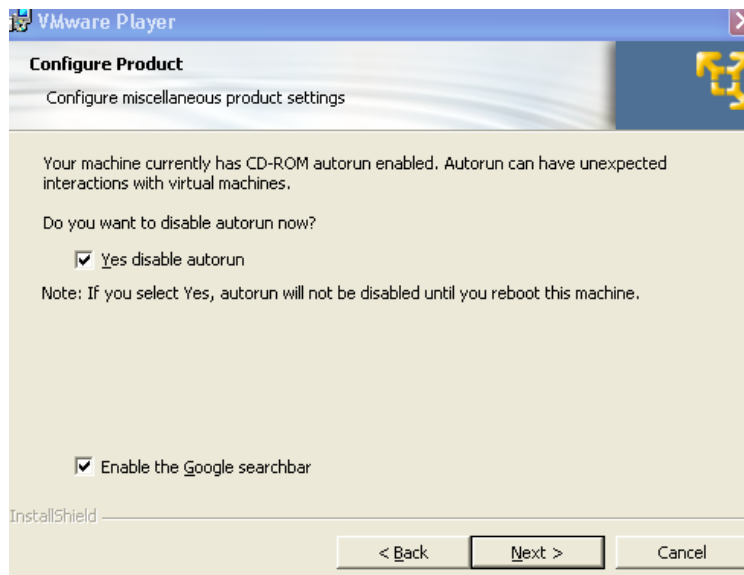


Figure 27: Configure Product VMWare Player

IF the CD-ROM properties within the virtual machine are configured to be connected when powered on, then a host system

with autorun enabled may interact with a virtual machine. It is recommended to always deselect the check box "connected" or "connect at power on" to the CD-ROM drive on a virtual machine when it is not needed to improve performance. The reason is because the host operating system or application is trying to read data from a CD-Rom that is not there and this slows down the virtual machine and host operating system.

Virtual appliances may be downloaded from the VMware website [7]. Most of the downloadable appliances do not have MD5 checksums to verify file integrity and SSL is not used to provide secure file transfers by verifying the source using a public certificate of authority. All appliances should be used with caution and it is recommended to research the developer prior to implementation of an appliance on a production network.

Virtual appliances are easy to implement and run on a host computer with either VMWare player or Server software installed. The virtual appliances are usually downloaded in an archived format with a file extension such as zip. Extract the files to a folder within an organized file structure that makes it easy to identify the appliance location. Start the VMware Server Console or VMWare Player and click the file open and browse to the virtual machine appliance. Figure 28 shows that, when the virtual appliance first starts, there is a dialog box advising

that if this virtual machine has been copied, then it should have a new universal unique identifier (UUID). The universal unique identifier is a standard used by the Open Software Foundation (OSF) as part of the Distributed Computing Environment (DCE). Every UUID is a 16 byte (128 bit) number which makes it mathematically improbable that a UUID number will randomly duplicate. Allowing a duplicate UUID by selecting “keep” in figure 28, could be used to create a duplicate virtual machine to masquerade as another computer on the network. This is a security concern.

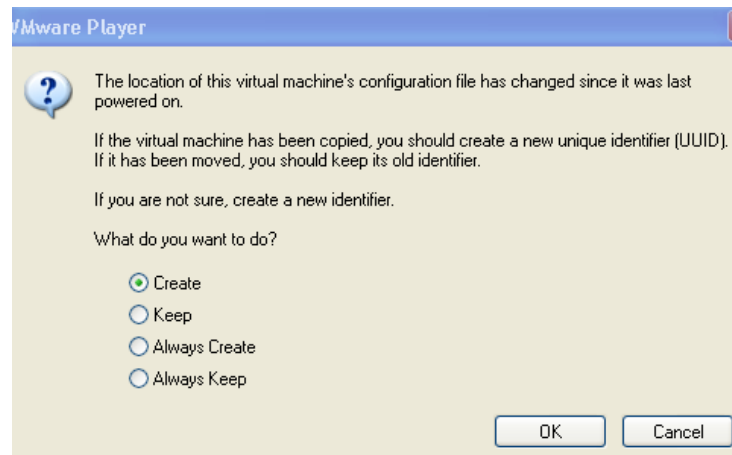


Figure 28: Unique identifier when new appliance starts

Demonstrations of Platform Capabilities

The objective of the following chapters is to demonstrate how to start and implement several downloadable, pre-configured, pre-installed, operating systems that are hardware independent and provide access to several security tools. The appliances provide all types of security applications. Some of the appliances provide intrusion detection systems, email security systems, penetration testing platforms, firewalls, VPN clients, computer forensics, hacking and networking tools and powerful port scanning software. Security appliances provide students the opportunity to apply the technical knowledge learned in class by implementing solutions to security vulnerabilities. The following appliances have been downloaded and tested; "Penguin Sleuth", "Security Platform, Hacking, Networking Security appliances" and "Endian Firewall".

Penguin Sleuth Linux

The Penguin Linux appliance is for computer forensics, incident response and testing. The appliance uses the Gentoo Linux distribution which involves more knowledge of Linux than some other distributions. After a few minor configuration changes that will be covered later in this chapter, the appliance and security tools were fully functional. This

appliance could be used to provide students more hands-on training for the "Intrusion Detection, Response and Recovery" course taught at Lewis University.

Penguin Sleuth Linux, a forensic tool was installed on a computer with a host operating system of Windows 2003 Standard Edition SP1 and the final release of VMWare Server software. This appliance could also be installed on a student's workstation using VMWare Player. After the appliance starts, logon with the user name root and password "penguin"; then type "startx" and the GUI opens.

A right click on the desktop shows the forensics and security GUI tools which include FWBuilder, Etherape, Ethereal, Nessus, Air Forensics, PY-lag Forensics browser, autopsy Forensics Browser, Regviewer. Additional tools accessed at the command prompt included snort, Rkhunter, John the ripper, netcat, qtparted - GUI Partitioning Tool, cryptcat and md5deep - MD5 Hashing Program.

The appliance is configured to accept an IP address from DHCP. In a classroom environment, each appliance needs a unique name. The hostname needs to be changed by updating the file /etc/conf.d/hostname. TCP/IP settings may be changed in the /etc/conf.d/net file, if a static IP address needs to be assigned. In addition, if the hostname is changed, update an

entry in the `/etc/hosts` file from “127.0.0.1 Penguin-Sleuth” to “127.0.0.1 new hostname” [12].

The Gentoo distribution uses a default editor called “nano” which is easy to use. The editor default may be set in the `/etc/re.conf` file to VI, if it is preferred. The size of the virtual machine was 3.3 GB. The appliance was also tested using the latest release of VMWare player installed on a Windows XP SP2 professional host and the appliance had full functionality.

The following screen shots demonstrate how easy it is to start the Penguin Sleuth Linux forensic tool with VMWare Player software. Click on the VMWare Player desktop Icon and browse to the virtual machine files as shown below in figure 29.

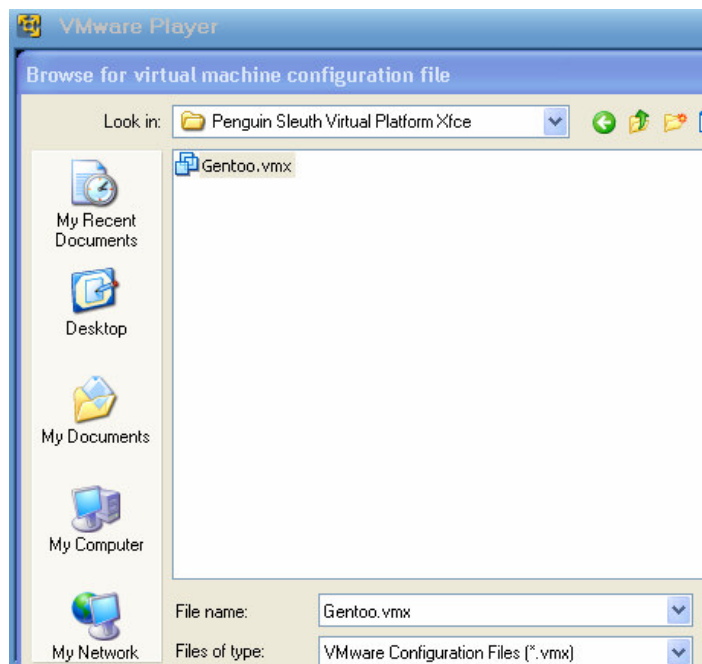


Figure 29: Select virtual machine with browser window

Click open and then the virtual server starts to load

within the Virtual Player console as shown below by figure 30.



Figure 30: Penguin Sleuth security appliance starting

Logon and then at the prompt, type the "startx" command.

The GUI opens as shown below in figure 31.



Figure 31: Penguin Sleuth security appliance started

On the top of the VMPlayer console, click the Ethernet icon and confirm the network adapter card is configured for the bridged interface and the appliance has full connectivity to the network. Press the "Ctrl+G" keys to access the virtual machine and "Ctrl+Alt" to switch to accessing the virtual machine console.

Security Platform, Hacking, Networking Security appliance

This appliance includes the majority of the security tools used for the "Securing Linux" course offered at Lewis University. The appliance may be used to allow each student to research several security tools and provide a hands-on demonstration on how to use the tool.

The "Security Platform and Hacking and Networking Security usage & Training appliance" was started on a computer with Windows XP professional SP2 and the latest release of VMWare Player installed. The virtual appliance operating system is Linux. The distribution is SUSE Linux Professional 9.3 with full functionality which includes YAST to modify system settings and add software. The root user password is "password". VMware tools did not run successfully when the appliance is started using the VMWare Player 1.0.2 released on 8/10/2006 with Build 29634. A critical error occurred "SeduSec authentication" when the appliance started. The appliance still started after clicking okay to continue. The appliance needed access to the Internet to download the VMWare tools. The VMWare tools improve the GUI performance and are necessary for configuration of the mouse and display resolution. The latest release of VMWare Player was uninstalled and an older version of VMWare Player 1.0.1 build 19317 was installed. This resolved all the issues and the

appliance had full functionality. These are minor issues that may be resolved with the next release of the appliance. The appliance is loaded with security tools and is rated highly on the VMWare website. The following screen shot figure 32, shows the virtual machine within the VMWare Player console.



Figure 32: Security platform and hacking and networking security usage & training appliance started within VMWare Player.

The network configuration was set to bridged. The screen shot in Figure 33 shows output from the NBTScan application when it is run from the command prompt and tested for functionality.

```

Scans IP addresses specified in file iplist.
linux2:~ # nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.1.0     Sendto failed: Permission denied
192.168.1.56    <unknown>      <unknown>
192.168.1.162   FOX            <server>  <unknown>    00-a0-c9-59-f6-d2
linux2:~ # █

```

Figure 33: Terminal screen outbound of NBTScan utility

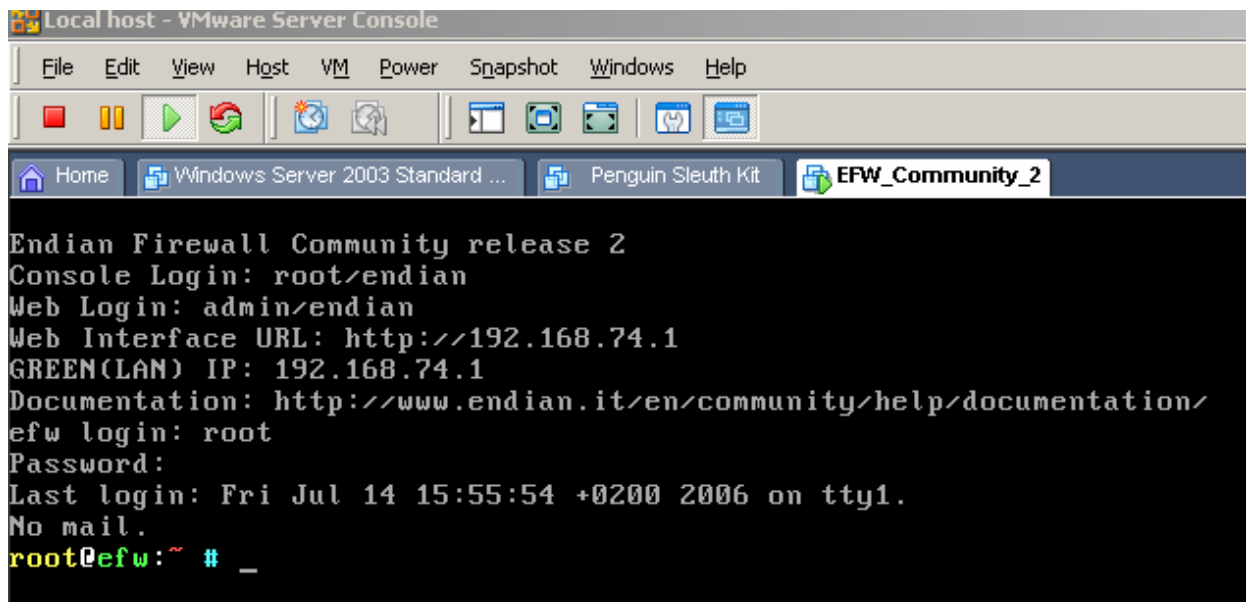
Endian Firewall open source appliance

The Endian Firewall may be used to demonstrate a firewall that provides stateful packet filtering, application-level proxies, spam filtering for email traffic, content filtering, VPN, antivirus and antispam functionality in a “turn key” linux distribution appliance. This appliance could easily be started from a student’s workstation using VMware Player and could be used for hands-on training in several of the security classes offered at Lewis University.

The Endian Firewall open source appliance was developed by the Endian Firewall Community [14]. The appliance is easy to install, use and manage. The Endian Firewall Administrative guide provides detailed documentation on how to use the appliance. The root password is “endian” to logon to the security appliance. When the appliance starts it provides the web interface URL. The application is configured from a client

using a web browser.

The appliance automatically creates three network adapters. When you initially connect to the Endian Firewall Server as shown in figure 33, remember that the IP address in this case is 192.168.74.1/24 by default. The client also has to be on the same segment to connect to the management web interface. Make the necessary changes to the client IP protocol settings to allow the client computer to initially communicate with the Endian Firewall Server.



```
Local host - VMware Server Console
File Edit View Host VM Power Snapshot Windows Help
Home Windows Server 2003 Standard ... Penguin Sleuth Kit EFW_Community_2
Endian Firewall Community release 2
Console Login: root/endian
Web Login: admin/endian
Web Interface URL: http://192.168.74.1
GREEN(LAN) IP: 192.168.74.1
Documentation: http://www.endian.it/en/community/help/documentation/
efw login: root
Password:
Last login: Fri Jul 14 15:55:54 +0200 2006 on tty1.
No mail.
root@efw:~ # _
```

Figure 33: Endian Firewall showing configuration

The management web interface was then accessed by typing <http://192.168.74.1> in the client browser and authenticating to the web interface with the user name and password. The user name

is "Admin" and the password is "endian". Once in the application, it should be easy to configure the firewall and make the necessary configuration changes to the three network interface cards attached to the appliance. Figure 34 shows the actual administrative web interface.

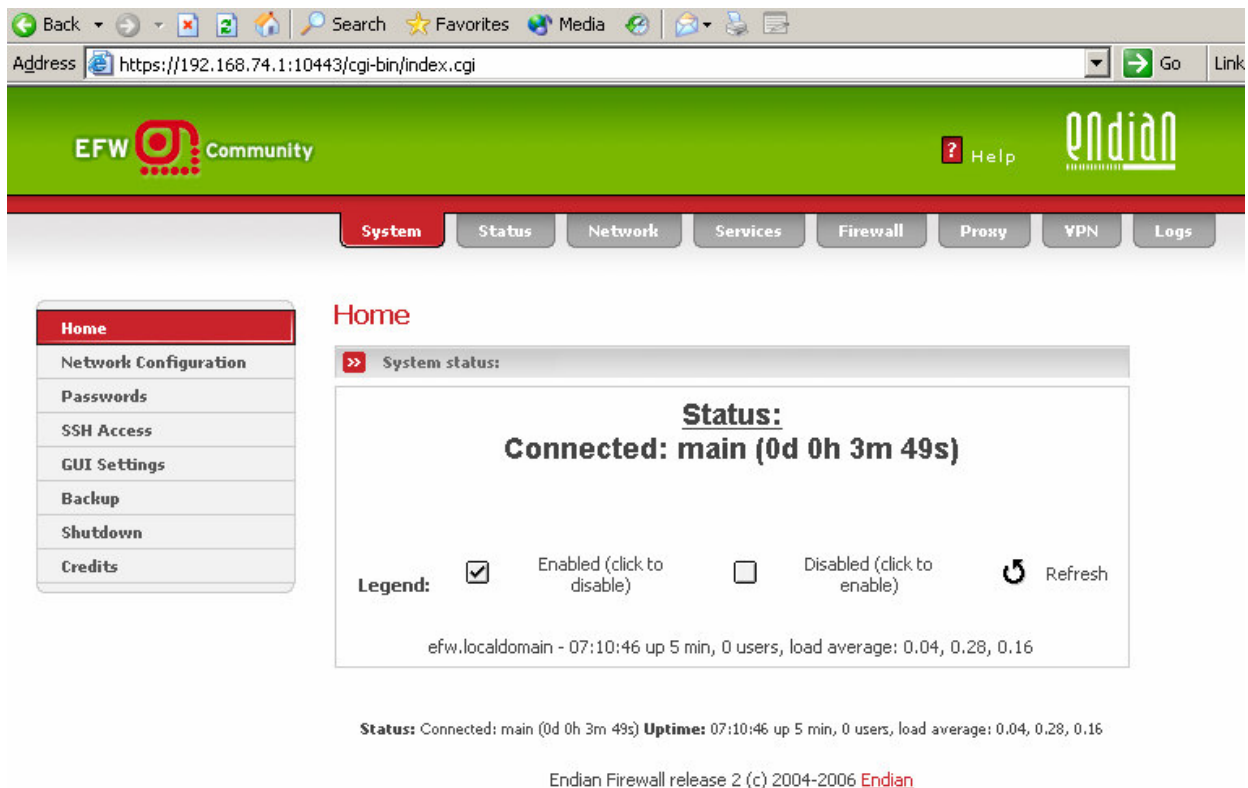


Figure 34: The Management Web interface

The Endian Firewall appliance was tested with both VMWare Server and Player.

Host requirements for optimum performance

VMware server was installed on a computer with Windows 2003 Server Standard Edition operating system with SP1 installed. The host operating system used for this testing has 768 MB of RAM and an Intel 1.80GHZ processor. The VMWare Server software had full functionality as long as a maximum of only two virtual servers ran at the same time. Figure 35 shows the VMWare Server Console with three virtual machines running simultaneously and the error message encountered when Fedora, the 4th virtual machine, attempted to start. This caused the software to stop responding and the Windows 2003 Server host machine needed to be rebooted. This problem could be resolved by adding additional memory to the host or reducing the amount of memory on each virtual machine. The Fedora machine has the recommended 256 MB of RAM as shown in figure 36. The allocated memory on each virtual machine may be lowered to allow all four virtual machines to run. This would cause memory swapping and poor performance on the virtual machines [21]. This issue may be remedied by adding more memory to the host server. A recommended amount of host memory for maximum performance running four to five virtual servers should be 2 GB of Memory and 4 GB of memory should provide enough memory for host server running between

eight to ten virtual machines. The software performance would also improve using a server class computer with a dual processor.

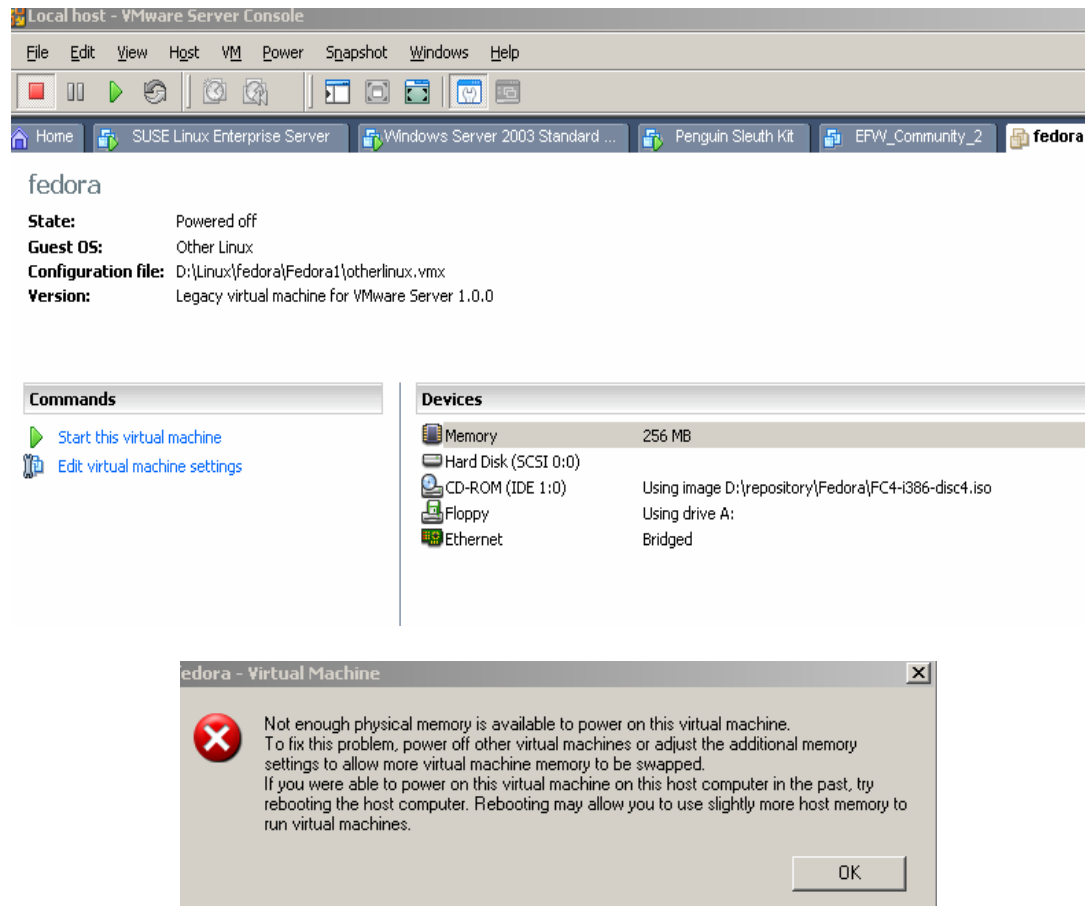


Figure 35: Console showing virtual memory error

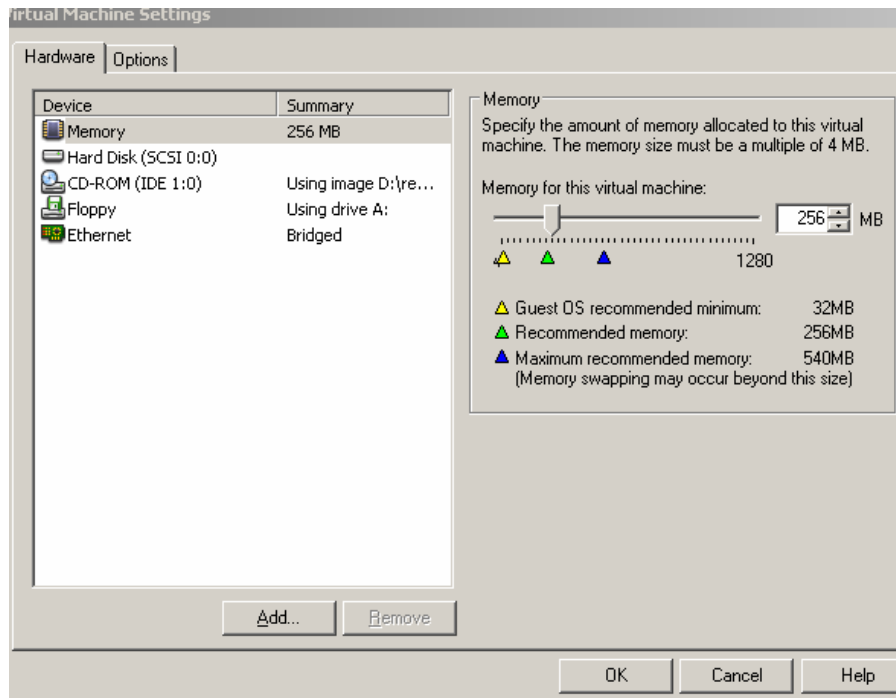


Figure 36: Recommended memory of virtual machine

VMware Player software was easy to install and was proven to be a very stable host system to run all the security appliances and custom-made virtual machines that were researched and tested. VMware player, as the name refers, is for only playing virtual machines and not creating virtual machines. Also, it does not have the advanced features such as "Virtual Network Editor" and "snapshot" available with VMWare Server. There is third-party software available that may be used to create a virtual machine and then run VMWare Player to install an operating system [16]. The name of the software is EasyVMX and it creates the actual virtual machine with a specified configuration. The file is then downloaded and extracted to a

folder on the local host computer. When the virtual machine starts, it looks for the specified ISO file or CD-Rom drive to run the operating system install. The EasyVMX web site was used during this research and testing to successfully create a Windows 2000 professional virtual machine.

Conclusion and Recommendations

This research has presented a proposal to install VMWare virtualization software in the computer lab used for the Master of Science in Information Security program. Virtualization software is the most effective technology to provide computer based training to students. The advantage of using the virtualization software in the computer training lab is that it provides flexibility to consistently create fully functional and well-documented computer lab environments that may be setup for scheduled computer lab lessons and hands-on learning for students.

Probably the most obvious advantage of using virtualization software is that a virtual lab can be dynamically created to provide a customized networking environment with minimal lab setup time and it does not require the same infrastructure and associated costs of ownership of a physical network. The present Information Security lab lacks the infrastructure and technical resources to provide the type of environment needed to provide the hands-on training that students require.

Another advantage of implementing VMWare Server and Player software in the Information Security computer lab is that vendors are rapidly developing more innovative virtualization software packages that will provide the consumer with more

efficient ways to apply the technology.

The VMWare Server software final release provides 100 licenses for both a Windows and Linux host operating system. The major difference between the VMware Player and Server is that Server allows for the configuration of new virtual machines and is designed for hosting multiple virtual machines. VMWare Server also provides a utility for configuring the network interfaces of the host machine and creating virtual networks that would be of great benefit in a computer lab used for teaching Information Security. The feature that would be most beneficial to a computer lab found only on the VMWare Server software is the "Snapshot" feature [4]. VMware offers extensive online documentation that provides the necessary information to research the virtualization software for this project. Both VMWare Player and Server have the capability to host downloadable security appliances to provide the students and instructors with pre-configured operating systems which could provide hands-on learning on various security topics including but not limited to security and forensic tools, intrusion detection systems and firewalls.

The advantages of using VMWare Server and Player may be summarized in a hypothetical computer lab scenario. An instructor has given the students an evening computer lab

assignment to give a presentation on a security topic using one of the many security appliances listed on the VMware website. Each student will start the security appliance using the VMware Player software installed on their workstation and demonstrate how it works in class. The instructor also plans to teach a morning class about server vulnerabilities associated with a Windows NT4 Server SP6 operating system. The NT4 Server was modified yesterday by members of the ethical hackers class and the virtual machine will not boot up. The instructor advises the lab assistant to revert the NT4 Server back to the virtual machine's pristine standard configuration by using the "snapshot" feature and the NT4 Server is ready for the early morning class. The instructor's afternoon class in intrusion detection involves creating a networked environment consisting of a firewall appliance, web servers, and application servers. The intrusion detection computer lab setup is well-documented and has repeatedly been tested for full functionality in demonstrating security tools covered in each lesson. The lab assistant looks at the documentation for today's lab and starts the required virtual machines. The students have VMware Player software installed on their workstations which make the security appliances fully functional and ready to use in the computer lab. At the beginning of the intrusion detection class, a

student informs the instructor that his security appliance to complete the hands-on computer lab assignment is not working. The instructor gives the student directions on how to download the appliance from a repository of available virtual machines located on the file server in the classroom.

Virtualization software will enable the Master of Science in Information Security program to offer more hands-on training opportunities to students without having to compromise undergraduate courses or build new lab space. Software virtualization can be implemented at little expense and with little administration effort. This thesis has demonstrated some of the opportunities that adopting a virtualization architecture would create.

References

[1] "VMware Server Documentation, "

http://www.vmware.com/support/pubs/server_pubs.html

[2] "Download VMWare Server, "

<http://register.vmware.com/content/eula.html>

[3] "Guest Operating System Installation Guide, "

<http://pubs.vmware.com/guestnotes/wwhelp/wwhimpl/js/html/wwhelp.htm>

[4] "VMWare Server online library, "

<http://pubs.vmware.com/server1/wwhelp/wwhimpl/js/html/wwhelp.htm>

[5] Rob Bastiaansen, 2005, ROB'S GUIDE TO USING VMWARE Second Edition, Books4Brains , p.18

[6] "Download VMware Player, "

<http://www.vmware.com/download/player/>

[7] "Browser Appliance, "

<http://www.vmware.com/vmtn/appliances/directory/browserapp.html>

[8] "Virtual Appliances, "

<http://www.vmware.com/vmtn/appliances/>)

[9] Diego Gagliardo Raphael Lechner Marco Sondermann Raphael Vallazza Peter Warasin, 2006,

<http://www.endian.it/en/community/help/documentation/>

[10] Rob Bastiaansen, 2005, ROB'S GUIDE TO USING VMWARE Second Edition, Books4Brains , pp. 33

[11] Rob Bastiaansen, 2005, ROB'S GUIDE TO USING VMWARE Second Edition, Books4Brains , pp. 141 - 161

[12] "Configuring your System, "

http://www.gentoo.org/doc/en/handbook/handbook-x86.xml?part=1&chap=8#doc_chap2

[13] "Vmware_player10.fm --,"

http://kb.vmware.com/vmtnkb/search.do?cmd=displayKC&docType=k&externalId=http--wwwvmwarecom-pdf-VMwarePlayerManual10pdf&sliceId=pdfPage_7&dialogID=807899&stateId=0%200%20809509&doctag=

[14] "EFW Community,"

<http://www.endian.it/en/community/about/>

[15] Diego Gagliardo Raphael Lechner Marco Sondermann Raphael Vallazza Peter Warasin, 2006,

<http://www.endian.it/fileadmin/documentation/efw-admin-guide/en/efw-admin-guide.html>

[16] "Create virtual machines for VMware Player,"

<http://www.easyvmx.com/>

[17] Richard Bejtlich, 2006,

<http://taosecurity.blogspot.com/2006/01/new-sguil-vm-with-client-hot-on-heels.html>

[18] ebaca,

<http://www.vmware.com/vmtn/appliances/directory/249>

[19] "Hacking and networking security usage & training tool,"

<http://www.vmware.com/vmtn/appliances/directory/348>

[20] "Virtual Appliances,"

<http://www.vmware.com/vmtn/appliances/>

[21] Rob Bastiaansen, 2005, ROB'S GUIDE TO USING VMWARE

Second Edition, Books4Brains , pp. 39, 125

[22] "Virtual lab management applications",

<http://www.Surgient.com>

[23] Ryan Naraine, 2005, VMWare: Virtual Machine Security Flaw

'Very Serious',

<http://www.eweek.com/article2/0,1895,1904647,00.asp>

[24] "The Snapshot Manager Window,"

http://www.vmware.com/support/ws55/doc/ws_preserve_sshot_manager_window.html

[25] "VMware Converter 3.0 Beta Program",

<http://www.vmware.com/products/beta/converter/>

[25] "VMWare Workstation 5.5,"

<http://www.vmware.com/products/ws/>